K. J. SOMAIYA COLLEGE OF ENGINEERING

INFORMATION SECURITY, IA-2 REPORT

Exploration of Penetration testing tool – *Burp Suite*

SUDHANSHU SHRIRAO (16010120051, TY COMPS A3)

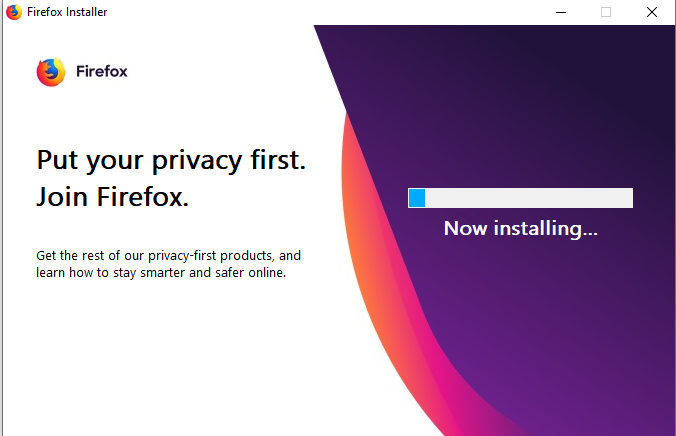
SIDDHI DOSHI (16010120068, TY COMPS A3)

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.

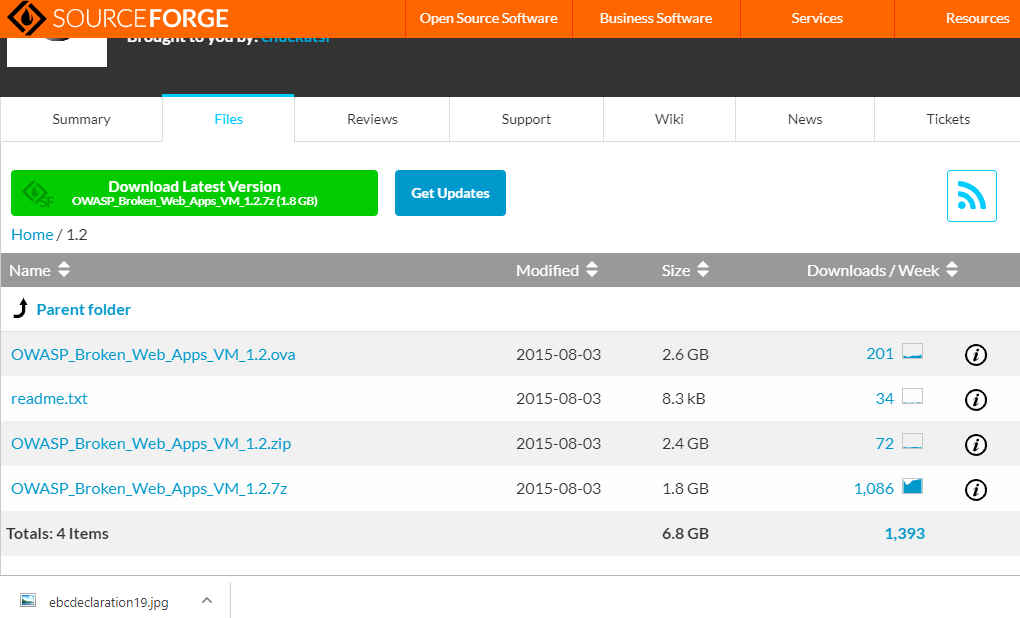
1. Installation
2. Install the Firefox browser



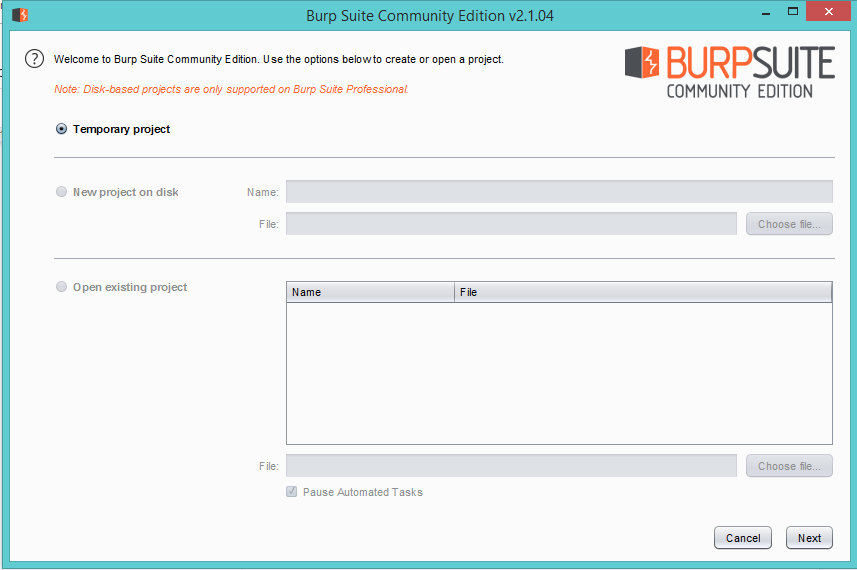
1. Download the Owasp Broken Web application project



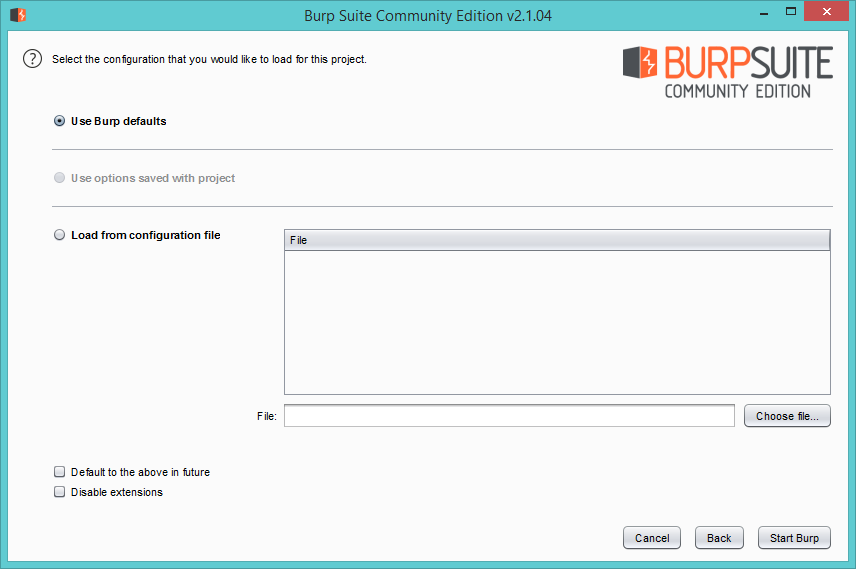
1. Download the .ova file



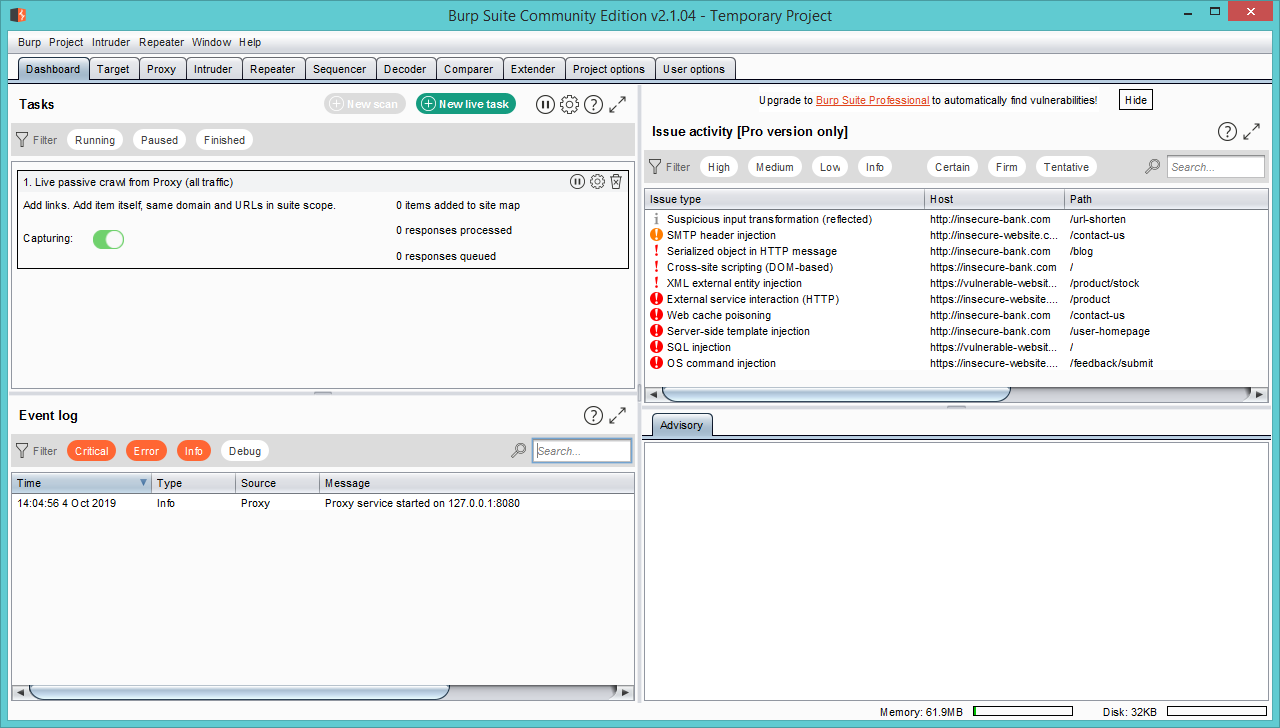
1. Download the burpsuite community edition and launch the application.



1. Accept the default settings



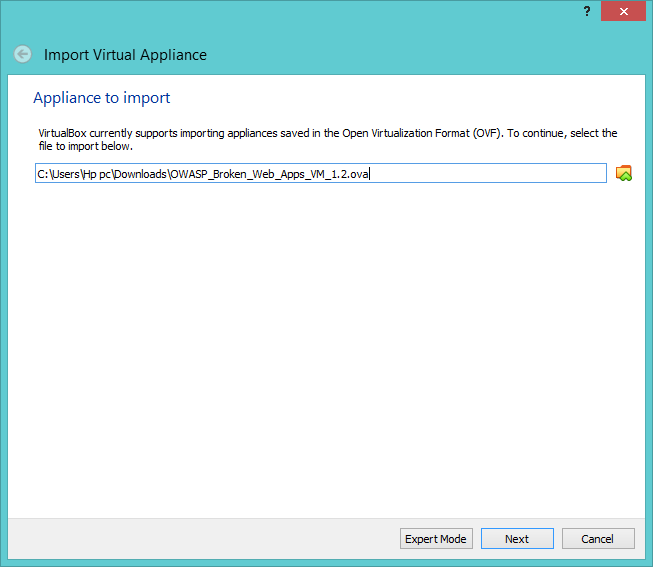
1. The dashboard looks like this

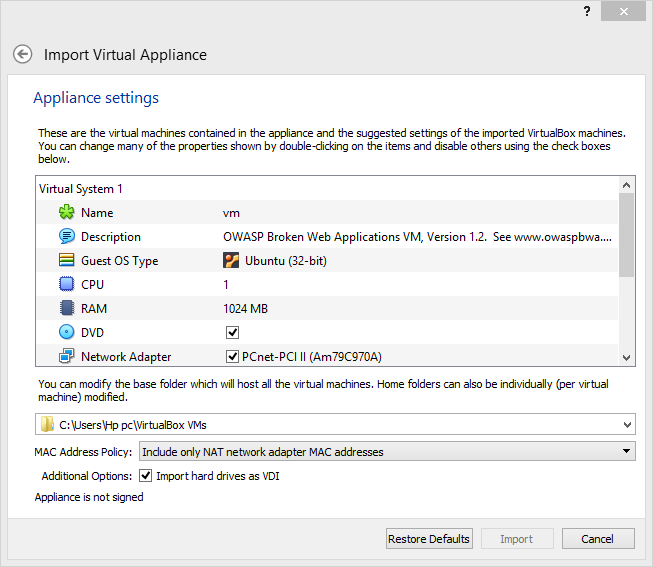


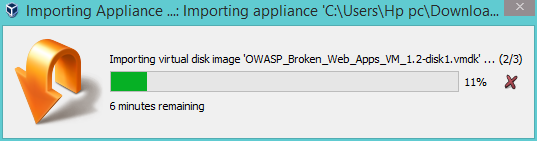
1. Install Virtualbox so we can use our OWASP broken web application



