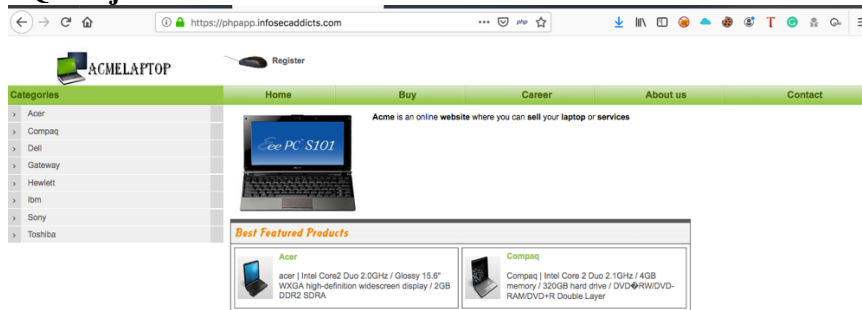


we are everywhere  
we are attackers  
we are defenders  
we are addicts

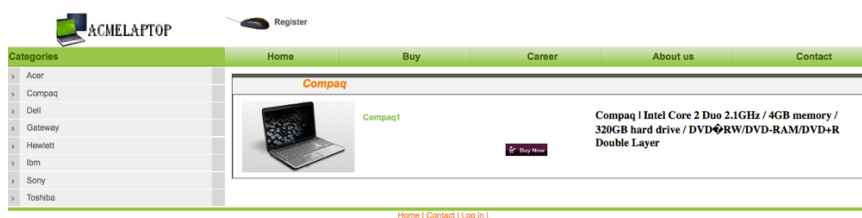


# 1. Injection:

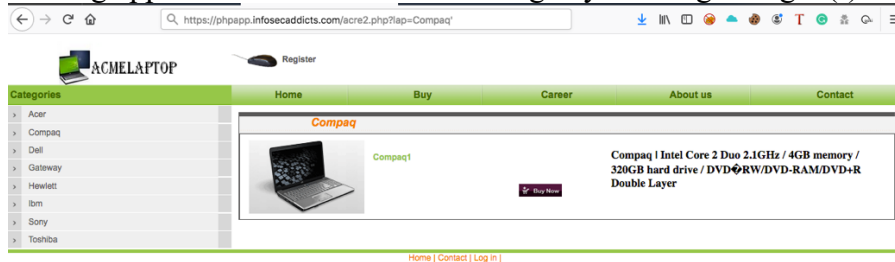
## SQL Injection:



## Buying a laptop



Forcing application to throw error message by entering a single (') in place of a number



## Result:



we are | everywhere  
we are | attackers  
we are | defenders  
we are | addicts



## Bypassing Authentication:

Go to login page:

Home	Buy
USERNAME:	<input type="text"/>
PASSWORD:	<input type="text"/>
	<input type="button" value="Login"/>

Attempt to fill out login form:

USERNAME:	<input type="text" value="shinobibughunter"/>
PASSWORD:	<input type="text" value="*****"/>
	<input type="button" value="Login"/>

Hello "shinobibughunter", Password failed, if you have forgotten your password, click on [forgot password](#).

Unable to login to application, but it does give information about how to further attack password.

## 2. Broken Authentication & Session Management:

Brute Forced Login:

Go to Login Page:

Home	Buy
USERNAME:	<input type="text"/>
PASSWORD:	<input type="text"/>
	<input type="button" value="Login"/>

Attempt to fill out the page and Capture with Burp's Proxy:

we are everywhere  
we are attackers  
we are defenders  
we are addicts



Request Response

Raw Params Headers Hex

```
GET /login.php?error=Invalid+Password+&username=test HTTP/1.1
Host: phpapp.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;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://phpapp.infosecaddicts.com/login.php?error=Invalid+Password+&username=ahinobibughunter
Connection: close
Cookie: __cfduid=dc6029645e59a799349b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __atu=4e20d75b16c5e988ea195b1a1af;
__atu=4e20d75b16c5e988ea195b1a1af; _trk_ip_mid=b53f895b-625c-4a04-8fa8-075c7bba70cf;
__fbp=fb.1.156495159850.417041806; _gid=GA1.2.1143145789.1566082771; PHPSESSID=nglrna9qe2abpad71nr6p4c6a3; _gat=1
Upgrade-Insecure-Requests: 1
```

