Web Application Security

Use Burp and cewl to enumerate users on the Mutillidae site

Robert Gabriel
Part 2 - 18 March 2016

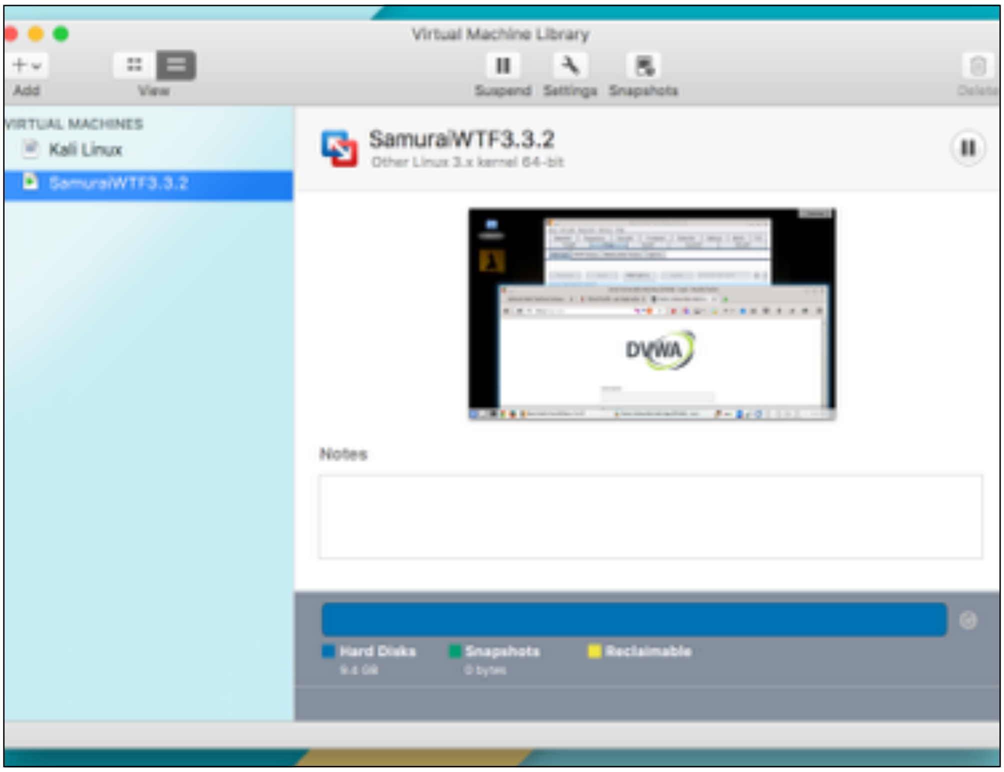
CIT CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

Setup

Open Your Vm Fusion

Instructions:

1. On Your Host Computer, Go To
2. Applications --> All Program --> VM Fusion
3. Select Samjuri.wtf and Boot the Vm

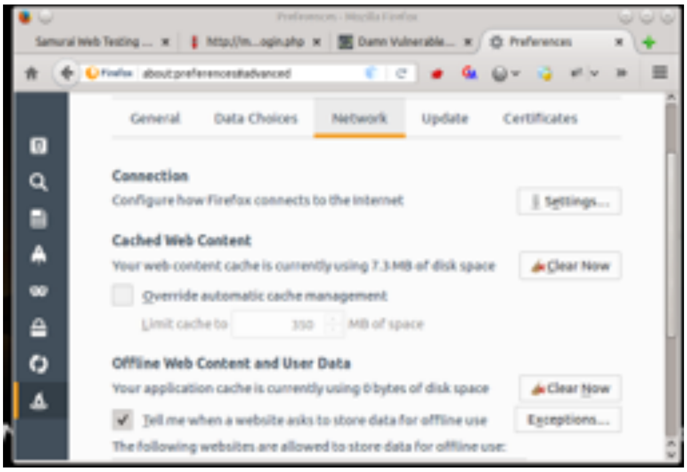


Open the following

1. **Burp Free Suite**
2. **Firefox**

Firefox Setup

1. Switch to Firefox
2. Go to options
3. Click
    1. Advanced
    2. Network tab
    3. Settings



Samurai Web Testing ... | http://m...ogin.php | Damn Vulnerable... | Preferences

about:preferences#advanced

General | Data Choices | Network | Update | Certificates

Connection

Configure how Firefox connects to the Internet — Settings...

Cached Web Content

Your web content cache is currently using 7.3 MB of disk space — Clear Now

□ Override automatic cache management

Limit cache to 350 MB of space

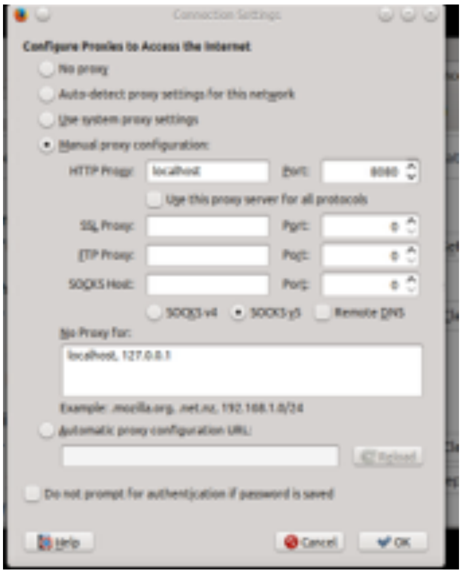
Offline Web Content and User Data

Your application cache is currently using 0 bytes of disk space — Clear Now

☑ Tell me when a website asks to store data for offline use — Exceptions...

The following websites are allowed to store data for offline use:

4. When opened, check Manual Proxy Configuration.
5. Make sure the Http Proxy is **localhost**
6. Make sure the Port is **8080**



Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: localhost Port: 8080

□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

SOCKS Host: Port: 0

○ SOCKS v4 ● SOCKS v5 □ Remote DNS

No Proxy for:

localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

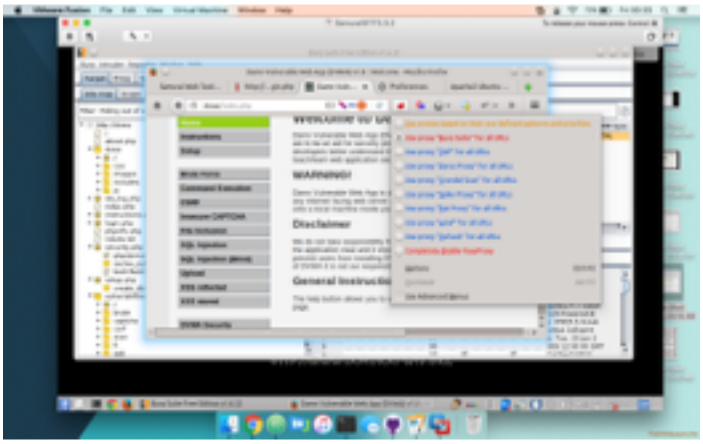
Reload

□ Do not prompt for authentication if password is saved

Help | Cancel | OK

Or

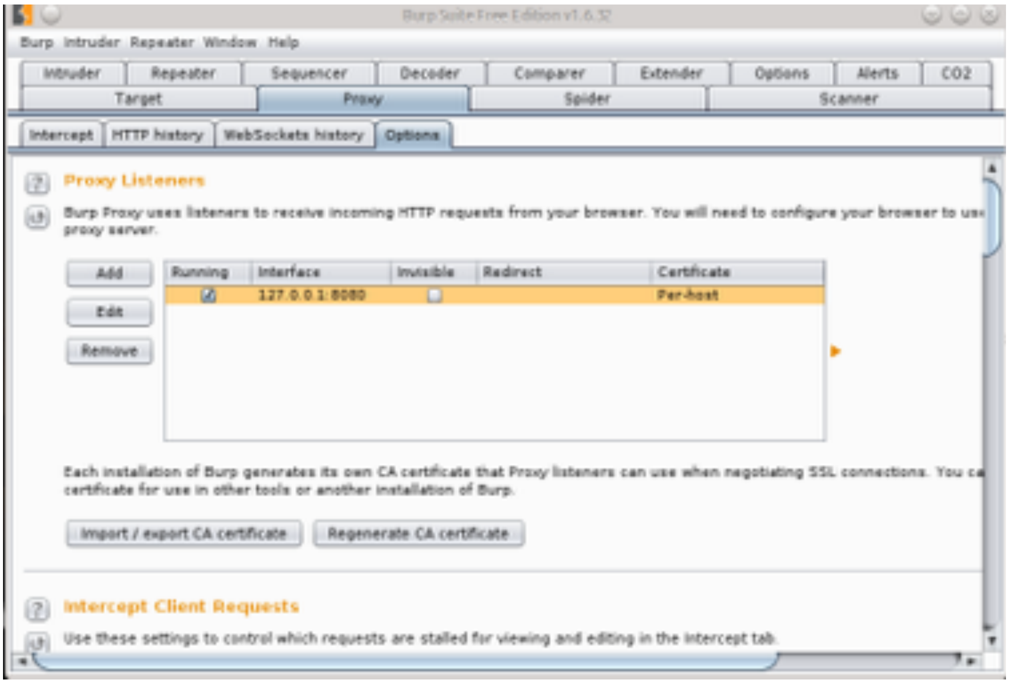
1. Click on foxy Proxy Add-on
2. Click Use “Burp settings”



Visit http://dvwa/login.php

Burp Setup

1. Switch Burp suite
2. Make sure you listening to **localhost:8080**
3. To Check this open Burp Suite and click Proxy -> Options


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts CO2
Target Proxy Spider Scanner
Intercept HTTP history WebSockets history Options
Add
Edit
Remove
Import / export CA certificate
Regenerate CA certificate

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to us proxy server.

