K. J. SOMAIYA COLLEGE OF ENGINEERING

CRYPTOGRAPHY AND SYSTEM SECURITY, IA-2 REPORT

Exploration of Penetration testing tool – *Burp Suite*

SHAILI SHAH (16010120114, B3)

KEYUR SHAH (16010120123, B3)

SARAUNSH JADHAV (16010120126, B3)

SAHIL SAYANI (16010120135,B3)

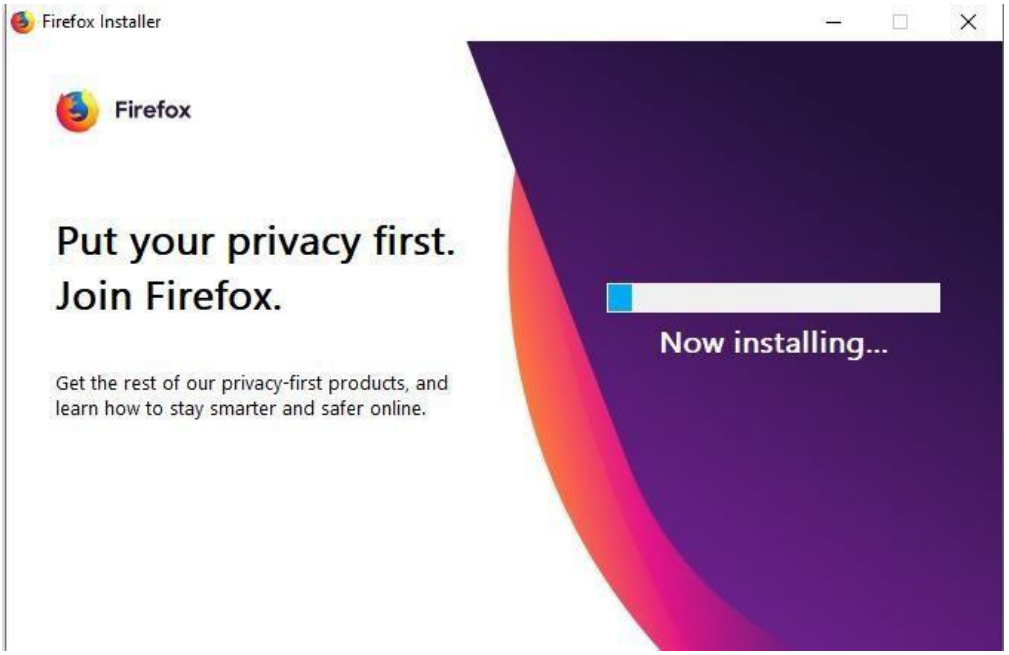
1. Introduction

Burp or Burp Suite is a graphical tool for testing Web application security. The tool is written in Java and developed by PortSwigger Web Security. The tool has three editions: a Community Edition that can be downloaded free of charge, a Professional Edition and an Enterprise Edition that can be purchased after a trial period. It intends to provide a comprehensive solution for web application security checks. In addition to basic functionality, such as proxy server, scanner and intruder, the tool also contains more advanced options such as a spider, a repeater, a decoder, a comparer, an extender and a sequencer.

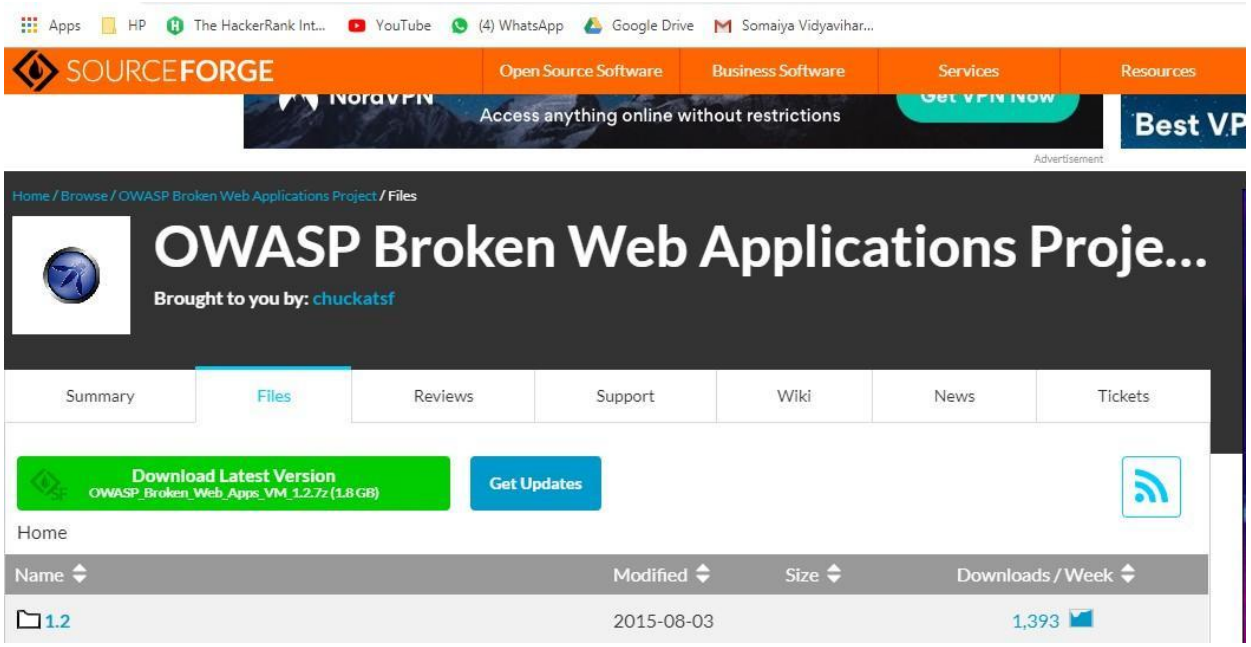
In its simplest form, Burp Suite can be classified as an Interception Proxy. While browsing their target application, a penetration tester can configure their internet browser to route traffic through the Burp Suite proxy server. Burp Suite then acts as a Man In The Middle by capturing and analysing each request to and from the target web application so that they can be analysed. Penetration testers can pause, manipulate and replay individual HTTP requests in order to analyse potential parameters or injection points. Injection points can be specified for manual as well as automated fuzzing attacks to discover potentially unintended application behaviours, crashes and error messages.

2. Installation

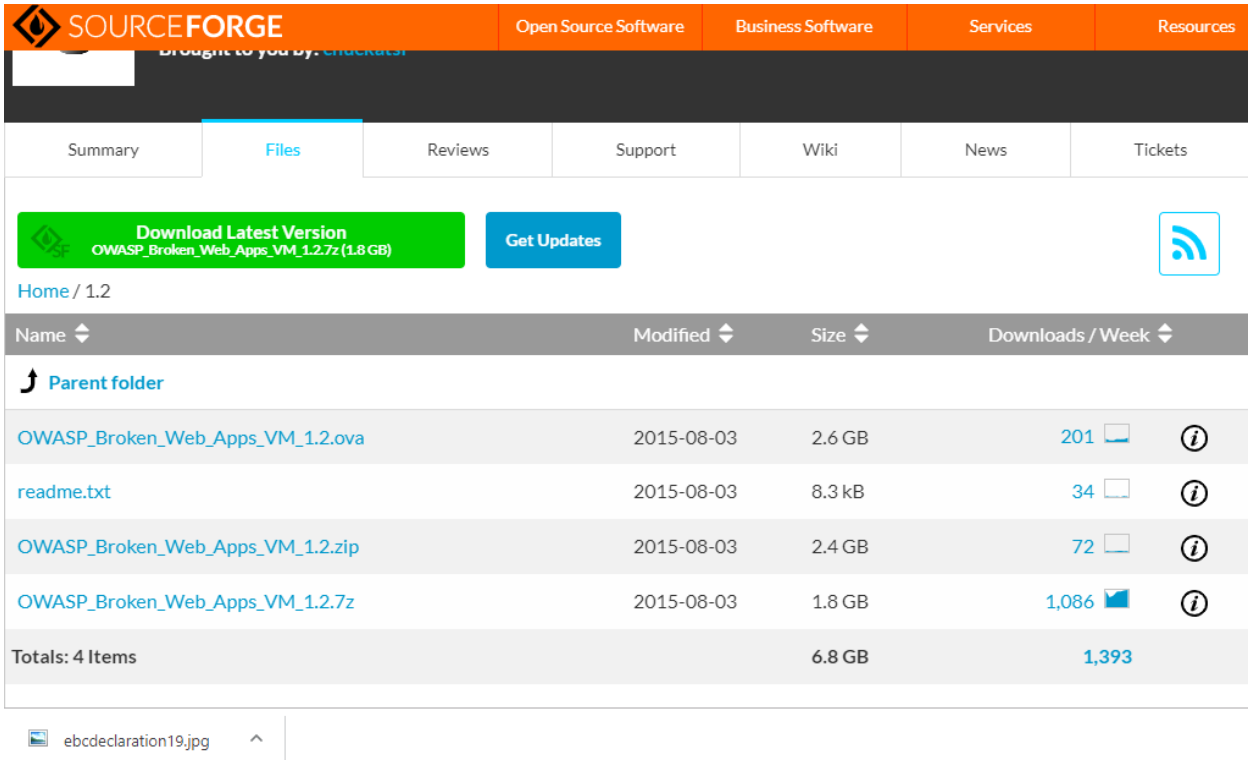
1. Install the firefox browser



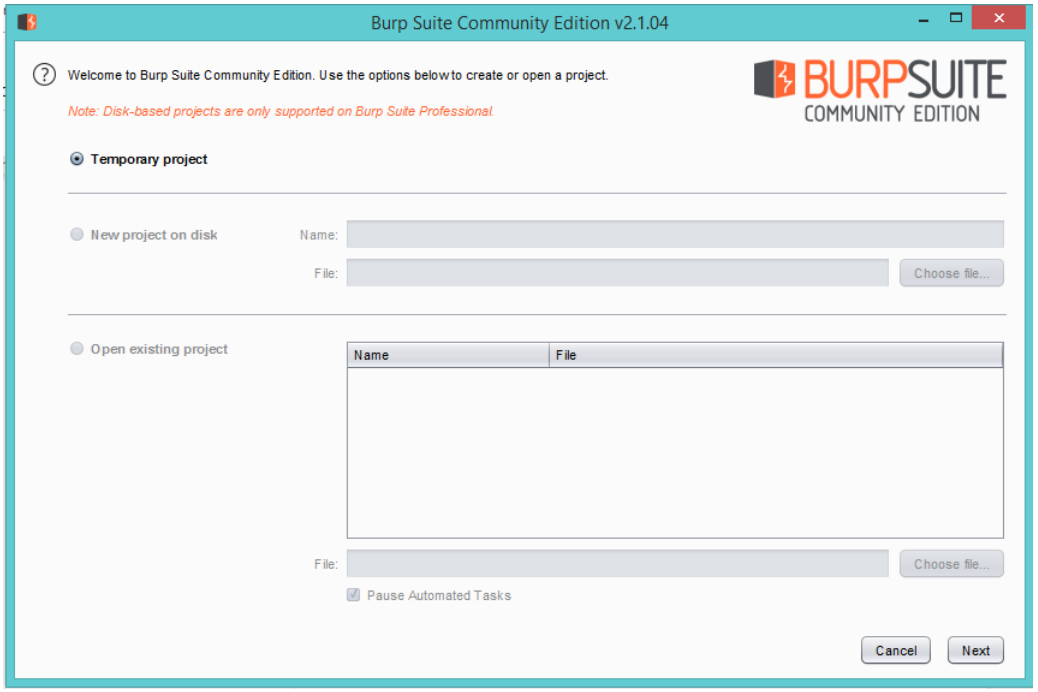
2. Download the Owasp Broken Web application project



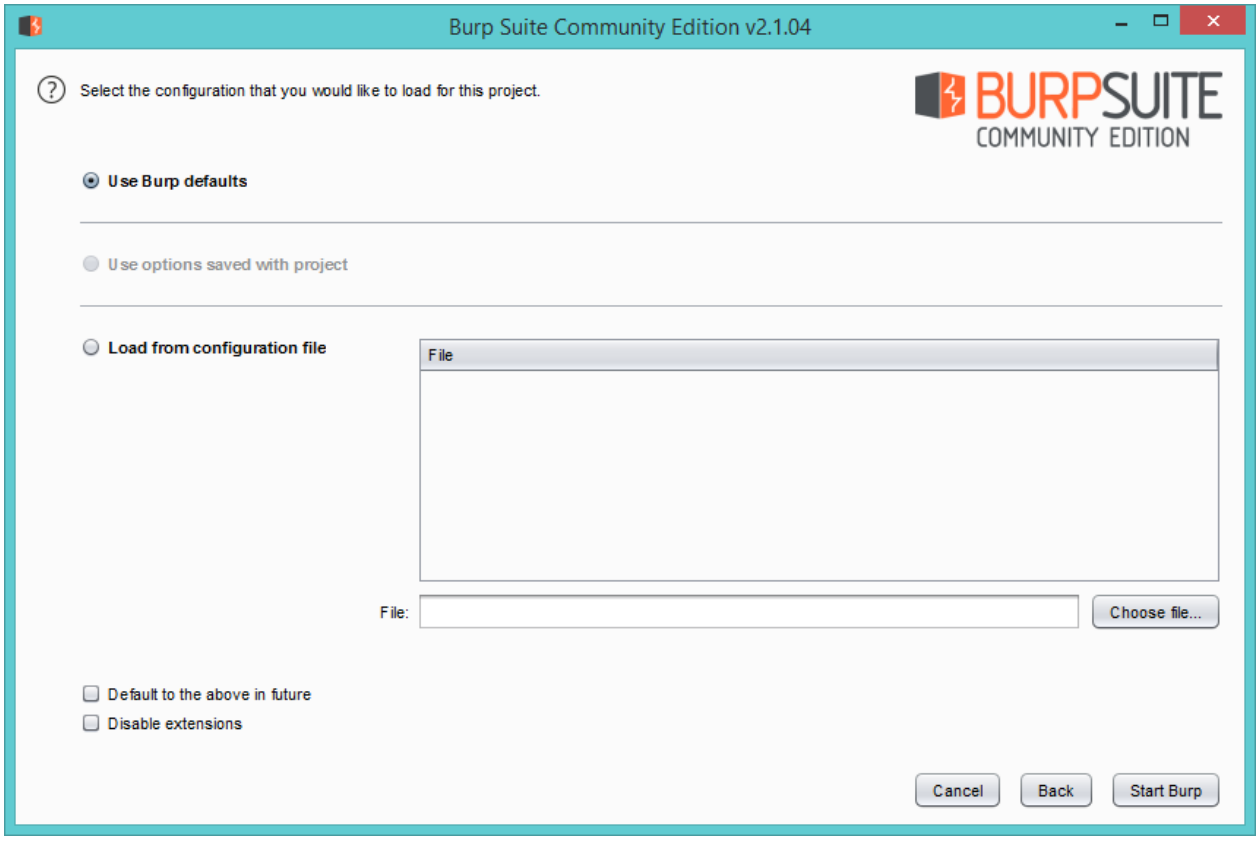
3. Download the .ova file



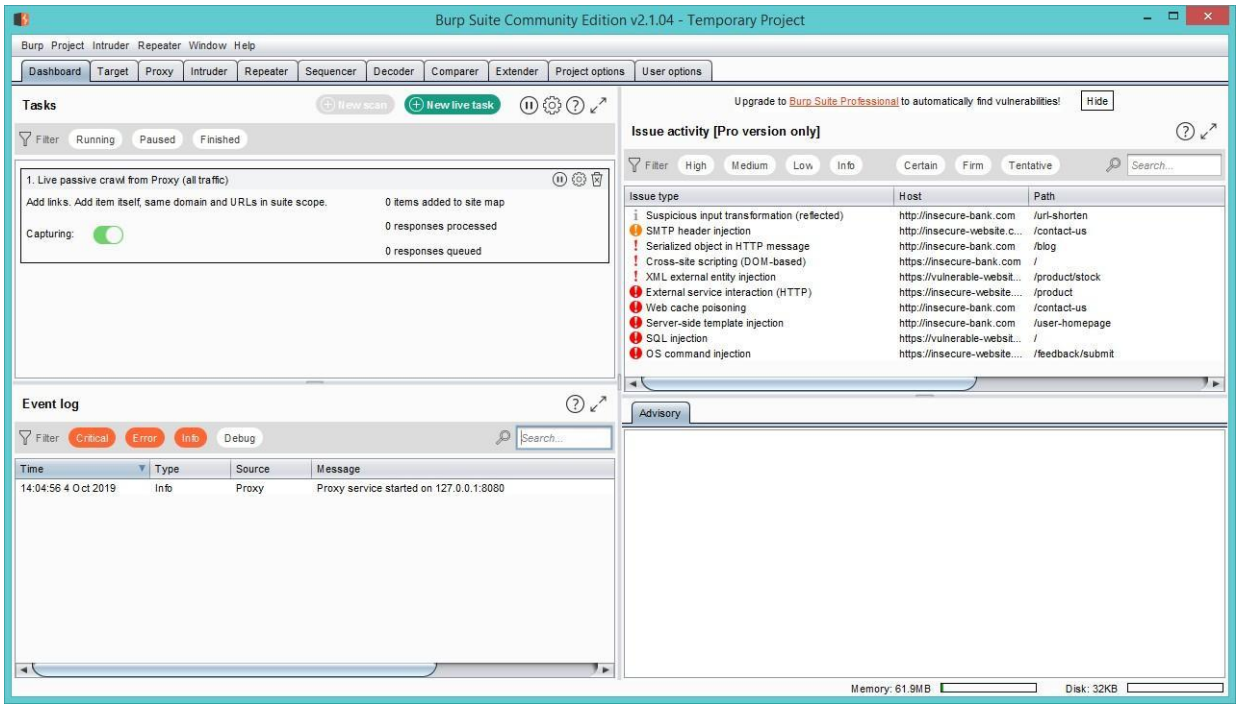
4. Download the burpsuite community edition and launch the application.