### Send to Intruder:

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

6

Target Positions Payloads Options

2 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 /ashanti/ctava.php HTTP/1.1
Host: phpapp.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;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://phpapp.infosecaddicts.com/login.php?error=Invalid+Password+&username=ahinobibughunter
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Connection: close
Cookie: __cfduid=dc6029645e59a799349b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __atu=4e20d75b16c5e988ea195b1a1af;
__atu=4e20d75b16c5e988ea195b1a1af; _trk_ip_mid=b53f895b-625c-4a04-8fa8-075c7bba70cf;
__fbp=fb.1.156495159850.417041806; _gid=GA1.2.1143145789.1566082771; PHPSESSID=nglrna9qe2abpad71nr6p4c6a3; _gat=1
Upgrade-Insecure-Requests: 1
username=test&response=2bd12b74e508297feaa3f1a0916066
```

### Select the attack:

Target Positions Payloads Options

2 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: 3  
Payload type: Simple list Request count: 6

2 Payload Options [Simple list]

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

Paste: test  
Load: ahinobibughunter  
Remove  
Clear

Add  
Add from list... (Pro version only)

### Start attack:

we are everywhere  
 we are attackers  
 we are defenders  
 we are addicts



Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	580	
1	1	test	302	<input type="checkbox"/>	<input type="checkbox"/>	580	
2	1	Chris	302	<input type="checkbox"/>	<input type="checkbox"/>	581	
3	1	shinobibughunter	302	<input type="checkbox"/>	<input type="checkbox"/>	592	
4	1	G3t1n135	302	<input type="checkbox"/>	<input type="checkbox"/>	584	
5	1	password	302	<input type="checkbox"/>	<input type="checkbox"/>	584	
6	1	123	302	<input type="checkbox"/>	<input type="checkbox"/>	579	
7	2	test	302	<input type="checkbox"/>	<input type="checkbox"/>	580	
8	2	Chris	302	<input type="checkbox"/>	<input type="checkbox"/>	580	
9	2	shinobibughunter	302	<input type="checkbox"/>	<input type="checkbox"/>	580	
10	2	G3t1n135	302	<input type="checkbox"/>	<input type="checkbox"/>	580	
11	2	password	302	<input type="checkbox"/>	<input type="checkbox"/>	580	
12	2	123	302	<input type="checkbox"/>	<input type="checkbox"/>	580	

Request Response

Raw Params Headers Hex

```

POST /authenticate.php HTTP/1.1
Host: phpapp.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://phpapp.infosecaddicts.com/login.php?error=Invalid+Password+&username=shinobibughunter
Content-Type: application/x-www-form-urlencoded
Content-Length: 67
Connection: close
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; _ga=GA1.2.781573119.1564954291;
  
```

Finished

### Attempt information findings:

Home
Buy

**USERNAME:**

**PASSWORD:**

### Results:

Hey ! Shinobibughunter Wel-Come

Categories
Home
Buy
Career
About us
Contact

- > Acer
- > Compaq
- > Dell
- > Gateway
- > Hewlett
- > Ibm
- > Sony
- > Toshiba

Acme is an online website where you can sell your laptop or services

**Best Featured Products**

**Acer**

acer | Intel Core2 Duo 2.00GHz / Glossy 15.6" WXGA high-definition widescreen display / 2GB DDR2 SDRAM

**Compaq**

Compaq | Intel Core 2 Duo 2.1GHz / 4GB memory / 320GB hard drive / DVD-RW/DVD-RAM/DVD-R Double Layer

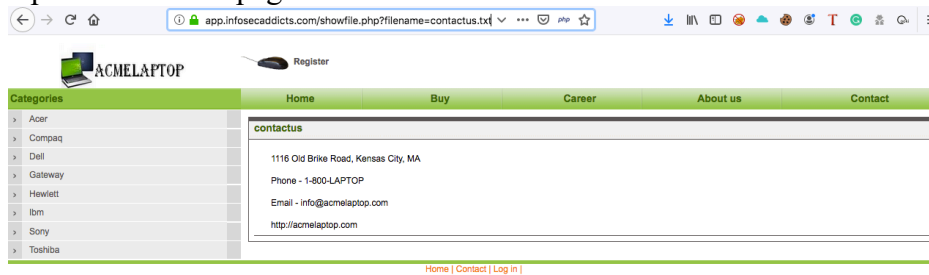
we are everywhere  
we are attackers  
we are defenders  
we are addicts



### 3. Cross-Site Scripting (XSS):

Reflected XSS:

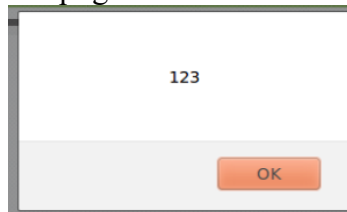
Open Contact Us page:



Injecting string in URL (Keeping extension as usual)

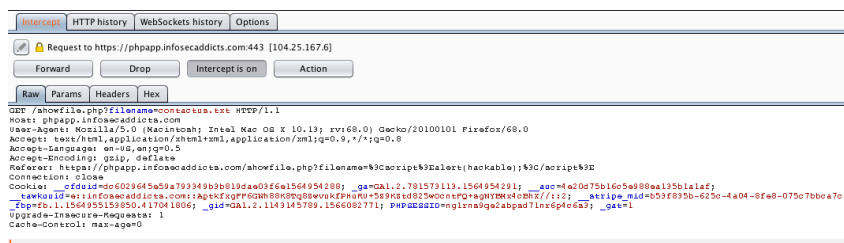


Script gets executed:



DOM-Based XSS:

Capture desired page in Proxy and Send to Repeater:



In Repeater, Change the "User-Agent" to: `<script>alert(123);</script>`

Go Cancel < >

**Request**

Raw Params Headers Hex

```
GET /showfile.php?filename=ontactua.txt HTTP/1.1
Host: phppapp.infosecaddicts.com
User-Agent: <script>alert(123);</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://phppapp.infosecaddicts.com/showfile.php?filename=%3Cscript%3Ealert(hackable);%3C/script%3E
Connection: close
Cookie: __cfduid=dc6029645e59a793949b3b819dae03f6e1564954288;
_ga=GA1.2.781573113.1564954291; __ac=4e20d75b16c5e988ea135b1a1af;
__twkuid=er:infosecaddicts.com:1ApktkfgPF6GWh88K0Cq8WvukEPuRU+589K8td825WontFQ+
agNYWx4cBhX//:2; __stripe_mid=b53f835b-625c-4a04-8fa8-075c7bba70f;
_fbp=fb.l.1564955153850.417041806; _gid=GA1.2.1143145789.1566082771;
PHPSESSID=nglrna9qe2abpad7lnr6p4c6a3; _gat=1
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

### Result:

**Response**

Raw Headers Hex HTML Render

Please enable cookies.