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080	□		Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You ca certificate for use in other tools or another installation of Burp.

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

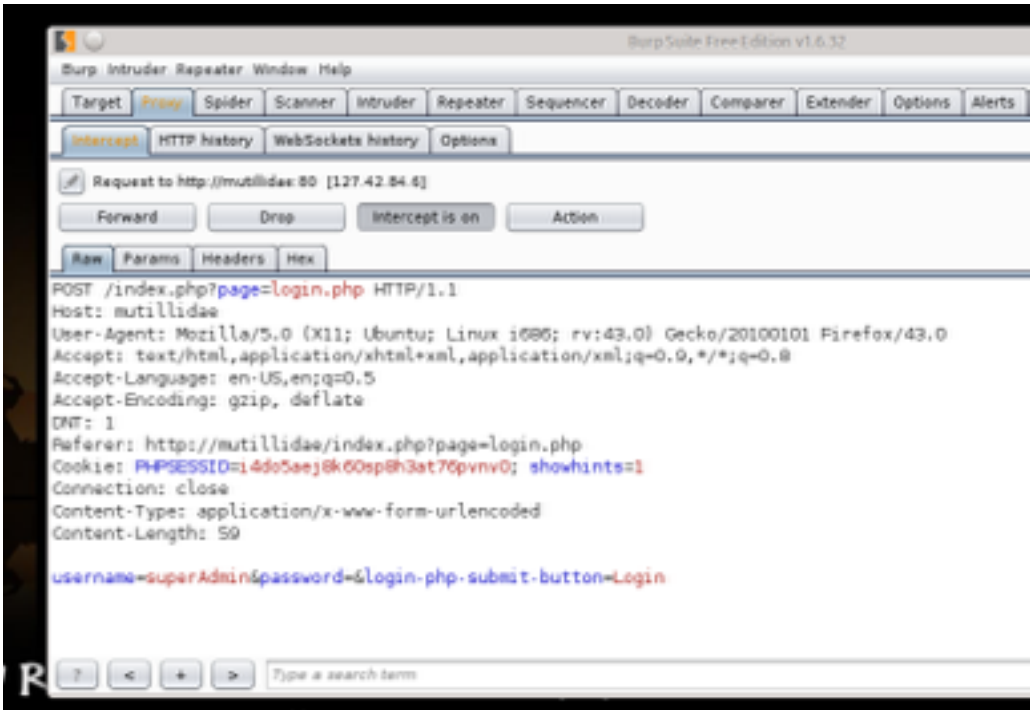
4. Next select Proxy and turn on intercept

Step 1

Now that we have everything set up with our proxy running and it incepting .

Valid account attempt

1. First open up **firefox** and open the following url http://mutillidae/index.php?page=login.php
2. Create an account, I created one called **superAdmin** with **password GTIBUDDY123**
3. In **Burp suite** we have set up so we incepted the request and we can see the request being made in this case **username=superAdmin&Password= GTIBUDDY123**
4. You then want to right click on the send to request and click send to repeater and then click forward.



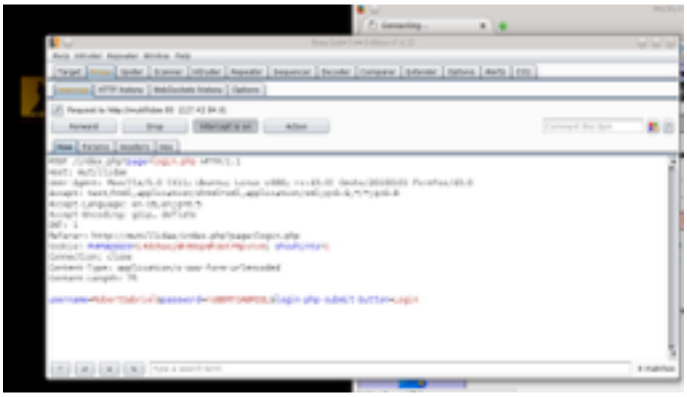
Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex
? < + >
Type a search term

Request to http://mutillidae:80 [127.42.84.6]

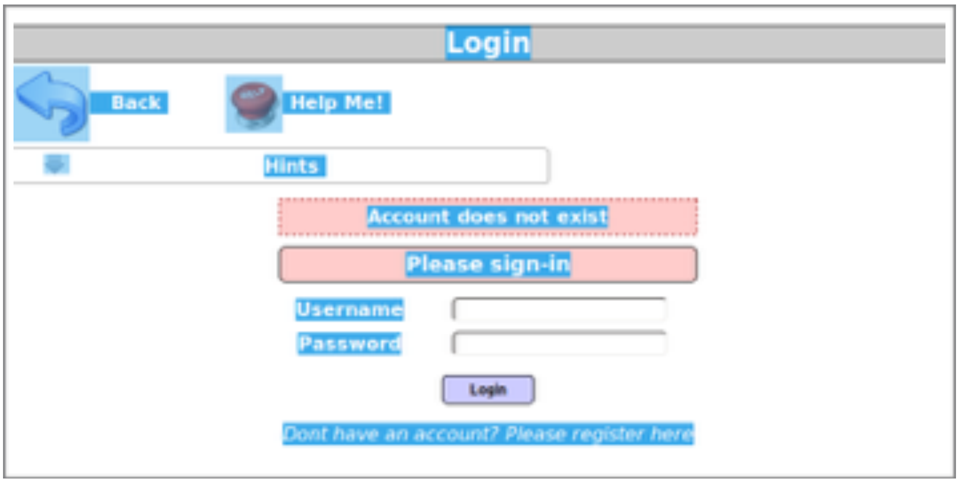
```
POST /index.php?page=login.php HTTP/1.1
Host: mutillidae
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://mutillidae/index.php?page=login.php
Cookie: PHPSESSID=i4do5aej8k60sp8h3at76pvnv0; showhints=1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 59

username=superAdmin&password=&login-php-submit-button=Login
```

Invalid login attempt

1. First open up **firefox** and open the following url http://mutillidae/index.php?page=login.php
2. On this page we will want to intercept a invalid login attempt to base our http request on.
3. In Burp suite we have incepted the request and we can see the request being made in this case **username=RobrtGabriel&Password=robertGABRIEL**
4. You then want to right click on the request and click send to repeater and then click forward.



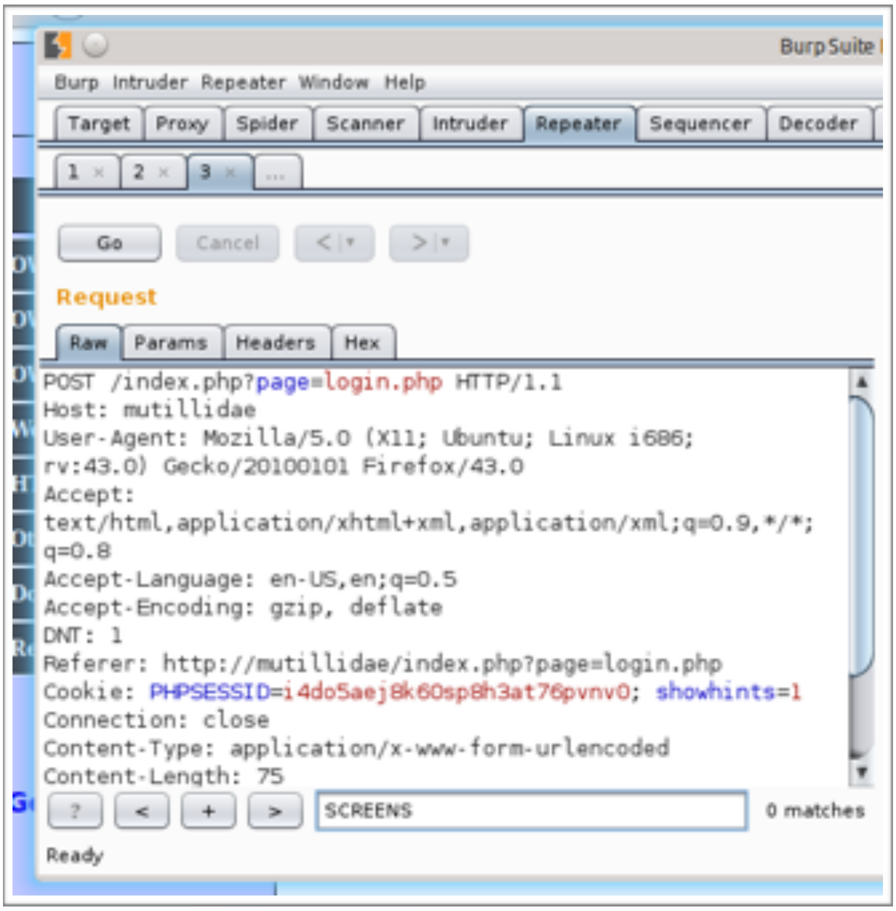
5. **If you switch back to firefox you will see that it say account not found. This is a bad thing, as it tells us the amount isn't there.**



Account does not exist

Please sign-in

6. Next Go back to Burp Suite and click on repeater. We need to check that its still working working, do this by clicking Go, this is because .net or newer systems will put in a type of hash to stop hash repeats

