
Exploration of Penetration testing tool – *Burp Suite*

SHAILI SHAH (16010120114, B3)

KEYUR SHAH (16010120123, B3)

SARAUNSH JADHAV (16010120126, B3)

SAHIL SAYANI (16010120135,B3)

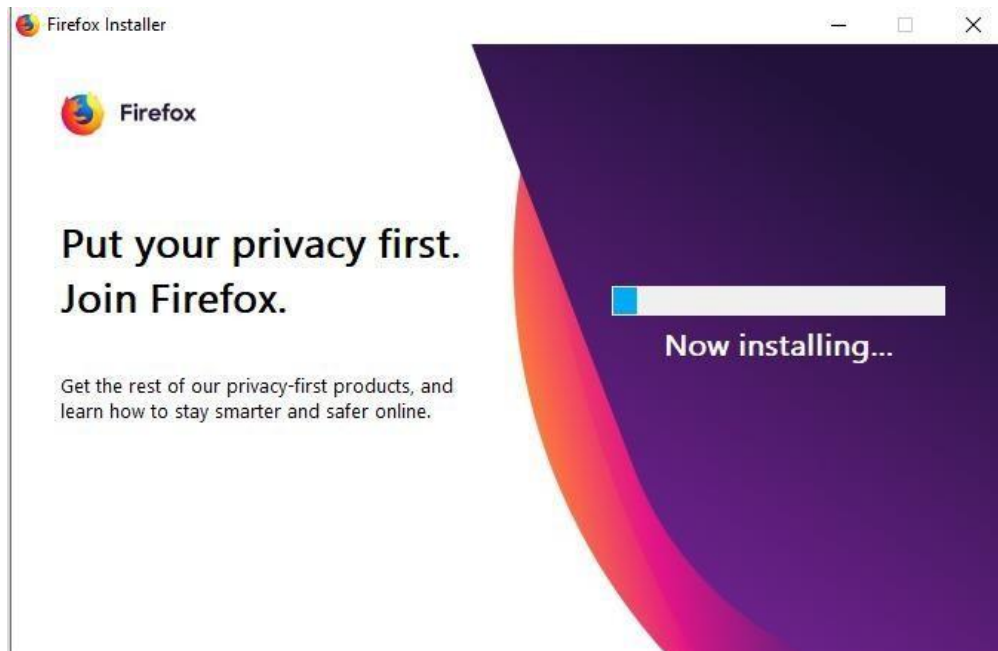
1. Introduction

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

Apps HP The HackerRank Int... YouTube (4) WhatsApp Google Drive Somaiya Vidyavihar...

SOURCEFORGE Open Source Software Business Software Services Resources

NORDVPN Access anything online without restrictions **GET VPN NOW** **Best VP**

Home / Browse / OWASP Broken Web Applications Project / Files

OWASP Broken Web Applications Proje...

Brought to you by: [chuckatsf](#)

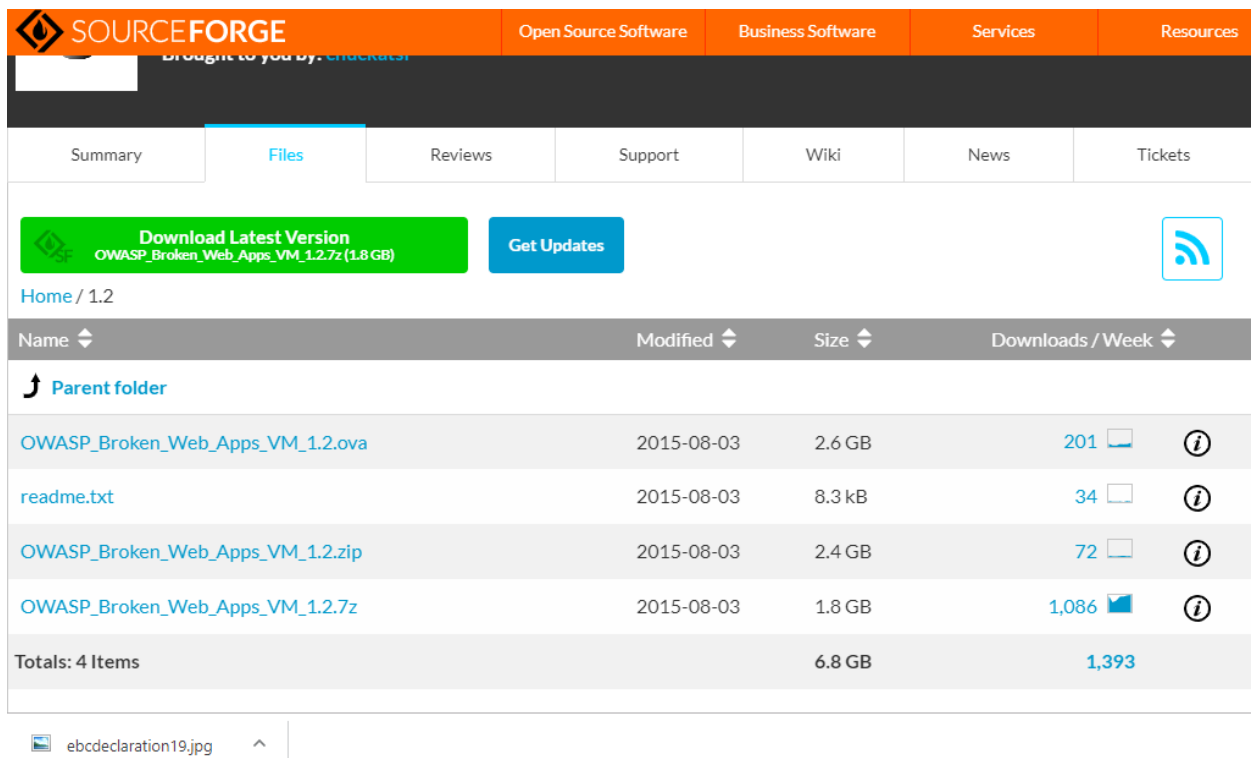
Summary **Files** Reviews Support Wiki News Tickets

Download Latest Version
OWASP Broken Web Apps VM 1.2.7z (1.8 GB) **Get Updates**

Home

| Name | Modified | Size | Downloads / Week |
|------|------------|------|------------------|
| 1.2 | 2015-08-03 | | 1,393 |

3. Download the .ova file



SOURCEFORGE Open Source Software Business Software Services Resources

Summary **Files** Reviews Support Wiki News Tickets

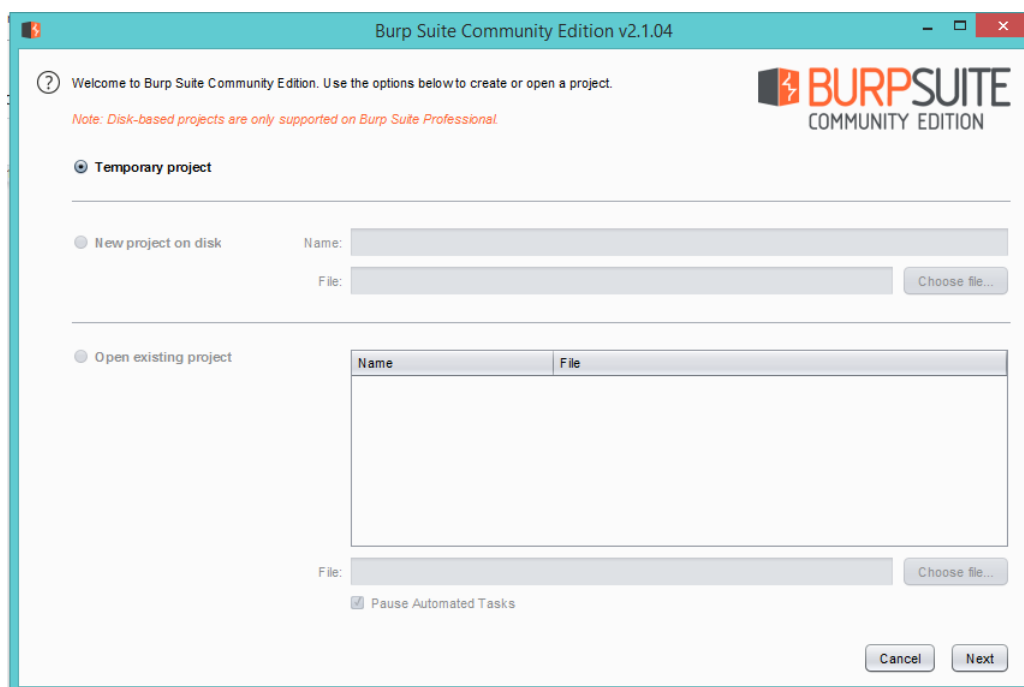
Download Latest Version
OWASP_Broken_Web_Apps_VM_1.2.7z (1.8 GB) **Get Updates**

Home / 1.2

| Name | Modified | Size | Downloads / Week |
|----------------------------------|------------|---------------|------------------|
| Parent folder | | | |
| OWASP_Broken_Web_Apps_VM_1.2.ova | 2015-08-03 | 2.6 GB | 201 |
| readme.txt | 2015-08-03 | 8.3 kB | 34 |
| OWASP_Broken_Web_Apps_VM_1.2.zip | 2015-08-03 | 2.4 GB | 72 |
| OWASP_Broken_Web_Apps_VM_1.2.7z | 2015-08-03 | 1.8 GB | 1,086 |
| Totals: 4 Items | | 6.8 GB | 1,393 |

ebcdeclaration19.jpg

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



Burp Suite Community Edition v2.1.04

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.