**Error 1010 Ray ID: 50900937abaa714d &bull; 2019-08-19 23:51:31 UTC**

**Access denied**

**What happened?**

The owner of this website (phppapp.infosecaddicts.com) has banned your access based on your browser's signature (50900937abaa714d-ua62).

Cloudflare Ray ID: **50900937abaa714d &bull;** Your IP: 73.106.77.20 &bull;; Performance & security by [Cloudflare](#)

It creates an error giving an attacker an idea about the application

Stored XSS:

Capture desired page in Proxy and Send to Repeater:

Intercept HTTP history WebSockets history Options

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

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
GET /showfile.php?filename=ontactua.txt HTTP/1.1
Host: phppapp.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://phppapp.infosecaddicts.com/showfile.php?filename=%3Cscript%3Ealert(hackable);%3C/script%3E
Connection: close
Cookie: __cfduid=dc6029645e59a793949b3b819dae03f6e1564954288; _ga=GA1.2.781573113.1564954291; __ac=4e20d75b16c5e988ea135b1a1af;
__twkuid=er:infosecaddicts.com:1ApktkfgPF6GWh88K0Cq8WvukEPuRU+589K8td825WontFQ+agNYWx4cBhX//:2; __stripe_mid=b53f835b-625c-4a04-8fa8-075c7bba70f;
_fbp=fb.l.1564955153850.417041806; _gid=GA1.2.1143145789.1566082771; PHPSESSID=nglrna9qe2abpad7lnr6p4c6a3; _gat=1
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

In Repeater choose the "Params" tab and inject the script:  
<script>alert(document.domain)</script>:

**Request**

Raw Params Headers Hex

GET request to /showfile.php

Type	Name	Value
URL	filename	<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	PHPSESSID	ng1rns9qe2abpsd71nr6p4c6s3
Cookie	_gat	1

Add Remove Up Down

Once again we get another error message, however, it gives the attacker information on what to try next:

**Response**

Raw Headers Hex HTML Render

Please enable cookies.

**Error 1010 Ray ID: 509016f6bd1bc530 • 2019-08-20 00:00:54 UTC**

**Access denied**

**What happened?**

The owner of this website (phpapp.infosecaddicts.com) has banned your access based on your browser's signature (509016f6bd1bc530-ua62).

Cloudflare Ray ID: 509016f6bd1bc530 • Your IP: 73.106.77.20 • Performance & security by [Cloudflare](#)

## 4. Insecure Direct Object Reference:

Login to the Application:

we are everywhere  
we are attackers  
we are defenders  
we are addicts



ACMELAPTOP

Hey! Shinobibughunter Wel-Come

Home Buy Career About us

Acme is an online website where you can sell your laptop or services

**Best Featured Products**

<p><b>Acer</b></p> <p>acer   Intel Core2 Duo 2.0GHz / Glossy 15.6" WXGA high-definition widescreen display / 2GB DDR2 SDRAM</p>	<p><b>Compaq</b></p> <p>Compaq   Intel Core 2 Duo 2.1GHz / 4GB memory / 320GB hard drive / DVD-RW/DVD-RAM/DVD+R Double Layer</p>
<p><b>Dell</b></p> <p>dell   Little Description about this product as given by owner</p>	<p><b>Gateway</b></p> <p>gateway   AMD Turion X2 RM-7D dual-core mobile processor 2.0GHz / 3GB PC6400 DDR2 SDRAM / Multifo</p>
<p><b>Hewlett</b></p> <p>Intel Atom - 1.6GHz / 10.1" TFT-LCD widescreen with 1024 x 600 resolution / 1GB DDR2 / SSD (Solid S</p>	<p><b>Ibm</b></p> <p>Intel Celeron 2.16GHz, 2GB RAM, DVD Burner, 160GB, Vista Home, 15.4" display / Built-in Atheros high</p>

### Capture page in Proxy:

Intercept HTTP history WebSockets history Options

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

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
GET /index.php HTTP/1.1
Host: phpapp.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://phpapp.infosecaddicts.com/login.php
Connection: close
Cookie: __cfduid=602945a59a7933493b194e03f6e1564954289; _ga=GA1.2.781573113.1564954291; __ssc=4e20d75b16c5a988ea135b1a1af; __lawauid=ei1infosecaddicts.com;ApkKfsgPF@Gm88K8G8wvKfPhRU+589Ksd825woonLPQ+agNYEM4o6hZ//i;2; __stripe_mid=b53f895b-625c-4a04-8fa8-075c7bba7cf; __fbclid=156495159850.417041806; __gid=GA1.2.1149145789.1566082771; PHPSESSID=ngina9qe2abpd71n6p4o6a3; __gat=1
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