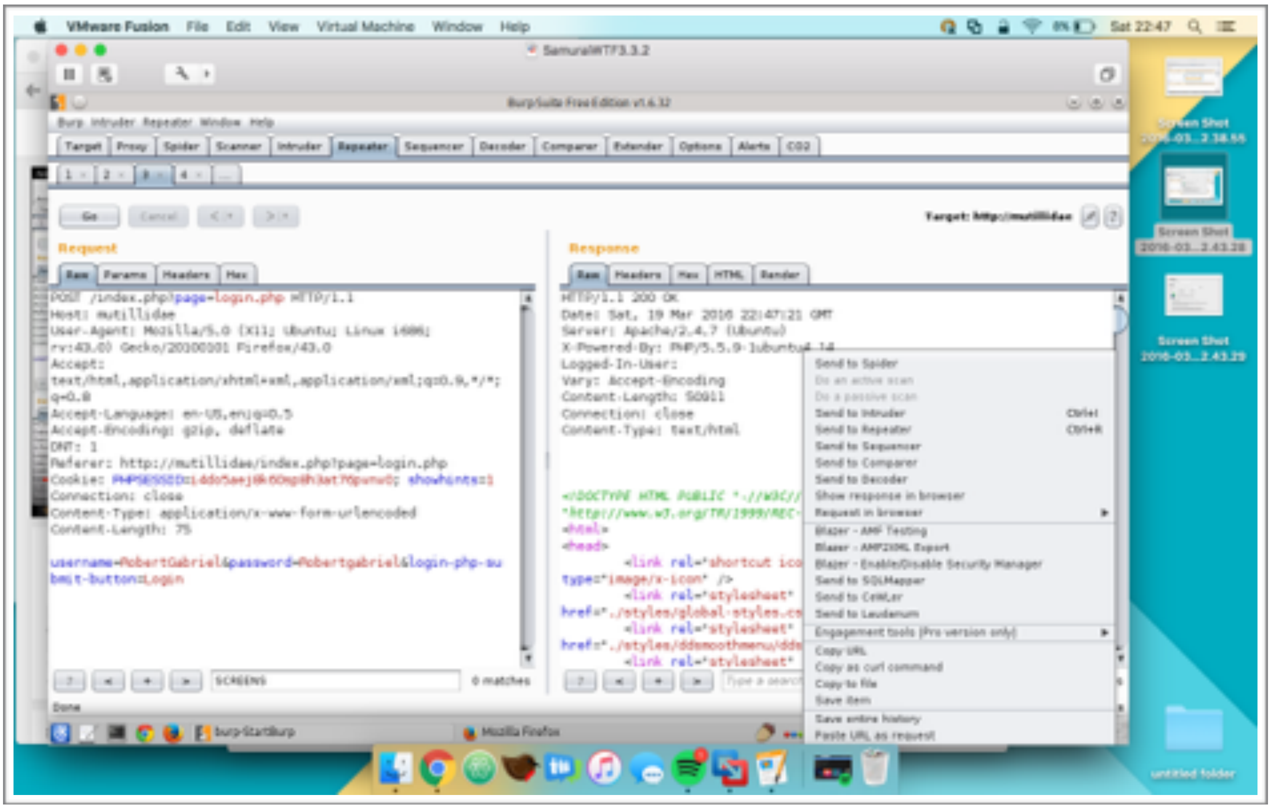


Burp Suite
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder
1 × 2 × 3 × ...
Go Cancel < >
Request
Raw Params Headers Hex

```
POST /index.php?page=login.php HTTP/1.1
Host: mutillidae
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686;
rv:43.0) Gecko/20100101 Firefox/43.0
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
DNT: 1
Referer: http://mutillidae/index.php?page=login.php
Cookie: PHPSESSID=i4do5aej8k60sp8h3at76pvnv0; showhints=1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 75
```

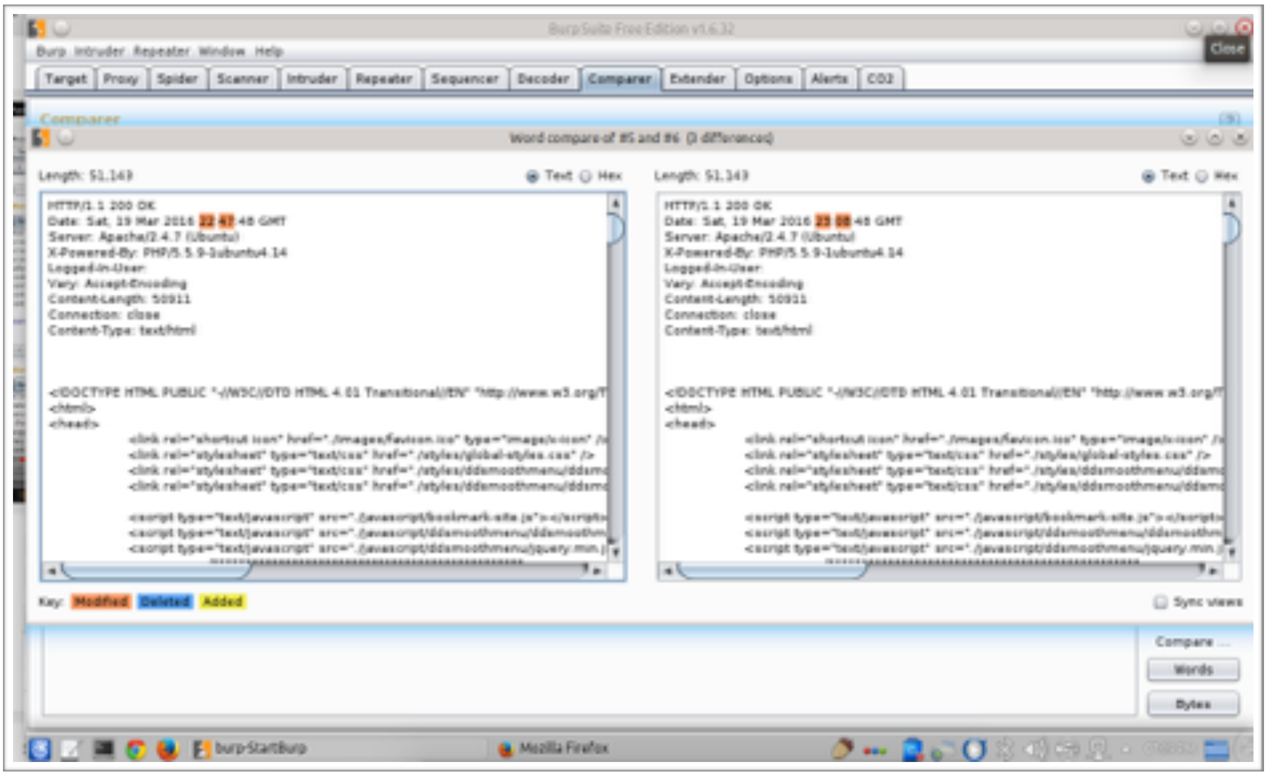
Comparing

So now go to the repeater tab and click go on both the valid and invalid requests. This will send the responses on the right hand side. Right click and send to to compare



```
POST /index.php?page=login.php HTTP/1.1
Host: mutillidae
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686;
rv:43.0) Gecko/20100101 Firefox/43.0
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
DNT: 1
Referer: http://mutillidae/index.php?page=login.php
Cookie: PHPSESSID=i4do5aej8k60mp8h3at70punu0; showhints=1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 75

username=RobertGabriel&password=Robertgabriel&login-php-su
bmit-button=Login
```

```
HTTP/1.1 200 OK
Date: Sat, 19 Mar 2016 22:47:21 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Logged-In-User:
Vary: Accept-Encoding
Content-Length: 50811
Connection: close
Content-Type: text/html



<!DOCTYPE HTML PUBLIC "-//W3C//
"http://www.w3.org/TR/1999/REC-
<html>
<head>
        <link rel="shortcut ico
type="image/x-icon" />
        <link rel="stylesheet"
href="./styles/global-styles.cs
        <link rel="stylesheet"
href="./styles/ddsmoothmenu/dds
        <link rel="stylesheet"
```