☒ **Temporary project**

☐ **New project on disk**
Name:
File: **Choose file...**

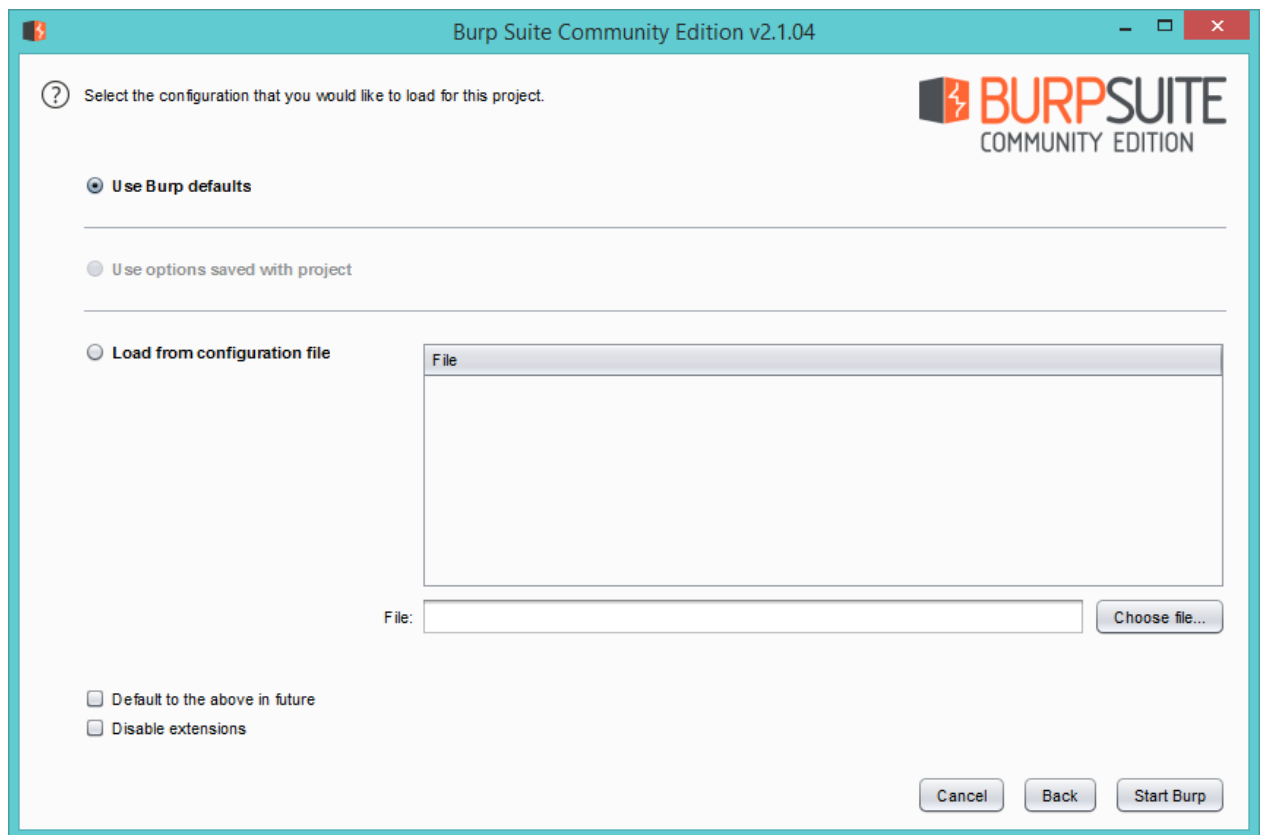
☐ **Open existing project**

| Name | File |
|------|------|
|------|------|

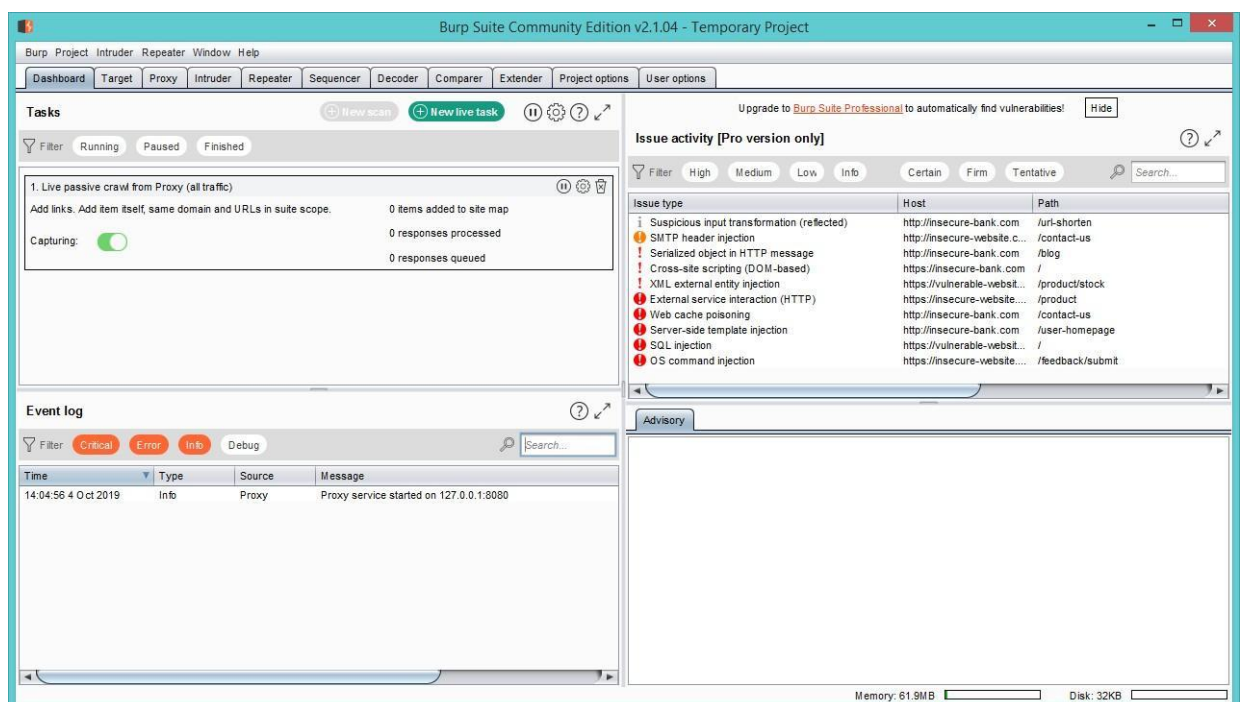
File: **Choose file...**
☒ **Pause Automated Tasks**

Cancel **Next**

5. Accept the default settings



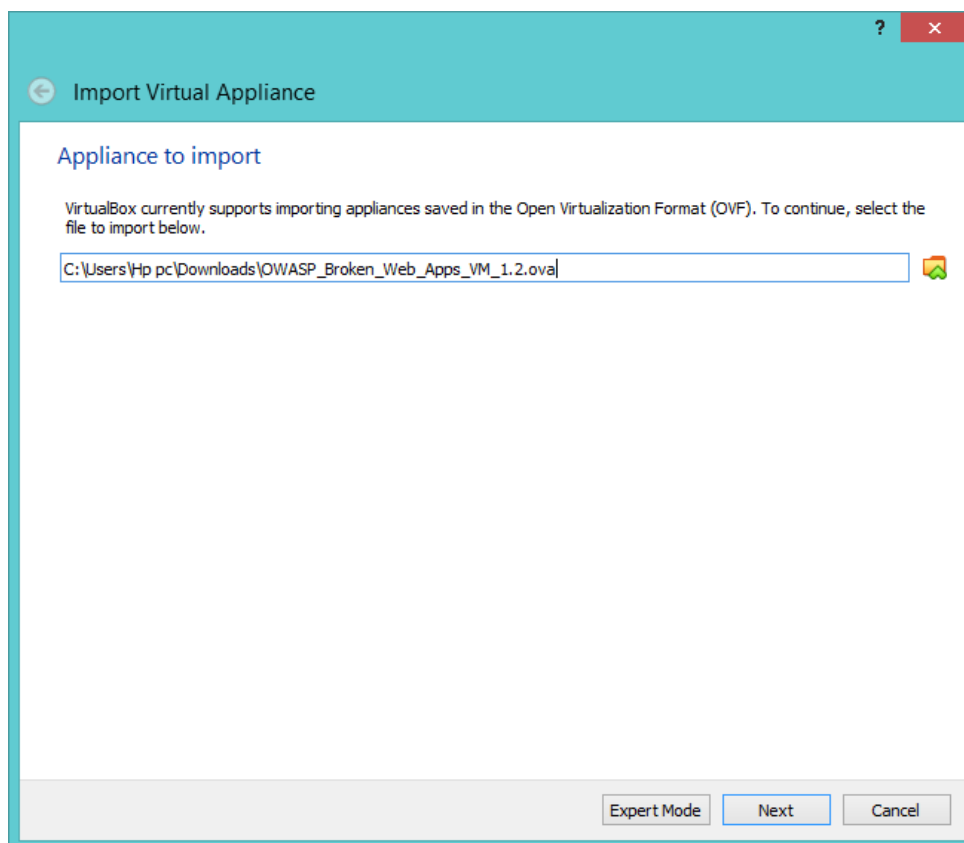
6. The dashboard looks like this

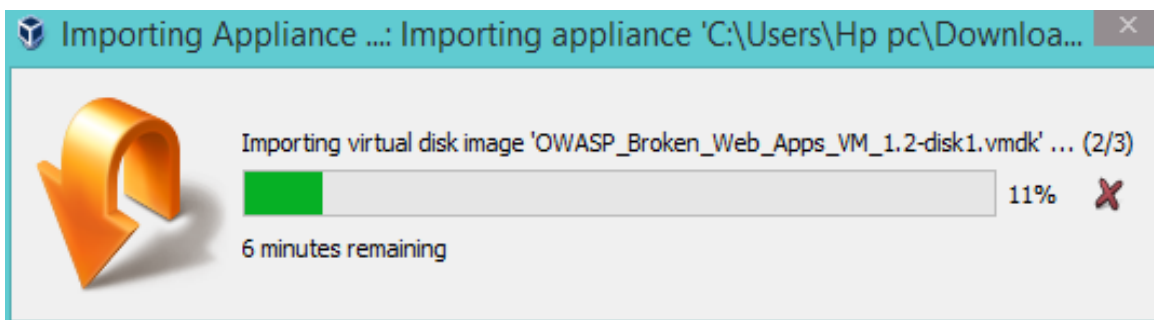
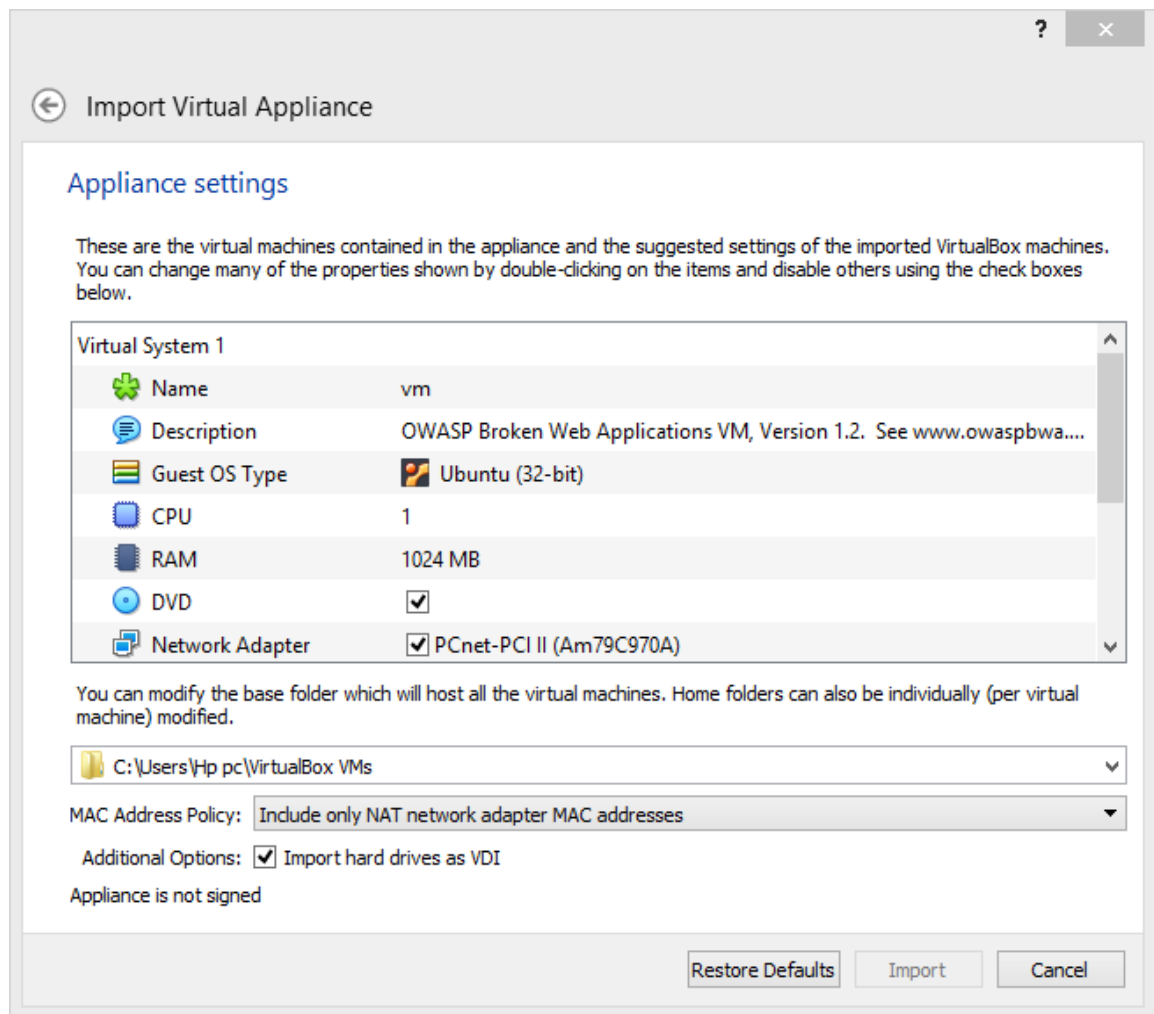