### Send to Intruder:

Intercept HTTP history WebSockets history Options

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

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
GET /index.php HTTP/1.1
Host: phpapp.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://phpapp.infosecaddicts.com/login.php
Connection: close
Cookie: __cfduid=602945a59a7933493b194e03f6e1564954289; _ga=GA1.2.781573113.1564954291; __ssc=4e20d75b16c5a988ea135b1a1af; __lawauid=ei1infosecaddicts.com;ApkKfsgPF@Gm88K8G8wvKfPhRU+589Ksd825woonLPQ+agNYEM4o6hZ//i;2; __stripe_mid=b53f895b-625c-4a04-8fa8-075c7bba7cf; __fbclid=156495159850.417041806; __gid=GA1.2.1149145789.1566082771; PHPSESSID=ngina9qe2abpd71n6p4o6a3; __gat=1
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

- Send to Spider
- Do an active scan
- Send to Intruder**
- Send to Repeater
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser
- Engagement tools [Pro version only]

### In Intruder select attack positions:

```
GET /index.php HTTP/1.1
Host: phpapp.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://phpapp.infosecaddicts.com/login.php
Connection: close
Cookie: __cfduid=602945a59a7933493b194e03f6e1564954289; _ga=GA1.2.781573113.1564954291; __ssc=4e20d75b16c5a988ea135b1a1af; __lawauid=ei1infosecaddicts.com;ApkKfsgPF@Gm88K8G8wvKfPhRU+589Ksd825woonLPQ+agNYEM4o6hZ//i;2; __stripe_mid=b53f895b-625c-4a04-8fa8-075c7bba7cf; __fbclid=156495159850.417041806; __gid=GA1.2.1149145789.1566082771; PHPSESSID=ngina9qe2abpd71n6p4o6a3; __gat=1
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

### Go to Payloads and select numbers & Click "Start Attack":



we are everywhere  
we are attackers  
we are defenders  
we are addicts



**Payload Sets** Start attack

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:  Request count: 1,000

**Payload Options [Numbers]**

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

**Number range**

Type:  Sequential  Random

From:   
To:   
Step:   
How many:

You can see results of the attack in a variety of means.

Looking at the results may require further investigation.

Intruder attack 3

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
83	83	404	<input type="checkbox"/>	<input type="checkbox"/>	652	
84	84	404	<input type="checkbox"/>	<input type="checkbox"/>	652	
85	85	404	<input type="checkbox"/>	<input type="checkbox"/>	652	
86	86	404	<input type="checkbox"/>	<input type="checkbox"/>	652	
87	87	404	<input type="checkbox"/>	<input type="checkbox"/>	652	
88	88	404	<input type="checkbox"/>	<input type="checkbox"/>	652	
89	89	404	<input type="checkbox"/>	<input type="checkbox"/>	652	
90	90	404	<input type="checkbox"/>	<input type="checkbox"/>	652	
91	91	404	<input type="checkbox"/>	<input type="checkbox"/>	652	
92	92	404	<input type="checkbox"/>	<input type="checkbox"/>	652	
93	93	404	<input type="checkbox"/>	<input type="checkbox"/>	652	
94	94	404	<input type="checkbox"/>	<input type="checkbox"/>	652	
95	95	404	<input type="checkbox"/>	<input type="checkbox"/>	652	
96	96	404	<input type="checkbox"/>	<input type="checkbox"/>	652	
97	97	404	<input type="checkbox"/>	<input type="checkbox"/>	652	

Request Response

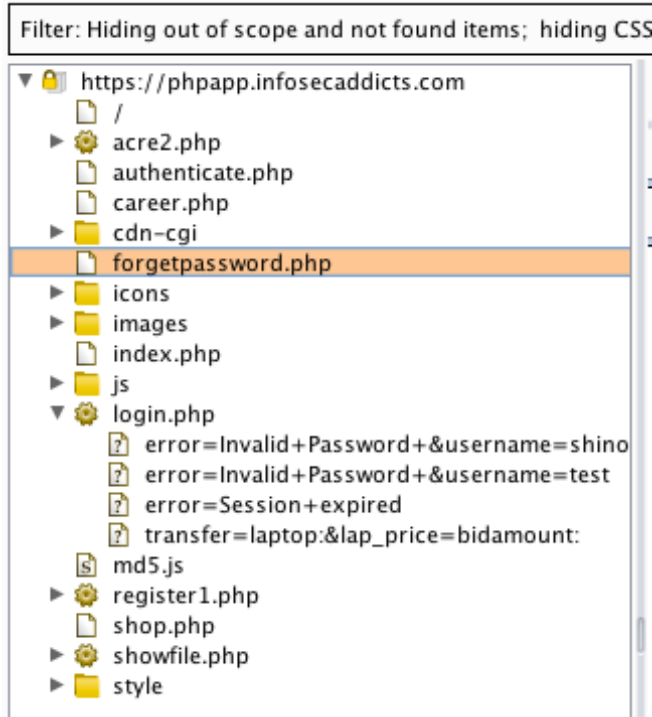
Raw Params Headers Hex