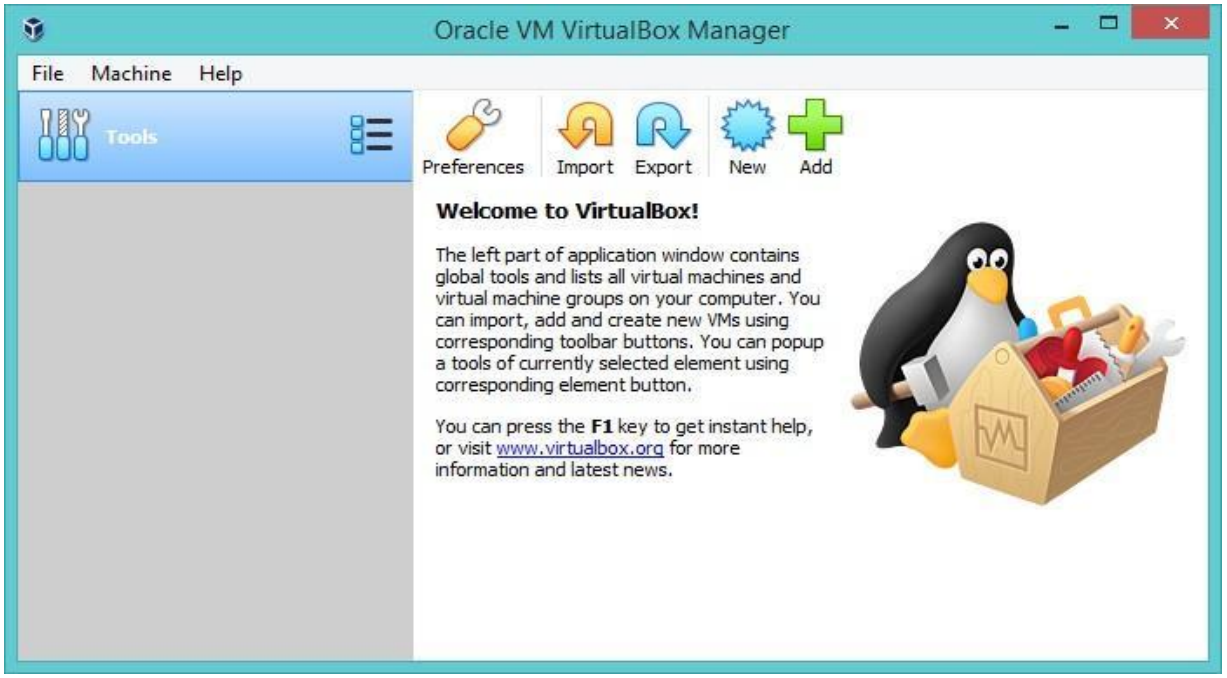
5. Accept the default settings



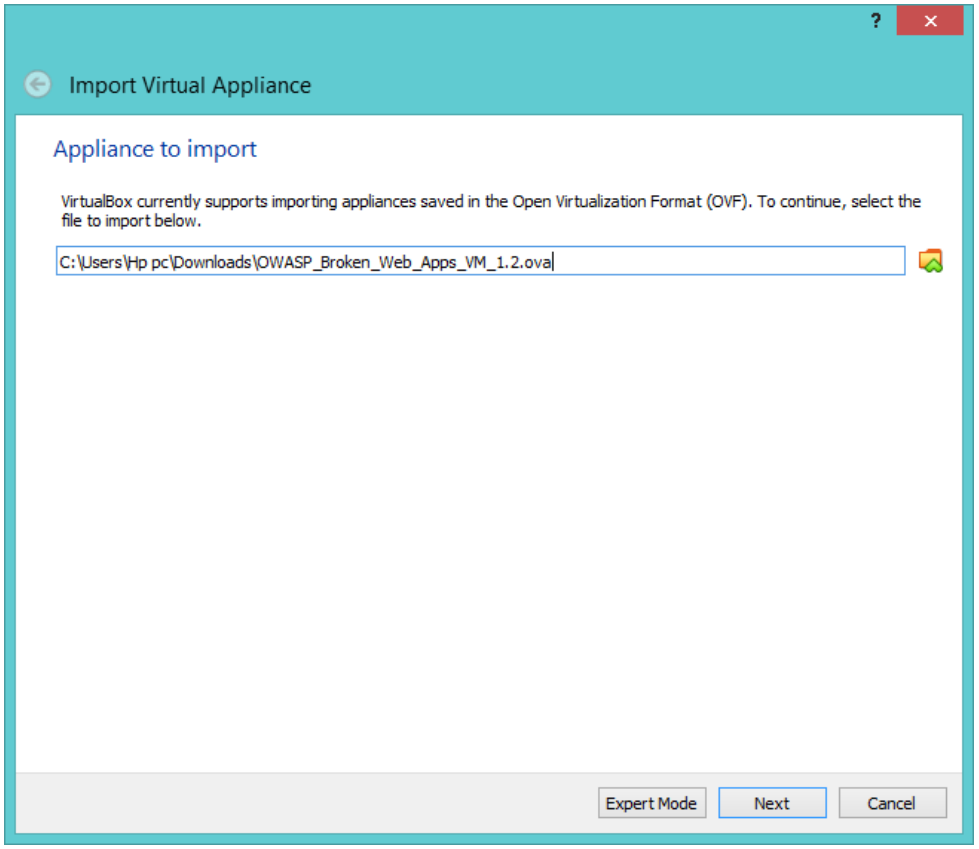
6. The dashboard looks like this

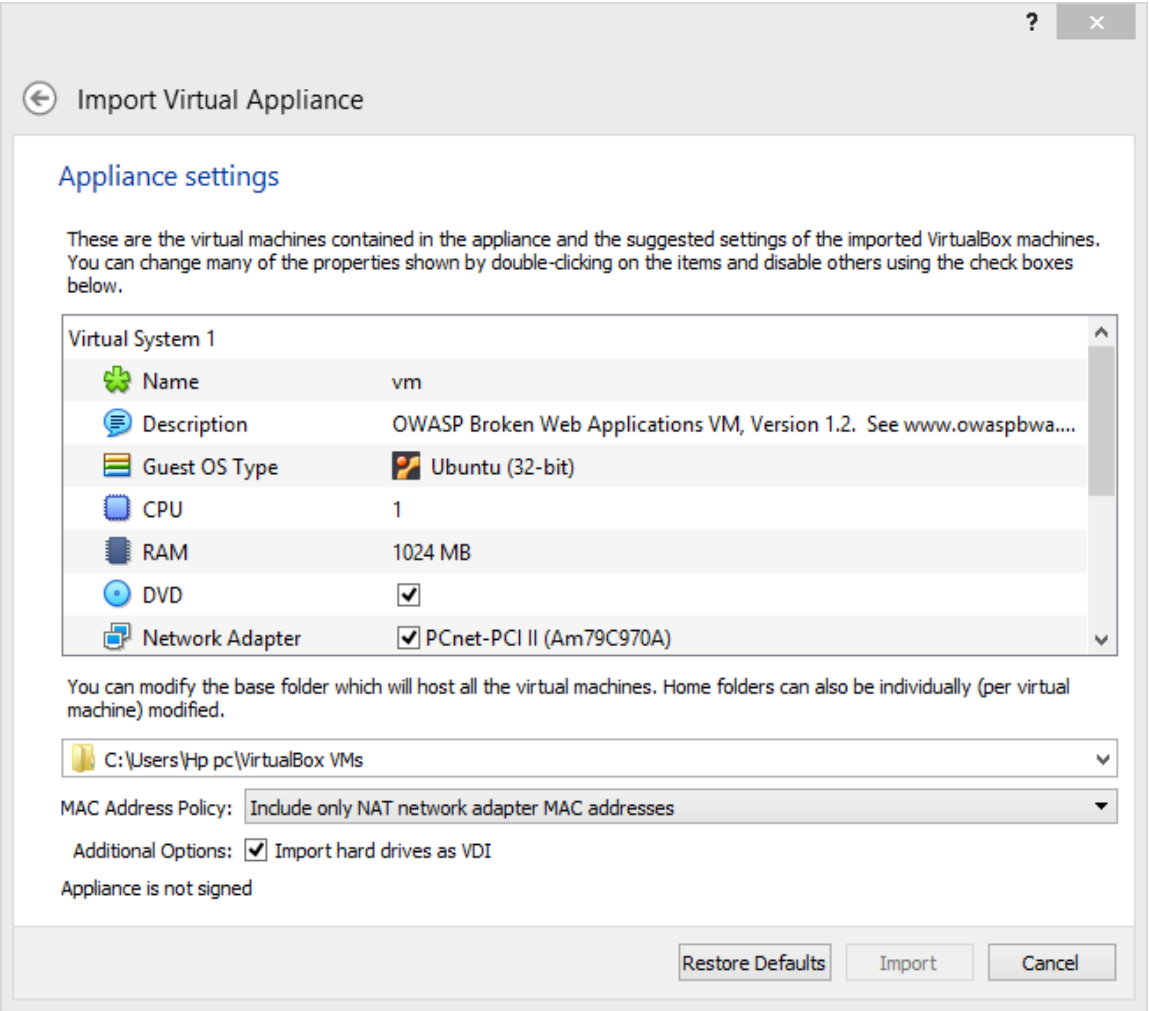


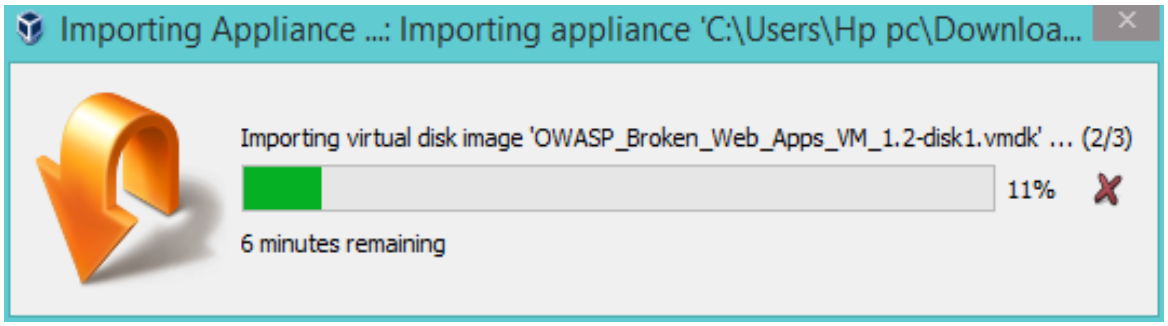
7. Install Virtualbox so we can use our OWASP broken web application