7. Install Virtualbox so we can use our OWASP broken web application

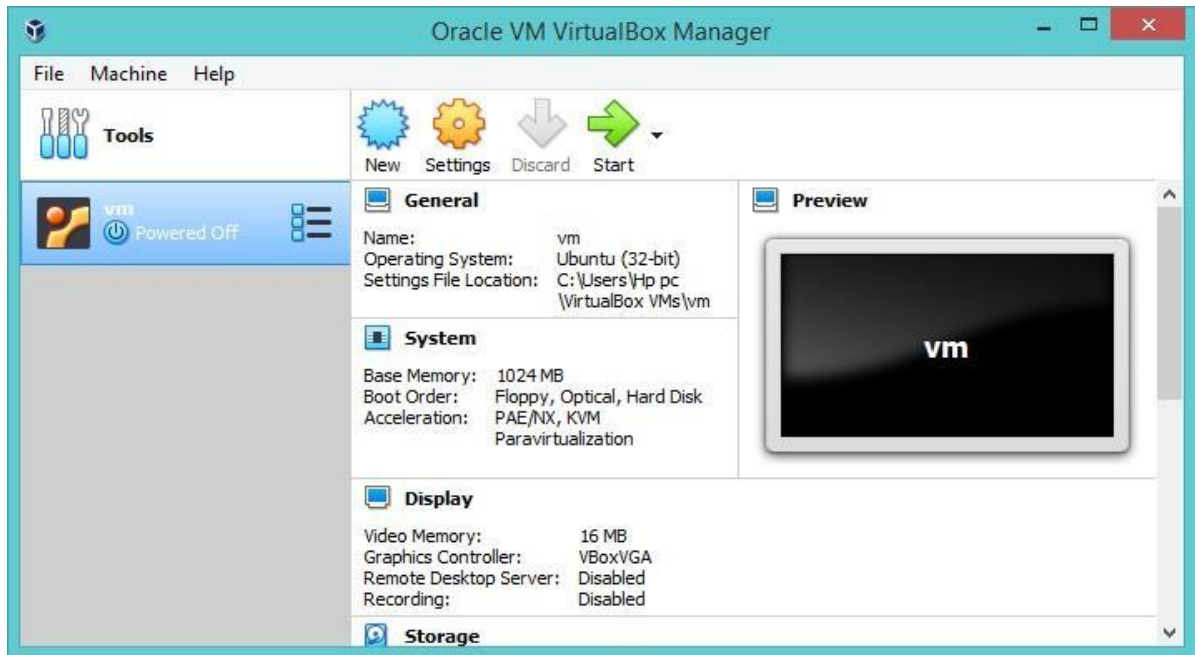


8. Import OWASP BWA

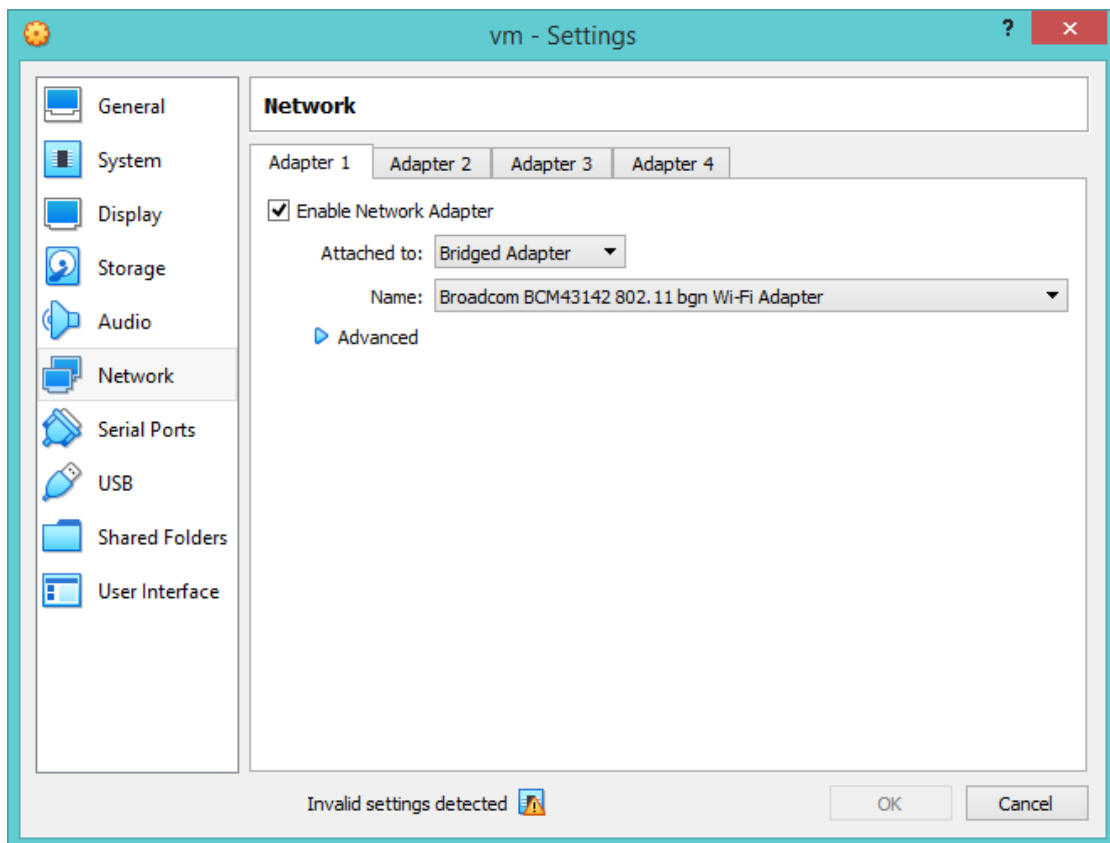




9. Now the appliance has been imported



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

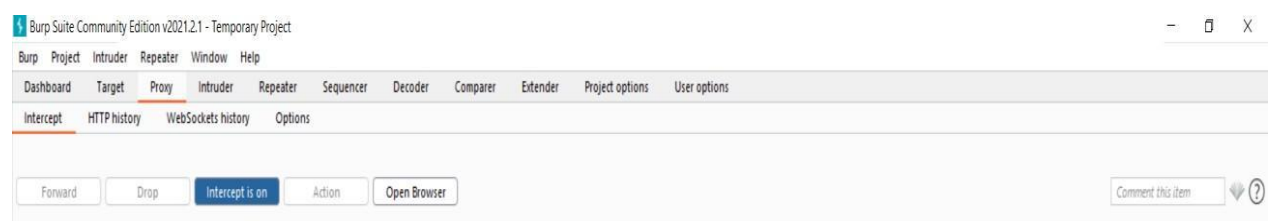
Using Burpsuite as a proxy

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.

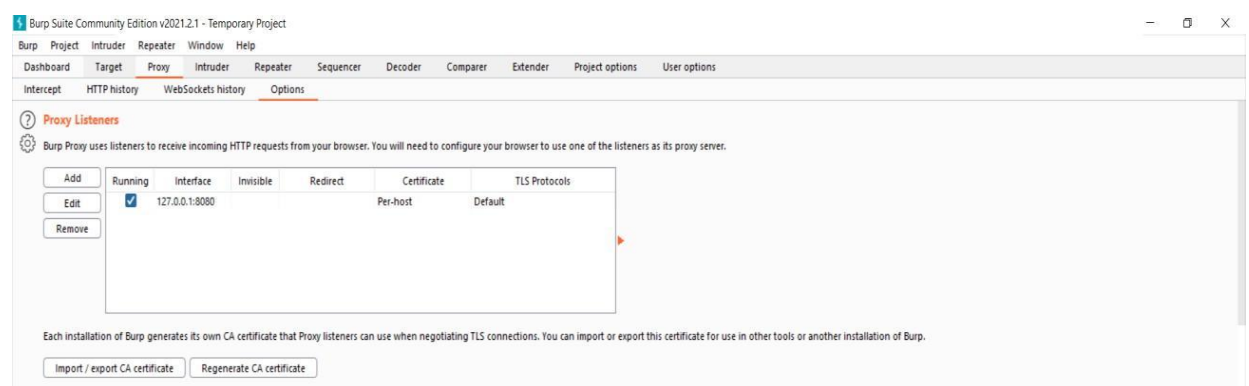


Intercept:

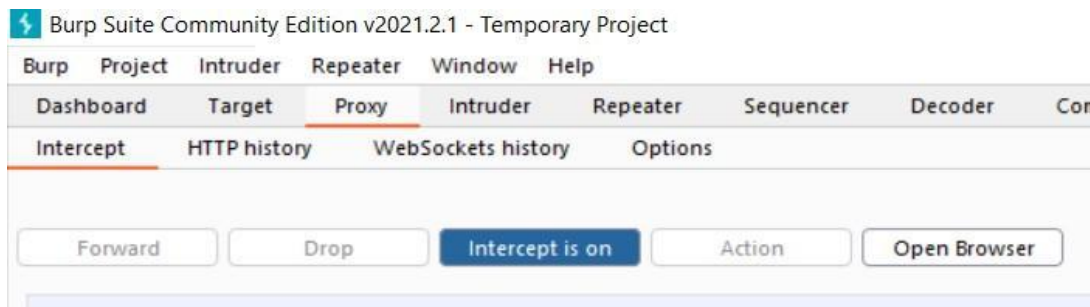
1. Go to the proxy tab and select the intercept option



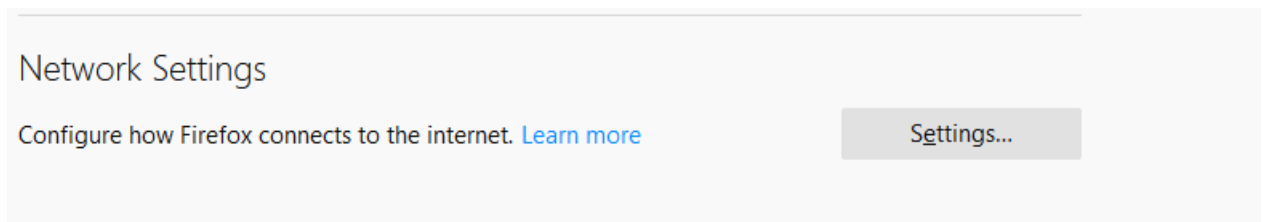
2. Select Options category and check if the proxy is listening on localhost, port 8080