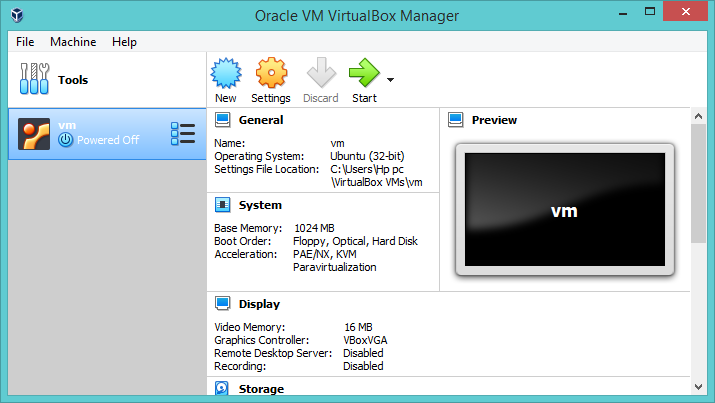
1. Import OWASP BWA



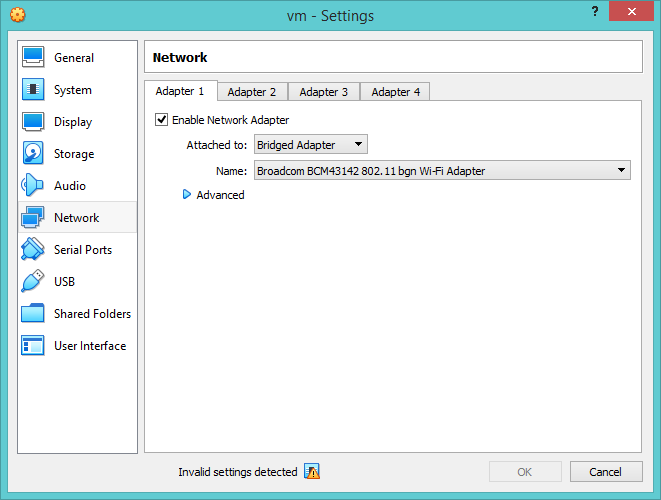


****

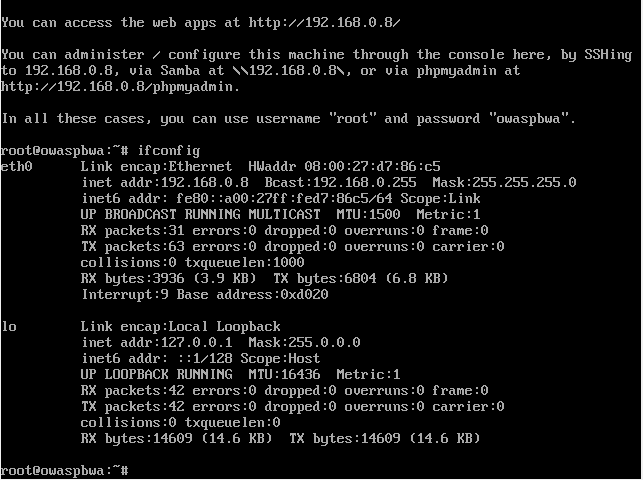
1. Now the appliance has been imported

****

1. Change network settings

****

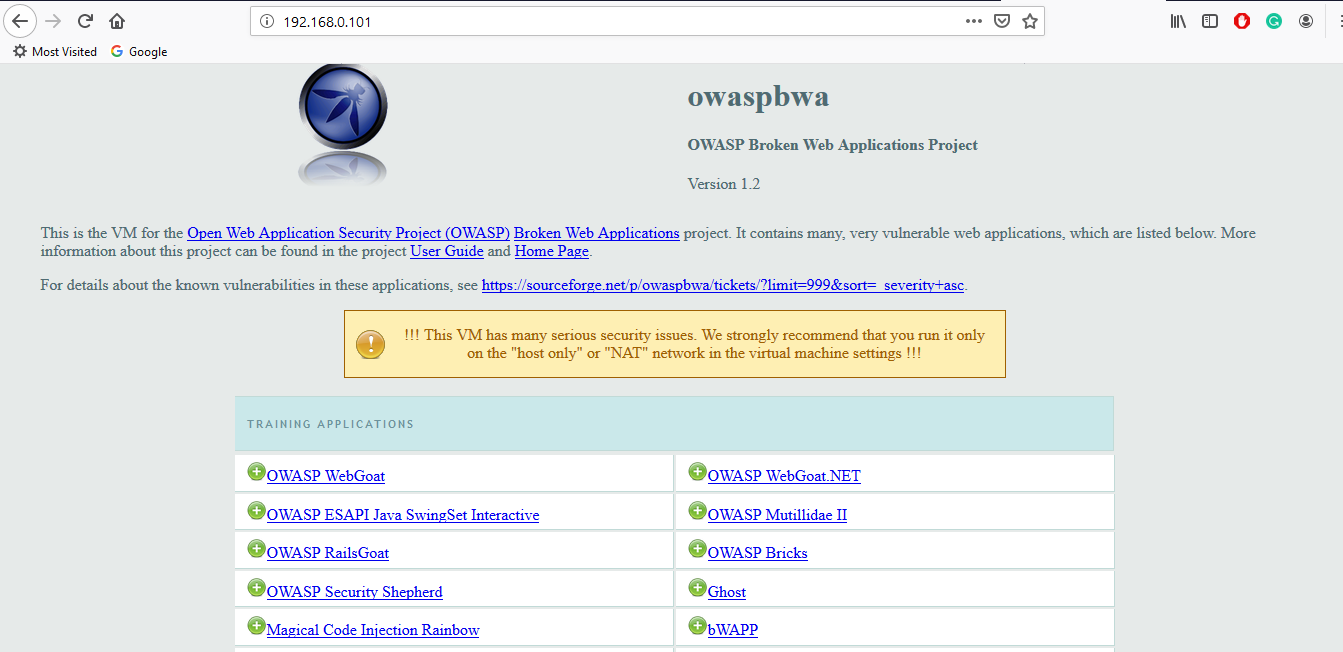
1. Start the machine, run the ifconfig command to get the address

****

1. Implementation
2. Proxy

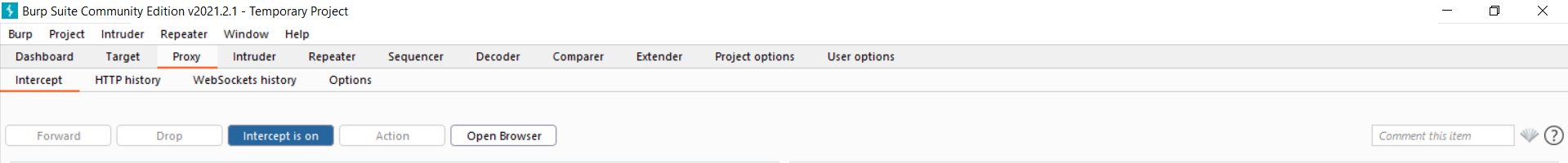
Using Burpsuite as a proxy

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:

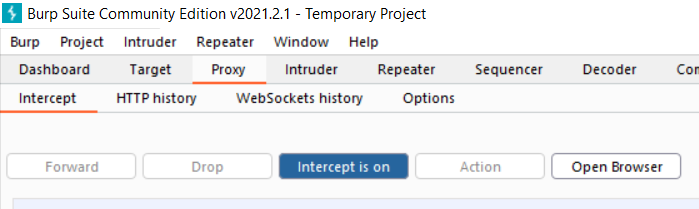
1. Go to the proxy tab and select the intercept option



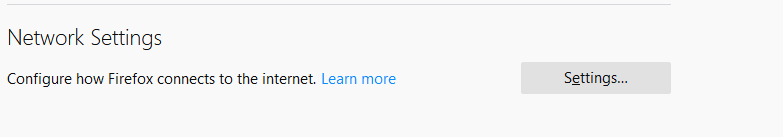
1. Select Options category and check if the proxy is listening on localhost, port 8080