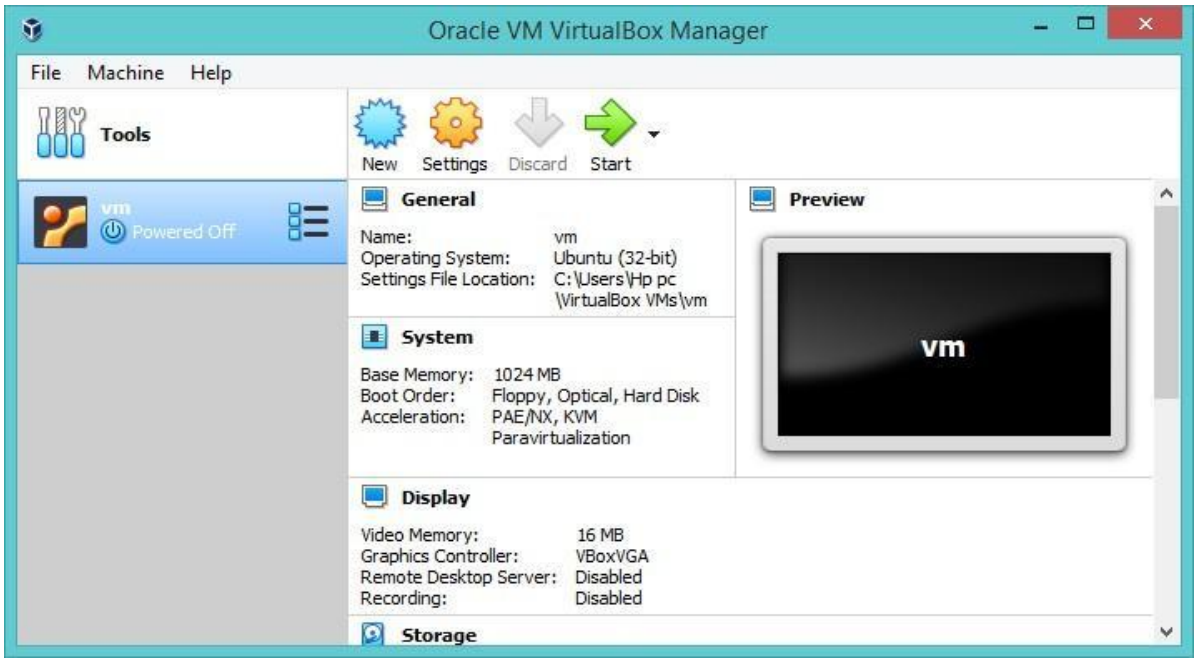
8. Import OWASP BWA



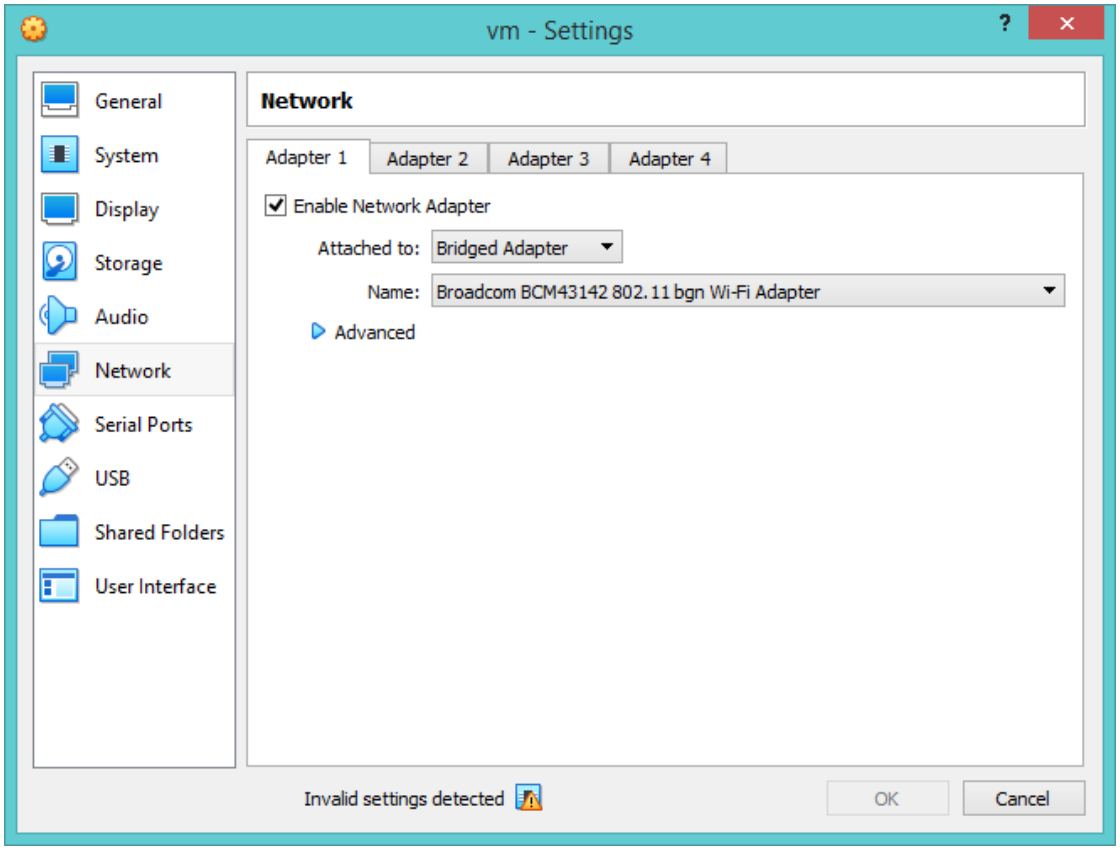

Import Virtual Appliance
Appliance settings
These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.
Virtual System 1
Name
vm
Description
OWASP Broken Web Applications VM, Version 1.2. See www.owaspbwa....
Guest OS Type
Ubuntu (32-bit)
CPU
1
RAM
1024 MB
DVD
Network Adapter
PCnet-PCI II (Am79C970A)
You can modify the base folder which will host all the virtual machines. Home folders can also be individually (per virtual machine) modified.
C:\Users\Hp pc\VirtualBox VMs
MAC Address Policy:
Include only NAT network adapter MAC addresses
Additional Options:
Import hard drives as VDI
Appliance is not signed
Restore Defaults
Import
Cancel


Importing Appliance ...: Importing appliance 'C:\Users\Hp pc\Downloa...
Importing virtual disk image 'OWASP_Broken_Web_Apps_VM_1.2-disk1.vmdk' ... (2/3)
11%
6 minutes remaining

9. Now the appliance has been imported



10. Change network settings



11. Start the machine, run the ifconfig command to get the address

```
You can access the web apps at http://192.168.0.8/

You can administer / configure this machine through the console here, by SSHing
to 192.168.0.8, via Samba at \\192.168.0.8\, or via phpmyadmin at
http://192.168.0.8/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d7:86:c5
          inet addr:192.168.0.8  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed7:86c5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:31 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3936 (3.9 KB)  TX bytes:6804 (6.8 KB)
          Interrupt:9 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14609 (14.6 KB)  TX bytes:14609 (14.6 KB)

root@owaspbwa:~#
```

3. Implementation

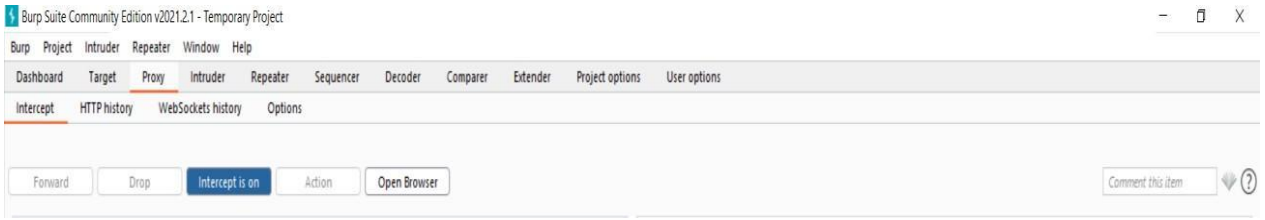
1. Proxy

Using Burpsuite as a proxy

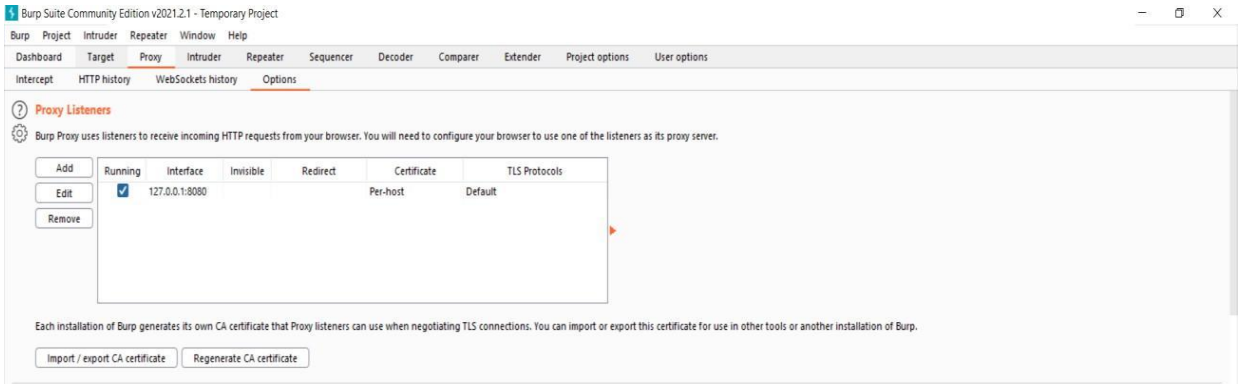
BurpSuite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit. It also lets the user send the request/response under monitoring to another relevant tool in BurpSuite, removing the burden of copy-paste. The proxy server can be adjusted to run on a specific loop-back ip and a port. The proxy can also be configured to filter out specific types of request-response pairs. Proxy feature is mainly used for intercepting our requests and also stores our HTTP history.

Intercept:

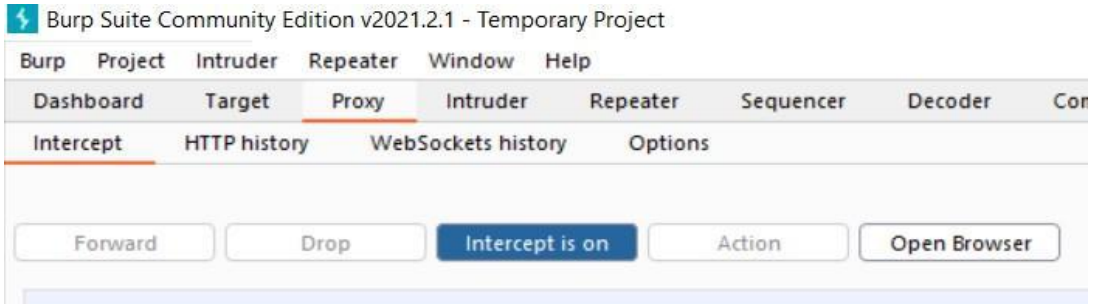
1. Go to the proxy tab and select the intercept option



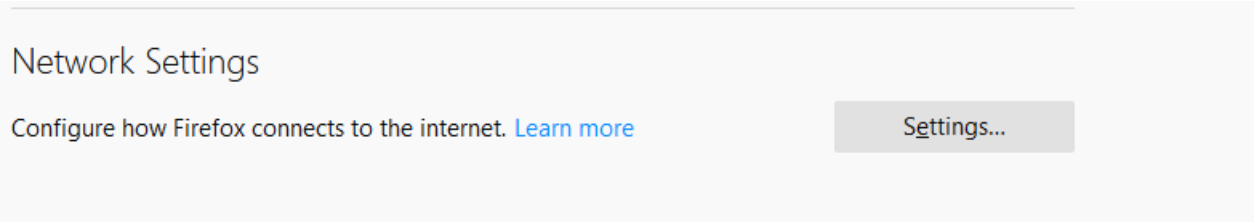
2. Select Options category and check if the proxy is listening on localhost, port 8080