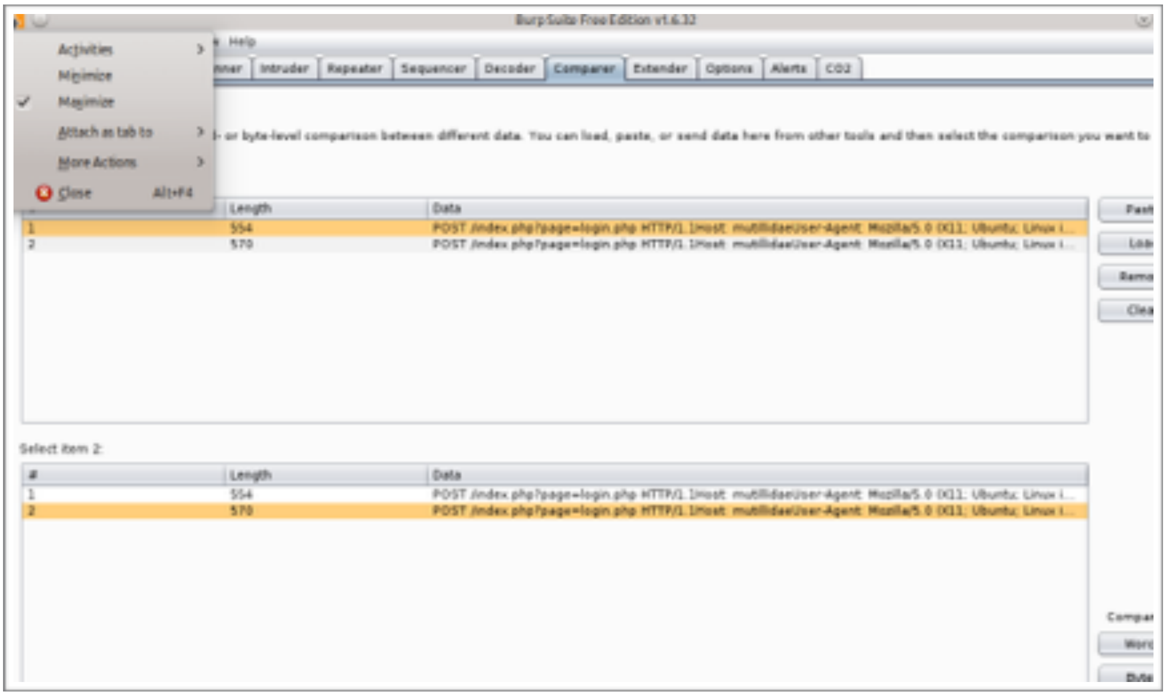

Burp Suite Free Edition v1.6.32
Close
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts CO2
Comparer
Word compare of #5 and #6 (3 differences)
Length: 51,143
● Text ○ Hex
Length: 51,143
● Text ○ Hex
Key: Modified Deleted Added
□ Sync views
Compare ...
Words
Bytes
burp-StartBurp
Mozilla Firefox

```
HTTP/1.1 200 OK
Date: Sat, 19 Mar 2016 22:47:48 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Logged-In-User:
Vary: Accept-Encoding
Content-Length: 50911
Connection: close
Content-Type: text/html


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/T
<html>
<head>
            <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />
            <link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
            <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmo
            <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmo

            <script type="text/javascript" src="./javascript/bookmark-site.js"></script
            <script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothm
            <script type="text/javascript" src="./javascript/ddsmoothmenu/jquery.min.j
```

```
HTTP/1.1 200 OK
Date: Sat, 19 Mar 2016 22:08:48 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Logged-In-User:
Vary: Accept-Encoding
Content-Length: 50911
Connection: close
Content-Type: text/html


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/T
<html>
<head>
            <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />
            <link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
            <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmo
            <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmo

            <script type="text/javascript" src="./javascript/bookmark-site.js"></script
            <script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothm
            <script type="text/javascript" src="./javascript/ddsmoothmenu/jquery.min.j
```

So now that we have sent both the valid and invalid request to the compare tab.

You want to click the compare words button on the bottom right.


Burp Suite Free Edition v1.6.32
Activities
Minimize
Maximize
Attach as tab to
More Actions
Close Alt+F4
Help
nner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts CO2
Past
Loa
Remo
Clea
Compar
Word
Byte

- or byte-level comparison between different data. You can load, paste, or send data here from other tools and then select the comparison you want to

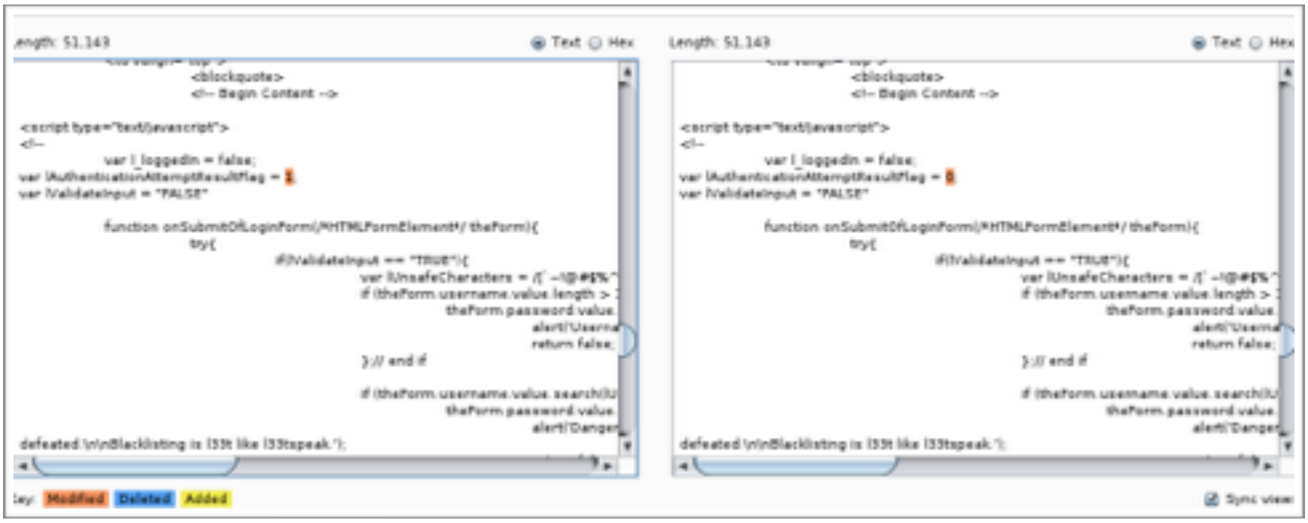
#	Length	Data
1	554	POST /index.php?page=login.php HTTP/1.1Host: mutillidaeUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i...
2	570	POST /index.php?page=login.php HTTP/1.1Host: mutillidaeUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i...

Select item 2:

#	Length	Data
1	554	POST /index.php?page=login.php HTTP/1.1Host: mutillidaeUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i...
2	570	POST /index.php?page=login.php HTTP/1.1Host: mutillidaeUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i...

We know want to compare the files and look for differences in the responses.

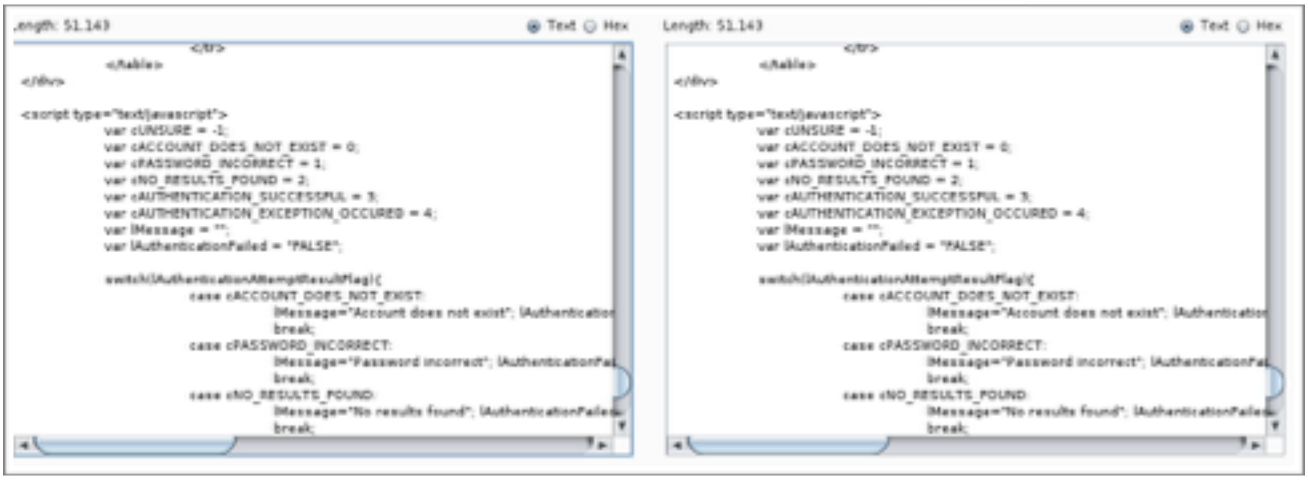
1. First thing we notice is the different flag numbers



```
                        <blockquote>
                        <!-- Begin Content -->

<script type="text/javascript">
<!--
            var l_loggedin = false;
var lAuthenticationAttemptResultFlag = 1
var lValidateInput = "FALSE"

            function onSubmitOfLoginForm(/*HTMLFormElement*/ theForm){
                        try{
                                    if(lValidateInput == "TRUE"){
                                                var lUnsafeCharacters = /['`~!@#$%^
                                                if (theForm.username.value.length > 1
                                                            theForm.password.value.
                                                                        alert('Userna
                                                                        return false;
                                                };// end if

                                                if (theForm.username.value.search(lU
                                                            theForm.password.value.
                                                                        alert('Danger
defeated.\n\nBlacklisting is l33t like l33tspeak.');
```

```
                        <blockquote>
                        <!-- Begin Content -->

<script type="text/javascript">
<!--
            var l_loggedin = false;
var lAuthenticationAttemptResultFlag = 0
var lValidateInput = "FALSE"

            function onSubmitOfLoginForm(/*HTMLFormElement*/ theForm){
                        try{
                                    if(lValidateInput == "TRUE"){
                                                var lUnsafeCharacters = /['`~!@#$%^
                                                if (theForm.username.value.length > 1
                                                            theForm.password.value.
                                                                        alert('Userna
                                                                        return false;
                                                };// end if

                                                if (theForm.username.value.search(lU
                                                            theForm.password.value.
                                                                        alert('Danger
defeated.\n\nBlacklisting is l33t like l33tspeak.');
```

2. Second thing is the error messages if we look one of the responses for **account does not exist**. We discover by searching that term is that the response is used in a javascript switch statement to display a message. So 1 will display account not found. It injects the message into the page after wards.