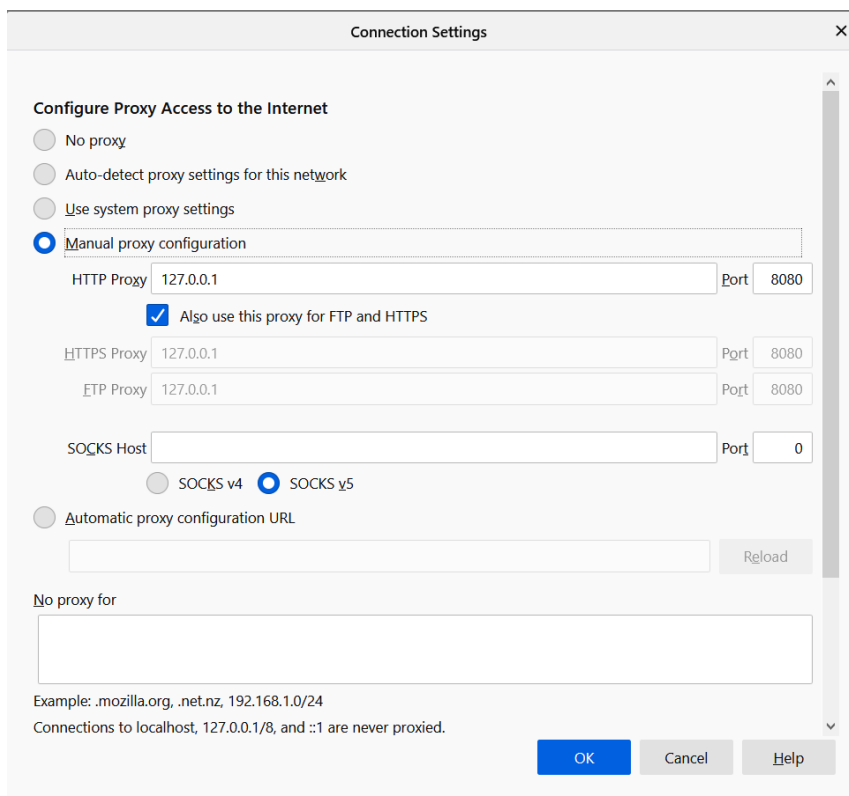
3. Turn the intercept on



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



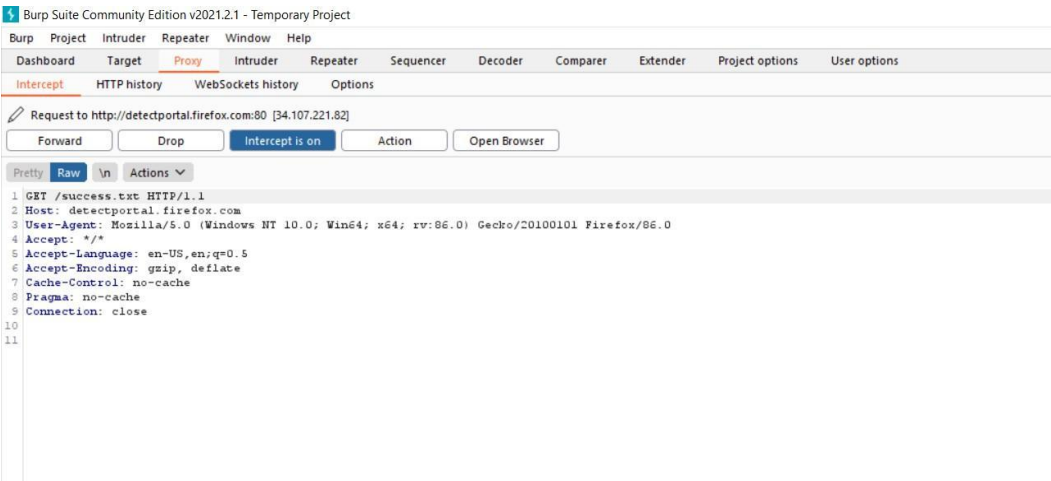
5. Select manual proxy configuration



6. Click on Owasp mutillidae – II



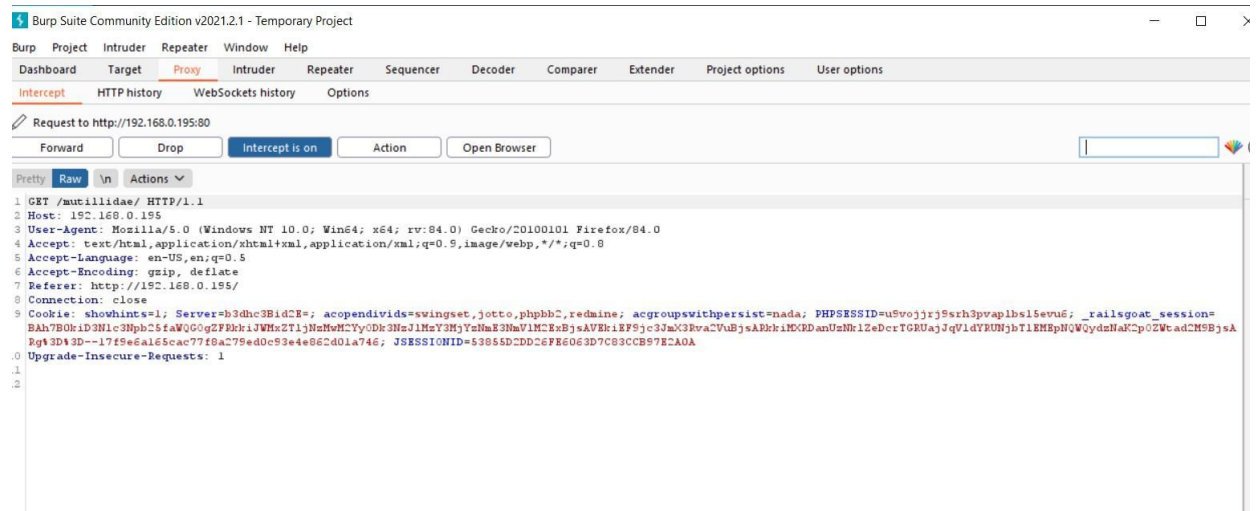
7. The following data is shown



8. The header format is as:

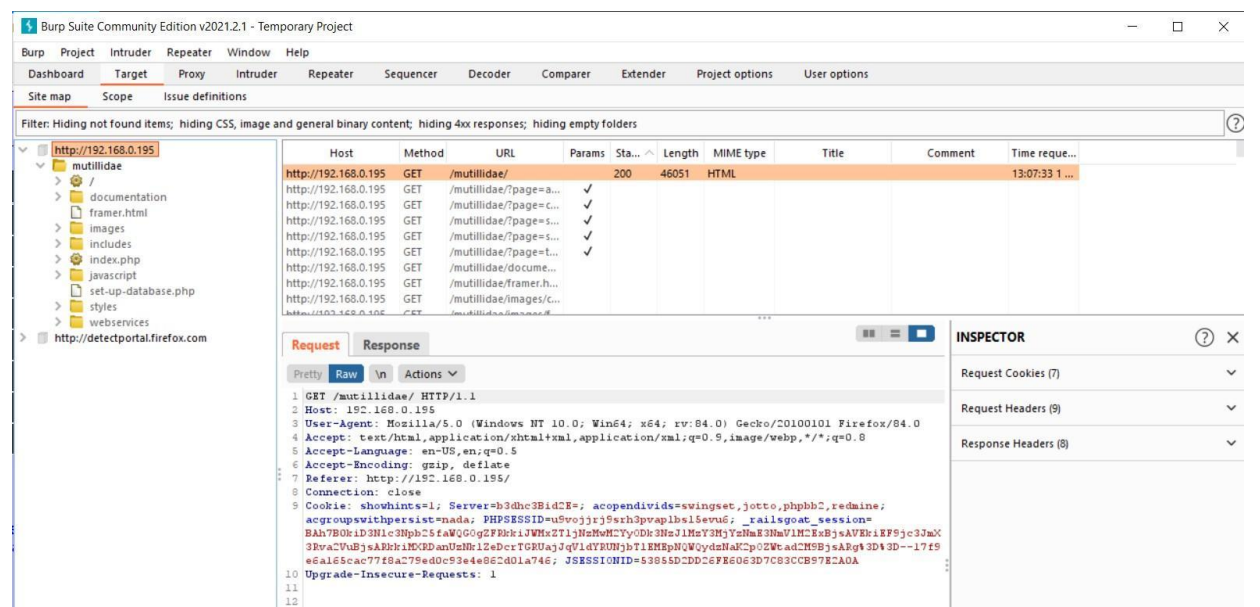
| Request Headers (9) | | |
|---------------------------|--|-------------------|
| NAME | VALUE | |
| Host | 192.168.0.8 | > |
| User-Agent | Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) ... | > |
| Accept | text/html,application/xhtml+xml,application/xml;q... | > |
| Accept-Language | en-US,en;q=0.5 | > |
| Accept-Encoding | gzip, deflate | > |
| Referer | http://192.168.0.8/ | > |
| Connection | close | > |
| Cookie | showhints=1; acopendivids=swingset,jotto,phpbb... | > |
| Upgrade-Insecure-Requests | 1 | > |
| | | Remove ^ v Add... |

Click on owasp mutillidae II



Steps:

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



2. Sitemap is created of the host

The screenshot shows the Burp Suite Community Edition v2021.2.1 interface. The 'Target' tab is selected, and the 'Site map' sub-tab is active. The site map on the left shows a tree structure for the host `http://192.168.0.195`, with a folder named `mutillidae` expanded. The main panel displays a table of HTTP history. The first entry is a GET request to `/mutillidae/` with a status of 200 and a length of 46051. The 'Inspector' panel on the right shows the request details, including the User-Agent: `Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0` and the Cookie: `showhints=1; Server=b3dnc3BIdCE=; acopendivids=swingset,jotto,phbb2,redmine; acgroupswithpersist=nada; PHPSESSID=u9vojjrj9wrb3pvpblb15evu6; _railsgoat_session=BAh7B0uID3Hlc3BpbC5zaWQ6G2FDbk1UWHs2T1jhaBwMCTyODk3Bw31MwY3MjY3Zmha83BhaVINCkEsBj4AVeB1EF9joc3mX3BvaCVuB3sA8kklMEGDanUaHk1ZaDcrTGRUajJqVldYRUNjbTlEMEpNWQy4dNaKCPoZWc adCH5B3sA8g3DA3D--17f9e6a165cac77f8ac79ed0c93e4e862d01a746; JSESSIONID=53855DDDD6FE6063D7C83CCB97E2A0A`.

| Host | Method | URL | Params | Sta... | Length | MIME type | Title | Comment | Time requ... |
|----------------------|--------|-------------------------|--------|--------|--------|-----------|-------|---------|----------------|
| http://192.168.0.195 | GET | /mutillidae/ | | 200 | 46051 | HTML | | | 13:07:33 1 ... |
| http://192.168.0.195 | GET | /mutillidae/?page=a... | | ✓ | | | | | |
| http://192.168.0.195 | GET | /mutillidae/?page=c... | | ✓ | | | | | |
| http://192.168.0.195 | GET | /mutillidae/?page=s... | | ✓ | | | | | |
| http://192.168.0.195 | GET | /mutillidae/?page=s... | | ✓ | | | | | |
| http://192.168.0.195 | GET | /mutillidae/?page=t... | | ✓ | | | | | |
| http://192.168.0.195 | GET | /mutillidae/docume... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/framer.h... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/c... | | | | | | | |

The screenshot shows the Burp Suite Community Edition v2021.2.1 interface. The 'Target' tab is selected, and the 'Site map' sub-tab is active. The site map on the left shows a tree structure for the host `http://192.168.0.195`, with a folder named `mutillidae` expanded. The main panel displays the site map structure, including folders for `/`, `documentation`, `framer.html`, `images`, `includes`, `index.php`, `javascript`, `styles`, and `webservices`.