```
GET /index.php 96 HTTP/1.1
Host: phpapp.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://phpapp.infosecaddicts.com/login.php
Connection: close
Cookie: __cfduid=dc6029c645e59a793349b3b819dae03f6e1564954288; __ga=GA1.2.701573113.1564954291;
__auc=e20d75b16c5e988aa135b1a1af;
__tawkuid=ei::infosecaddicts.com::AptkfxgPF6GWh88K8Tq8SvvukFPHuRu+589KSed825wOontPG+agNYEMx4oBhX//i:2;
```

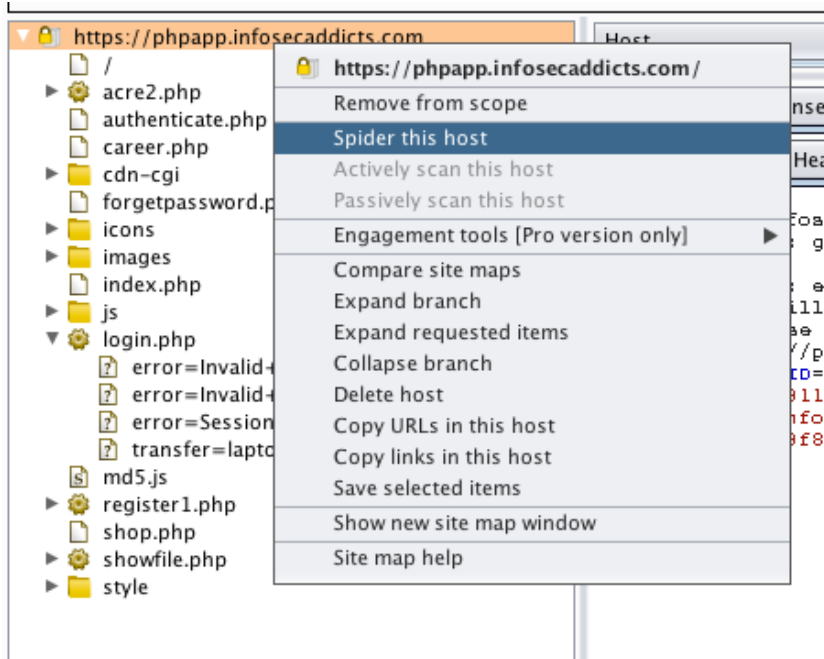
142 of 1000

## 5. Security Misconfiguration:

Go to the “Target” tab and then the site map in Burp:

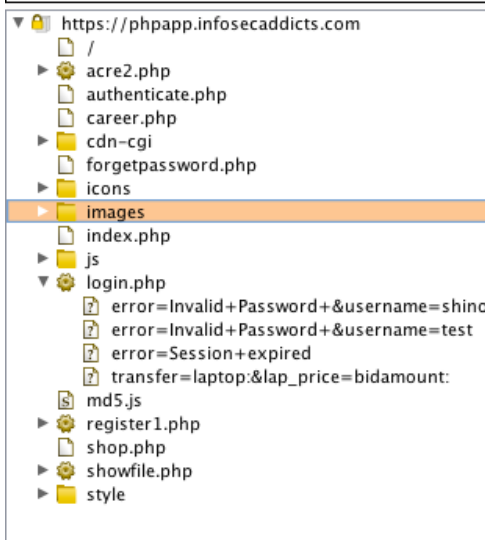


Select Spider:



You can see the directory of the site.

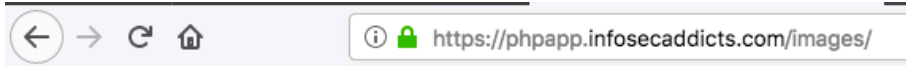
Choose a directory, in our case we'll choose "images":



Return to the browser and access the directory we selected by adding it to the URL:

<https://phpapp.infosecaddicts.com/images/>

we are | everywhere  
we are | attackers  
we are | defenders  
we are | addicts



## Index of /images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>		-	
<a href="#">Compaq.jpg</a>	2018-09-18 16:18	19K	
<a href="#">Thumbs.db</a>	2018-09-18 16:18	235K	
<a href="#">a1.jog.jpg</a>	2018-09-18 16:18	16K	
<a href="#">a2.jpg</a>	2018-09-18 16:18	15K	
<a href="#">a3.jpg</a>	2018-09-18 16:18	15K	
<a href="#">a4.jpg</a>	2018-09-18 16:18	10K	
<a href="#">a5.jpg</a>	2018-09-18 16:18	34K	
<a href="#">acer.jpg</a>	2018-09-18 16:18	5.3K	
<a href="#">c1.jpg</a>	2018-09-18 16:18	5.9K	
<a href="#">c2.jpg</a>	2018-09-18 16:18	7.1K	
<a href="#">c3.jpg</a>	2018-09-18 16:18	6.3K	
<a href="#">c4.jpg</a>	2018-09-18 16:18	6.7K	
<a href="#">c5.jpg</a>	2018-09-18 16:18	8.0K	
<a href="#">c6.jpg</a>	2018-09-18 16:18	1.9K	
<a href="#">d1.jpg</a>	2018-09-18 16:18	6.3K	
<a href="#">d2.jpg</a>	2018-09-18 16:18	6.3K	
<a href="#">d3.jpg</a>	2018-09-18 16:18	2.2K	
<a href="#">d4.jpg</a>	2018-09-18 16:18	1.2K	

Explore the links inside the directory.

## 6. Sensitive Data Exposure:

Insecure Processing of Credit Card Data

Select an item you wish to purchase:



we are | everywhere  
we are | attackers  
we are | defenders  
we are | addicts



Hey ! Shinobibughunter Wel-Come

Home Buy Career About us Contact

**Acer**

	acer1	acer   Intel Core2 Duo 2.0GHz / Glossy 15.6" WXGA high-definition widescreen display / 2GB DDR2 SDRA	<input type="button" value="Buy Now"/>
	acer2	acer   Intel Pentium M 740 1.73GHz / 512MB DDR2 400 / 60GB hard drive / 14.1-inch XGA TFT LCD / CD-	<input type="button" value="Buy Now"/>

Home | Contact | Logout |

On the Payment Processing Page, fill out information and submit it:

Hey ! Shinobibughunter Wel-Come

Home Buy Career About us Contact

BUY

**Fill buy on Acme**

Your Total Price :	599.99
Your Quantity :	1
Your Name :	Shinobibughunter
Type of card:	VISA
Credit Card no:	<input type="text"/>
CVE number:	<input type="text"/>

Once you've the form has been submitted go back and attempt buy another item,

You'll see your Credit Card no. has been cached:

Hey ! Shinobibughunter Wel-Come

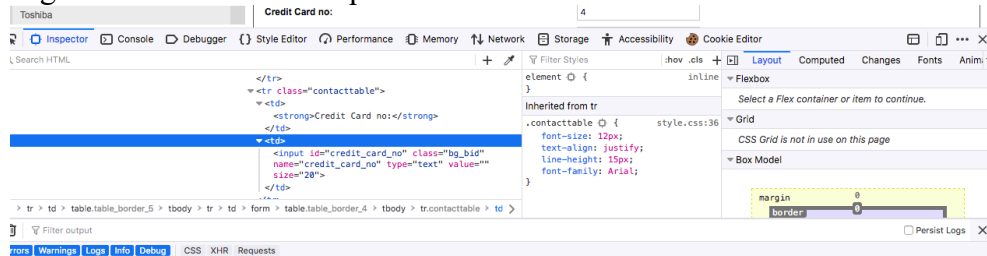
Home Buy Career About us Contact

BUY

**Fill buy on Acme**

Your Total Price :	599.99
Your Quantity :	1
Your Name :	Shinobibughunter
Type of card:	VISA
Credit Card no:	4  4444444444444444
CVE number:	<input type="text"/>

Right click and choose Inspect element:



Select the Credit card section and find the name "credit\_card\_no":