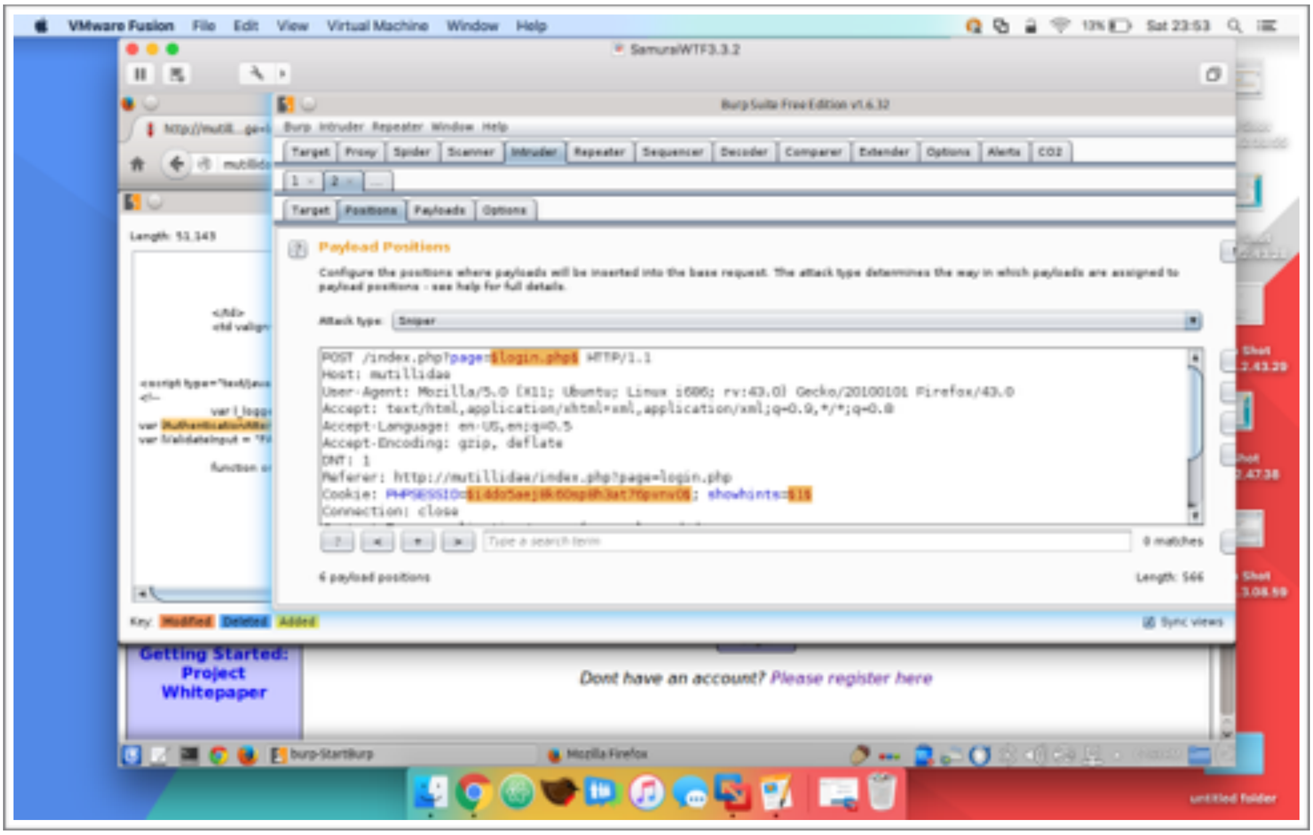
```
                        </tr>
            </table>
</div>

<script type="text/javascript">
            var cUNSURE = -1;
            var cACCOUNT_DOES_NOT_EXIST = 0;
            var cPASSWORD_INCORRECT = 1;
            var cNO_RESULTS_FOUND = 2;
            var cAUTHENTICATION_SUCCESSFUL = 3;
            var cAUTHENTICATION_EXCEPTION_OCCURED = 4;
            var lMessage = "";
            var lAuthenticationFailed = "FALSE";

            switch(lAuthenticationAttemptResultFlag){
                        case cACCOUNT_DOES_NOT_EXIST:
                                    lMessage="Account does not exist"; lAuthenticatio
                                    break;
                        case cPASSWORD_INCORRECT:
                                    lMessage="Password incorrect"; lAuthenticationFa
                                    break;
                        case cNO_RESULTS_FOUND:
                                    lMessage="No results found"; lAuthenticationFaile
                                    break;
```

```
                        </tr>
            </table>
</div>

<script type="text/javascript">
            var cUNSURE = -1;
            var cACCOUNT_DOES_NOT_EXIST = 0;
            var cPASSWORD_INCORRECT = 1;
            var cNO_RESULTS_FOUND = 2;
            var cAUTHENTICATION_SUCCESSFUL = 3;
            var cAUTHENTICATION_EXCEPTION_OCCURED = 4;
            var lMessage = "";
            var lAuthenticationFailed = "FALSE";

            switch(lAuthenticationAttemptResultFlag){
                        case cACCOUNT_DOES_NOT_EXIST:
                                    lMessage="Account does not exist"; lAuthenticatio
                                    break;
                        case cPASSWORD_INCORRECT:
                                    lMessage="Password incorrect"; lAuthenticationFa
                                    break;
                        case cNO_RESULTS_FOUND:
                                    lMessage="No results found"; lAuthenticationFaile
                                    break;
```

Next we have to take and remember the variable lAuthenticationAttemptResultFlag.

Next to back to the repeater and send the reponcse to the intruder for **lAuthenticationAttemptResultFlag = 1**

Here you see all the items are highlighted , clear this by clicking on the right.


VMware Fusion File Edit View Virtual Machine Window Help
SamuraiWTF3.3.2
Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts CO2
Target Positions Payloads Options
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

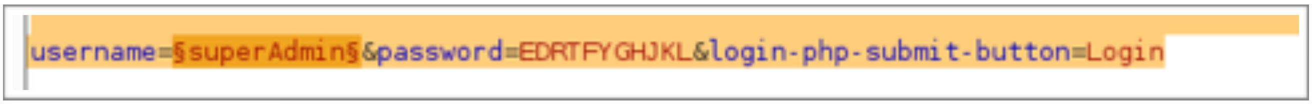
```
POST /index.php?page=§login.php§ HTTP/1.1
Host: mutillidae
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://mutillidae/index.php?page=login.php
Cookie: PHPSESSID=§1ddo5aej8k60sp8h3at7tpvnv0§; showhints=§1§
Connection: close
```

6 payload positions

Length: 566

Dont have an account? Please register here

Next highlight the username variable and add it by clicking on the right side button add. Also add a fake password input.



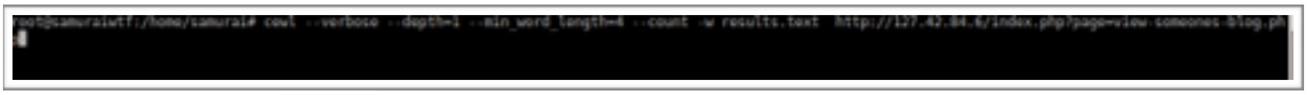
```
username=§superAdmin§&password=EDRTFYGHJKL&login-php-submit-button=Login
```

Next click on the payload tab, we will need to get a list of usernames for the payload. Where going to do this using a tool called **cewl.**
It will scrap usernames from the site to make our list, in which to try muiltpy access attempts on.

Remember to Turn off FoxyProxy.

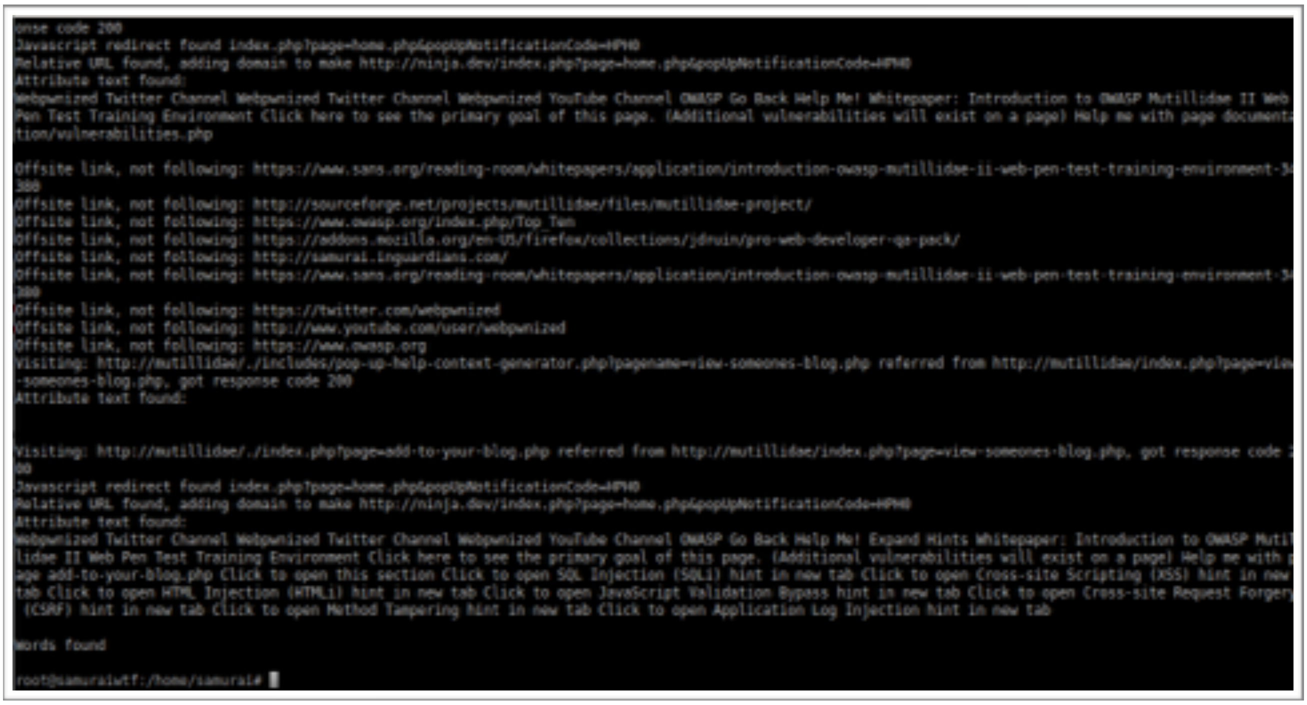
First open up the command line.
Enter the following, we are setting the following

1. **depth** = 1 the amount of links we need follow from the base url we set.
2. **min-word-length = 4** , the current default is two short of 3, so 4 is better. (Did this betraying to see what was the shortest username I could create with.)
3. **—write, to write the results to a file .**
4. **—verbose** flag will show us what is happening while we are working.