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.

Burp Suite Community Edition v2021.2.1 - Temporary Project
 Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Site map Scope Issue definitions

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


| Host | Method | URL | Params | Sta... | Length | MIME type | Title | Comment | Time reque... |
|----------------------|--------|-------------------------|--------|--------|--------|-----------|-------|---------|----------------|
| http://192.168.0.195 | GET | /mutillidae/ | | 200 | 46051 | HTML | | | 13:07:33 1 ... |
| http://192.168.0.195 | GET | /mutillidae/includes... | ✓ | 200 | 690 | HTML | | | 13:10:45 1 ... |
| http://192.168.0.195 | GET | /mutillidae/?page=a... | ✓ | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/?page=c... | ✓ | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/?page=s... | ✓ | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/?page=t... | ✓ | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/docume... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/framer.h... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/c... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/f... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/images/... | | | | | | | |
| http://192.168.0.195 | GET | /mutillidae/index.php | | | | | | | |

owaspbwa OWASP Broken We... | Jeremy Druin (@webpwnized) | +

https://twitter.com/webpwnized

Explore
 Settings

Jeremy Druin
 1,078 Tweets


 Follow

Jeremy Druin
 @webpwnized
 Professional pen-tester, Mutillidae developer, trainer and cat-header.
 Derbycon-ville, USA | ellipsisinfosec.com | Joined October 2011
 41 Following | 4,021 Followers

Tweets | Tweets & replies | Media | Likes

Jeremy Druin @webpwnized · Feb 27
 Mutillidae 2.8.21 released. Lots of bugs fixed and generally making it easier to use.

webpwnized/mutillidae
 OWASP Mutillidae II is a free, open source.

Don't miss what's happening
 People on Twitter are the first to know.

Log in | Sign up

Type here to search

13:12
 01-03-2021

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

**OWASP Mutillidae II: Web Pwn in Mass Production**

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

[Login/Register](#) | [Toggle Hints](#) | [Show Popup Hints](#) | [Toggle Security](#) | [Enforce SSL](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#)

Login

 **Help Me!**

Hints

Please sign-in

Username


Password

Login

Dont have an account? [Please register here](#)

Check the request on burpsuite:

Intercept HTTP history WebSockets history Options

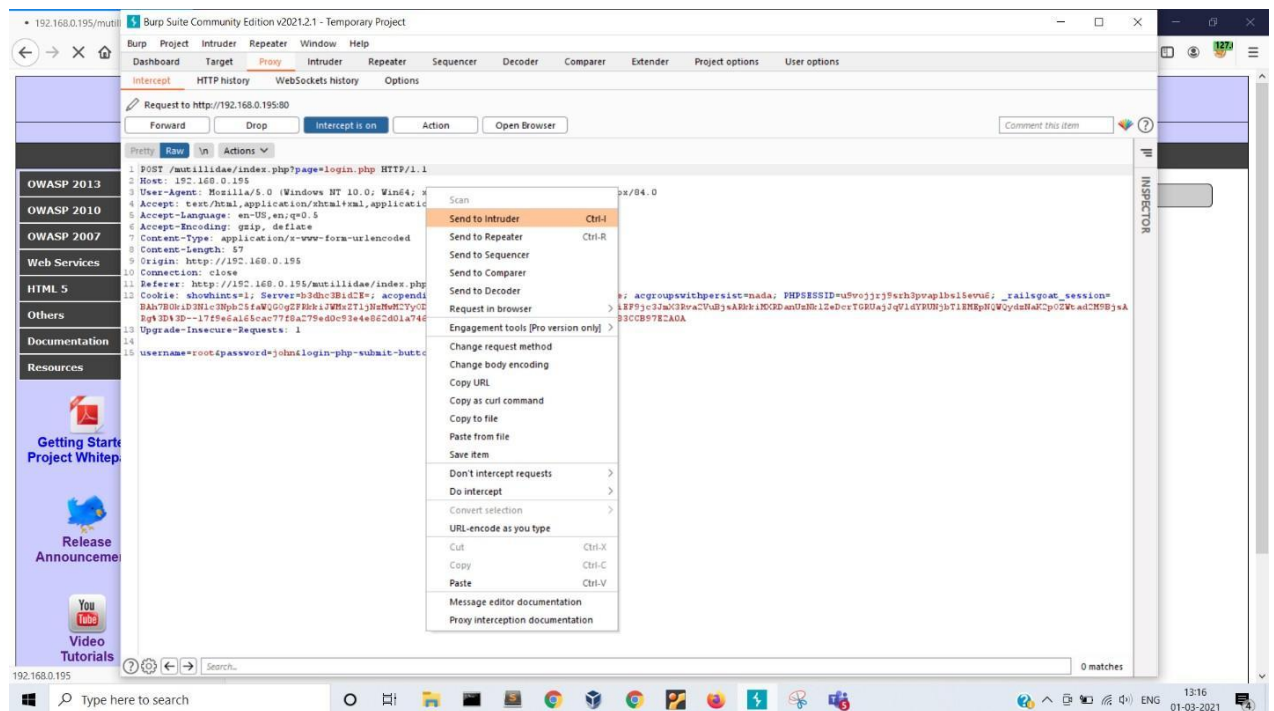
 Request to http://192.168.0.195:80

Forward Drop Intercept is on Action Open Browser

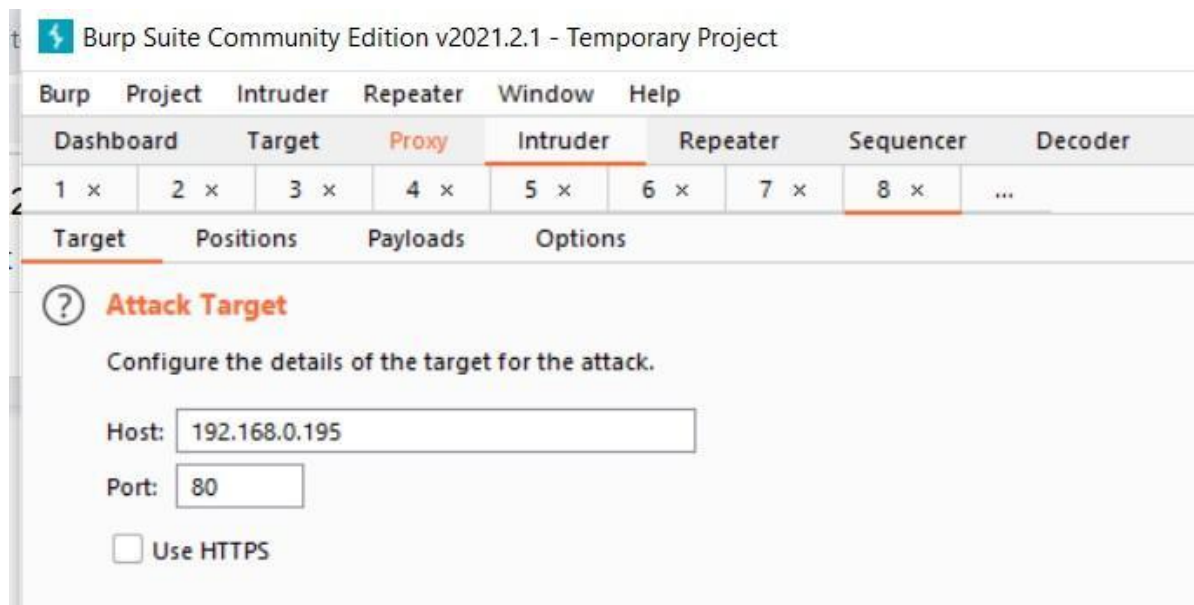
Pretty Raw \n Actions ▼

```
1 POST /mutillidae/index.php?page=login.php HTTP/1.1
2 Host: 192.168.0.195
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 57
9 Origin: http://192.168.0.195
10 Connection: close
11 Referer: http://192.168.0.195/mutillidae/index.php?page=login.php
12 Cookie: showhints=1; Server=b3dhc3Bid2E=; acopendivids=swingset,jotto,phpb2,redmine; acgroupswithperBAh7B0kriD3Nlc3Npb25faWQOG2FkZkRkZT1jNmMwM2YyODk3NmZlMzY3MjYzNmE3NmVlMCExBjsAVEkIEF9jc3JmX3Rva2VuB
Rgt3D3D--17f9e6al65cac77f8a279ed0c93e4e862d01a746; JSESSIONID=53855D2DD26FE6063D7C83CCB97E2A0A
13 Upgrade-Insecure-Requests: 1
14
15 username=root&password=john&login-php-submit-button=Login
```


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:

Menu: Burp Project Intruder Repeater Window Help

Sub-menu: Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x ...

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:

```
1 POST /mutillidae/index.php?page=login.php HTTP/1.1
2 Host: 192.168.0.195
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 57
9 Origin: http://192.168.0.195
10 Connection: close
11 Referer: http://192.168.0.195/mutillidae/index.php?page=login.php
12 Cookie: showhints=1; Server=b3dhc3BidCE=; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=u5vojrrj9srh3pvapibsl5evu6;
    _railsgoat_session=
    BAh7B0kiD3Nlc3RpbC25faWQ0GgZFRkhiJWVhZTljNmVhZDk3NmZlMmY3MjY2aWwE3NaVlMCEsBjsAVEkIEF9jC3JmX3Rva2VubGjsARhkImXEDanUzHk1ZeDcrTGRUajJqV1dYRUNjbTlEMEpNQWQydcN
    aKp0ZWtadZMSBjsARgt3D43D--17f9e6a165cac77f8a279ed0c93e4e862d01a746; JSESSIONID=53855DDDD26FE6063D7C83CCB97E2A0A
13 Upgrade-Insecure-Requests: 1
14
15 username=root&password=$john$&login-php-submit-button=Login
```

Start attack

▼

▼

Add \$

Clear \$

Auto \$

Refresh

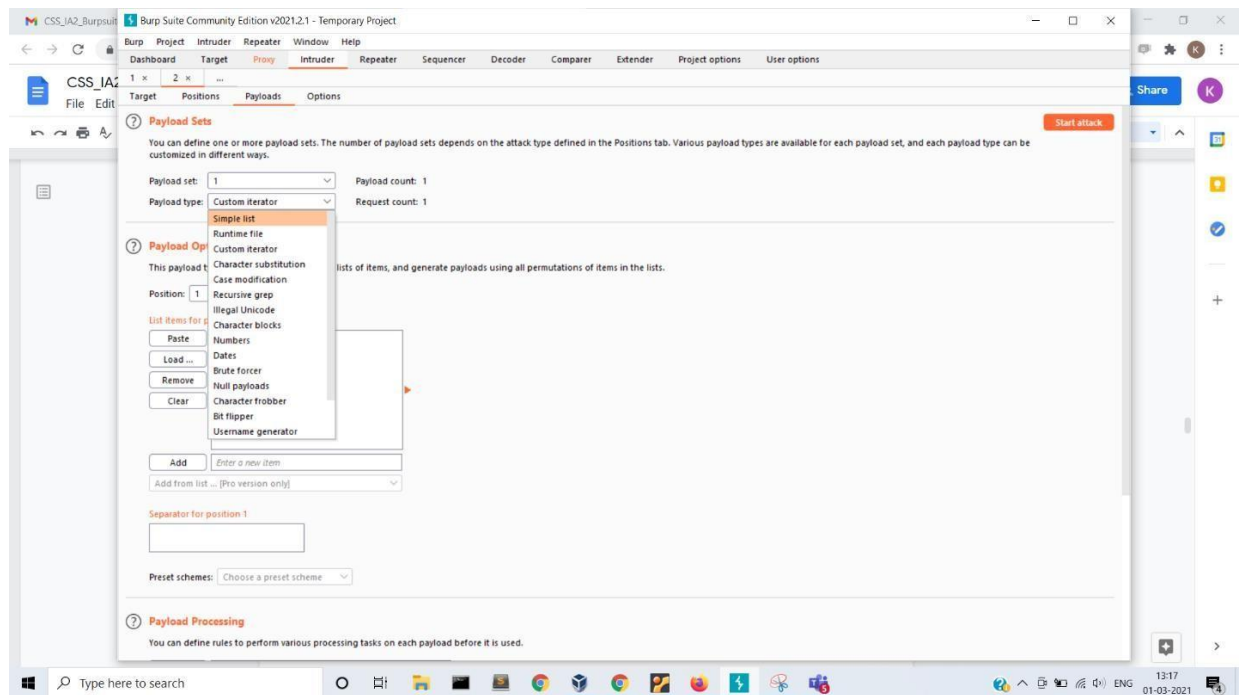
... 3 ...