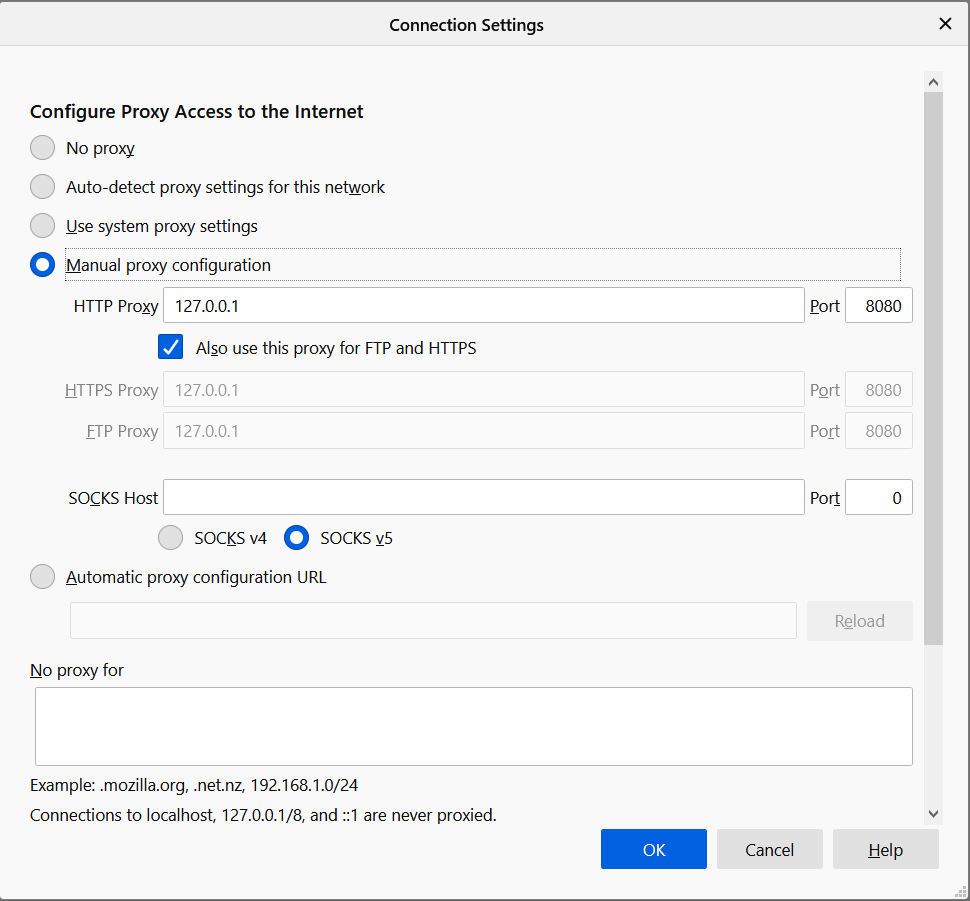
1. Turn the intercept on



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



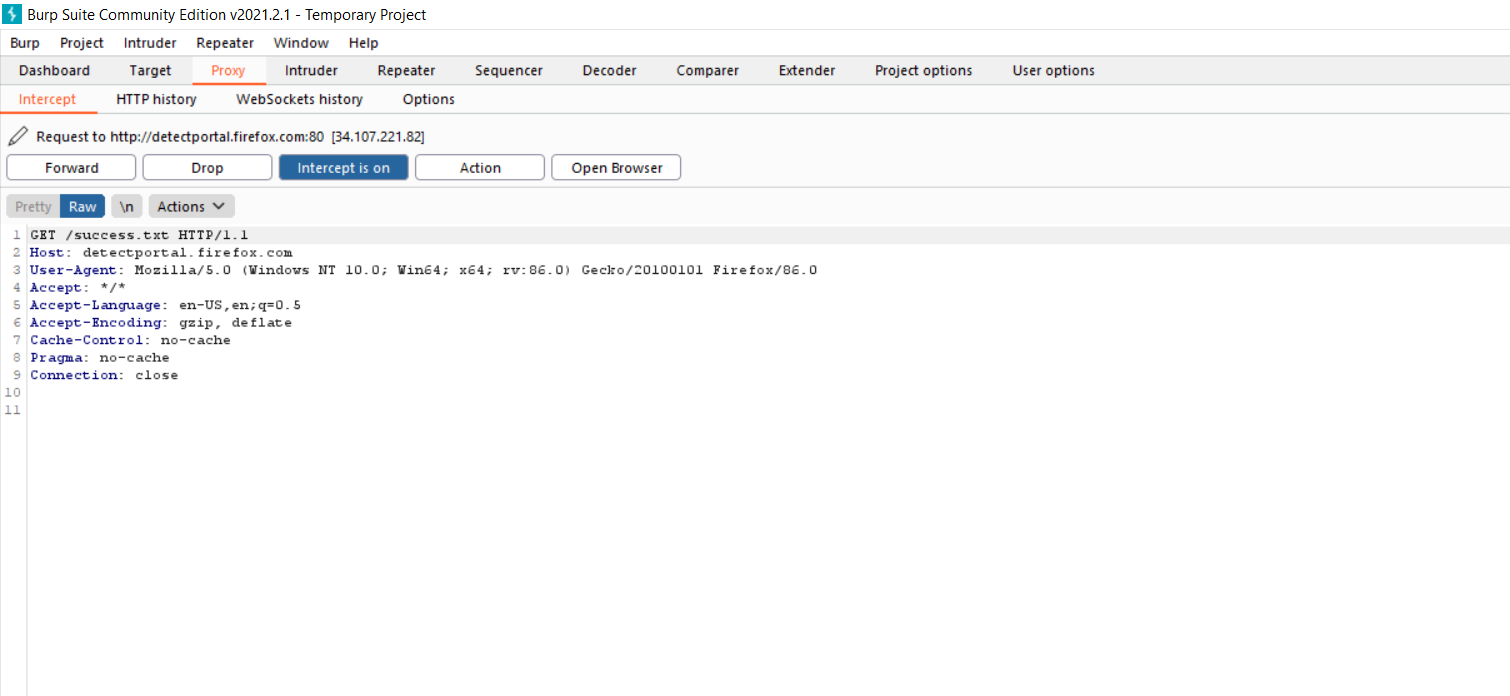
1. Select manual proxy configuration



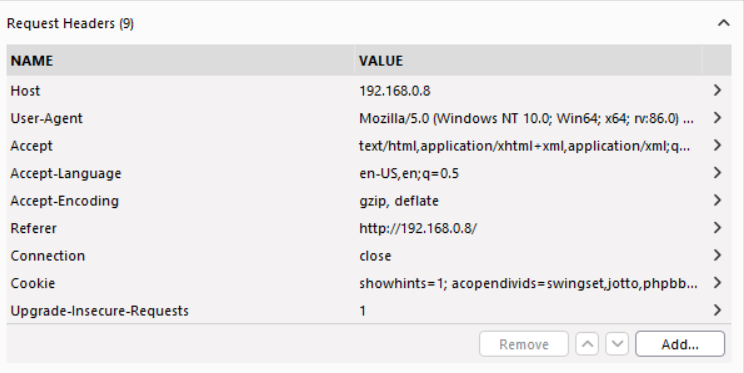
1. Click on Owasp mutillidae – II



1. The following data is shown

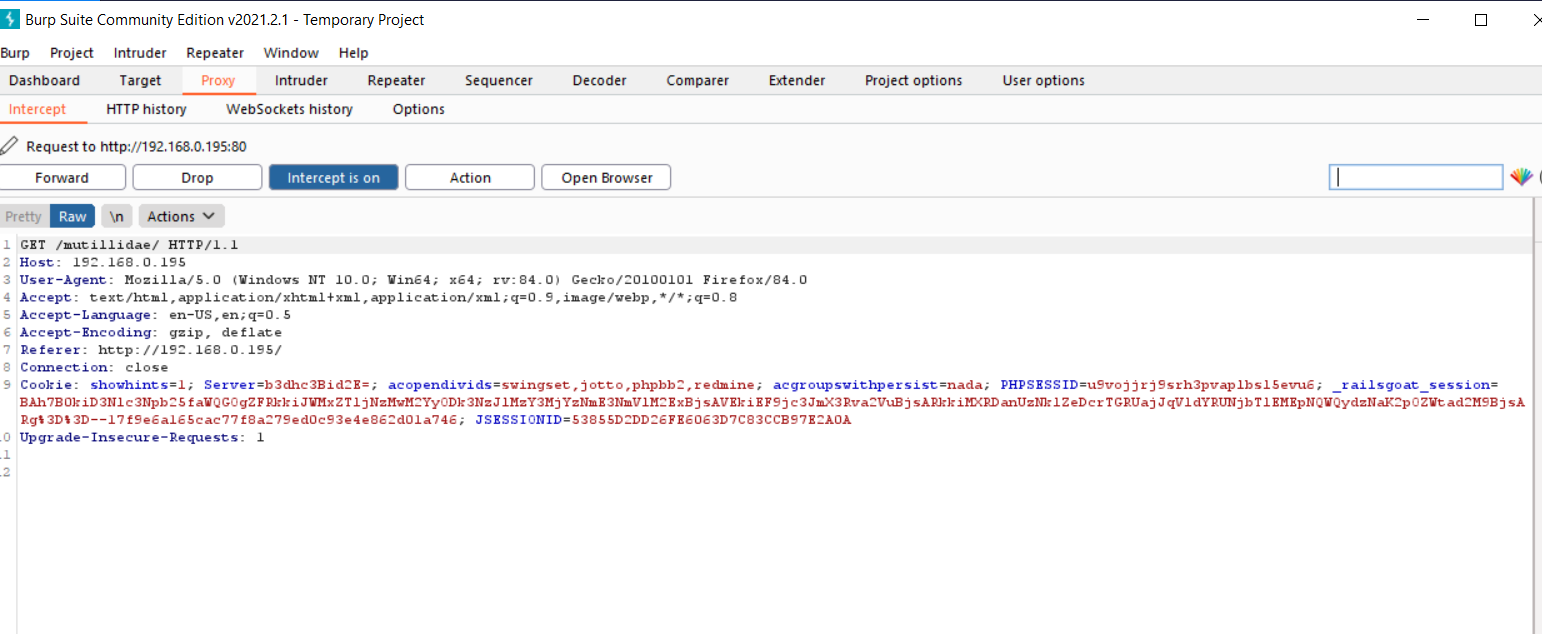


1. The header format is as:



2. SiteMap

Click on owasp mutillidae II

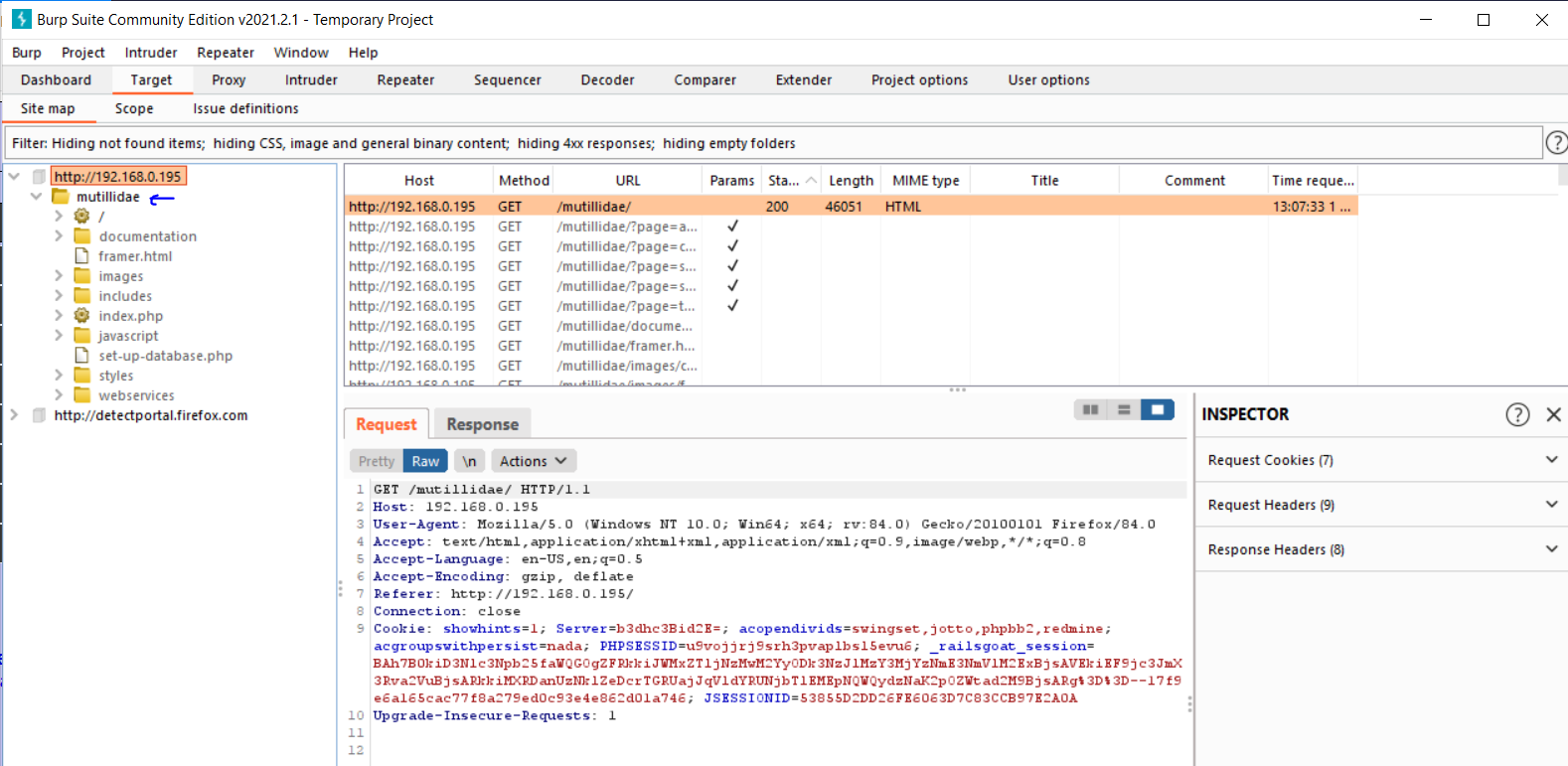
****

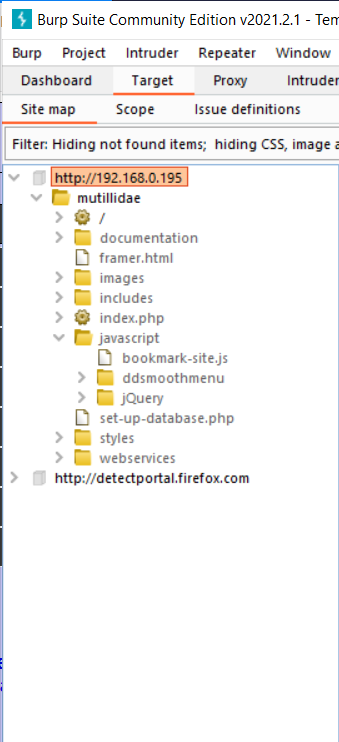
Steps:

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



1. Sitemap is created of the host

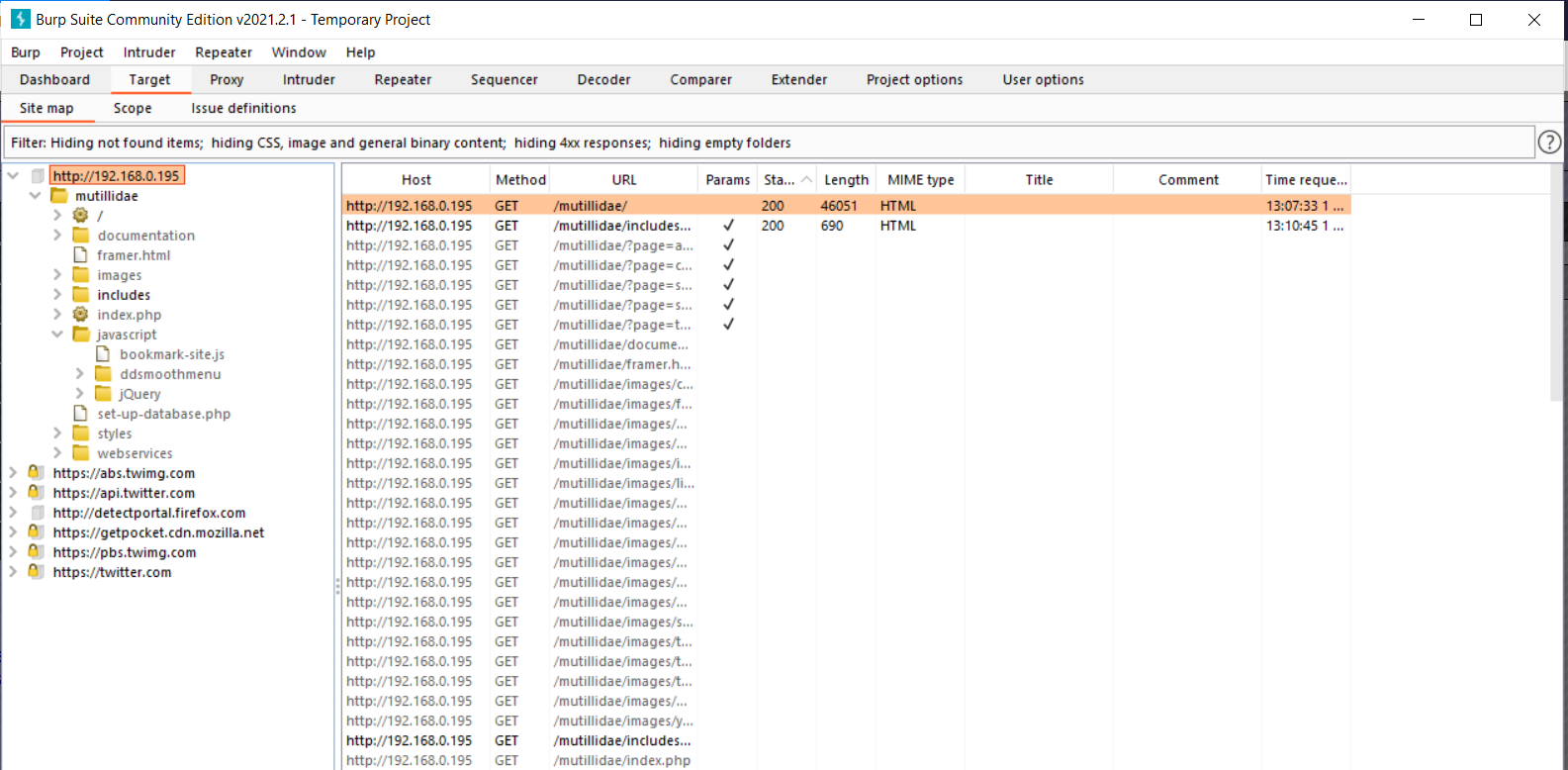


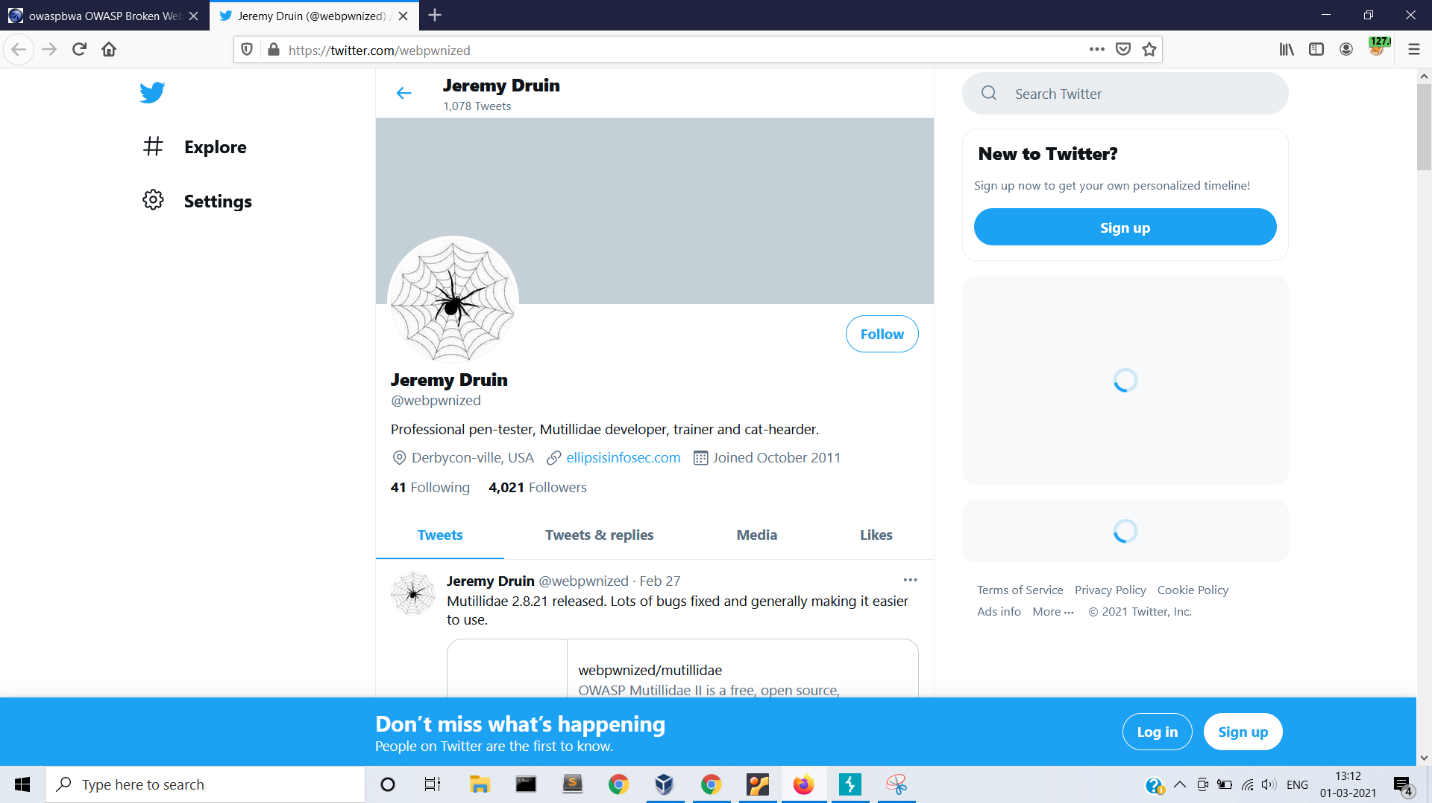


1. Whenever we open a url, Burpsuite stores that URL in the sitemap. Now sitemap of mutillidae is created.

Burpsuite spider crawls the entire website and store all URLs in that particular

Sitemap.



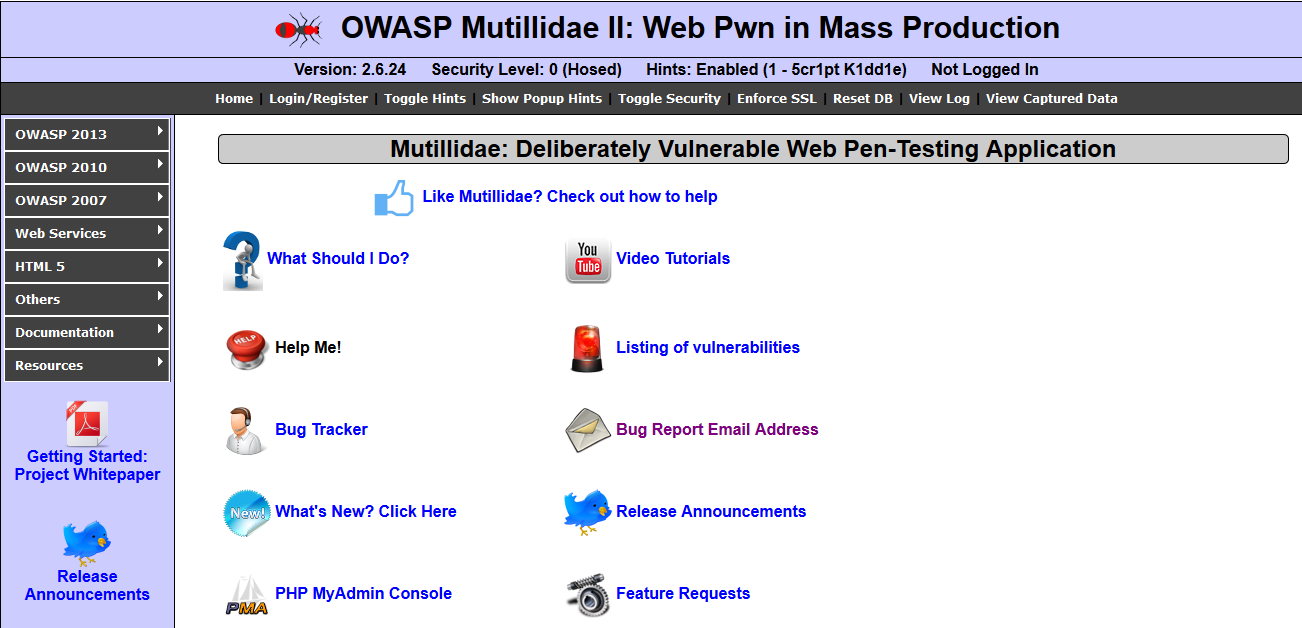


Sitemap of Owasp Bricks

3. Intruder

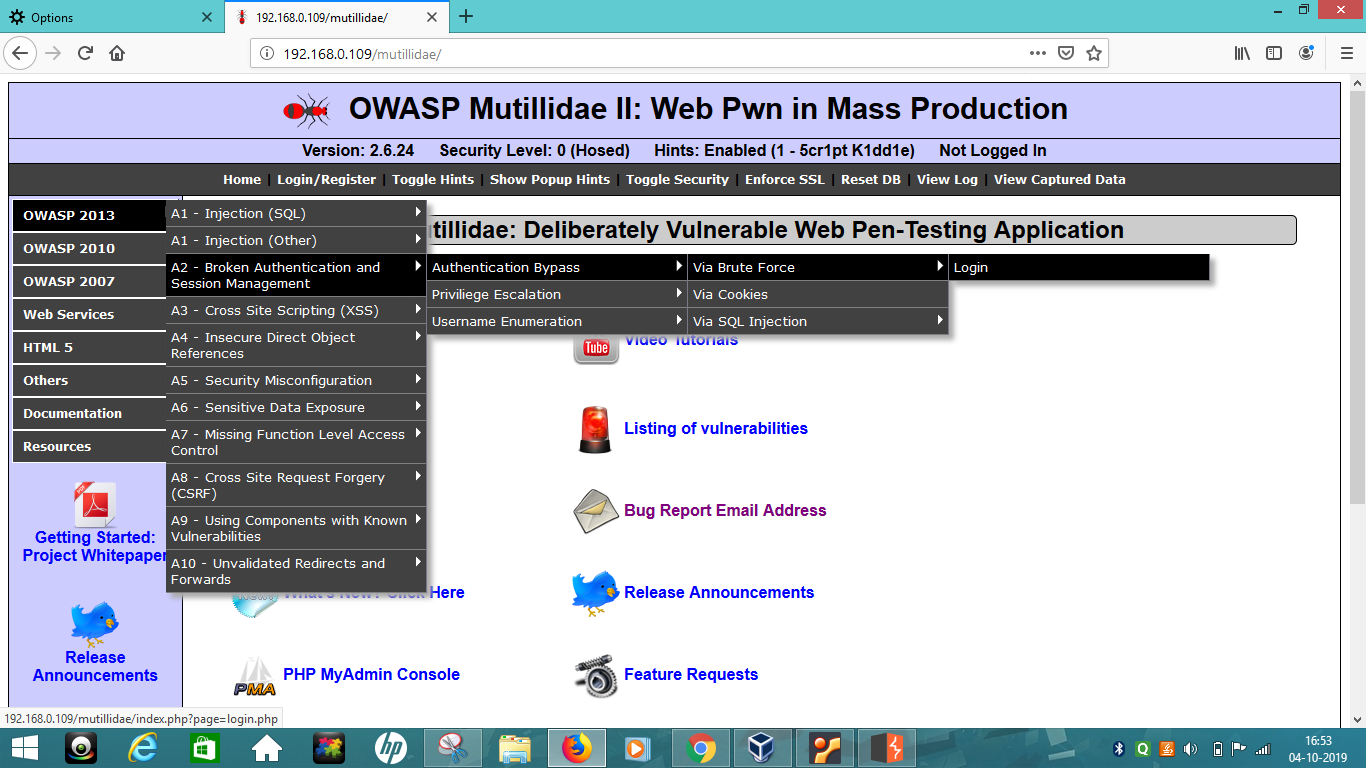
Used to crack passwords and automate request tampering