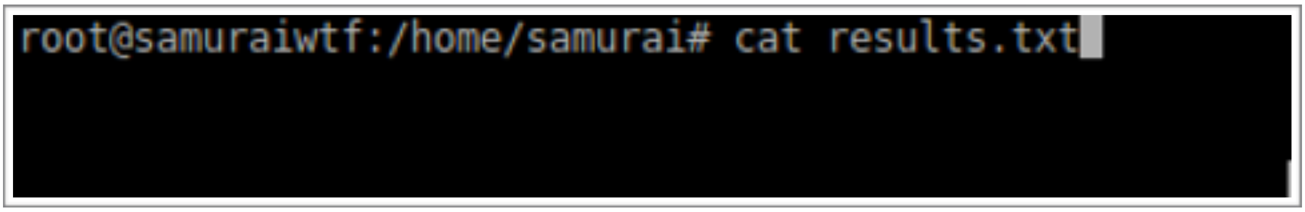
```
root@samuraiwtf:/home/samurai# cewl --verbose --depth=1 --min_word_length=4 --count -w results.text  http://127.42.84.6/index.php?page=view-someones-blog.ph
```

When we run it we get the following:



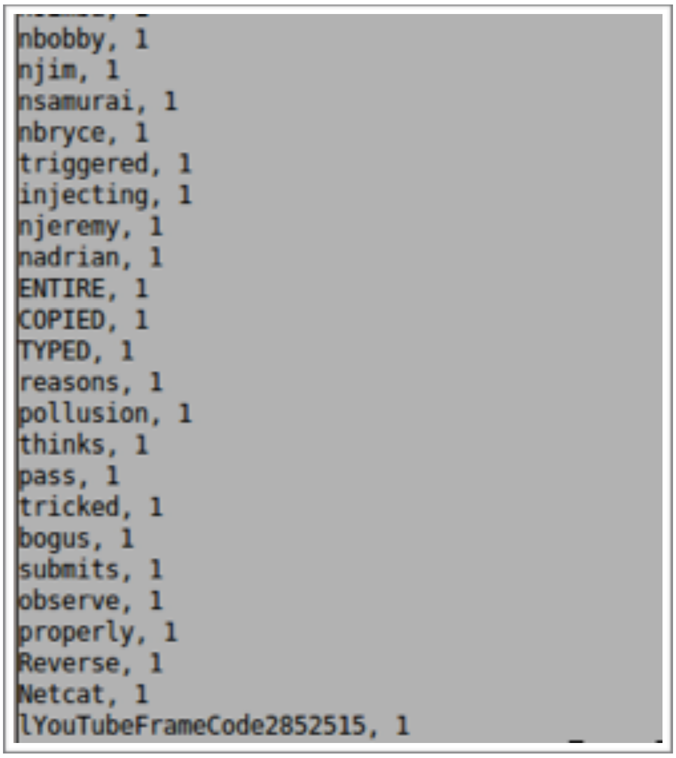
```
onse code 200
Javascript redirect found index.php?page=home.php&popUpNotificationCode=HPH0
Relative URL found, adding domain to make http://ninja.dev/index.php?page=home.php&popUpNotificationCode=HPH0
Attribute text found:
Webpwnized Twitter Channel Webpwnized Twitter Channel Webpwnized YouTube Channel OWASP Go Back Help Me! Whitepaper: Introduction to OWASP Mutillidae II Web
Pen Test Training Environment Click here to see the primary goal of this page. (Additional vulnerabilities will exist on a page) Help me with page documenta
tion/vulnerabilities.php

Offsite link, not following: https://www.sans.org/reading-room/whitepapers/application/introduction-owasp-mutillidae-ii-web-pen-test-training-environment-34
380
Offsite link, not following: http://sourceforge.net/projects/mutillidae/files/mutillidae-project/
Offsite link, not following: https://www.owasp.org/index.php/Top_Ten
Offsite link, not following: https://addons.mozilla.org/en-US/firefox/collections/jdruin/pro-web-developer-qa-pack/
Offsite link, not following: http://samurai.inguardians.com/
Offsite link, not following: https://www.sans.org/reading-room/whitepapers/application/introduction-owasp-mutillidae-ii-web-pen-test-training-environment-34
380
Offsite link, not following: https://twitter.com/webpwnized
Offsite link, not following: http://www.youtube.com/user/webpwnized
Offsite link, not following: https://www.owasp.org
Visiting: http://mutillidae/./includes/pop-up-help-context-generator.php?pagename=view-someones-blog.php referred from http://mutillidae/index.php?page=view
-someones-blog.php, got response code 200
Attribute text found:


Visiting: http://mutillidae/./index.php?page=add-to-your-blog.php referred from http://mutillidae/index.php?page=view-someones-blog.php, got response code 2
00
Javascript redirect found index.php?page=home.php&popUpNotificationCode=HPH0
Relative URL found, adding domain to make http://ninja.dev/index.php?page=home.php&popUpNotificationCode=HPH0
Attribute text found:
Webpwnized Twitter Channel Webpwnized Twitter Channel Webpwnized YouTube Channel OWASP Go Back Help Me! Expand Hints Whitepaper: Introduction to OWASP Mutil
lidae II Web Pen Test Training Environment Click here to see the primary goal of this page. (Additional vulnerabilities will exist on a page) Help me with p
age add-to-your-blog.php Click to open this section Click to open SQL Injection (SQLi) hint in new tab Click to open Cross-site Scripting (XSS) hint in new
tab Click to open HTML Injection (HTMLi) hint in new tab Click to open JavaScript Validation Bypass hint in new tab Click to open Cross-site Request Forgery
 (CSRF) hint in new tab Click to open Method Tampering hint in new tab Click to open Application Log Injection hint in new tab

Words found

root@samuraiwtf:/home/samurai# 
```

Next we need to view the words we got.
Do this by opening up the file we wrote, unlike the video are files are saved in /opt/samurai/cewl. Then we run cat results.txt



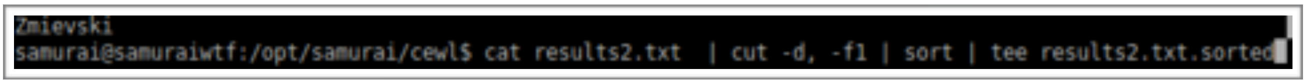
```
root@samuraiwtf:/home/samurai# cat results.txt
```

This was in the results, I then removed all defy not user names.



```
nbobby, 1
njim, 1
nsamurai, 1
nbryce, 1
triggered, 1
injecting, 1
njeremy, 1
nadrian, 1
ENTIRE, 1
COPIED, 1
TYPED, 1
reasons, 1
pollusion, 1
thinks, 1
pass, 1
tricked, 1
bogus, 1
submits, 1
observe, 1
properly, 1
Reverse, 1
Netcat, 1
lYouTubeFrameCode2852515, 1
```

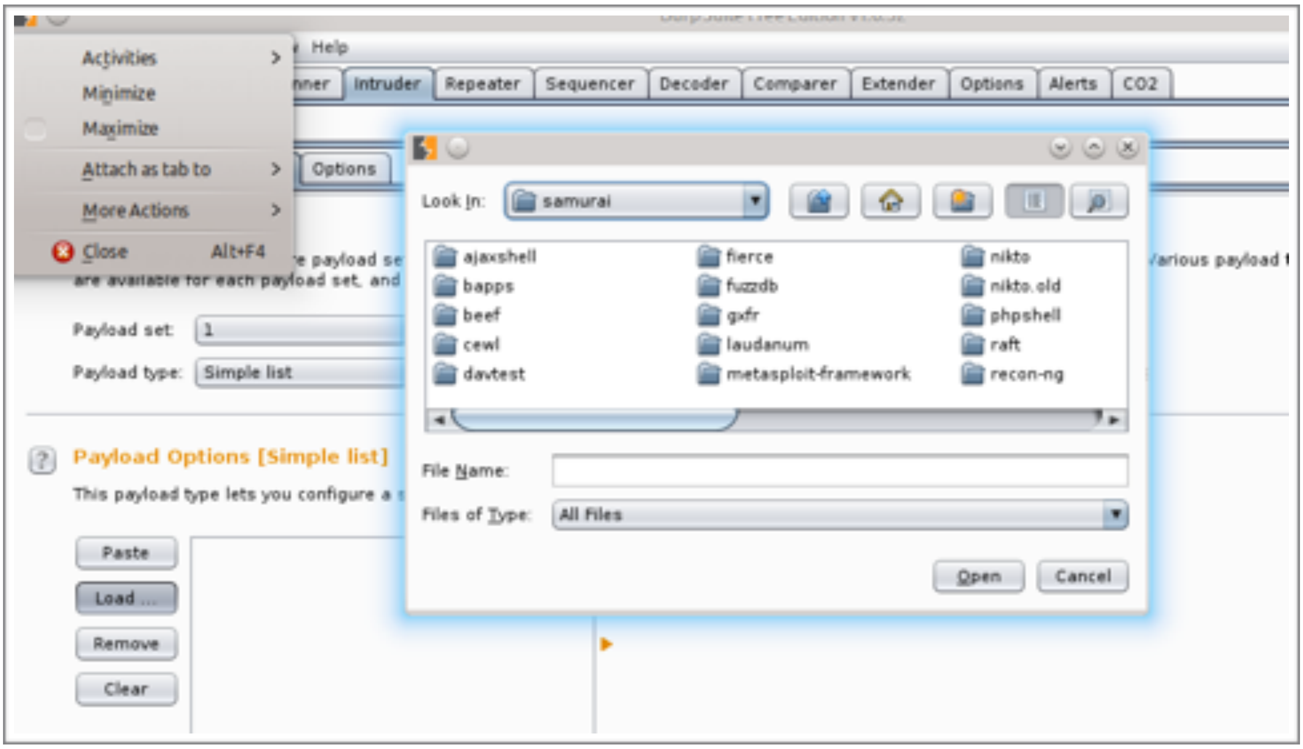
I then removed the **, 1** . This was the depth of the text was found at, 1 being one link off.
To do that I i did the following command



```
Zmievski
samurai@samuraiwtf:/opt/samurai/cewl$ cat results2.txt  | cut -d, -f1 | sort | tee results2.txt.sorted
```

This gave me the final list of what is needed.