```
<td>
  <strong>Credit Card no:</strong>
</td>
<td>
  <input id="credit_card_no" class="bg_bid"
  name="credit_card_no" type="text" value=""
  size="20">
</td>
</tr>
<tr class="contacttable">
</tbody>
```

As you can see, there isn't any "Auto-complete off" here and that is why the credit card number is being cached.

So the we have Insecure Processing of Credit Card Data.

## 7. Missing Function Level Access Control:

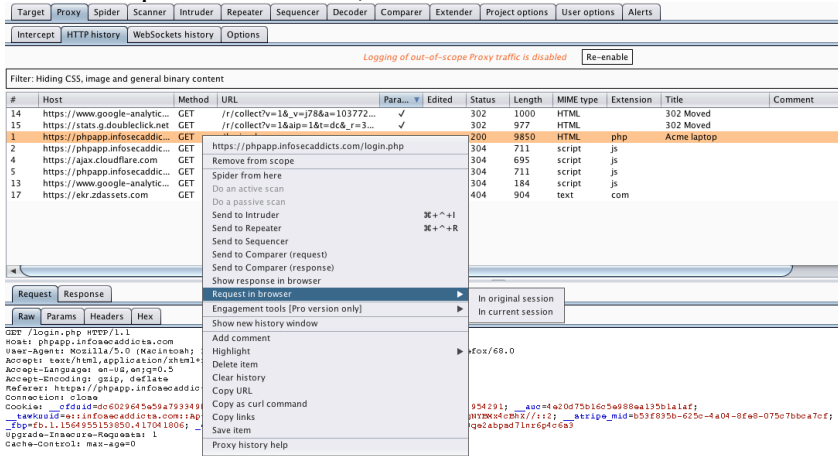
Testing for Access Controls:

Login using the lower-privileged account:

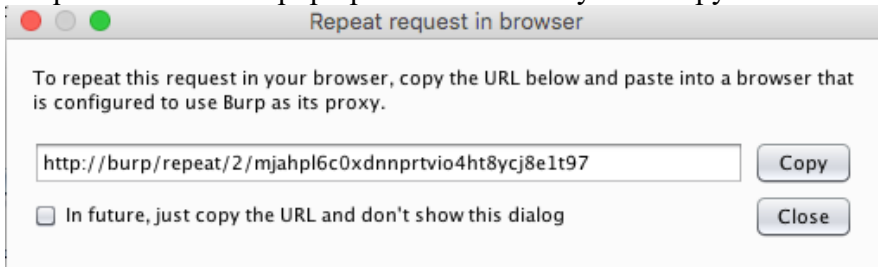
**USERNAME:**

**PASSWORD:**

Locate the area we are testing in Burp's Site map or HTTP history. Right click on the entry to bring up the context menu. Click "Request in browser", then "In current session".



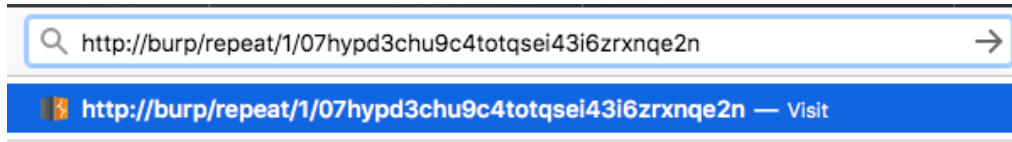
The "Request in browser" pop up window allows you to copy the URL of the required



page.

Click the "Copy" button.

Post the URL into the browser to attempt access the individual page we're testing:



In this case we weren't successful. So it appears the appropriate controls are in place.

## Not Found

he requested URL /repeat/1/07hydp3chu9c4totqsei43i6zrxnqe2n was not found on this server.

cache/2.4.29 (Ubuntu) Server at www.inert.com Port 80

## 8. Cross-Site Request Forgery (CSRF):

Unable to find Cross-Site Request Forgery Vulnerability in this application

## 9. Test for Components with Known Vulnerabilities:

Go to the "HTTP history" tab:

#	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=78&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   aspd...		✓	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=78&a=151677...	✓		302	1002	HTML		302 Moved		✓	64.233.185.138	

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





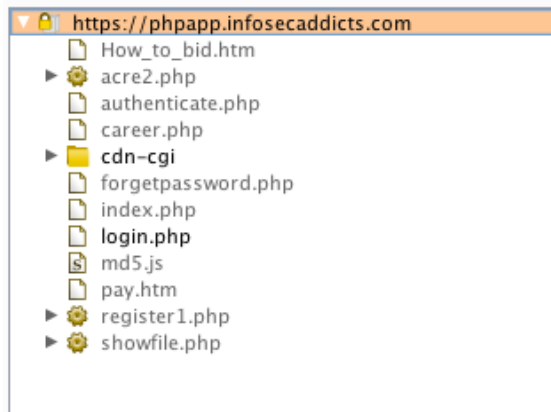
```
Request Response
Raw Headers Hex HTML Render ViewState
HTTP/1.1 200 OK
Date: Sun, 18 Aug 2019 13:02:08 GMT
Content-Type: text/html; charaet=utf-8
Connection: close
Cache-Control: private
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Strict-Transport-Security: max-age=0
X-Content-Type-Options: noaniff
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.