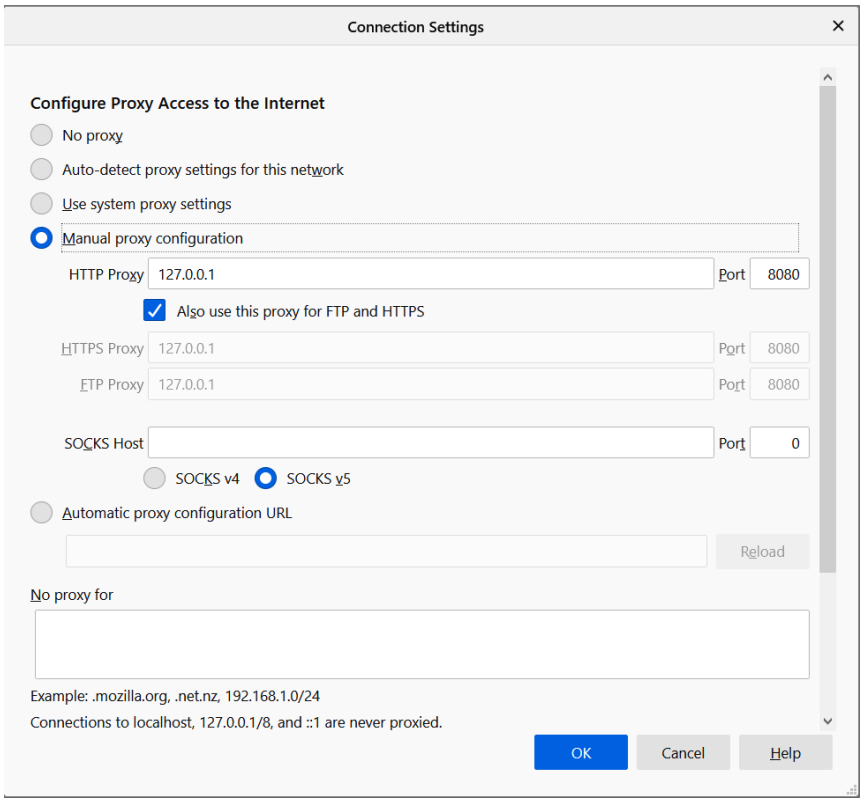
3. Turn the intercept on



4. Open browser, firefox in this case, go to network settings

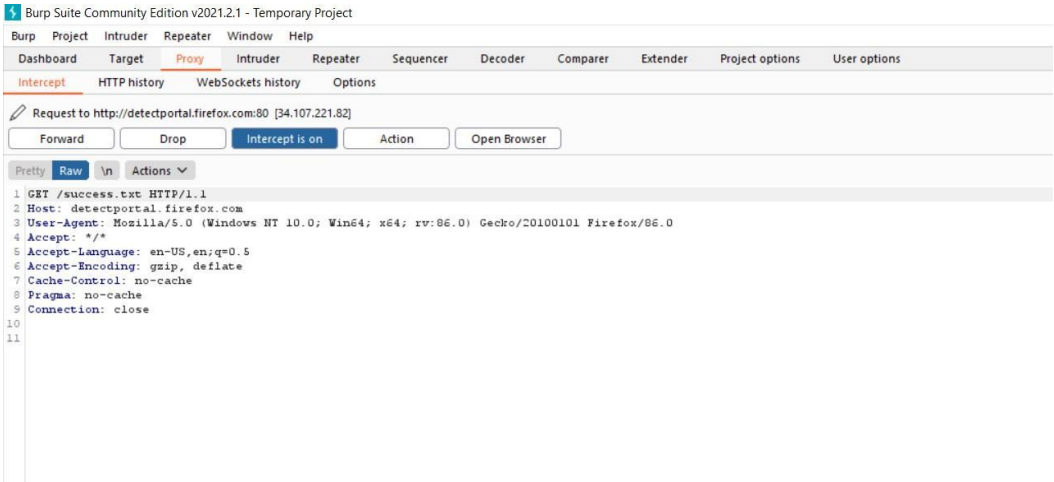


5. Select manual proxy configuration

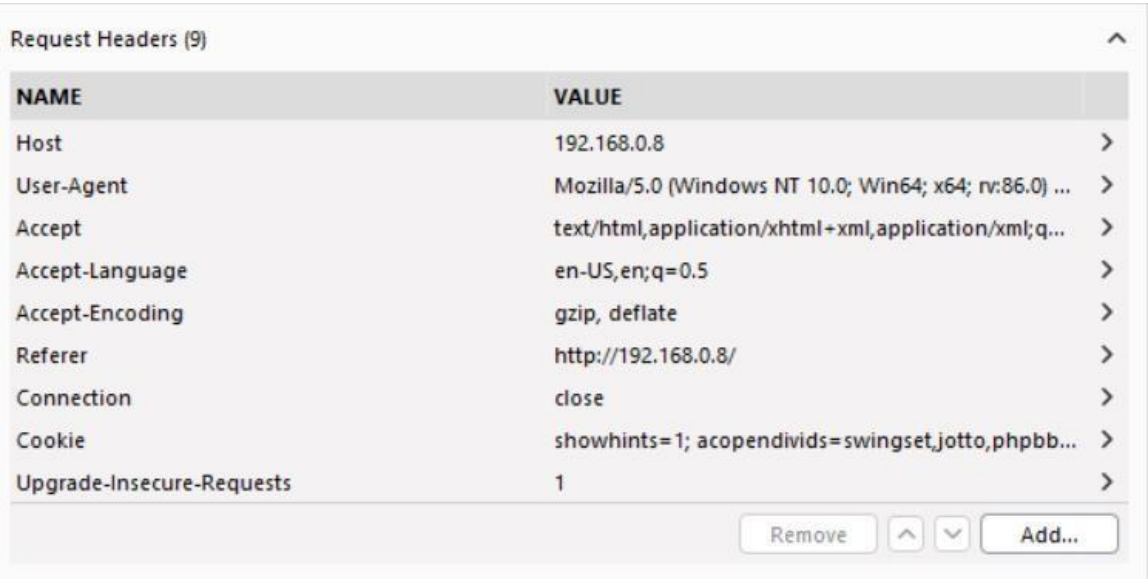


6. Click on Owasp mutillidae – II

7. The following data is shown

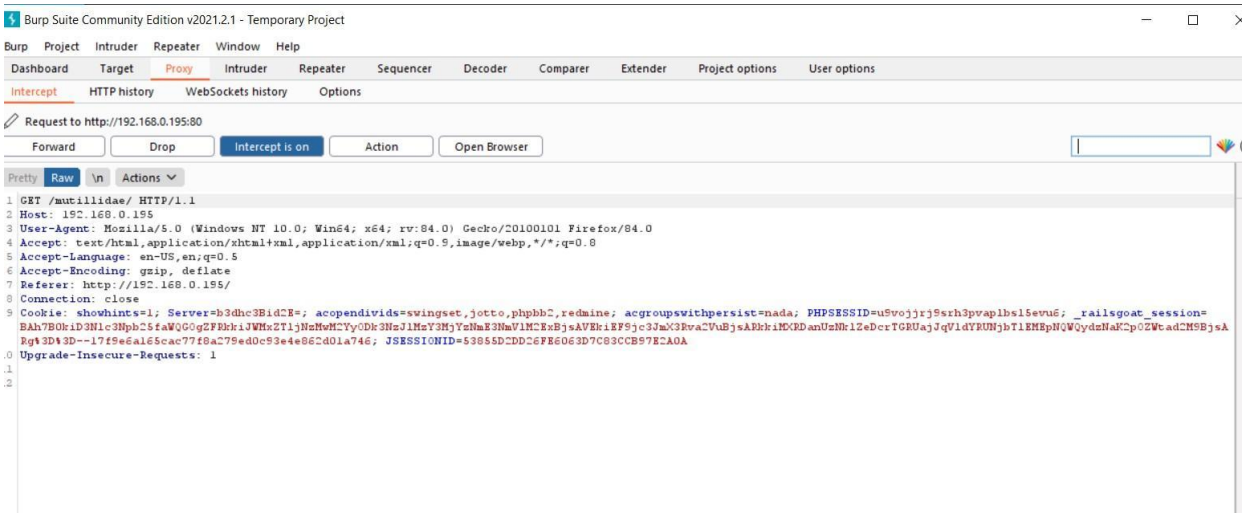


8. The header format is as:



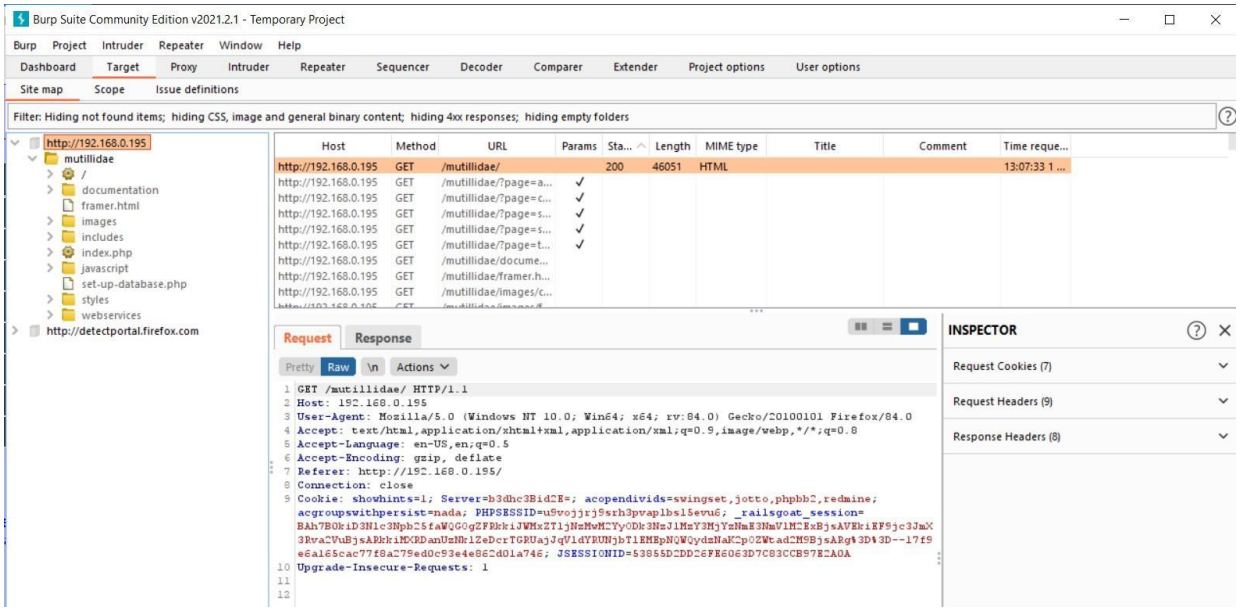
2. SiteMap

Click on owasp mutillidae II

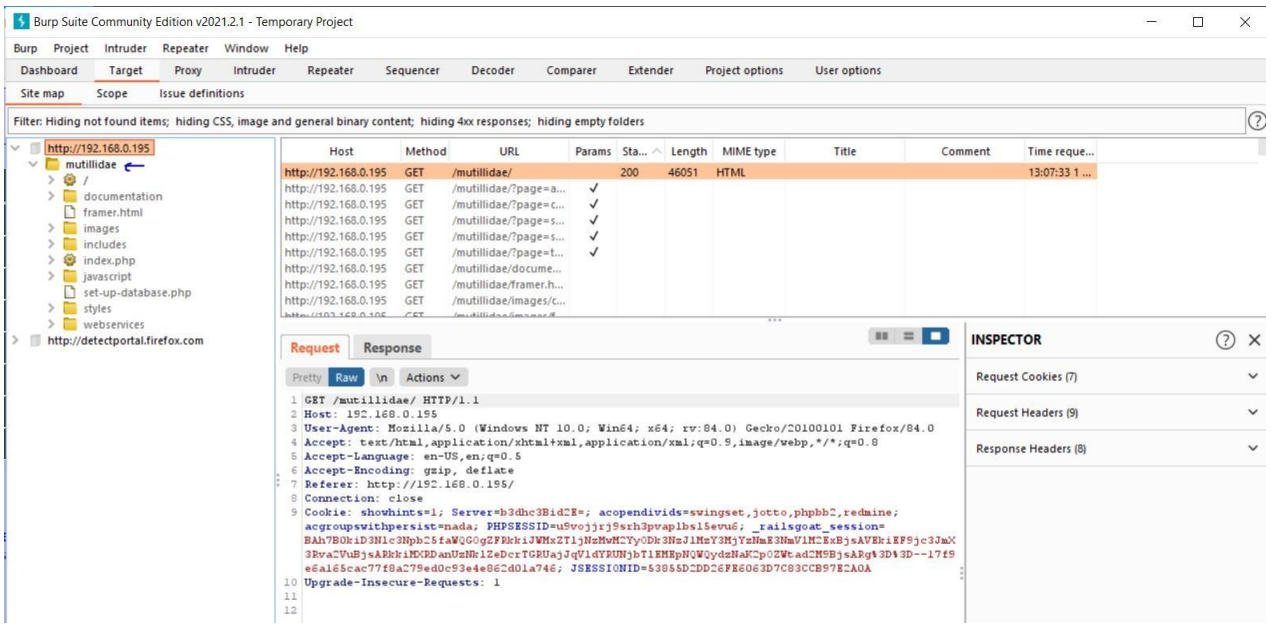


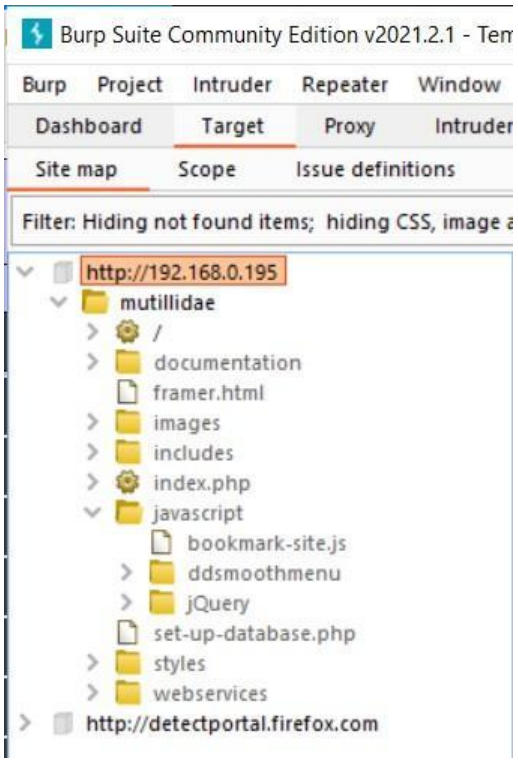
Steps:

1. Then click on forward. Target tab starts blinking.

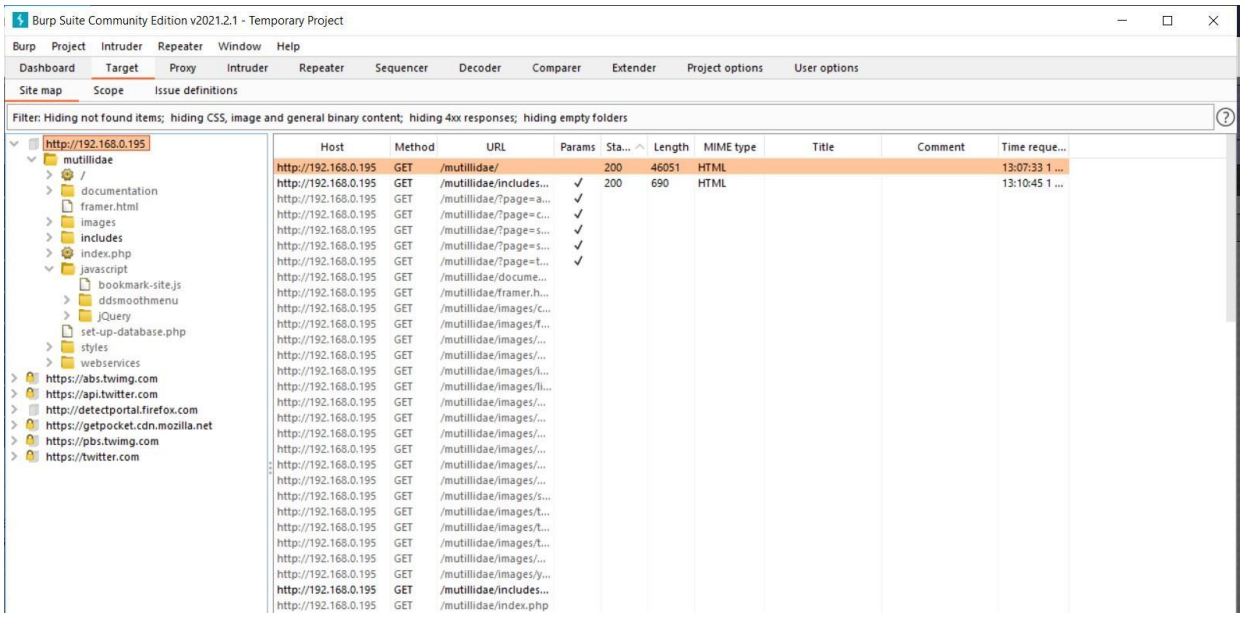


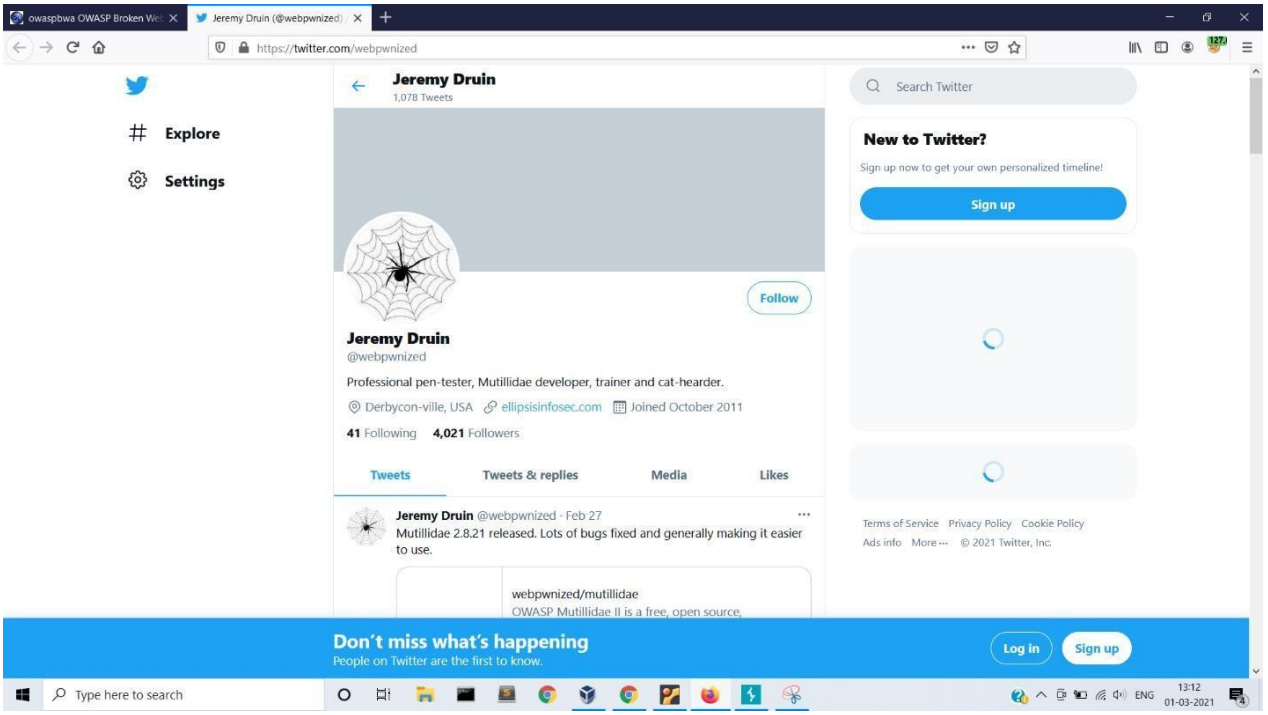
2. Sitemap is created of the host





3. Whenever we open a url, Burpsuite stores that URL in the sitemap. Now sitemap of mutillidae is created.
   Burpsuite spider crawls the entire website and store all URLs in that particular Sitemap.





Sitemap of Owasp Bricks

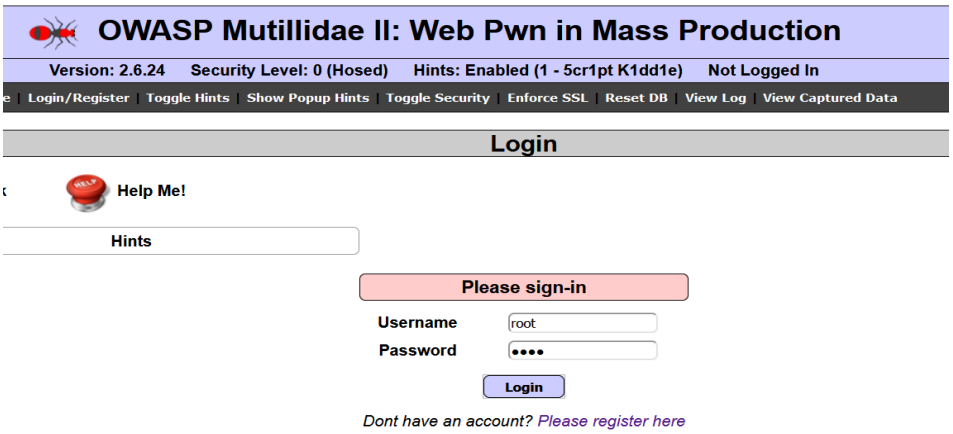
3. Intruder

Used to crack passwords and automate request tampering

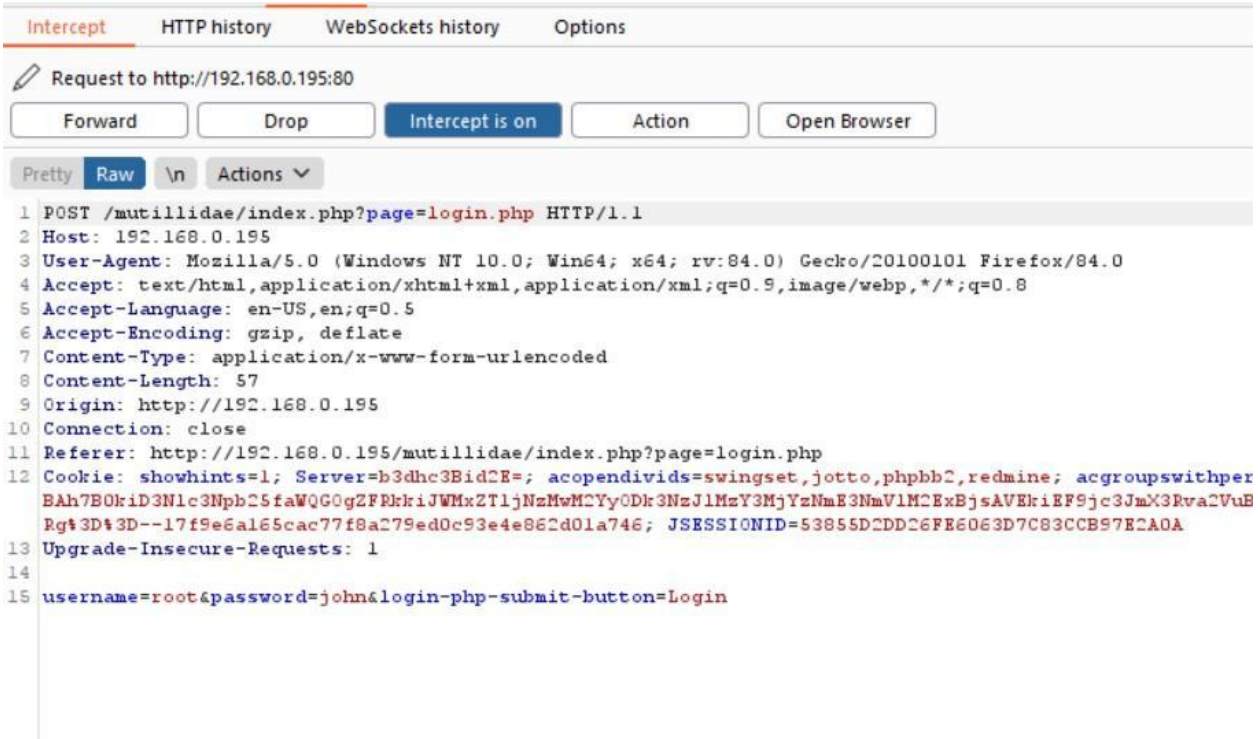
Open owasp mutillidae

Choose a suitable broken web app to launch attack. We select authentication bypass option.