So now with me having the final list, Go over to burp suite and load our sorted file into the payload



e payload se
are available for each payload set, and

/arious payload t

Payload set: 1

Payload type: Simple list

Payload Options [Simple list]

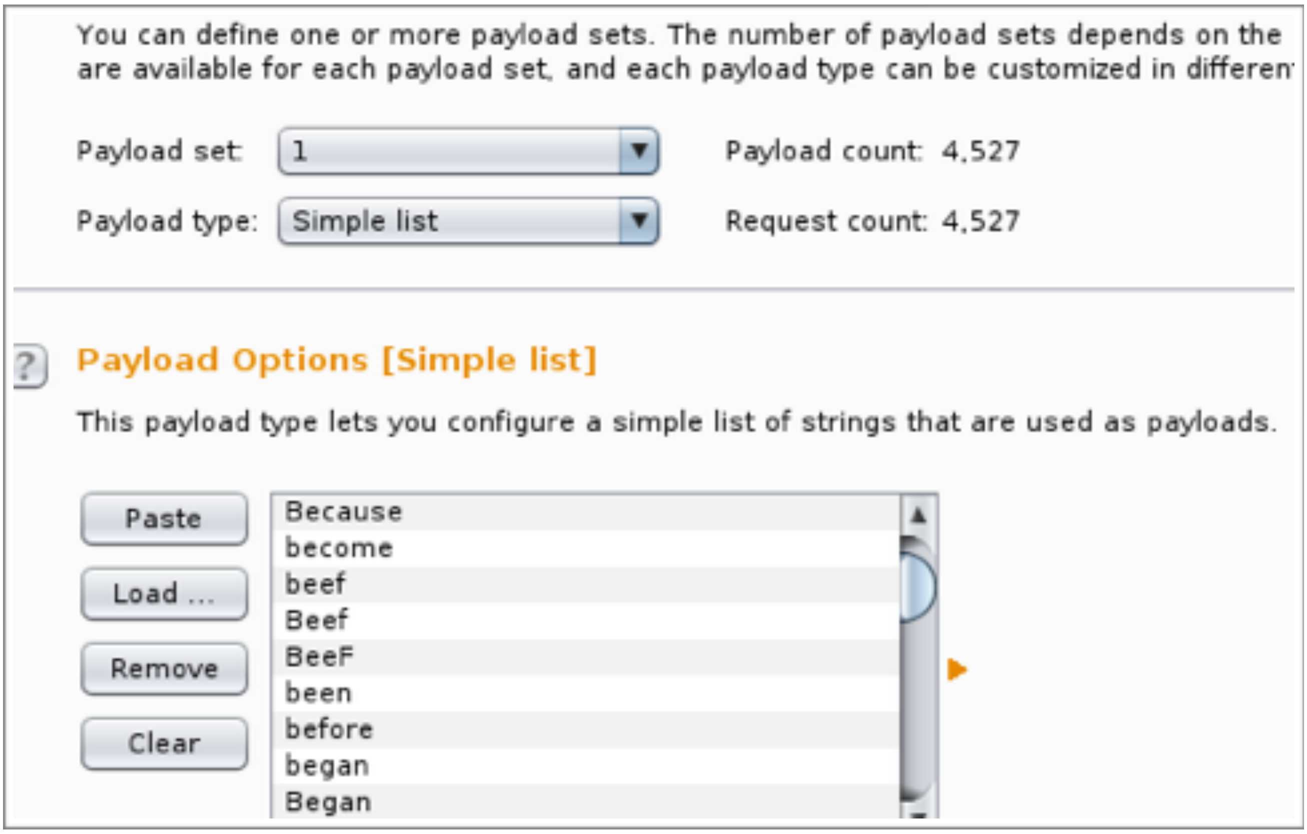
This payload type lets you configure a s

Look In: samurai

File Name:

Files of Type: All Files

There might look like theres repeats but theres captain letters.



You can define one or more payload sets. The number of payload sets depends on the
are available for each payload set, and each payload type can be customized in differen

Payload set: 1

Payload type: Simple list

Payload count: 4,527

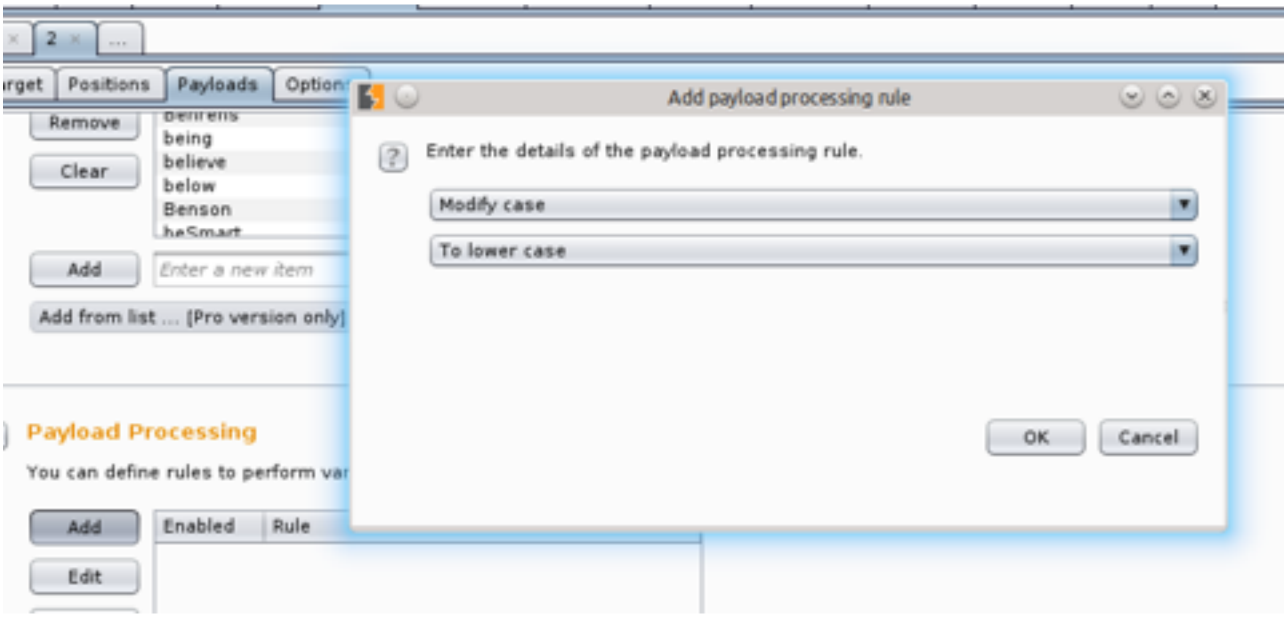
Request count: 4,527

Payload Options [Simple list]

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

Because
become
beef
Beef
BeeF
been
before
began
Began

Next go to the payload processing, as we are going to write a rule.
Where going to pick modify case and choice lower case as we are not sure if the site changes it to upper or lower or not at all but normally is lower.



Add payload processing rule

Enter the details of the payload processing rule.

Modify case

To lower case

Payload Processing

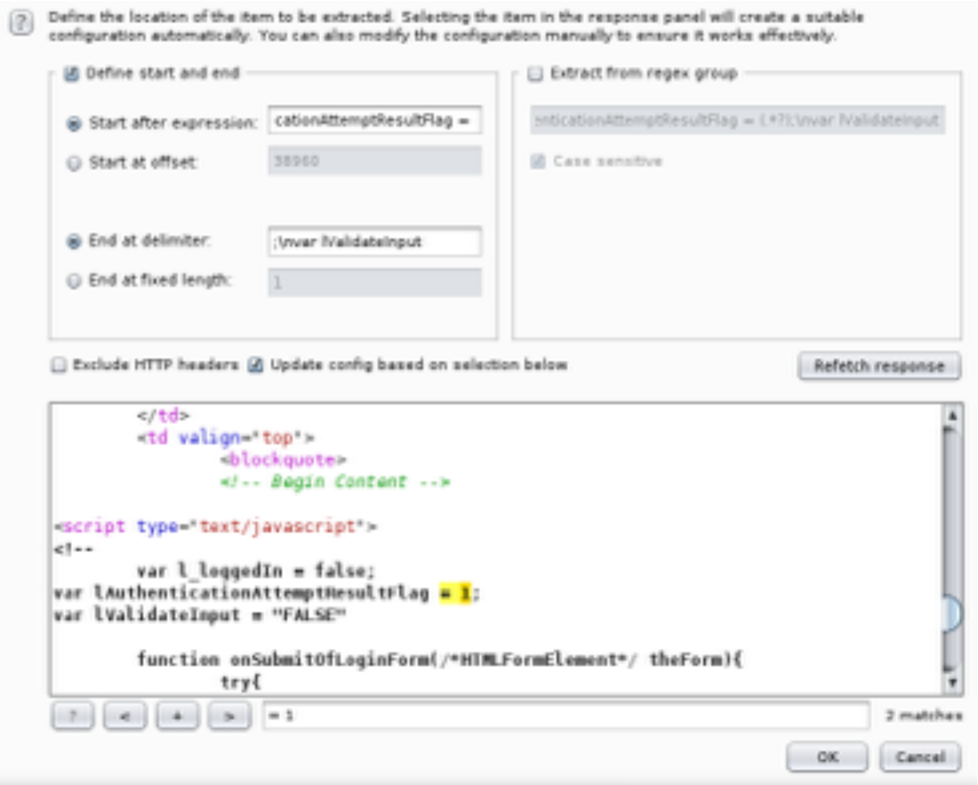
You can define rules to perform var

being
believe
below
Benson

Next go to the options menu.