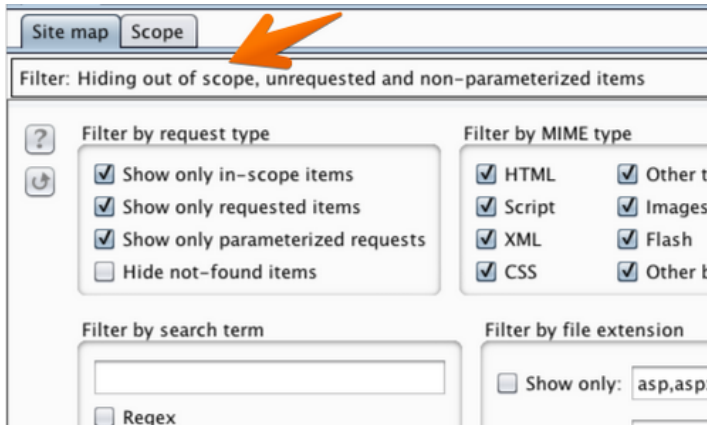
This information can help with information gathering process.

## 10.Redirects and Forwards:

After Intercepting our desired page go to spider:

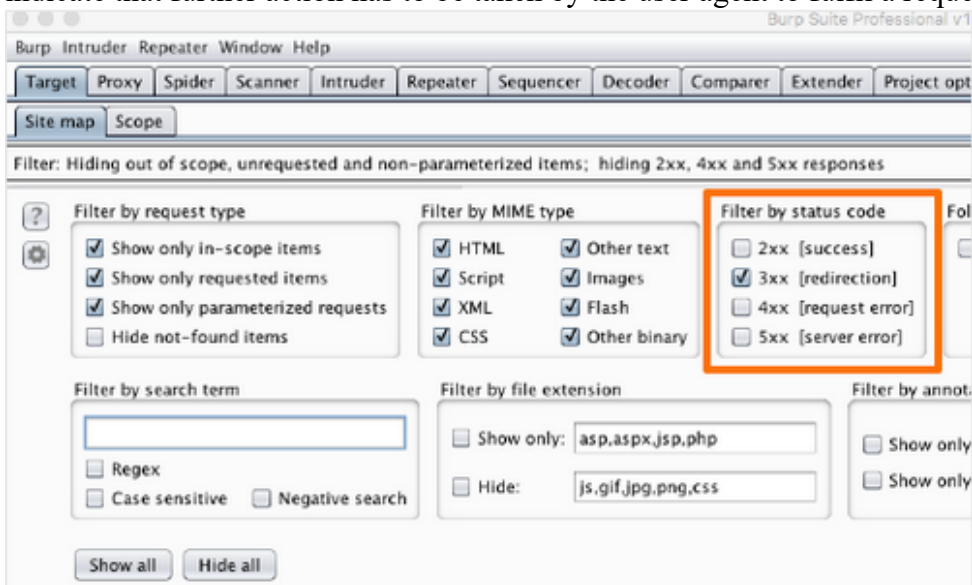


Go to “Site map filter” to search for any redirects or forwards used by the Site map.



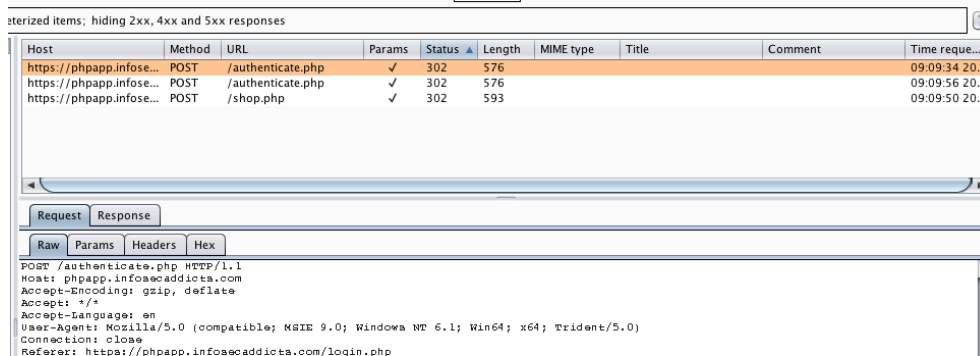
We can “Filter by status code”:

In this case we are searching for the “3xx” class of status codes. These status codes indicate that further action has to be taken by the user agent to fulfil a request.