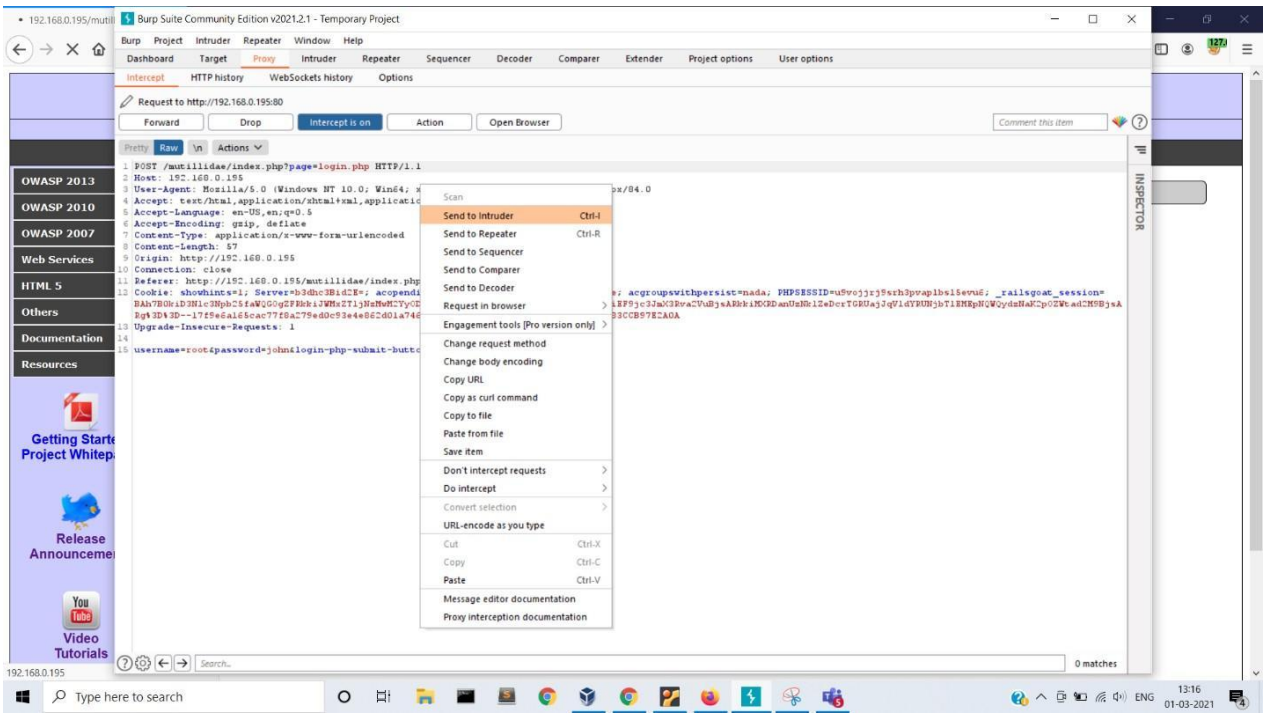
Enter random credentials for login



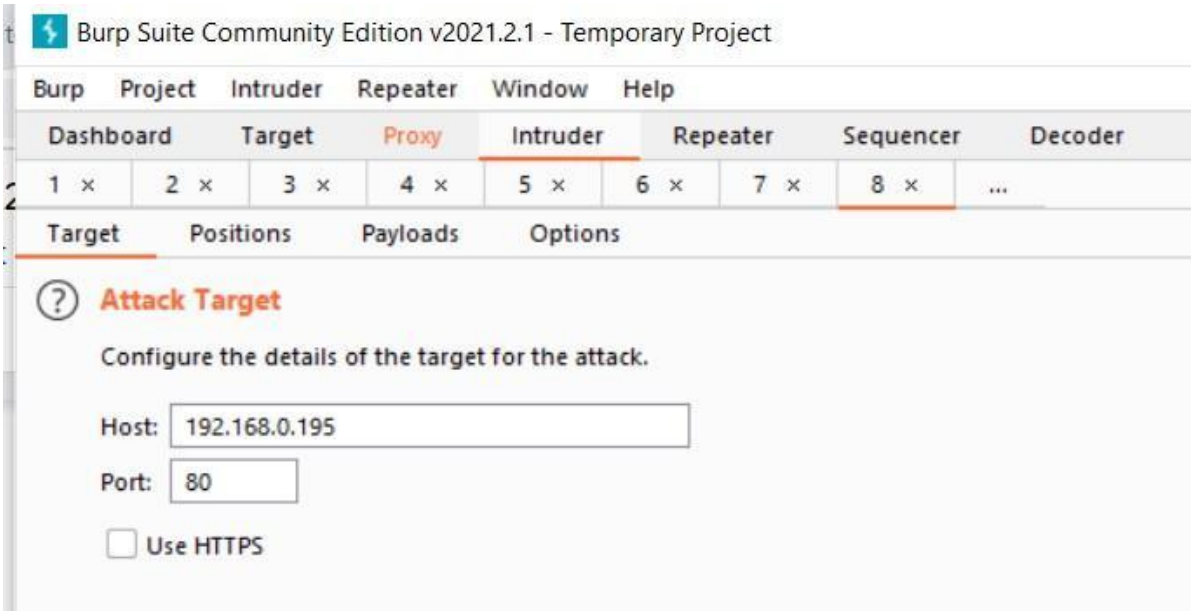
Check the request on burpsuite:



Right click and select send to intruder:



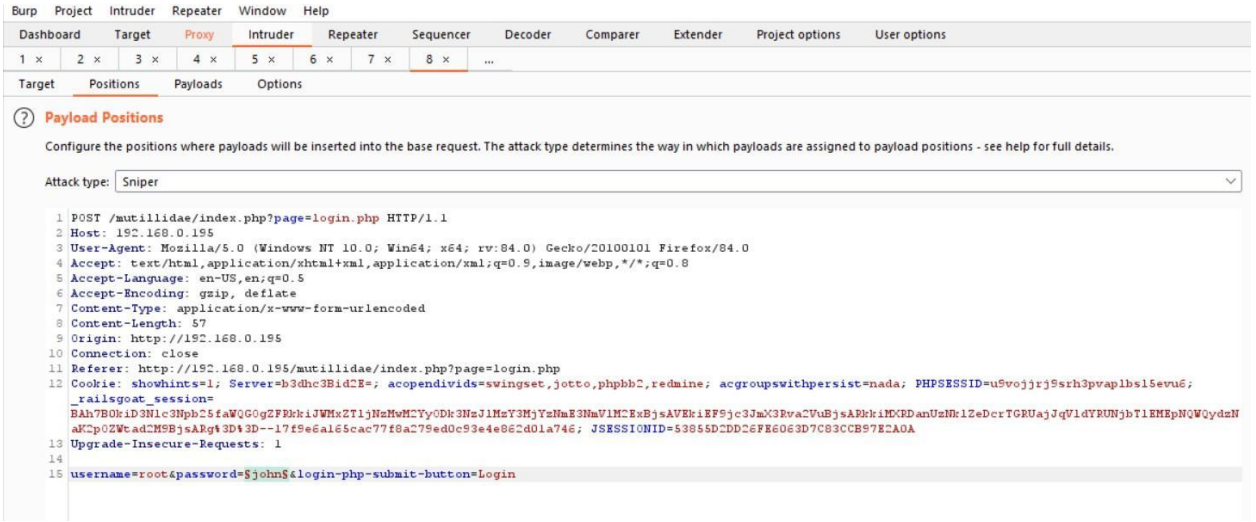
Now open the intruder tab:

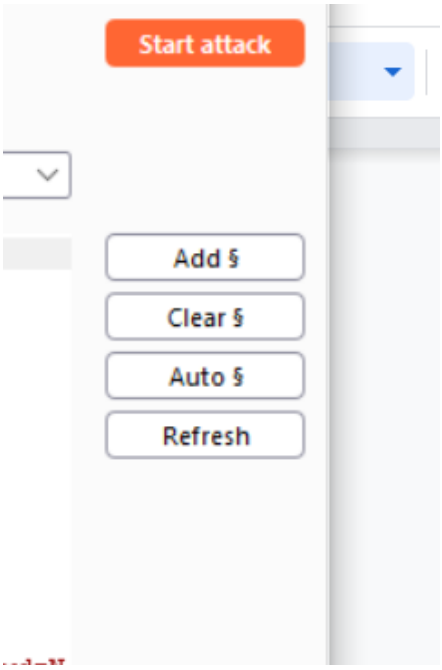


Click positions tab to check the variable params

Clear all

Then add one param that you want to vary. In this case password:

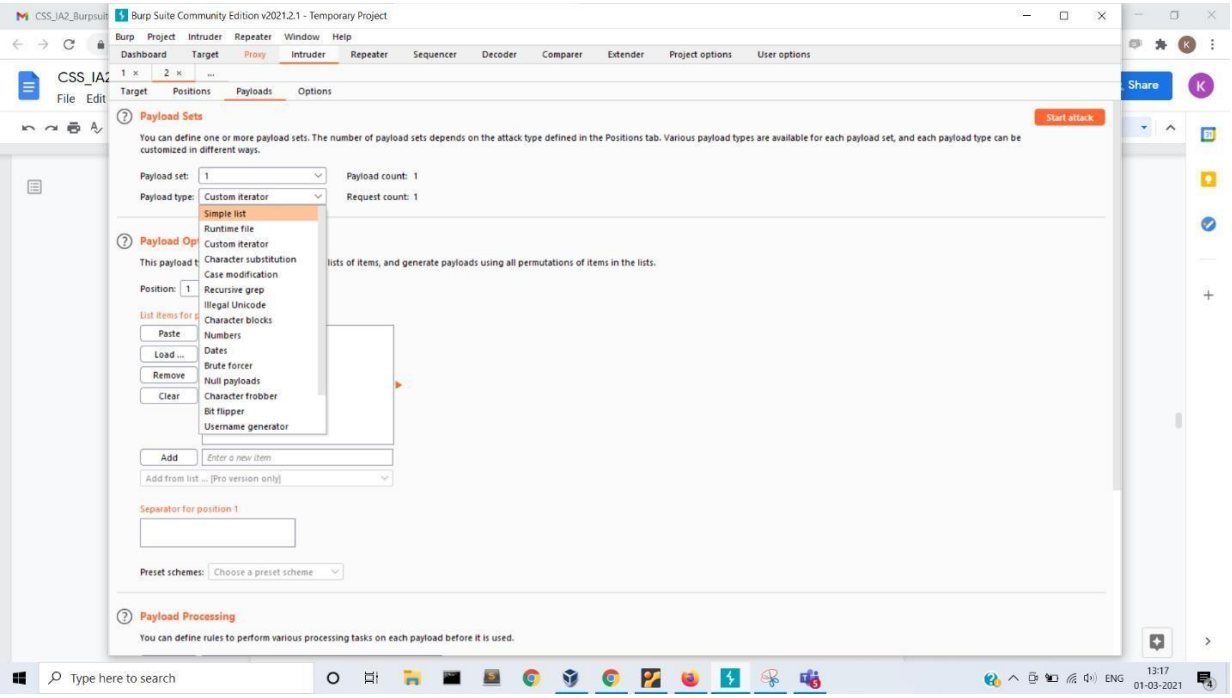




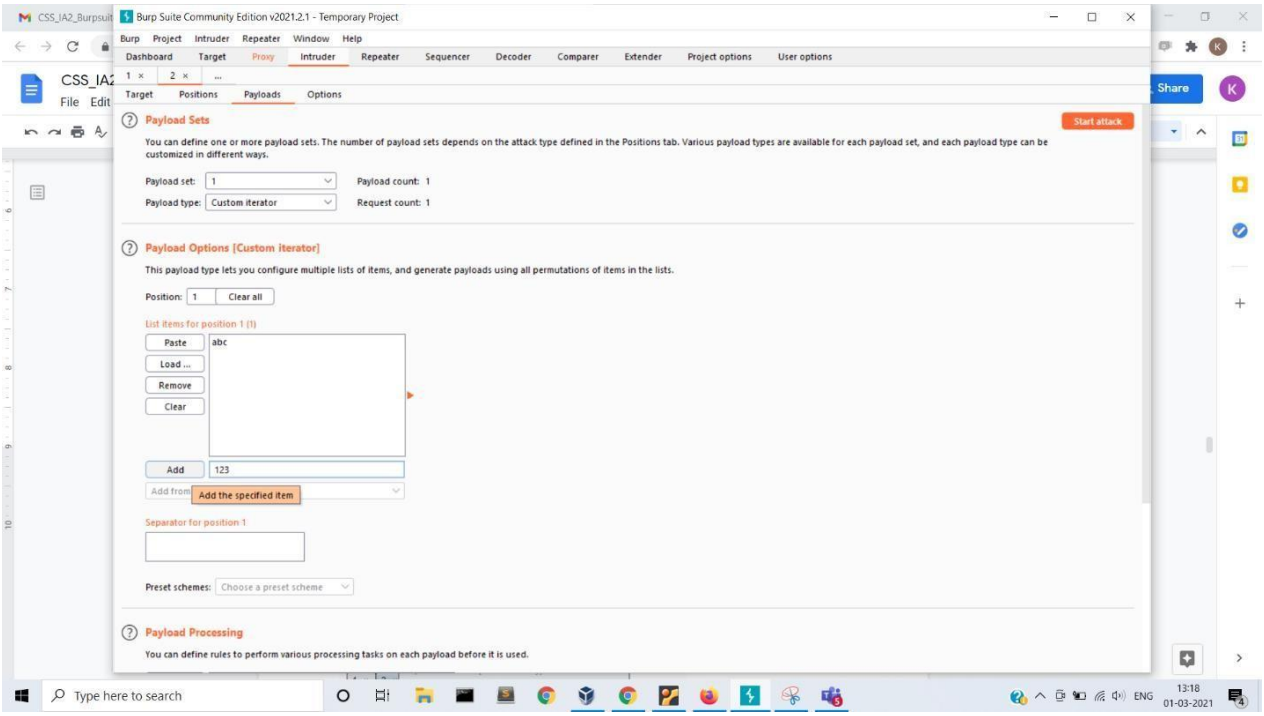
Select attack type as Sniper:

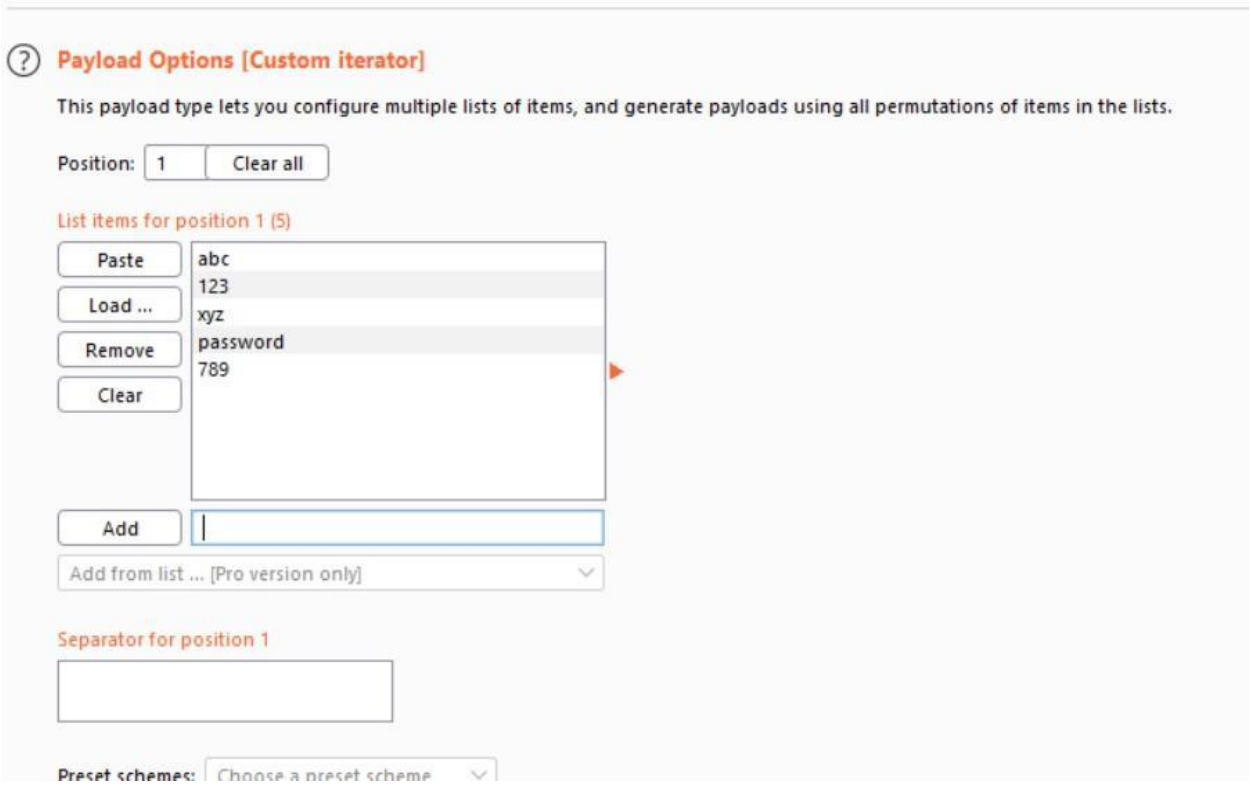
Click on payload tab:

Select payload type as simple list

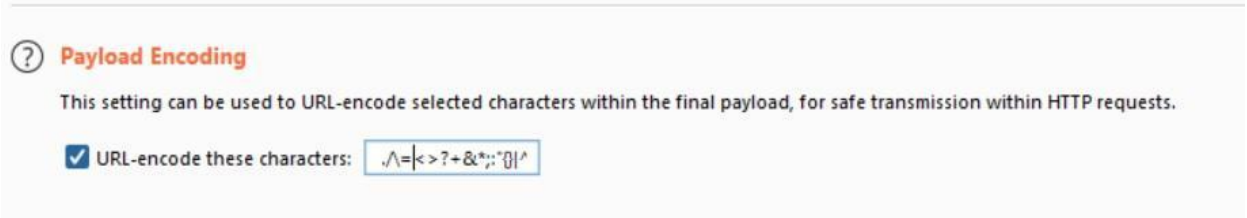


Enter a list of words:

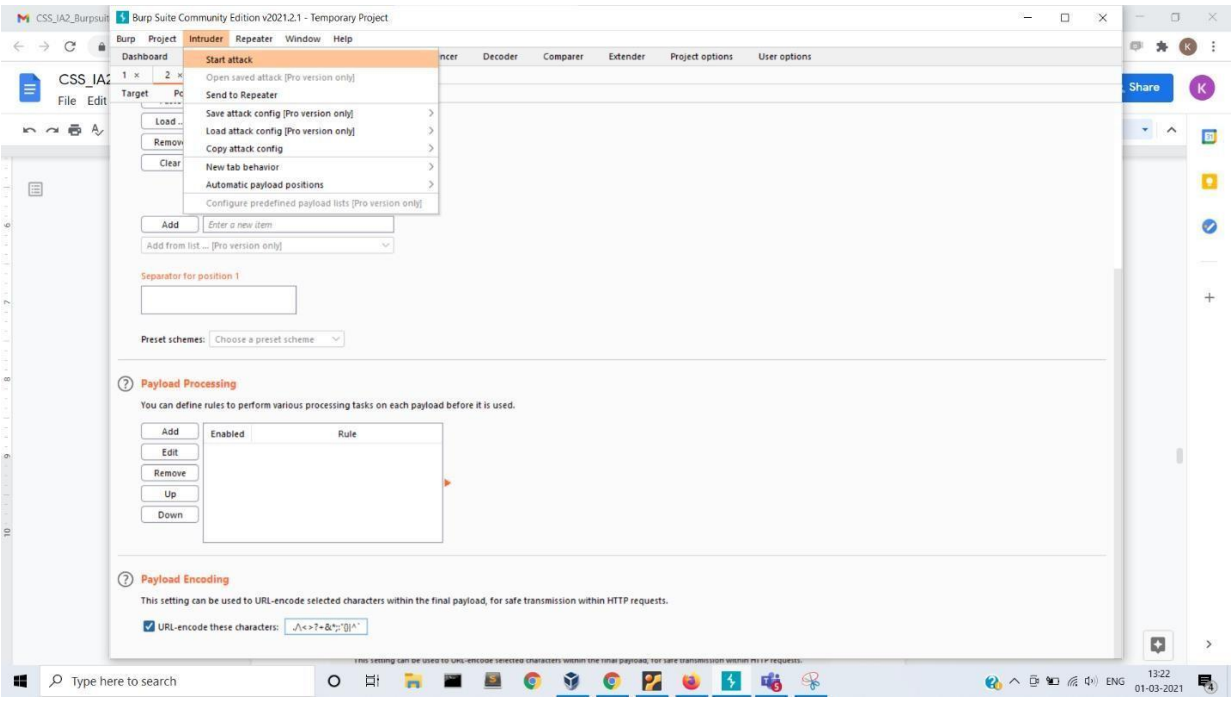




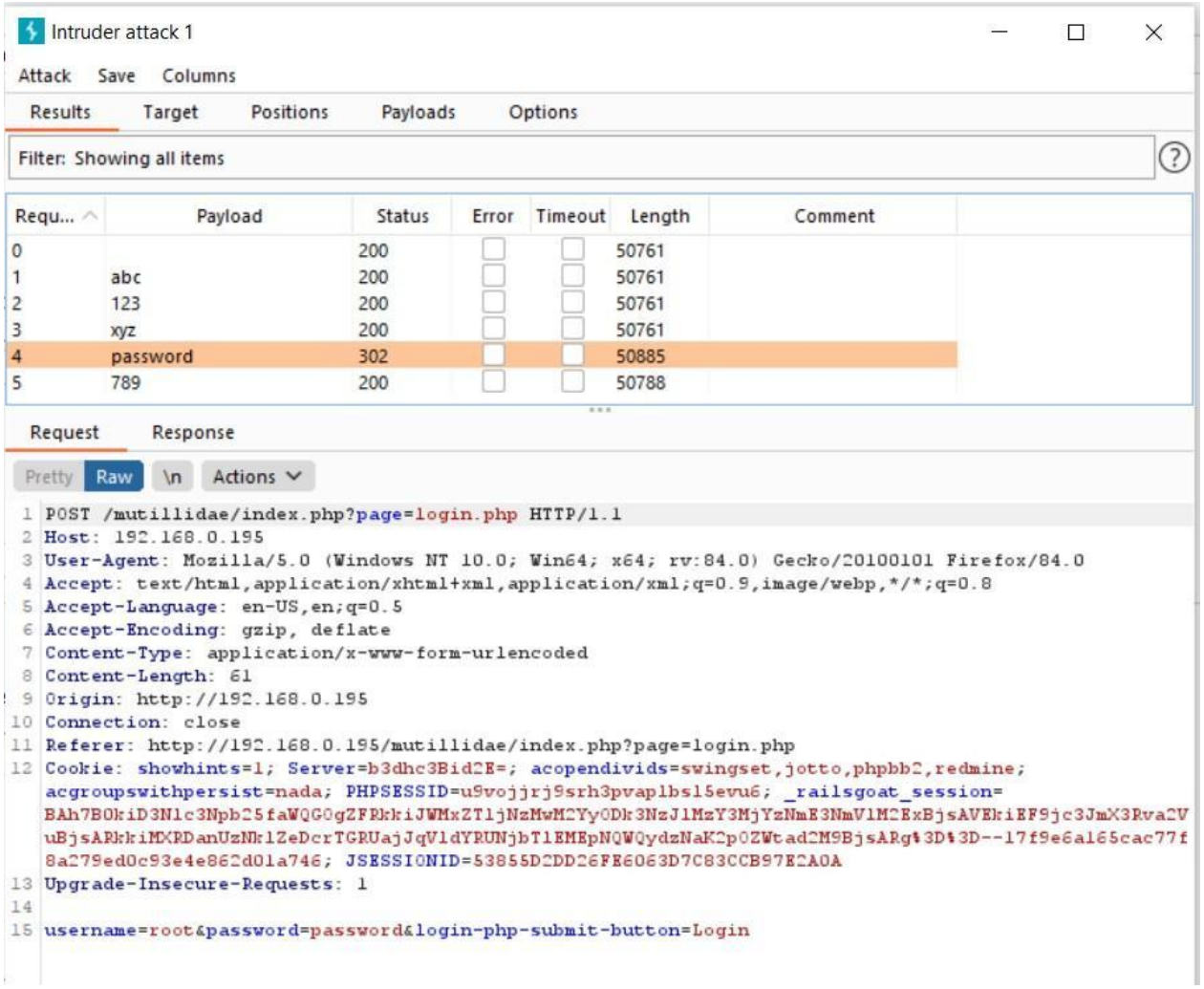
Remove the equal to sign from payload encoding:



Start the attack



Inspect the requests that are sent:



Status for password is 302

Now check response and render it

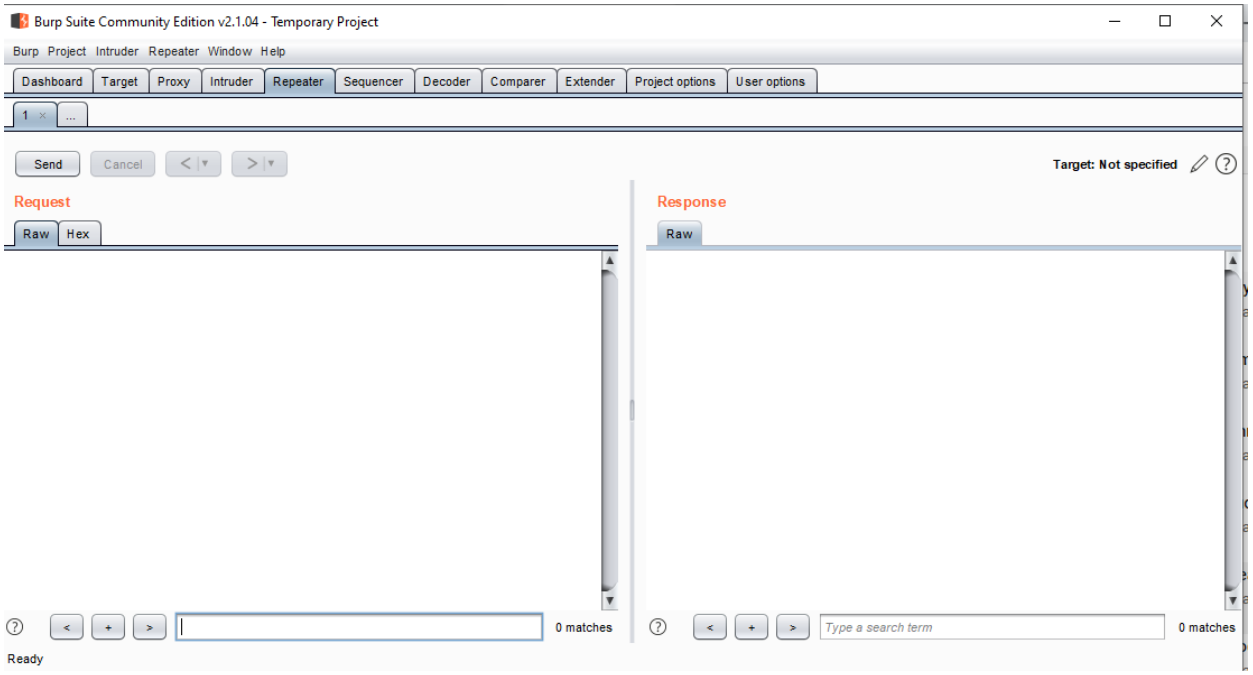
Password was the correct password and you are now logged in

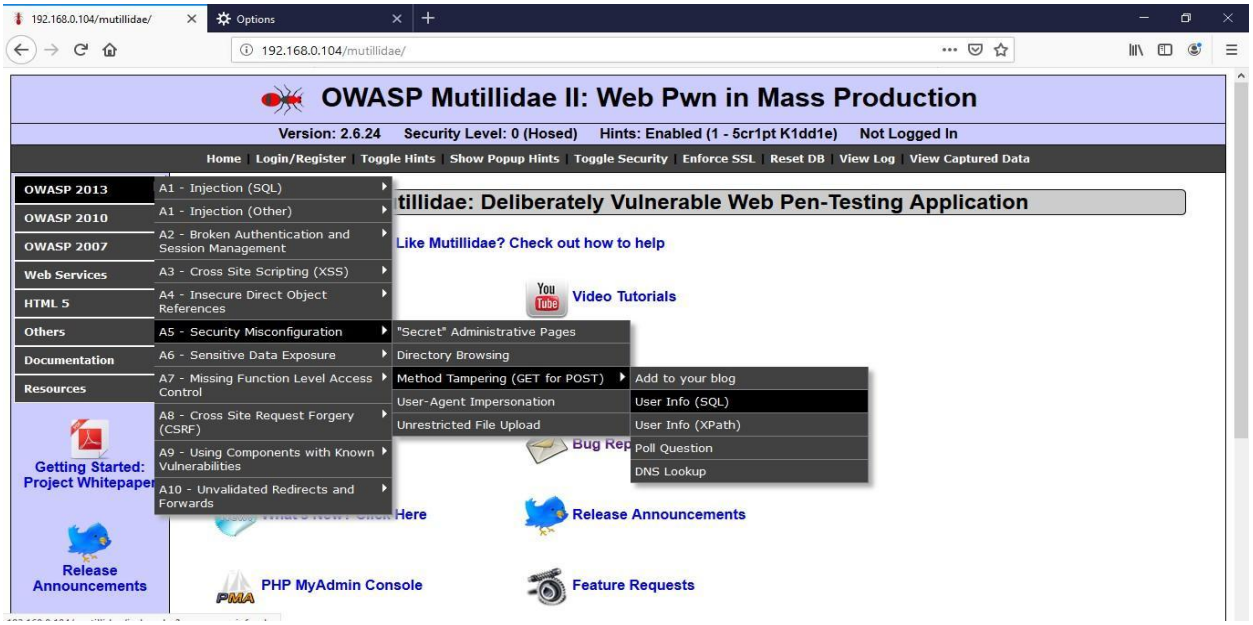
4. Repeater

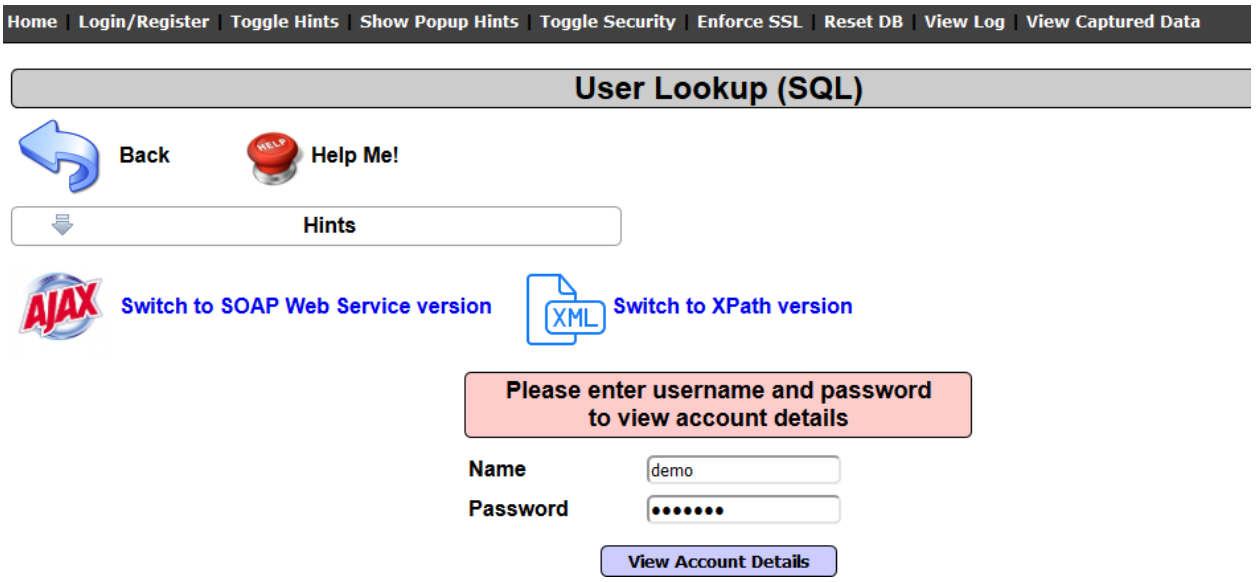
Used to send multiple Http requests.