Select attack type as Sniper:

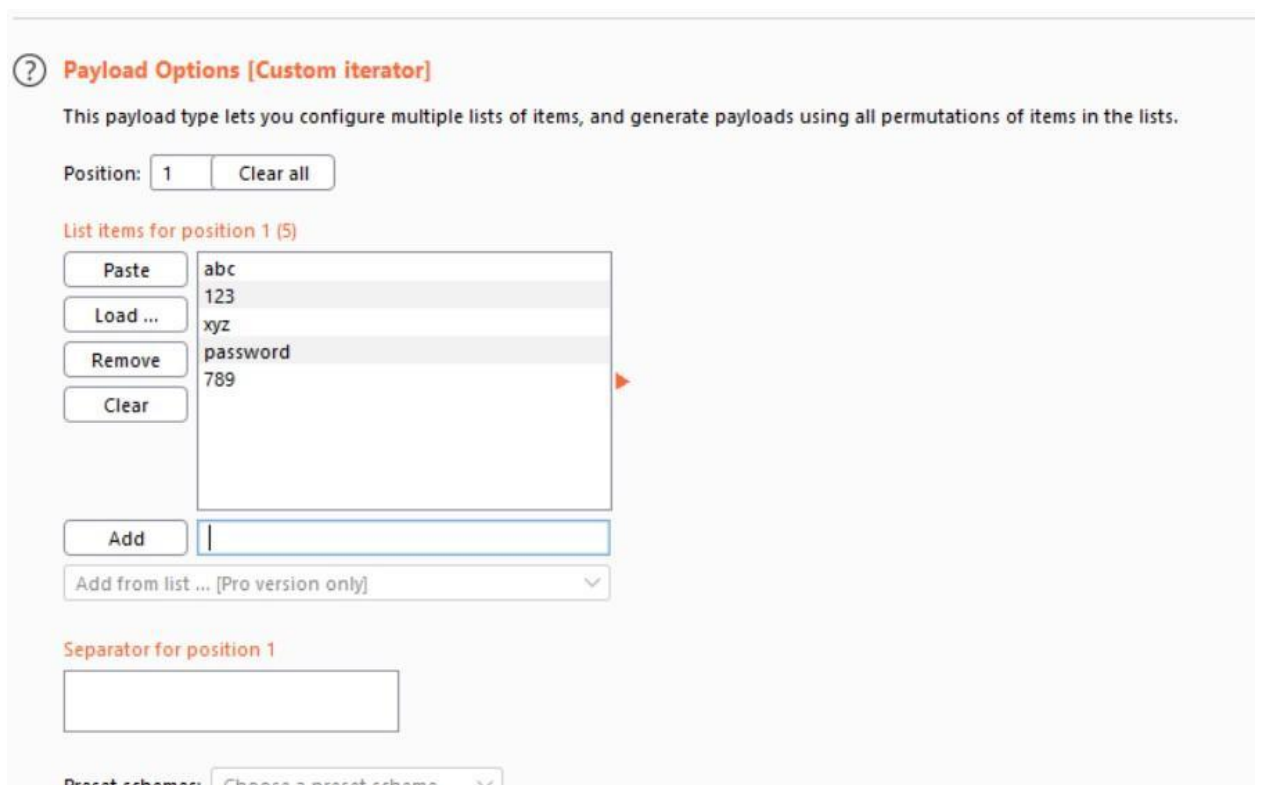
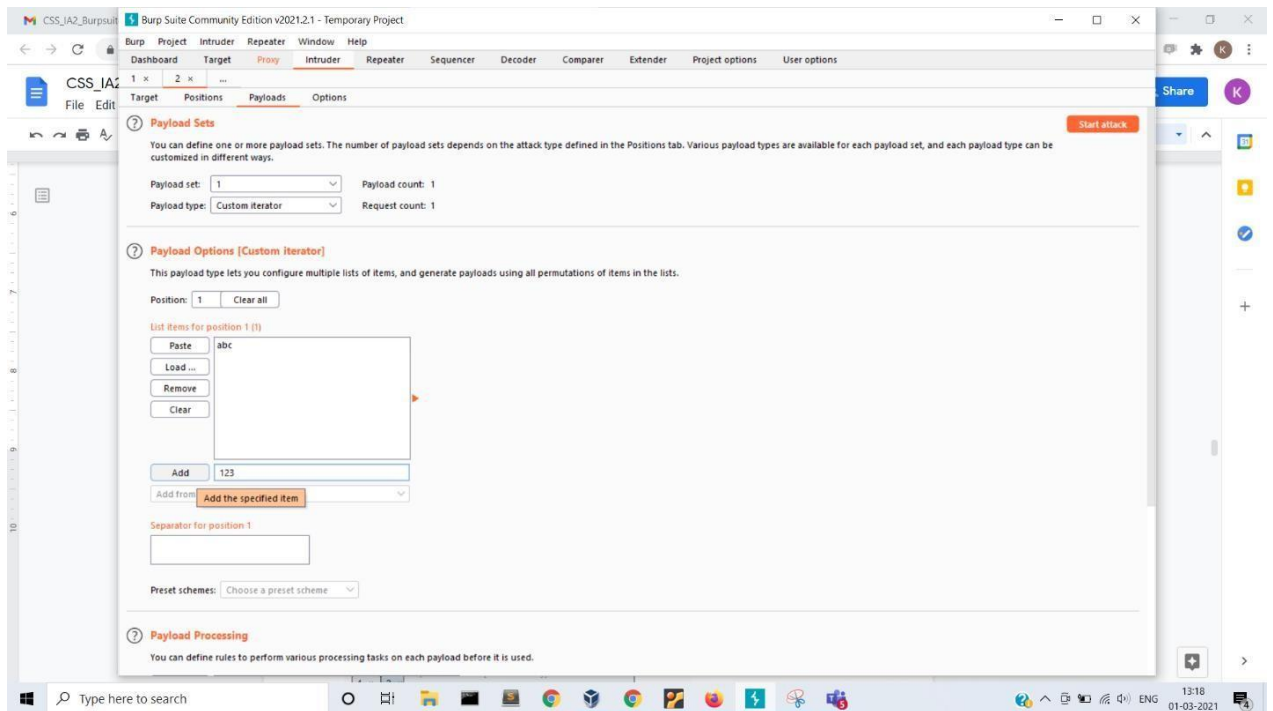


Click on payload tab:

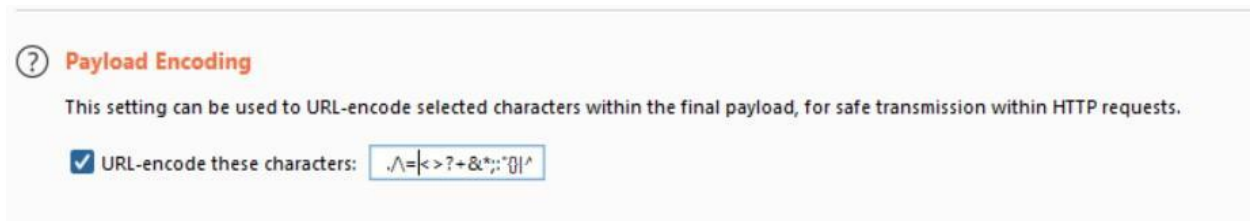
Select payload type as simple list



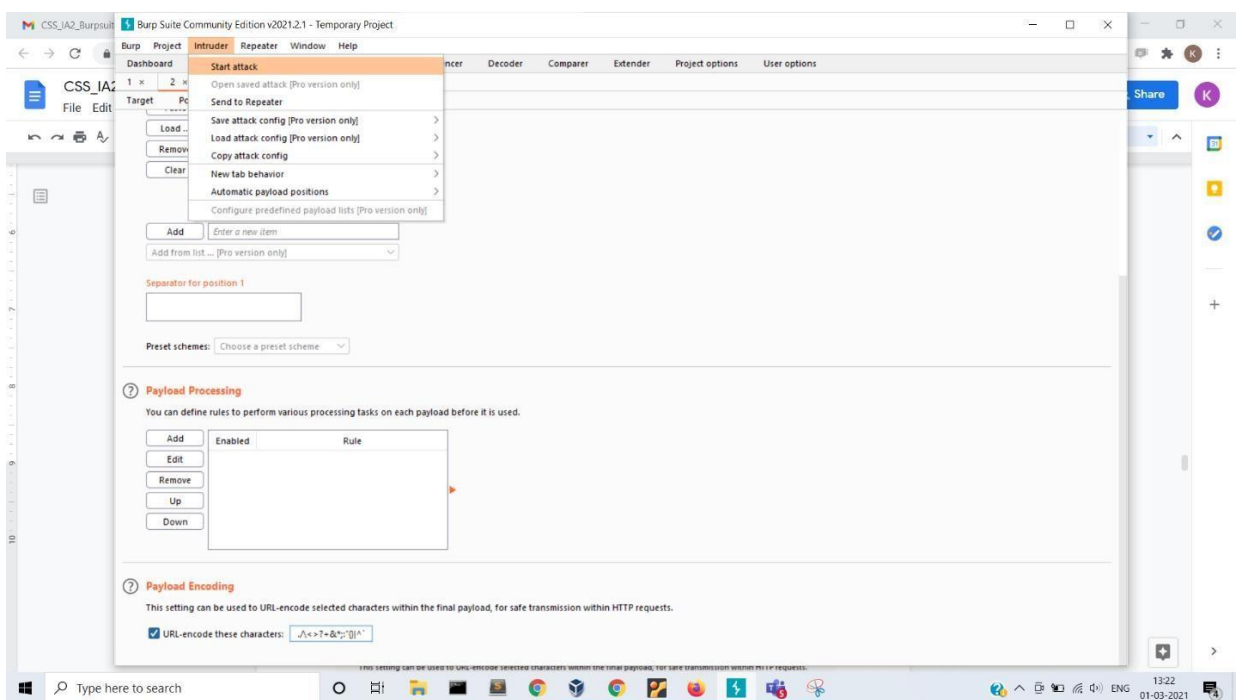
Enter a list of words:



Remove the equal to sign from payload encoding:



Start the attack



Inspect the requests that are sent:

The screenshot shows the 'Intruder attack 1' window in Burp Suite. It displays a table of requests with the following data:

| Requ... | Payload | Status | Error | Timeout | Length | Comment |
|---------|----------|--------|--------------------------|--------------------------|--------|---------|
| 0 | | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 50761 | |
| 1 | abc | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 50761 | |
| 2 | 123 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 50761 | |
| 3 | xyz | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 50761 | |
| 4 | password | 302 | <input type="checkbox"/> | <input type="checkbox"/> | 50885 | |
| 5 | 789 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 50788 | |

Below the table, the 'Request' tab is selected, showing the raw HTTP request for the 4th request (payload 'password'). The request is a POST to /mutillidae/index.php?page=login.php with various headers and a body containing login credentials.

```
1 POST /mutillidae/index.php?page=login.php HTTP/1.1
2 Host: 192.168.0.195
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 61
9 Origin: http://192.168.0.195
10 Connection: close
11 Referer: http://192.168.0.195/mutillidae/index.php?page=login.php
12 Cookie: showhints=1; Server=b3dhc3Bid2E=; acopendivids=swingset,jotto,phpbb2,redmine;
    acgroupswithpersist=nada; PHPSESSID=u9vojrrj9srh3pvap1bs15evu6; _railsgoat_session=
    BAh7B0kiD3N1c3Npb25faWQGOgZFbkkiJWMxZTljNzMwMzYyODk3NzJlMzY3MjYzNmE3NmVlMzExBjsAVEkiEF9jc3JmX3Rva2V
    uBjsARkriMDRlanUzNk1ZeDcrTGRUajJqVldYRUNjbTlEMEpnQWQydzNaK2p0ZWtad2M9BjsARgt3D13D--17f9e6al65cac77f
    8a279ed0c93e4e862d01a746; JSESSIONID=53855D2DD26FE6063D7C83CCB97E2A0A
13 Upgrade-Insecure-Requests: 1
14
15 username=root&password=password&login-php-submit-button=Login
```

Status for password is 302

Now check response and render it

Password was the correct password and you are now logged in

 **OWASP Mutillidae II: Web Pwn in Mass Production**

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Logged In User: **root** ()

[Home](#) | [Logout](#) | [Toggle Hints](#) | [Show Popup Hints](#) | [Toggle Security](#) | [Enforce SSL](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#)

Login

 **Back**  **Help Me!**

 **Hints**

You are logged in as root

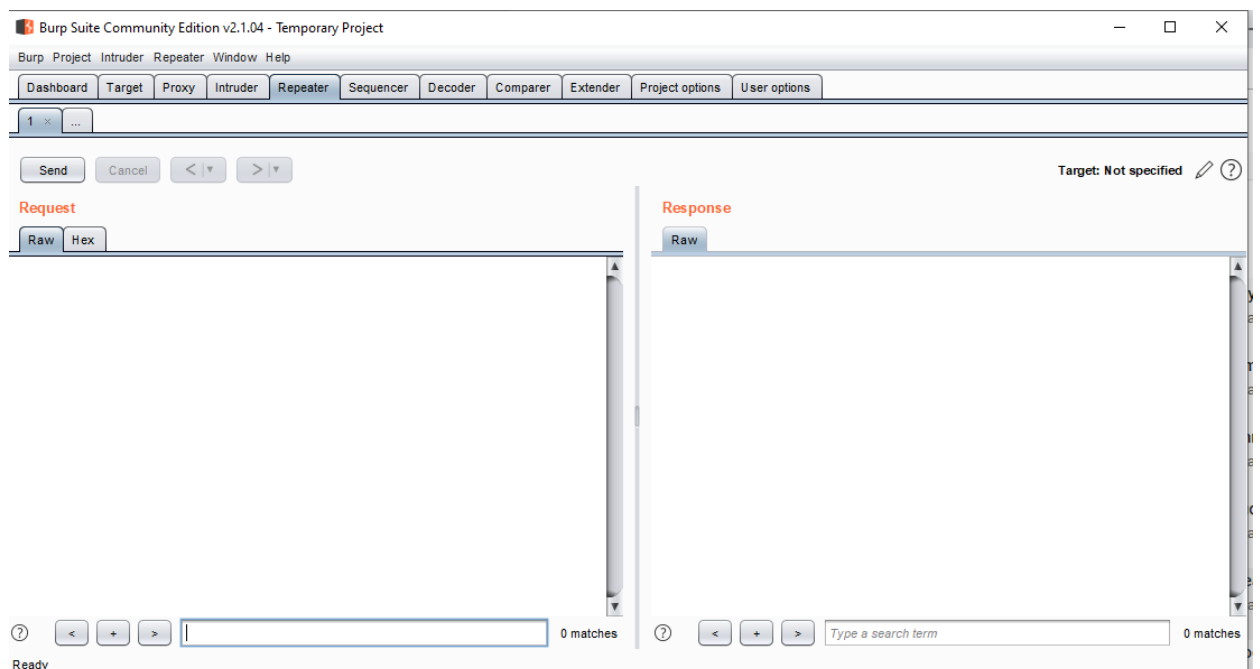
Logout

4. Repeater

Used to send multiple Http requests.

Server response can be monitored

Initial view:



The screenshot shows the Burp Suite Community Edition v2.1.04 interface, specifically the Repeater tab. The window title is "Burp Suite Community Edition v2.1.04 - Temporary Project". The menu bar includes "Burp", "Project", "Intruder", "Repeater", "Window", and "Help". The toolbar contains buttons for "Dashboard", "Target", "Proxy", "Intruder", "Repeater" (selected), "Sequencer", "Decoder", "Comparer", "Extender", "Project options", and "User options". Below the toolbar, there is a tab labeled "1" with a close button and an ellipsis. The main area is divided into two panes: "Request" on the left and "Response" on the right. The "Request" pane has a "Raw" button and a "Hex" button. The "Response" pane has a "Raw" button. At the bottom, there are search bars for both panes, each with a "0 matches" indicator. The status bar at the very bottom says "Ready".

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 | A1 - Injection (SQL) | tillidae: Deliberately Vulnerable Web Pen-Testing Application |
| OWASP 2010 | A1 - Injection (Other) | |
| OWASP 2007 | A2 - Broken Authentication and Session Management | Like Mutillidae? Check out how to help |
| Web Services | A3 - Cross Site Scripting (XSS) | Video Tutorials |
| HTML 5 | A4 - Insecure Direct Object References | |
| Others | A5 - Security Misconfiguration | "Secret" Administrative Pages |
| Documentation | A6 - Sensitive Data Exposure | Directory Browsing |
| Resources | A7 - Missing Function Level Access Control | Method Tampering (GET for POST) |
| | | User-Agent Impersonation |
| | | Unrestricted File Upload |
| | | Bug Rep |
| | | |
| | A8 - Cross Site Request Forgery (CSRF) | |
| | A9 - Using Components with Known Vulnerabilities | |
| | A10 - Unvalidated Redirects and Forwards | |

Getting Started: Project Whitepaper

Release Announcements

PHP MyAdmin Console

Feature Requests

Release Announcements

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

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

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; acgroupsg35n5e1km6mk1ks2
 Upgrade-Insecure-Requests: 1

Comment this item 

- 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 x ...

Send
Cancel
<
>

Request

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; acgroupswithpersist=nada; PHPSESSID=hl46hb6gmjg35n5elkm6mk1ks2
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

Response

Raw
Headers
Hex
HTML
Render

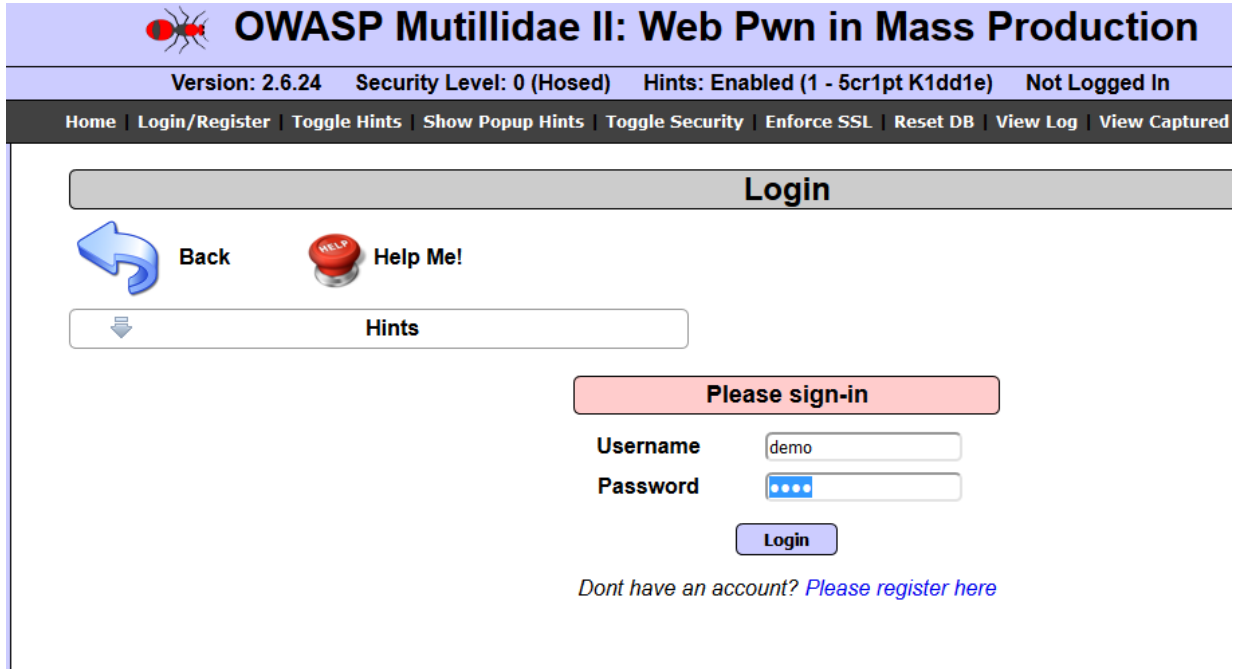
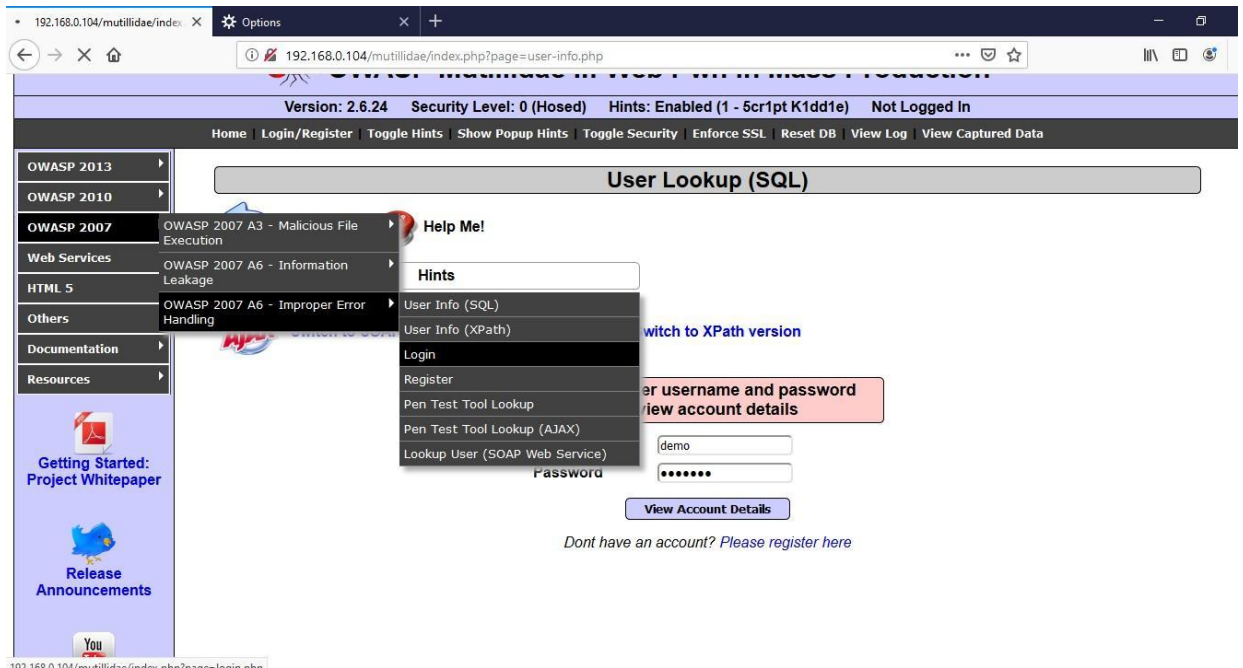
HTTP/1.1 200 OK
Date: Fri, 04 Oct 2019 10:57:48 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-lubuntu4.30
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"
/>