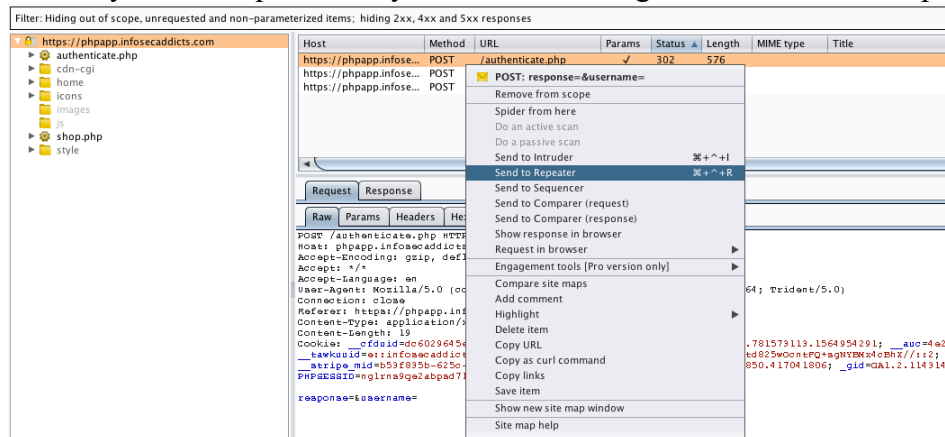


The “Site map” table should now only show HTTP requests of the “3xx” class.

You can now manually step through these requests to look for “interesting” URLs. These include any items in which the redirection target appears to be specified within a request parameter.



Send any HTTP requests that you want to investigate further to the “Repeater” tab.



On the “Repeater” tab, Click “Go” to check that the redirect occurs:

we are everywhere  
we are attackers  
we are defenders  
we are addicts



Go Cancel < > Follow redirection

**Request**

Raw Params Headers Hex

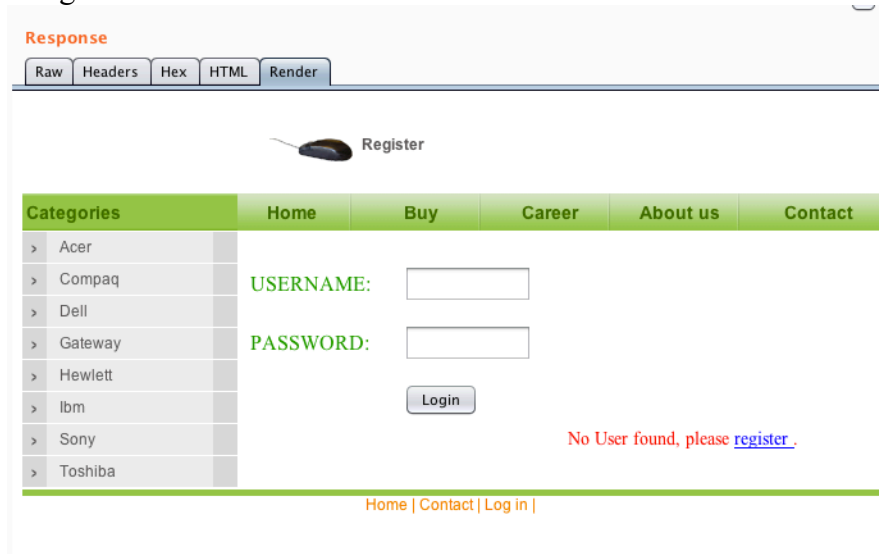
```
POST /authenticate.php HTTP/1.1
Host: phppapp.infosecaddicts.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64;
x64; Trident/5.0)
Connection: close
Referer: https://phppapp.infosecaddicts.com/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Cookie: __cfduid=dc6029645e59a793349b3b819dae03f6e1564954288;
__ga=GAL.2.781573113.1564954291; __auc=4e20d75b16c5e988ea135b1a1af;
__tawkuid=e::infosecaddicts.com::AptkfxgPF6GWh88K8Tg88wvukfPHuRU+589K8td
825wOontPQ+agNYEMx4cBhX//:::2;
__atripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;
__fbp=fb.1.1564955153850.417041806; __gid=GAL.2.1143145789.1566082771;
PHPSESSID=nglxna9qe2abpad71nr6p4c6a3

response=Username=
```

We get taken to here:

**Response**

Raw Headers Hex HTML Render



The screenshot shows a web page with a navigation menu and a registration form. The navigation menu includes links for Home, Buy, Career, About us, and Contact. A sidebar lists computer brands: Acer, Compaq, Dell, Gateway, Hewlett, Ibm, Sony, and Toshiba. The main content area contains a registration form with fields for USERNAME and PASSWORD, a Login button, and a message: "No User found, please register.". The footer includes links for Home, Contact, and Log in.

So a Re-direction doesn't happen here.

we are | everywhere  
we are | attackers  
we are | defenders  
we are | addicts