Server response can be monitored

Initial view:




192.168.0.104/mutillidae/
Options
192.168.0.104/mutillidae/
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Cross Site Scripting (XSS)
A4 - Insecure Direct Object References
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Function Level Access Control
A8 - Cross Site Request Forgery (CSRF)
A9 - Using Components with Known Vulnerabilities
A10 - Unvalidated Redirects and Forwards
"Secret" Administrative Pages
Directory Browsing
Method Tampering (GET for POST)
User-Agent Impersonation
Unrestricted File Upload
Add to your blog
User Info (SQL)
User Info (XPath)
Poll Question
DNS Lookup
tillidae: Deliberately Vulnerable Web Pen-Testing Application
Like Mutillidae? Check out how to help
Video Tutorials
Getting Started: Project Whitepaper
Release Announcements
Release Announcements
PHP MyAdmin Console
Feature Requests


Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
User Lookup (SQL)
Back
Help Me!
Hints
Switch to SOAP Web Service version
Switch to XPath version
Please enter username and password to view account details
Name
demo
Password
View Account Details

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

Intercept | HTTP history | WebSockets history | Options

Request to http://192.168.0.104:80

Forward | Drop | Intercept is on | Action

Raw | Params | Headers | Hex

GET request to /mutillidae/index.php

Type	Name	Value
URL	page	user-info.php
URL	username	demo
URL	password	demo123
URL	user-info-php-submit-button	View Account Details
Cookie	showhints	1
Cookie	acopendivids	swingset,jotto,phpbb2,redmine
Cookie	acgroupswithpersist	nada
Cookie	PHPSESSID	h146hb6gmjg35n5e1km6mk1ks2

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

Intercept | HTTP history | WebSockets history | Options

Request to http://192.168.0.104:80

Forward | Drop | Intercept is on | Action | Comment this item

Raw | Params | Headers | Hex

```
GET /mutillidae/index.php?page=user-info.php&username=demo&password=demo123&user-info-php-submit-button=View+Account+Details HTTP/1.1
Host: 192.168.0.104
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
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
Referer: http://192.168.0.104/mutillidae/index.php?page=user-info.php
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroup
Upgrade-Insecure-Requests: 1
```

g35n5e1km6mk1ks2

- Scan [Pro version only]
- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser ▶
- Engagement tools [Pro version only] ▶
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests ▶
- Do intercept ▶

< + > Type a search term 0 mat

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

1 × ...

Send | Cancel | < | >

Request

Raw | Params | Headers | Hex

```
GET
/mutillidae/index.php?page=user-info.php&username=demo&password=demo123&u
ser-info-php-submit-button=View+Account+Details HTTP/1.1
Host: 192.168.0.104
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0)
Gecko/20100101 Firefox/69.0
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
Referer: http://192.168.0.104/mutillidae/index.php?page=user-info.php
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada; PHPSESSID=h146hb6gmjg3Sn5elkm6mklks2
Upgrade-Insecure-Requests: 1
```

Response

Raw

On clicking send, we get the response

Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

Target: http://192.168.0.104

```
nfo.php&username=demo&password=demo123&u
ccount+Details HTTP/1.1

NT 10.0; Win64; x64; rv:69.0)

ml+xml,application/xml;q=0.9,*/*;q=0.8


illidae/index.php?page=user-info.php
=swingset,jotto,phpbb2,redmine;
ID=h146hb6gmjg3Sn5elkm6mklks2
```

term 0 matches

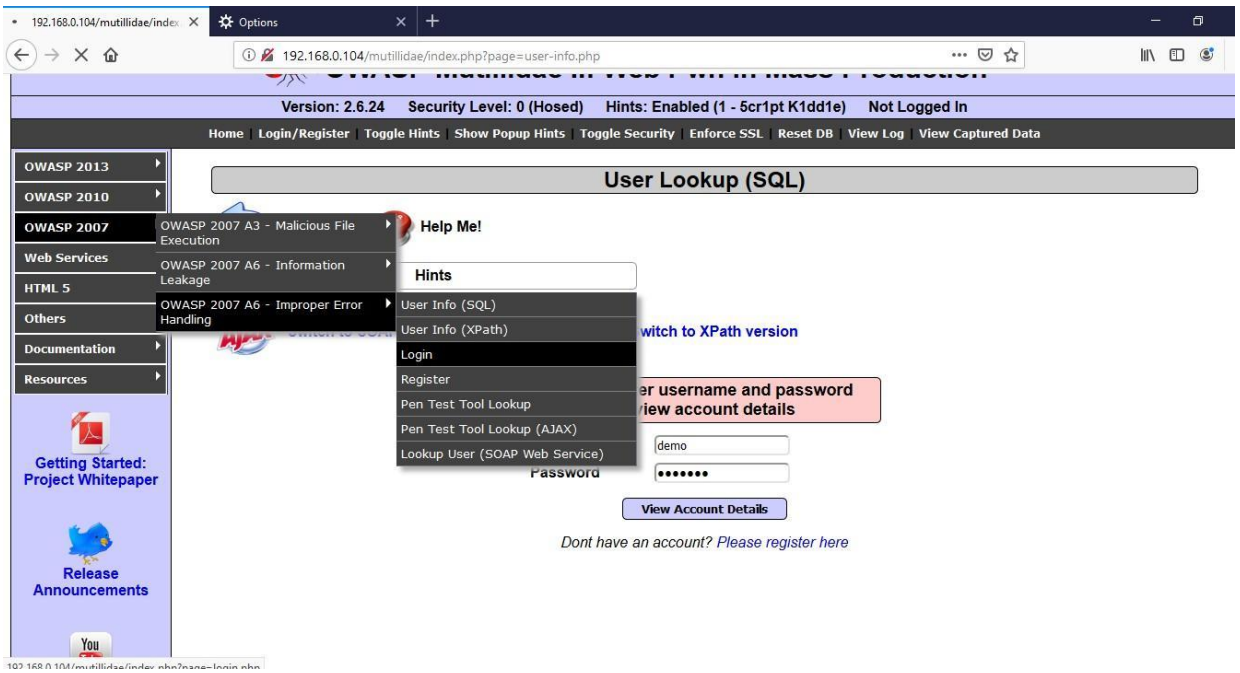
Response

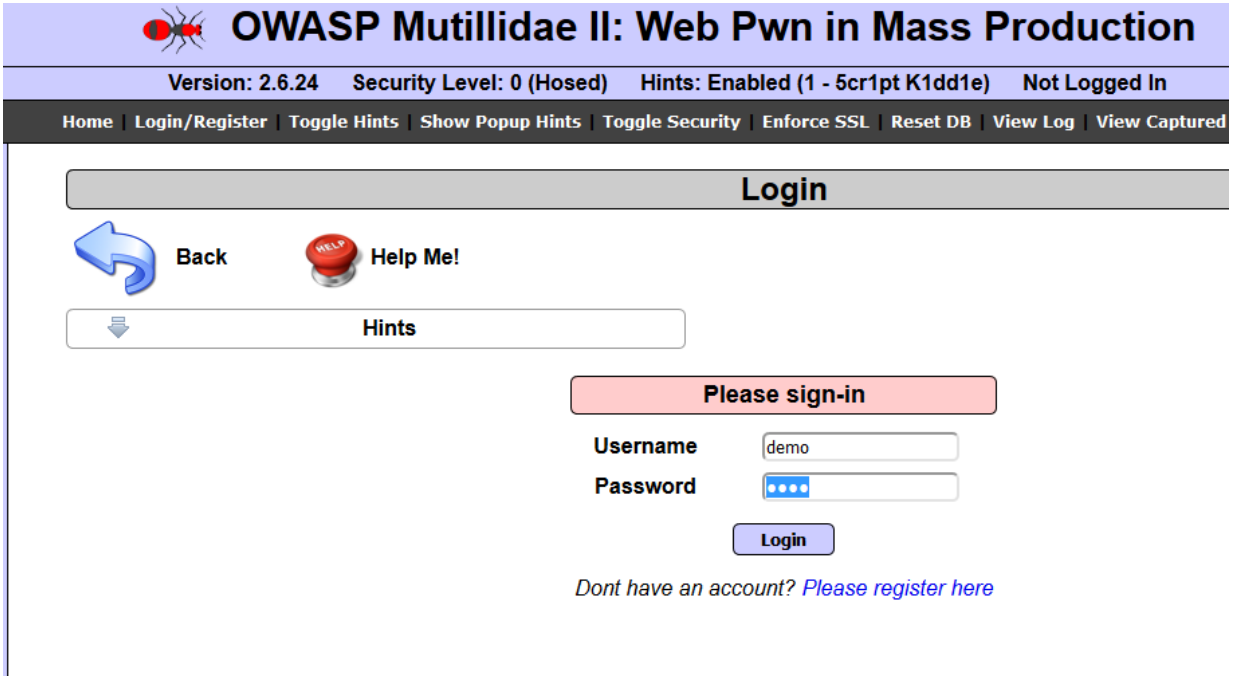
Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Date: Fri, 04 Oct 2019 10:57:48 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with
Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14
OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Logged-In-User:
Vary: Accept-Encoding
Content-Length: 48890
Connection: close
Content-Type: text/html


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
<html>
<head>
        <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon"
/>
```

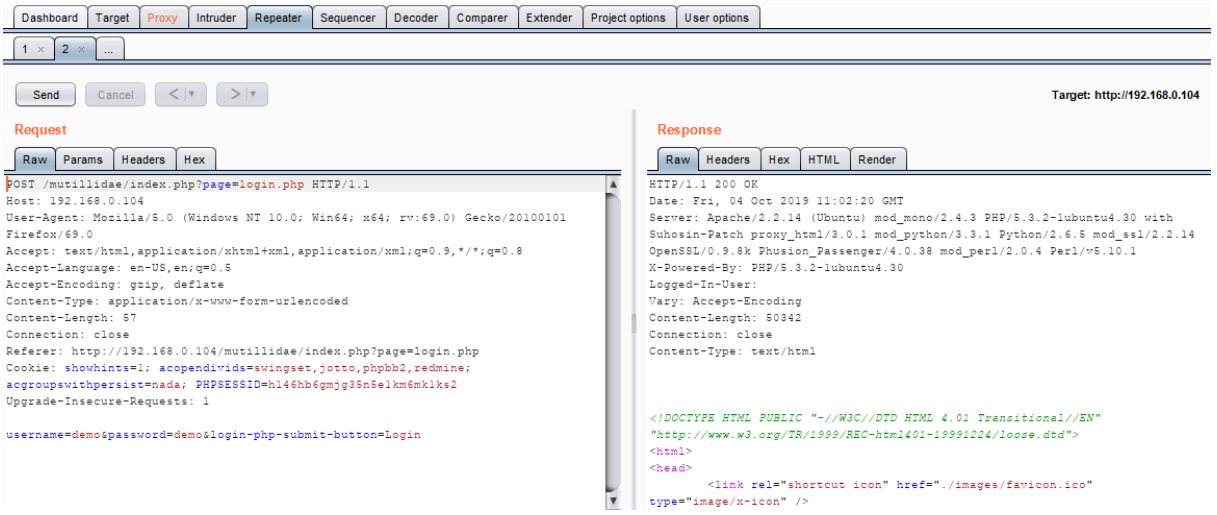
< + > Type a search term 0 matches

Improper error handling – login

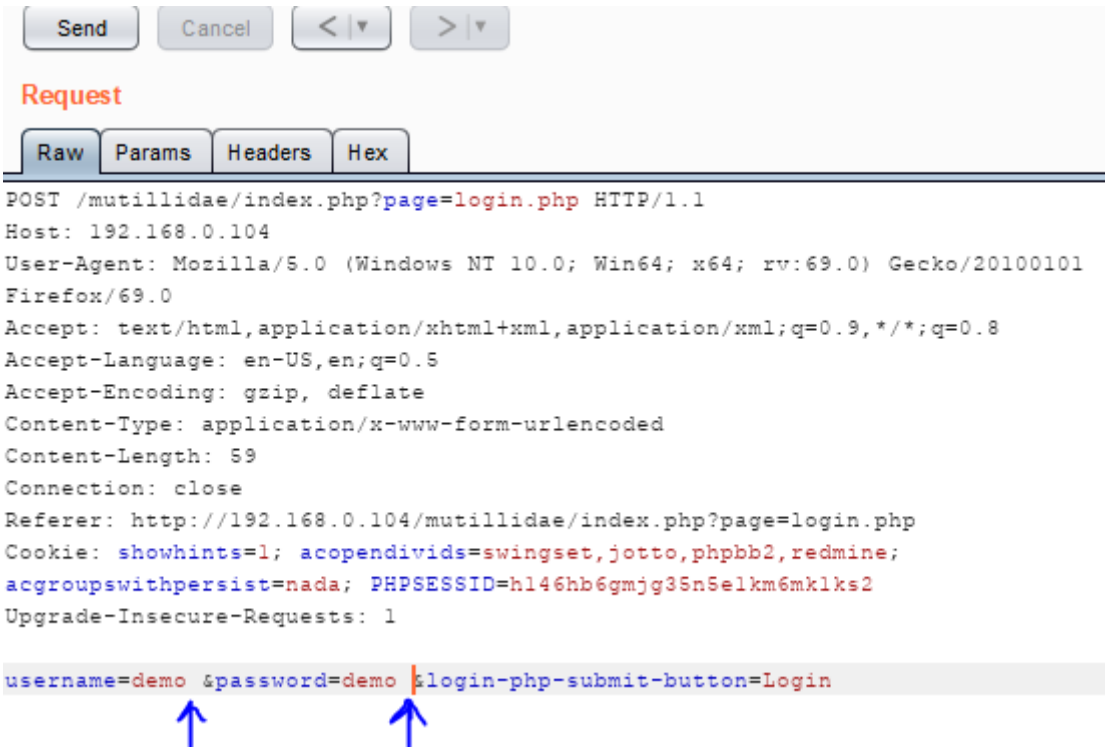




Again send to repeater and click send



On performing SQL injection, error is shown in response window



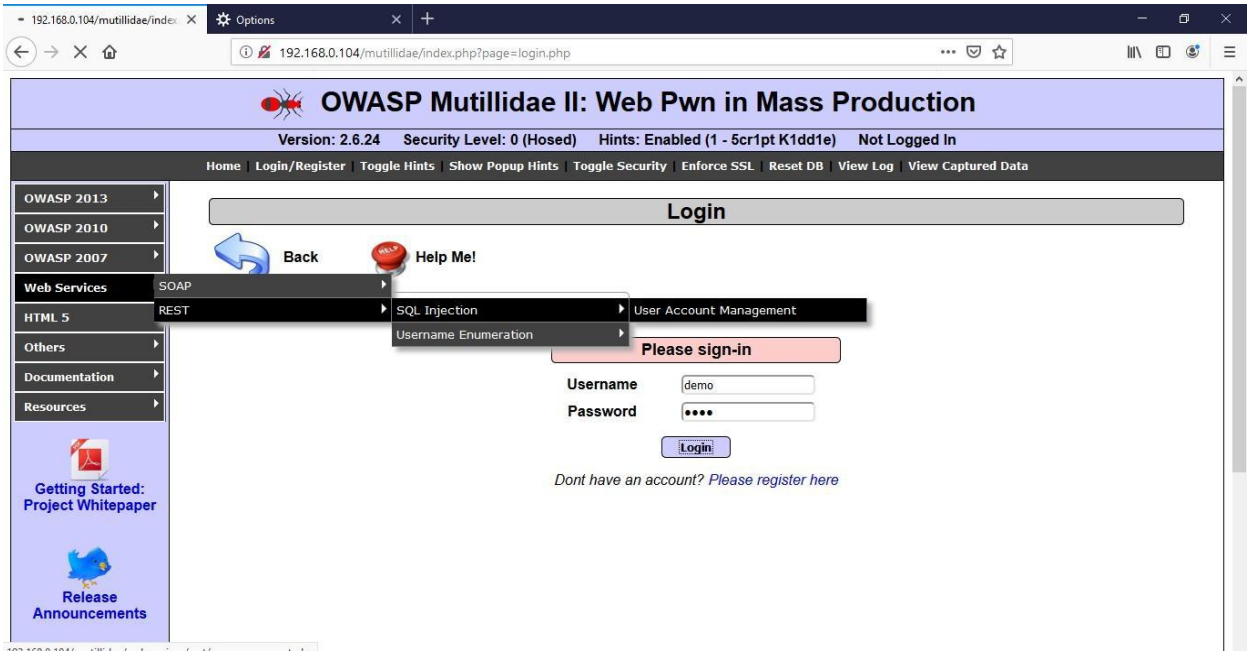
Space was added in the request (SQL injection)

Response

Raw | Headers | Hex | HTML | Render