Then go to the grep - extract tab and choose add. If you remember the pattern or error message code from earlier where going to use this here. Add a new exact option and carefully highlight the one. burp will auto create the regular expression.

As you can see below it has the pattern, very handy for sql swell.



Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

☑ Define start and end

● Start after expression: cationAttemptResultFlag =

○ Start at offset: 38960

● End at delimiter: ;\nvar lValidateInput

○ End at fixed length: 1

□ Extract from regex group

enticationAttemptResultFlag = (.*?);\nvar lValidateInput

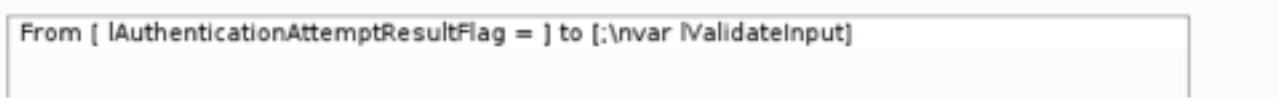
☑ Case sensitive

□ Exclude HTTP headers ☑ Update config based on selection below

```
          </td>
          <td valign="top">
                    <blockquote>
                    <!-- Begin Content -->

<script type="text/javascript">
<!--
          var l_loggedIn = false;
var lAuthenticationAttemptResultFlag = 1;
var lValidateInput = "FALSE"

          function onSubmitOfLoginForm(/*HTMLFormElement*/ theForm){
                    try{
```

= 1

2 matches

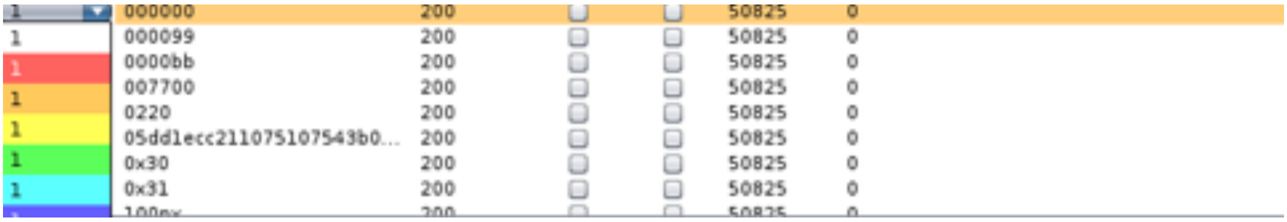


From [lAuthenticationAttemptResultFlag =] to [;\nvar lValidateInput]

Now lets start the attack

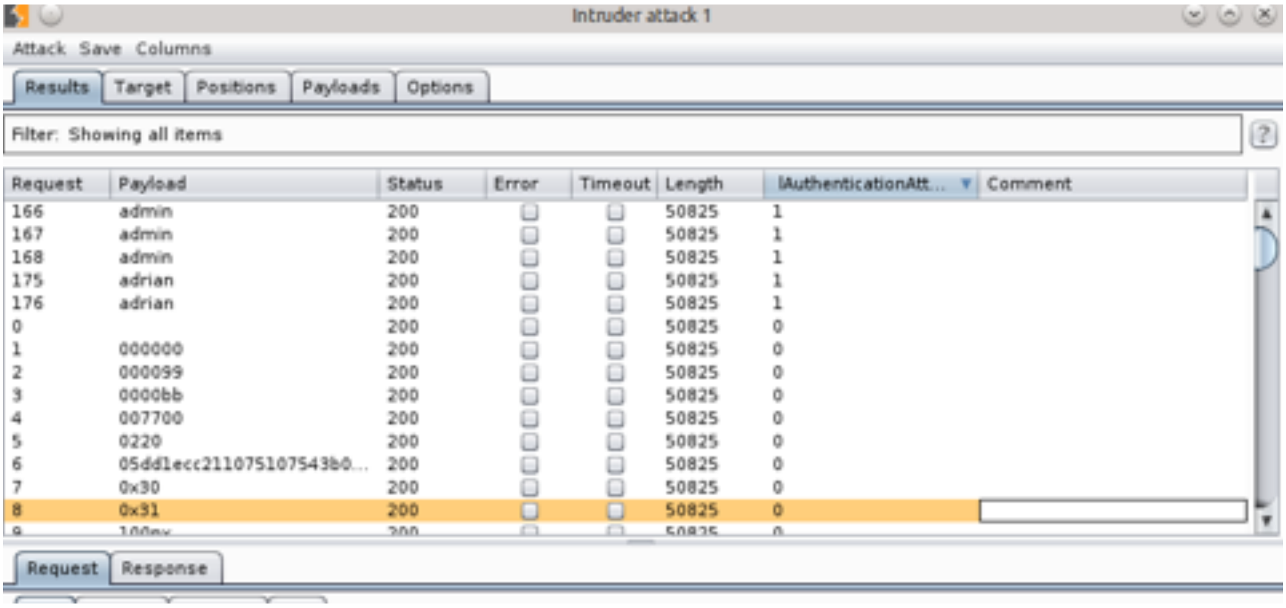
1. Go to intruder
2. Click on start attack

You will see it try everything from the payload list.
Its important to note is it responds.
The list of responds with 1 mean they are real accounts.



1	000000	200	□	□	50825	0
1	000099	200	□	□	50825	0
1	0000bb	200	□	□	50825	0
1	007700	200	□	□	50825	0
1	0220	200	□	□	50825	0
1	05dd1ecc211075107543b0...	200	□	□	50825	0
1	0x30	200	□	□	50825	0
1	0x31	200	□	□	50825	0
	100px	200	□	□	50825	0

This then is an example of more accounts that are real

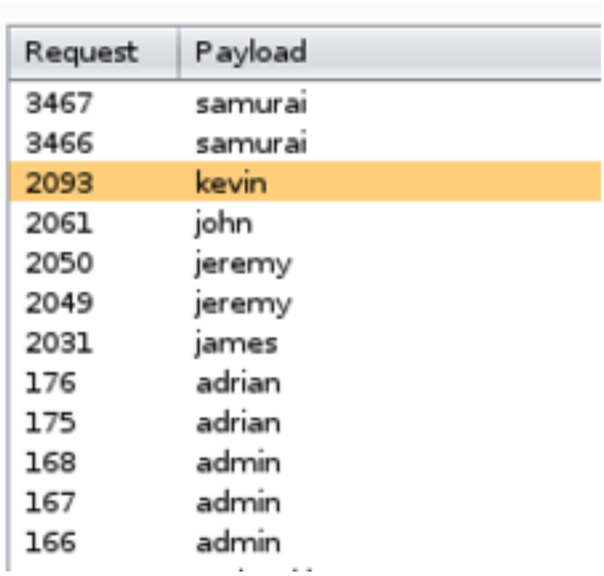


Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	lAuthenticationAtt...	Comment
166	admin	200	□	□	50825	1	
167	admin	200	□	□	50825	1	
168	admin	200	□	□	50825	1	
175	adrian	200	□	□	50825	1	
176	adrian	200	□	□	50825	1	
0		200	□	□	50825	0	
1	000000	200	□	□	50825	0	
2	000099	200	□	□	50825	0	
3	0000bb	200	□	□	50825	0	
4	007700	200	□	□	50825	0	
5	0220	200	□	□	50825	0	
6	05dd1ecc211075107543b0...	200	□	□	50825	0	
7	0x30	200	□	□	50825	0	
8	0x31	200	□	□	50825	0	
9	100px	200	□	□	50825	0	

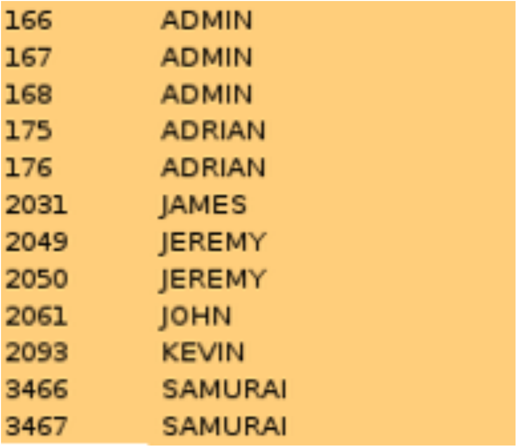
Then what is left is to brute force using the list of real usernames. THIS TOOK 3 DAYS….. I hope I get full marks for this.

List of all real accounts



Request	Payload
3467	samurai
3466	samurai
2093	kevin
2061	john
2050	jeremy
2049	jeremy
2031	james
176	adrian
175	adrian
168	admin
167	admin
166	admin

Then I tired it with all uppercase



166	ADMIN
167	ADMIN
168	ADMIN
175	ADRIAN
176	ADRIAN
2031	JAMES
2049	JEREMY
2050	JEREMY
2061	JOHN
2093	KEVIN
3466	SAMURAI
3467	SAMURAI

These are the active accounts , so we can brute force passwords on.