term 0 matches

0 matches

Improper error handling – login



Again send to repeater and click send

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left displays an HTTP POST request to `/mutillidae/index.php?page=login.php`. The 'Response' pane on the right shows an HTTP 200 OK response from the target server. The target URL is `http://192.168.0.104`.

Request:

```
POST /mutillidae/index.php?page=login.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
Content-Type: application/x-www-form-urlencoded
Content-Length: 87
Connection: close
Referer: http://192.168.0.104/mutillidae/index.php?page=login.php
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=hl46hb6gmjg35n5elkm6mklks2
Upgrade-Insecure-Requests: 1

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

Response:

```
HTTP/1.1 200 OK
Date: Fri, 04 Oct 2019 11:02:20 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/2.6.6 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
Logged-In-User:
Vary: Accept-Encoding
Content-Length: 50342
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" />
```

On performing SQL injection, error is shown in response window

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left displays an HTTP POST request to `/mutillidae/index.php?page=login.php`. The payload is a SQL injection attempt: `username=demo &password=demo'&login-php-submit-button=Login`. Two blue arrows point to the single quote characters in the payload, indicating the injection point.

Request:

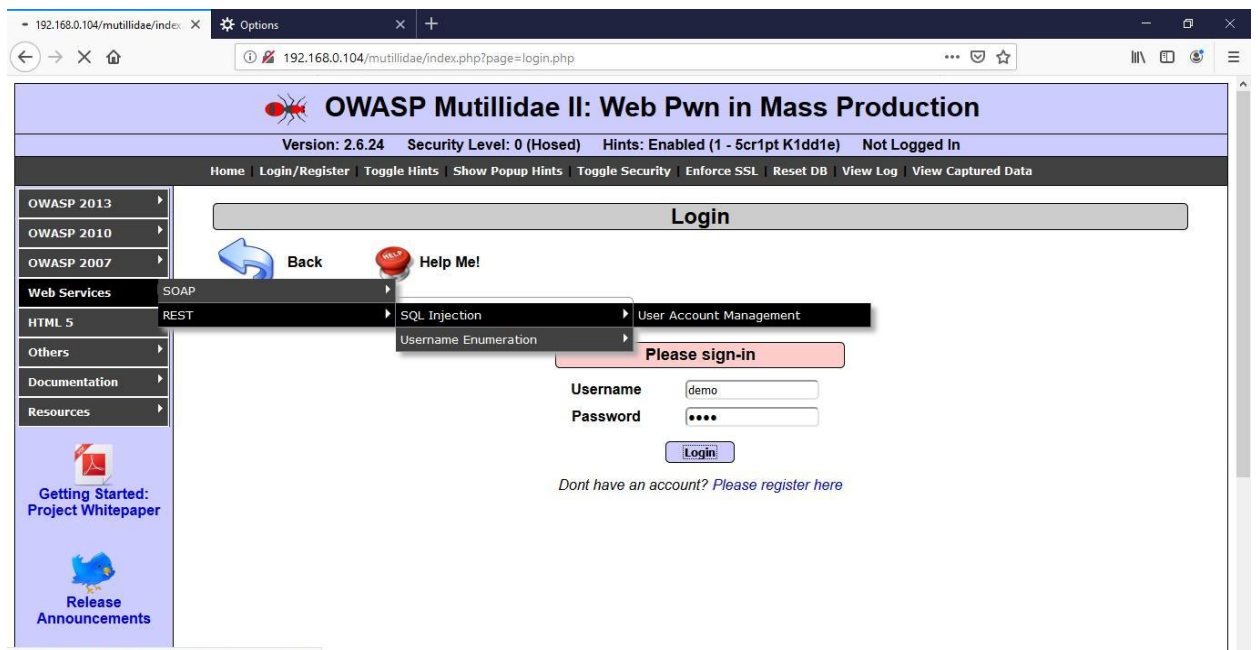
```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.0.104
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 59
Connection: close
Referer: http://192.168.0.104/mutillidae/index.php?page=login.php
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=hl46hb6gmjg35n5elkm6mklks2
Upgrade-Insecure-Requests: 1

username=demo &password=demo'&login-php-submit-button=Login
```

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 -
      <ul>
        <li><a
```

Lastly REST:



192.168.0.104/mutillidae/webse... 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 x 2 x 3 x ...

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=svingsat,jotto,phbb2,redmine; acgroupswithpersist=nada; PHPSESSID=h146hb6gmjg38n5e1km6mk1ks2
Upgrade-Insecure-Requests: 1
```

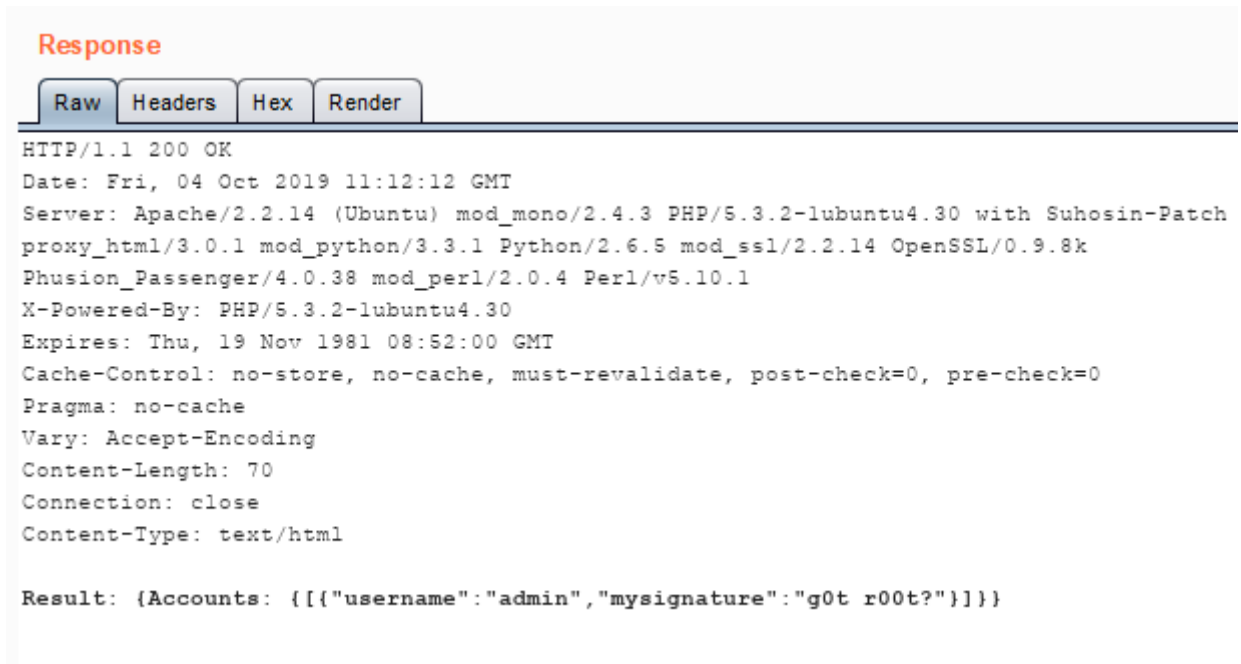
Response

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-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: 523
Connection: close
Content-Type: text/html

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

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

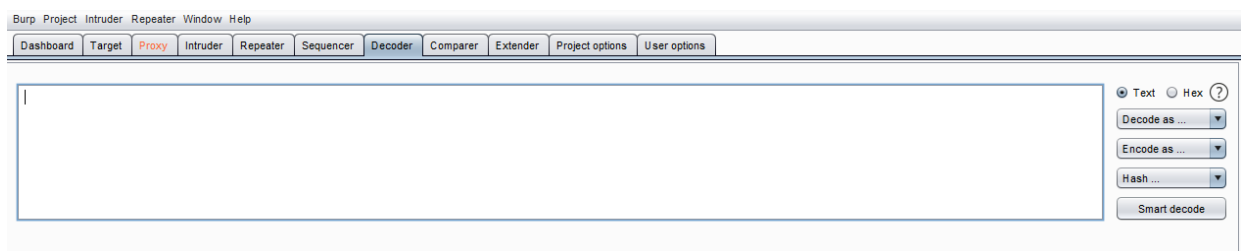


So using repeater tab we can send multiple requests by means of changing parameters also.

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

utillidae: Deliberately Vulnerable Web Pen-Testing Application

[Like Mutillidae? Check out how to help](#)

[Video Tutorials](#)

[Bug Rep](#)

[Release](#)

[Feature](#)

[Getting Started: Project Whitepaper](#)

[Release Announcements](#)

[PHP MyAdmin Console](#)

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/
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,red
Upgrade-Insecure-Requests: 1

```

Scan [Pro version only]
Send to Intruder
Send to Repeater
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

Ctrl+I
Ctrl+R

ID=h146hb6gmjg36n5e1xm6mk1ks

| | | | | | | | | | | |
|-----------|--------|-------|----------|----------|-----------|---------|----------|----------|-----------------|--------------|
| 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-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

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

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

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

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

HELLO

☒ Text ☐ Hex

Decode as ...

Encode as ...

Hash ...

Smart decode

| | | | | | | | | | | | | | | | | | |
|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|
| 0 | 01 | 2d | 91 | 45 | 4b | d2 | 3d | 1b | 8c | c1 | f7 | e4 | 81 | 72 | 27 | 01 | □-□EKÒ=□□Á÷ã□r□ |
| 1 | e6 | 5e | 2d | d5 | 60 | 4d | 18 | 23 | ad | e7 | 76 | 98 | 12 | c9 | 72 | 36 | æ^~Õ`M□#-çv□□Ér6 |

☐ Text ☒ Hex

Decode as ...

Encode as ...

Hash ...

Smart decode