```
<ul>
<li>
<a
href="https://www.owasp.org/index.php/Top_10_2013-A1-Injection"
target="_blank">A1 - Injection (SQL)</a>
<ul>
<li>
<a href="">SQLi -
Extract Data</a>
<ul>
<li><a
href="index.php?page=user-info.php">User Info (SQL)</a></li>
</ul>
</li>
<li>
<a href="">SQLi -
Bypass Authentication</a>
<ul>
<li><a
```

Lastly REST:



192.168.0.104/mutillidae/webs... | Options

192.168.0.104/mutillidae/webservices/rest/ws-user-account.php

Back to Home Page

Help: This service exposes GET, POST, PUT, DELETE methods. This service is vulnerable to SQL injection in security level 0.

DEFAULT GET: (without any parameters) will display this help plus a list of accounts in the system.

Optional params: None.

GET: Either displays usernames of all accounts or the username and signature of one account.

Optional params: username AS URL parameter. If username is "*" then all accounts are returned.

Example(s):

Get a particular user: /mutillidae/webservices/rest/ws-user-account.php?username=adrian
Get all users: /mutillidae/webservices/rest/ws-user-account.php?username=*

Example Exploit(s):

SQL injection: /mutillidae/webservices/rest/ws-user-account.php?username=jeremy'+union+select+concat('The+password+for+',username,'+is+',+password),mysignature+from+accounts+--+

POST: Creates new account.

Required params: username, password AS POST parameter.
Optional params: signature AS POST parameter.

PUT: Creates or updates account.

Required params: username, password AS POST parameter.
Optional params: signature AS POST parameter.

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

1 × | 2 × | 3 × | ...

Send | Cancel | < | >

Target: http://192.168.0.104

Request

Raw | Params | Headers | Hex

```
GET /mutillidae/webservices/rest/ws-user-account.php?username=* HTTP/1.1
Host: 192.168.0.104
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101
Firefox/69.0
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
Referer: http://192.168.0.104/mutillidae/webservices/rest/ws-user-account.php
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada; PHPSESSID=h146hb6gmjg36n5e1km6mk1ks2
Upgrade-Insecure-Requests: 1
```

Response

Raw | Headers | Hex | Render

```
HTTP/1.1 200 OK
Date: Fri, 04 Oct 2019 11:08:06 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 523
Connection: close
Content-Type: text/html

Result: {Accounts:
{[{"username":"admin"},{"username":"adrian"},{"username":"john"},{"username":"jeremy"},{"username":"br
yce"},{"username":"samurai"},{"username":"jim"},{"username":"bobby"},{"username":"simba"},{"username"
:"dreveil"},{"username":"scotty"},{"username":"cal"},{"username":"john"},{"username":"kevin"},{"usern
ame":"dave"},{"username":"patches"},{"username":"rocky"},{"username":"tim"},{"username":"ABaker"},{"u
sername":"PPan"},{"username":"CHook"},{"username":"james"},{"username":"user"},{"username":"ed"}]}}
```

Changing username=* in the request window to username=admin. The response is

Response

Raw | Headers | Hex | Render

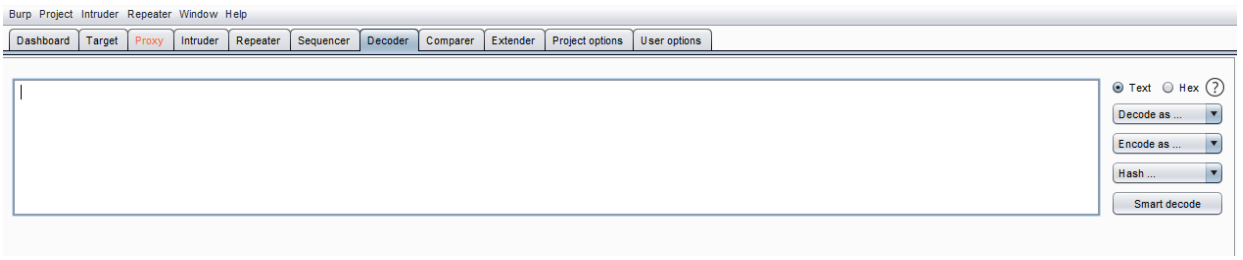
```
HTTP/1.1 200 OK
Date: Fri, 04 Oct 2019 11:12:12 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-lubuntu4.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 70
Connection: close
Content-Type: text/html

Result: {Accounts: {[{"username":"admin","mysignature":"g0t r00t?"}]}}
```

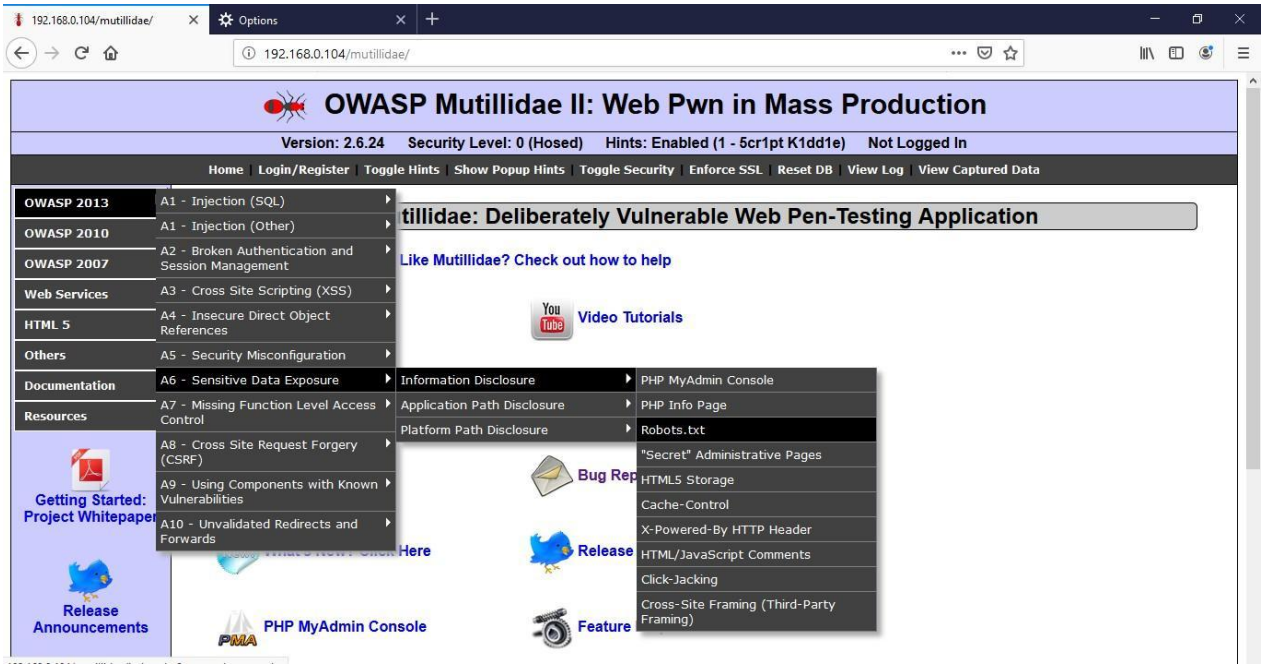
So using repeater tab we can send multiple requests by means of changing parameters also.

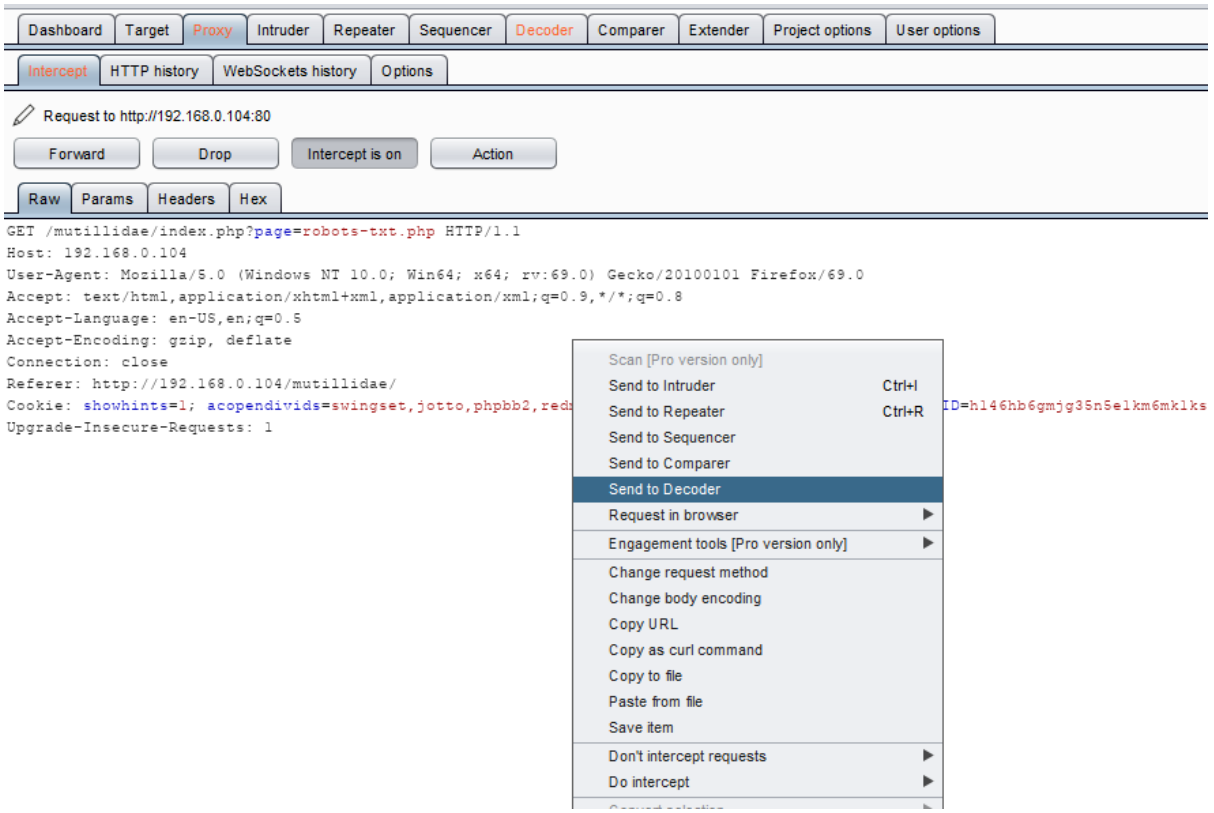
5. Decoder

One of the best feature of Burpsuite
Helps us convert, encode, decodes strings into -
Hex
URL
base64
Binary
MD5
Hash
SHA 256 Hash

The decoder tab is as:




192.168.0.104/mutillidae/
Options
192.168.0.104/mutillidae/
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Cross Site Scripting (XSS)
A4 - Insecure Direct Object References
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Function Level Access Control
A8 - Cross Site Request Forgery (CSRF)
A9 - Using Components with Known Vulnerabilities
A10 - Unvalidated Redirects and Forwards
Information Disclosure
Application Path Disclosure
Platform Path Disclosure
PHP MyAdmin Console
PHP Info Page
Robots.txt
"Secret" Administrative Pages
HTML5 Storage
Cache-Control
X-Powered-By HTTP Header
HTML/JavaScript Comments
Click-Jacking
Cross-Site Framing (Third-Party Framing)
tillidae: Deliberately Vulnerable Web Pen-Testing Application
Like Mutillidae? Check out how to help
Video Tutorials
Getting Started: Project Whitepaper
Release Announcements
PHP MyAdmin Console
Release
Feature


Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Intercept
HTTP history
WebSockets history
Options
Request to http://192.168.0.104:80
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
GET /mutillidae/index.php?page=robots-txt.php HTTP/1.1
Host: 192.168.0.104
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
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
Referer: http://192.168.0.104/mutillidae/
Upgrade-Insecure-Requests: 1
Scan [Pro version only]
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

```
GET /mutillidae/index.php?page=robots-txt.php HTTP/1.1
Host: 192.168.0.104
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
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
Referer: http://192.168.0.104/mutillidae/
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada;
```

Text Hex

Decode as ...

Encode as ...

Hash ...

Smart decode

Encoding PHPSESSID into Base64

Dashboard | Target | Proxy | Intruder | Repeater

Sequencer | Decoder | Comparer | Extender | Project options | User options

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101
Firefox/69.0
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
Referer: http://192.168.0.104/mutillidae/
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada; PHPSESSID=h146hb6gmjg35n5e1km6mk1ks2
```

Text Hex

Decode as ...

Encode as ...

Hash ...

Smart decode

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101
Firefox/69.0
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
Referer: http://192.168.0.104/mutillidae/
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada; PHPSESSID=aDE0NmhiNmdtamczNW41ZTFrbTZtazFrczIN
```

Text Hex

Decode as ...

Encode as ...

Hash ...

Smart decode

Decoding it back

Dashboard | Target | Proxy | Intruder | Repeater
Sequencer | Decoder | Comparer | Extender | Project options | User options

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101
Firefox/69.0
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
Referer: http://192.168.0.104/mutillidae/
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada; PHPSESSID=h146hb6gmjg35n5e1km6mk1ks2
```

Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

```
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
Referer: http://192.168.0.104/mutillidae/
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada; PHPSESSID=aDE0NmhiNmdtamczNW41ZTFrbTZtazFrczIN
Upgrade-Insecure-Requests: 1
```

Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

```
Firefox/69.0
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
Referer: http://192.168.0.104/mutillidae/
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada; PHPSESSID=h146hb6gmjg35n5e1km6mk1ks2
Upgrade-Insecure-Requests: 1
```

Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

Encoding close to ASCII hex

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.0.104/mutillidae/
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada; PHPSESSID=h146hb6gmjg35n5e1km6mk1ks2
Upgrade-Insecure-Requests: 1
```

Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

```
Firefox/69.0
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: 636c6f73650d
Referer: http://192.168.0.104/mutillidae/
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada; PHPSESSID=h146hb6gmjg35n5e1km6mk1ks2
```

Text Hex
Decode as ...
Encode as ...
Hash ...

SHA-256 hash of HELLO