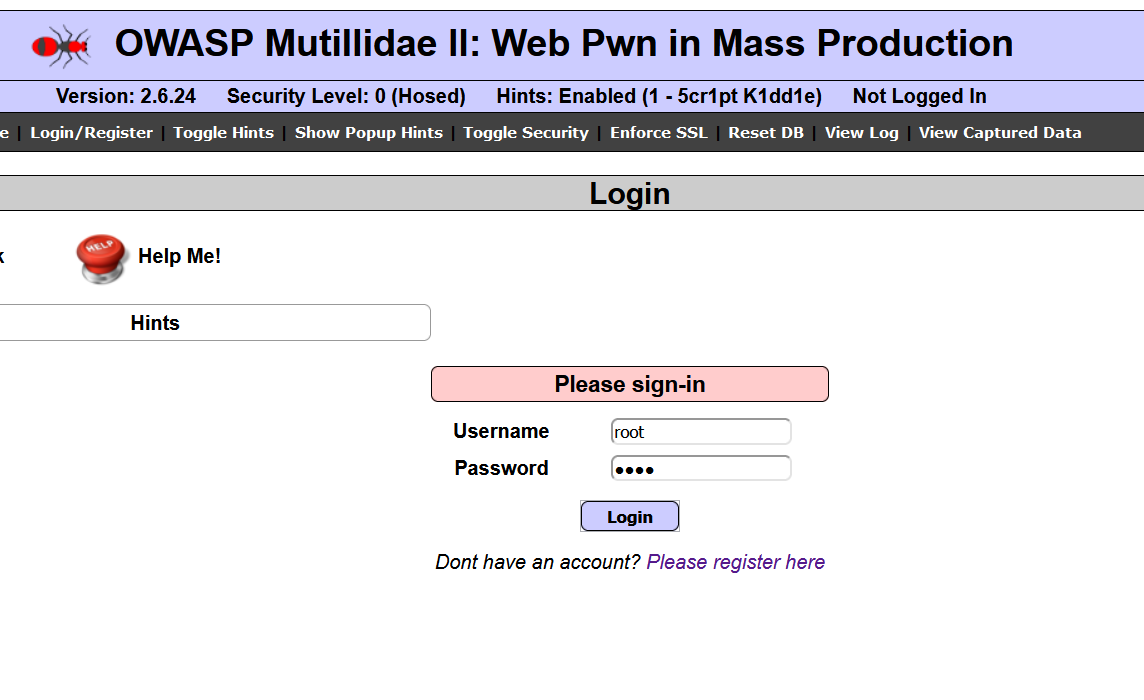
Open owasp mutillidae



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

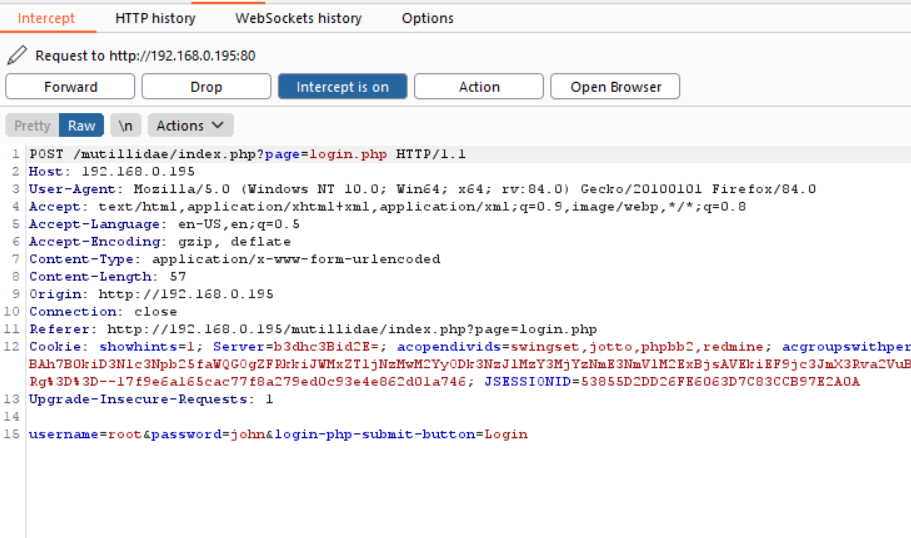
option.



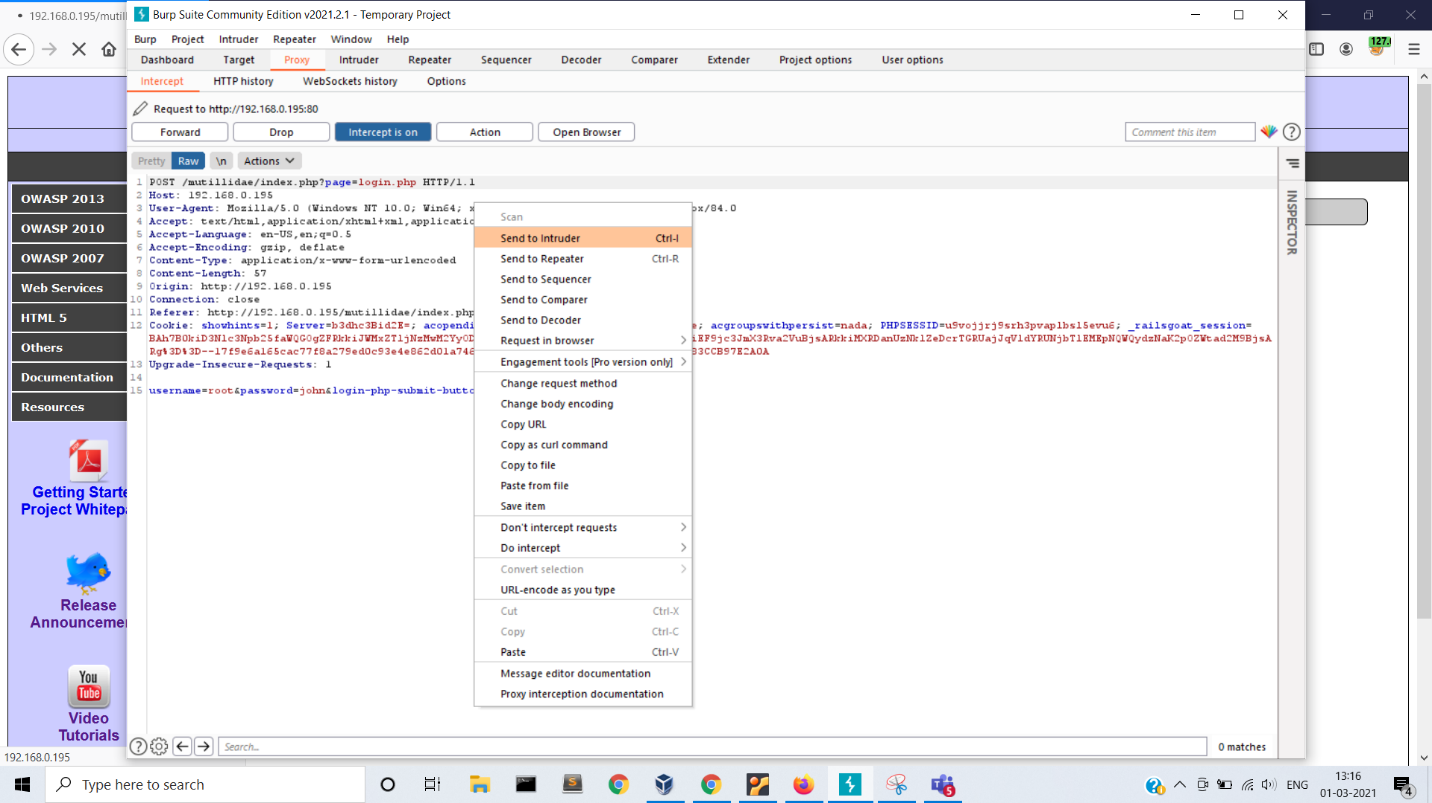
 Enter random credentials for login

‘

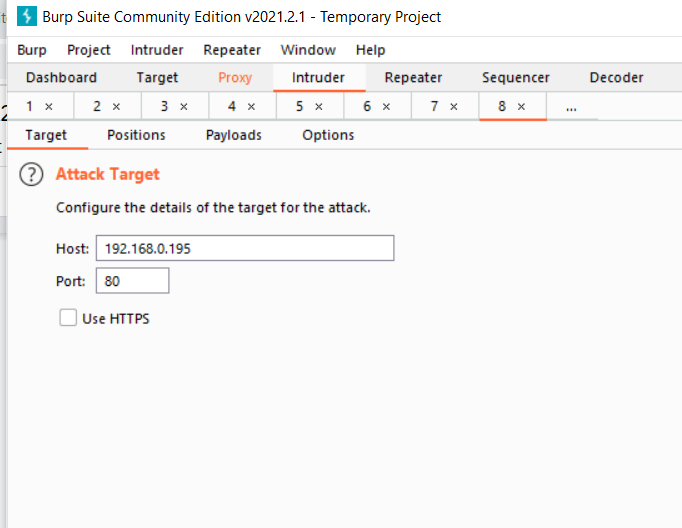
Check the request on burpsuite:



Right click and select send to intruder:



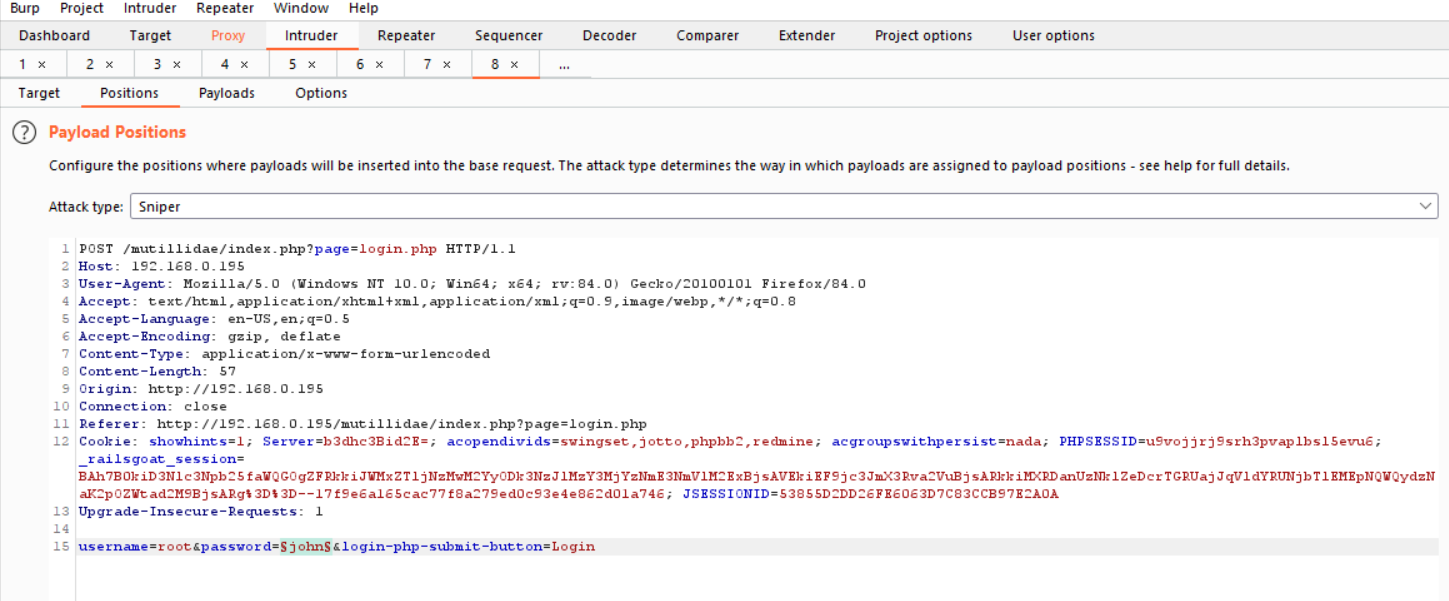
Now open the intruder tab:

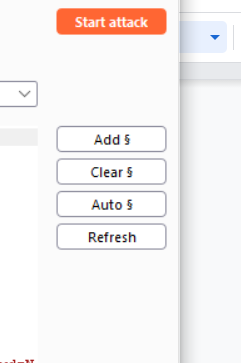


Click positions tab to check the variable params

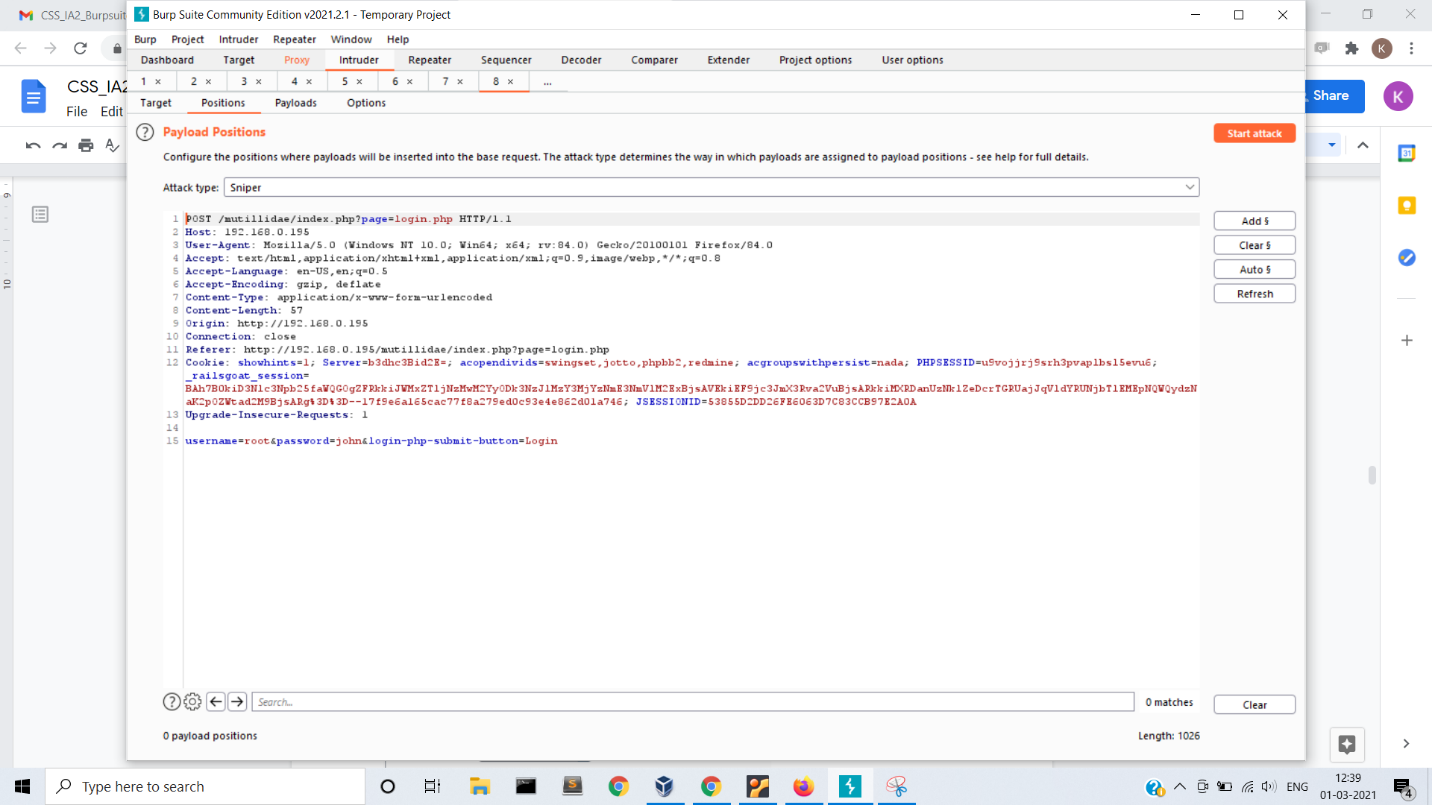
Clear all

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



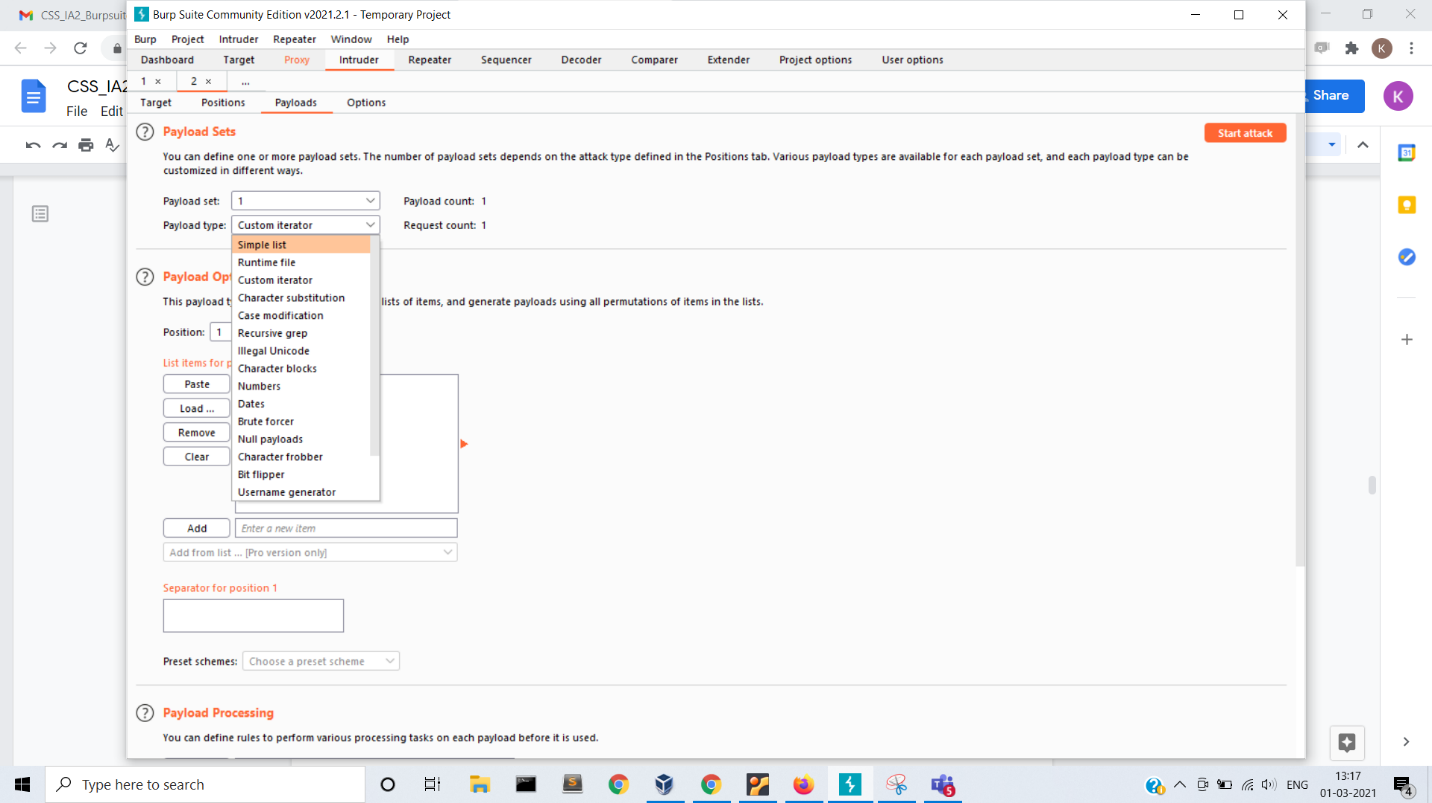


Select attack type as Sniper:

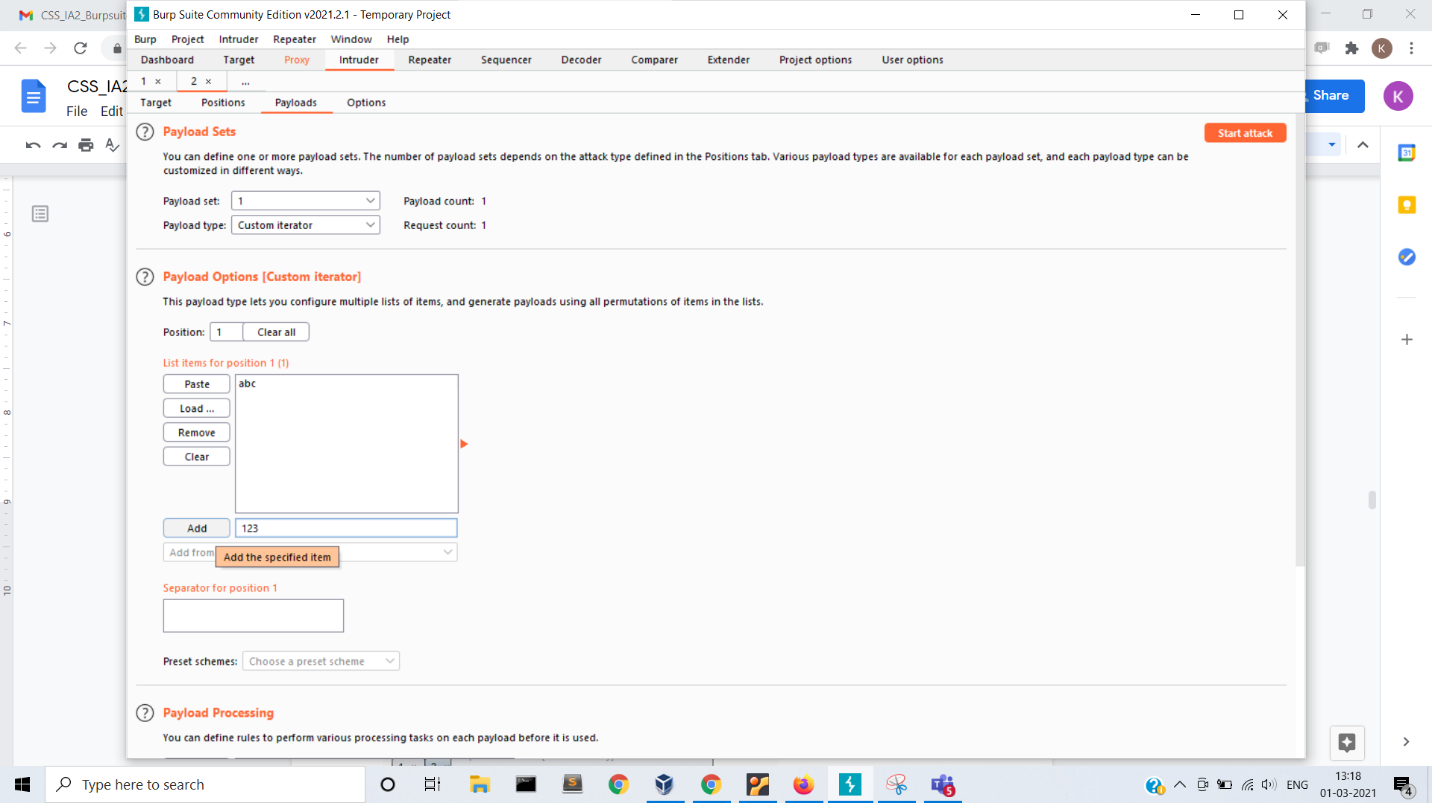


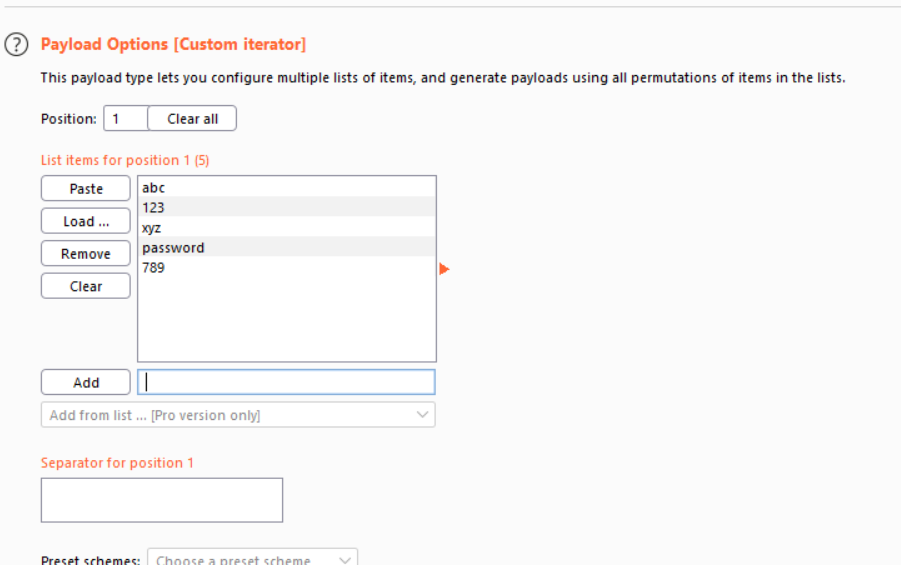
Click on payload tab:

Select payload type as simple list

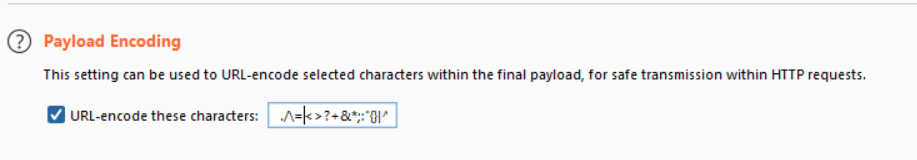


Enter a list of words:

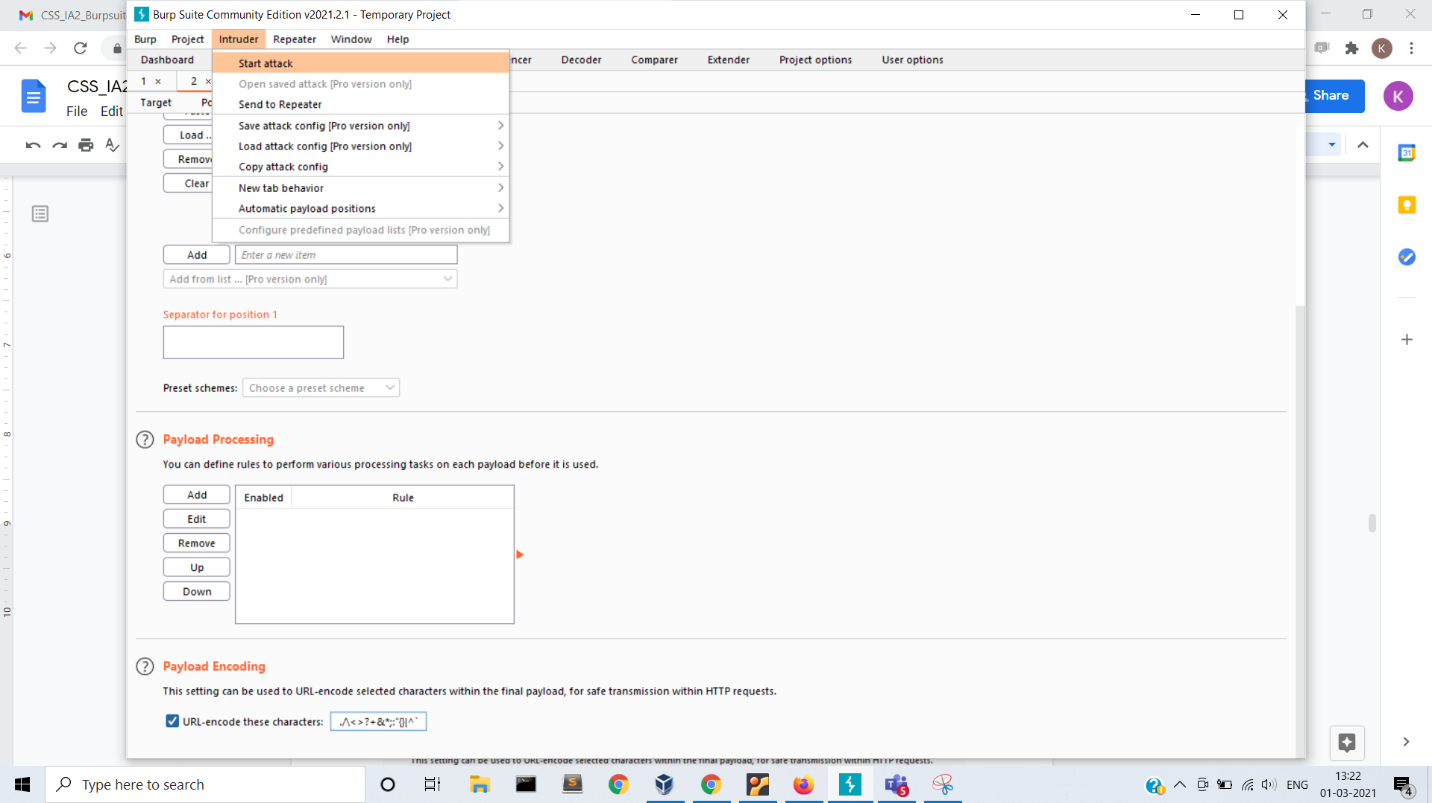




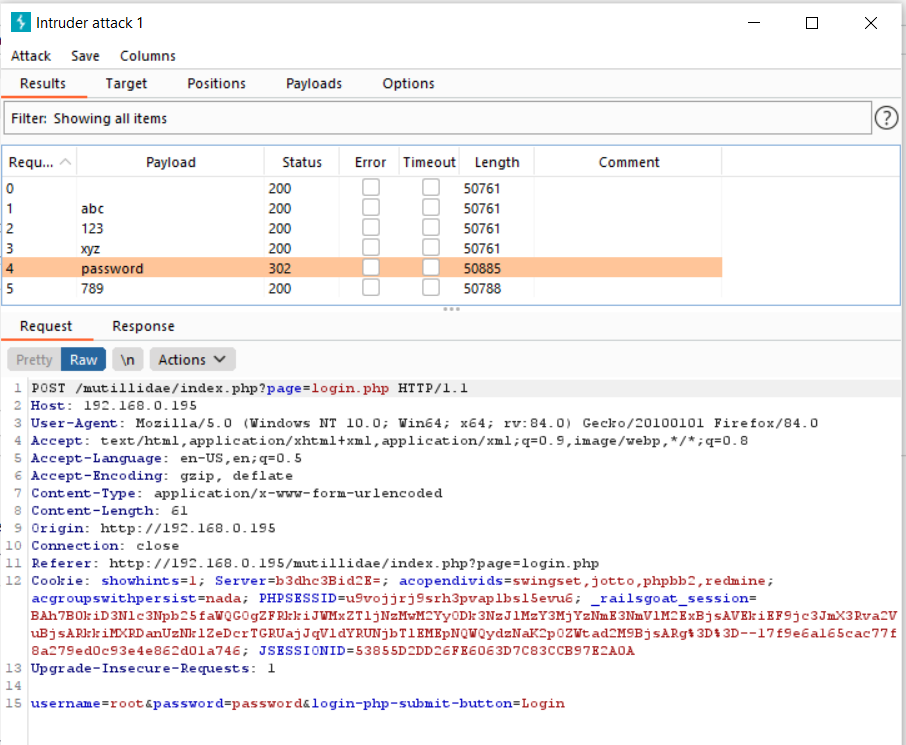
Remove the equal to sign from payload encoding:



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

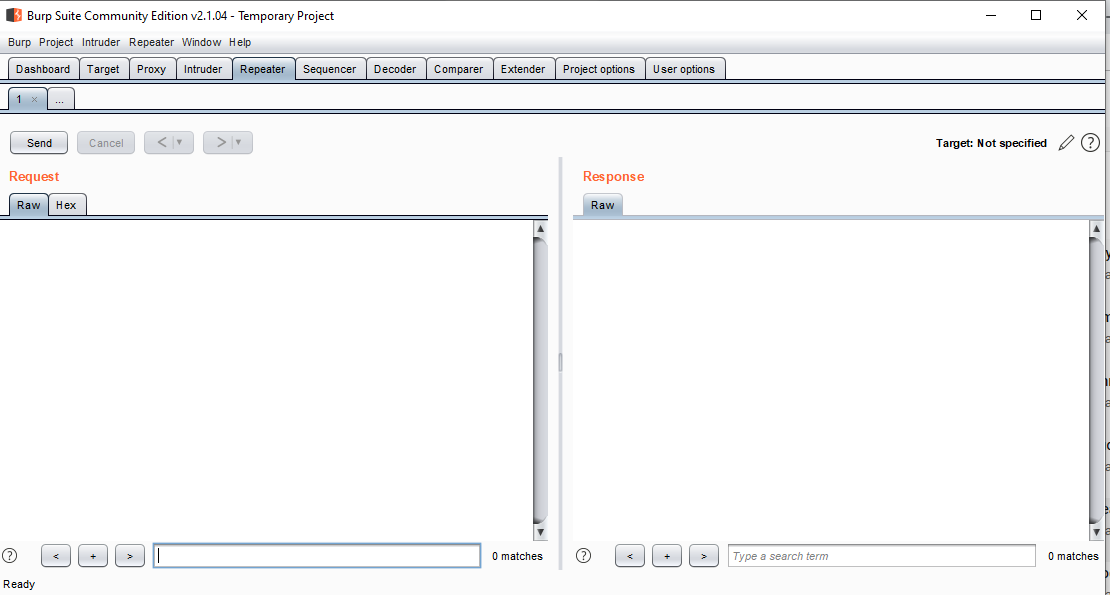


1. Repeater

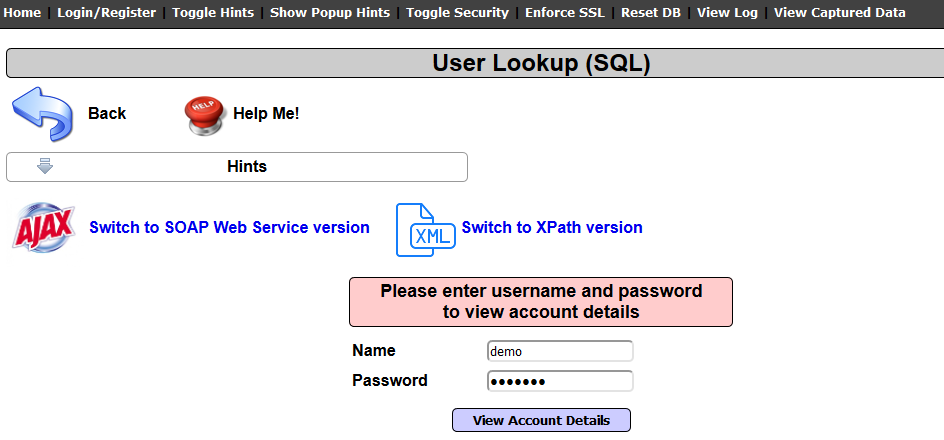
Used to send multiple Http requests.

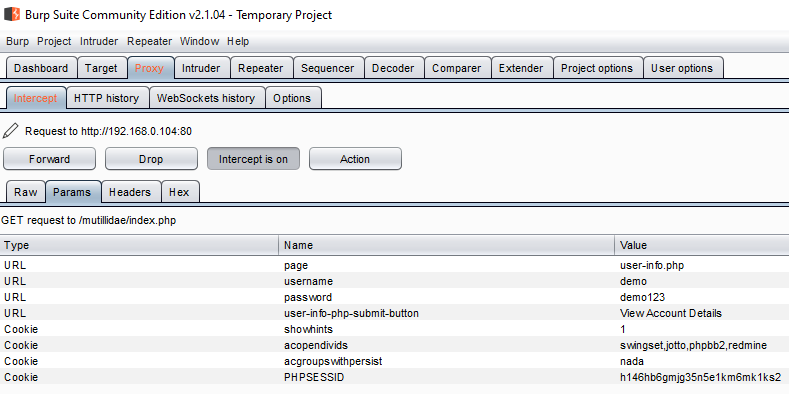
Server response can be monitored

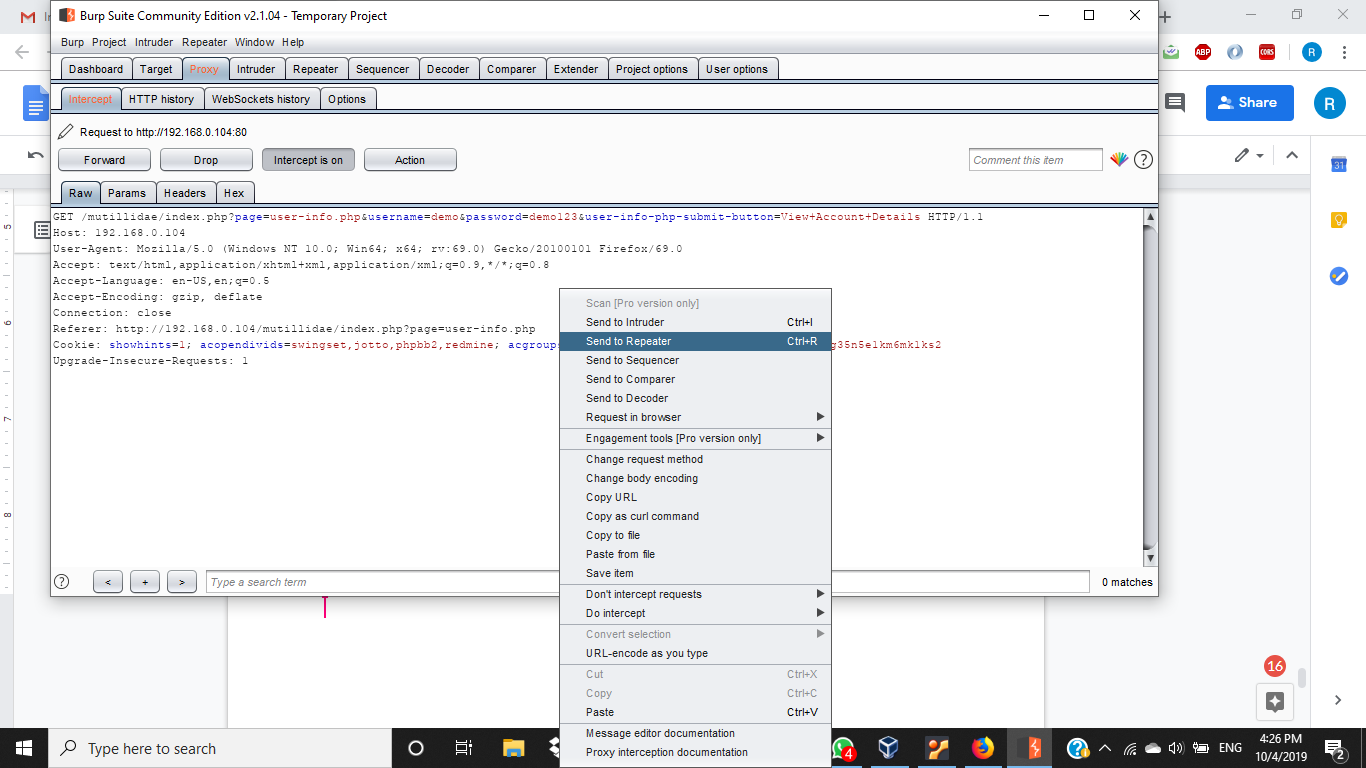
Initial view:

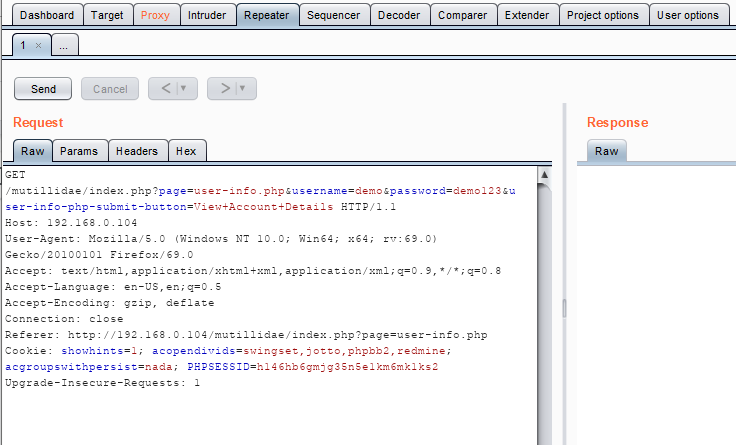


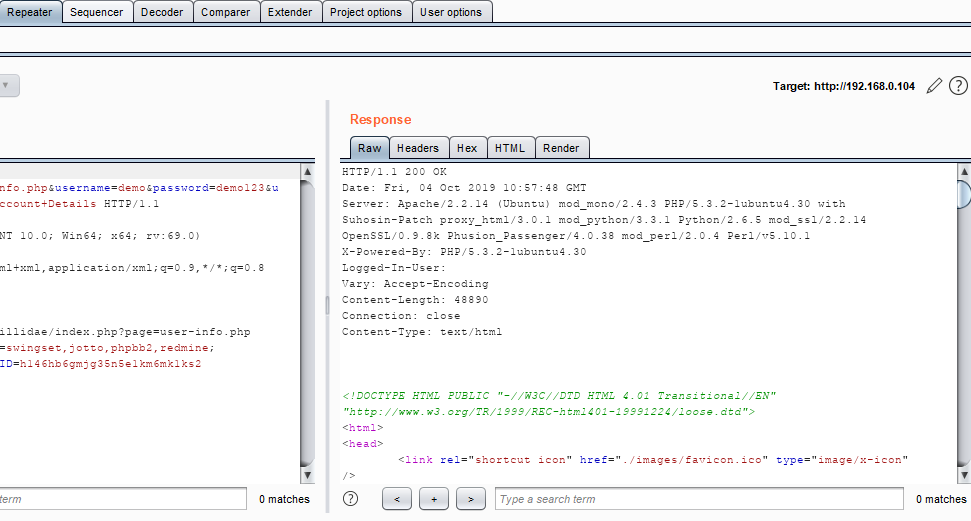




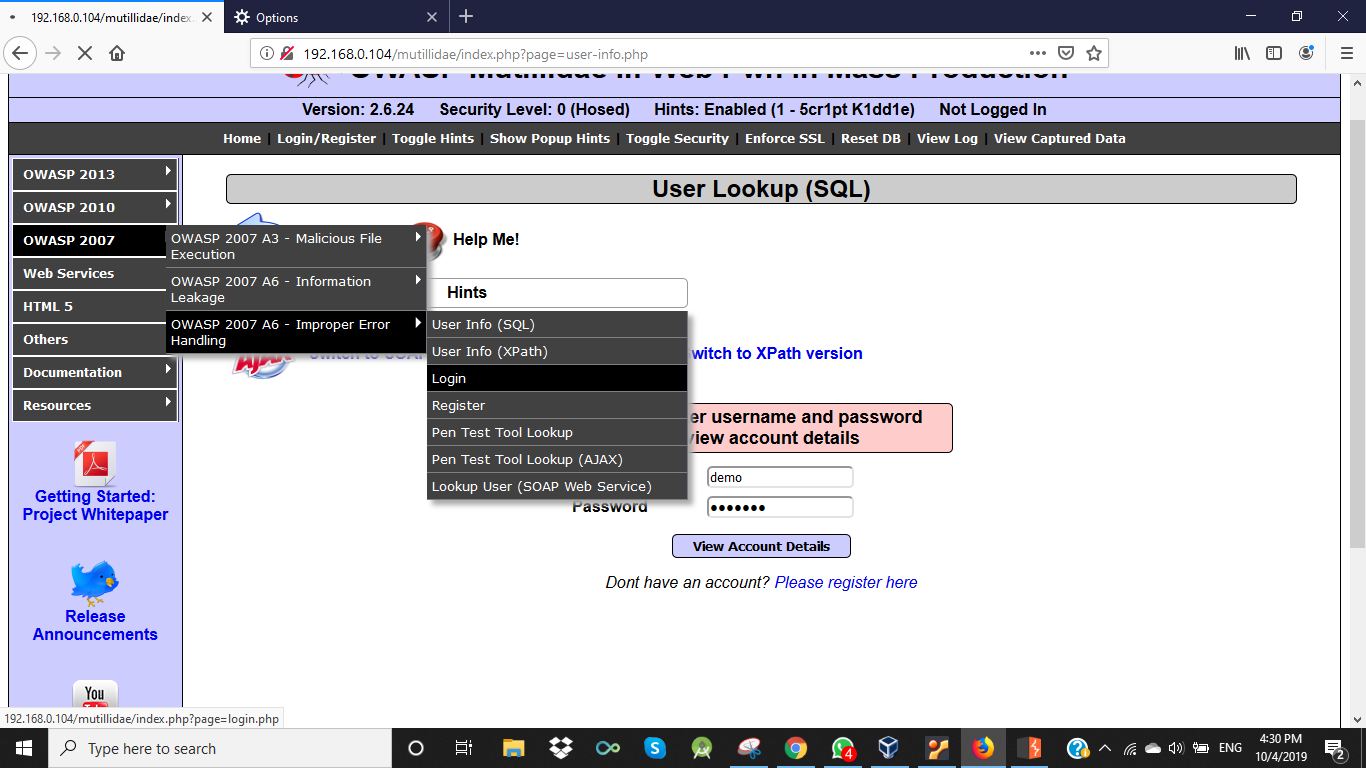


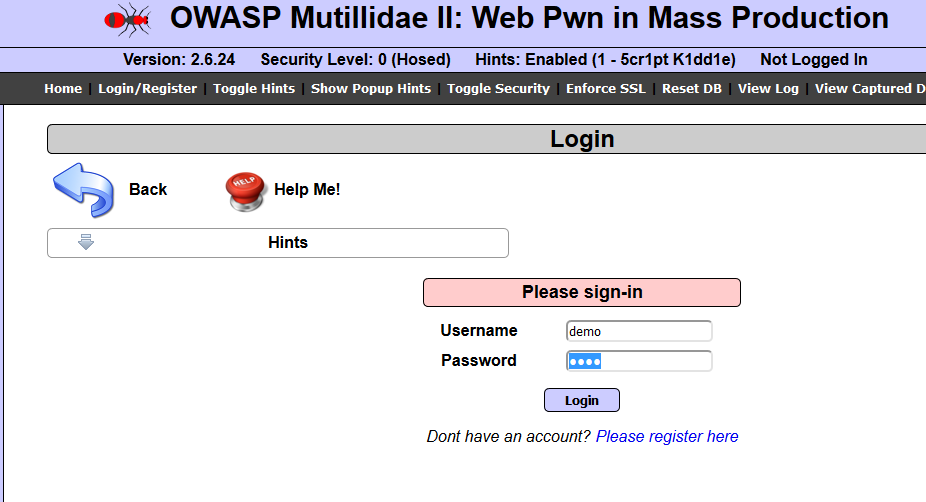




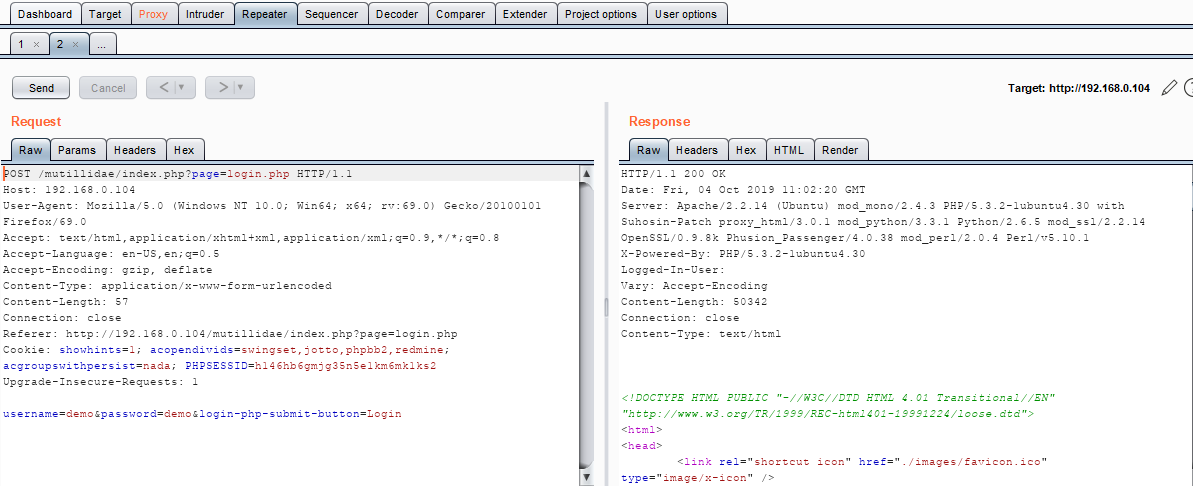
On clicking send, we get the response

Improper error handling – login

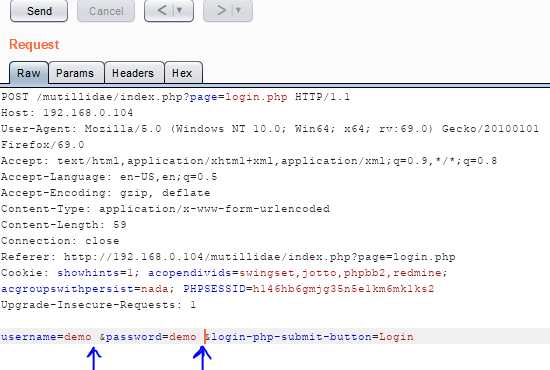




Again send to repeater and click send



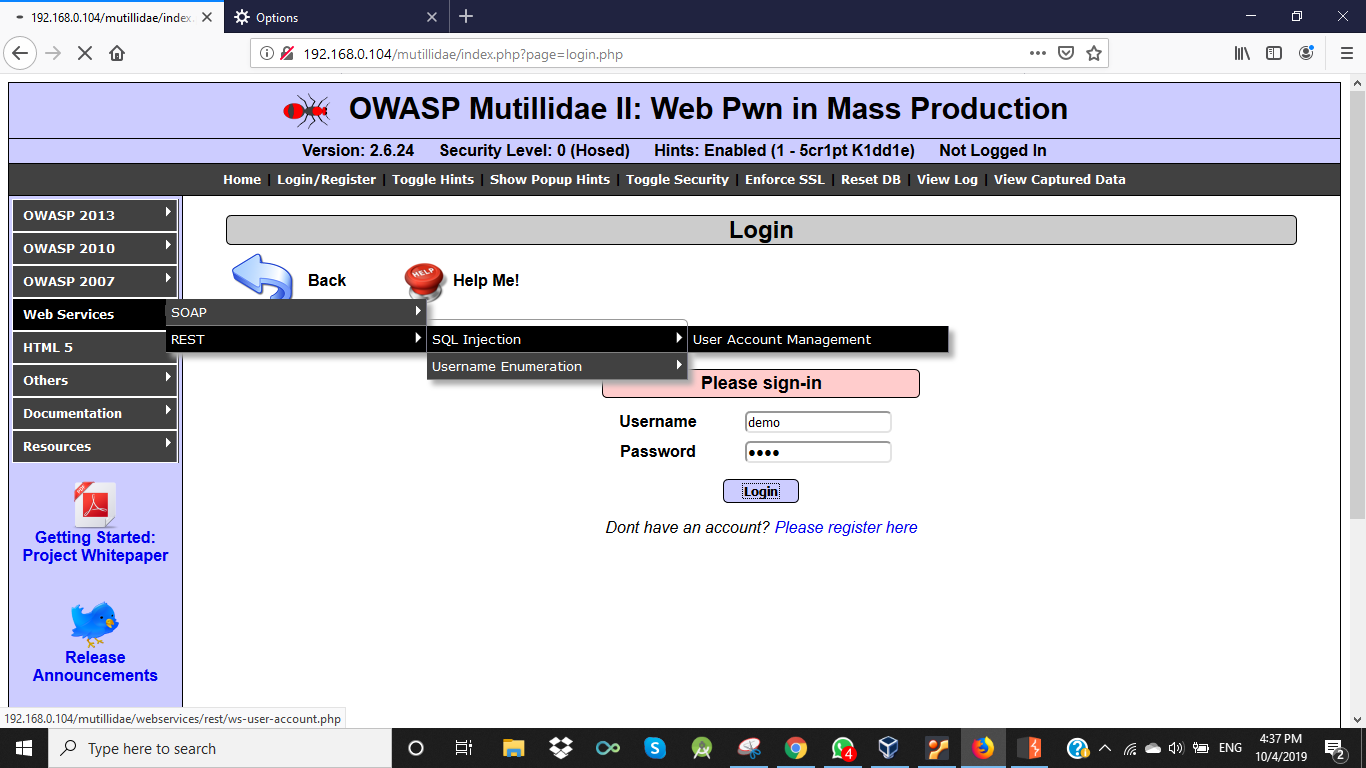
On performing SQL injection, error is shown in response window

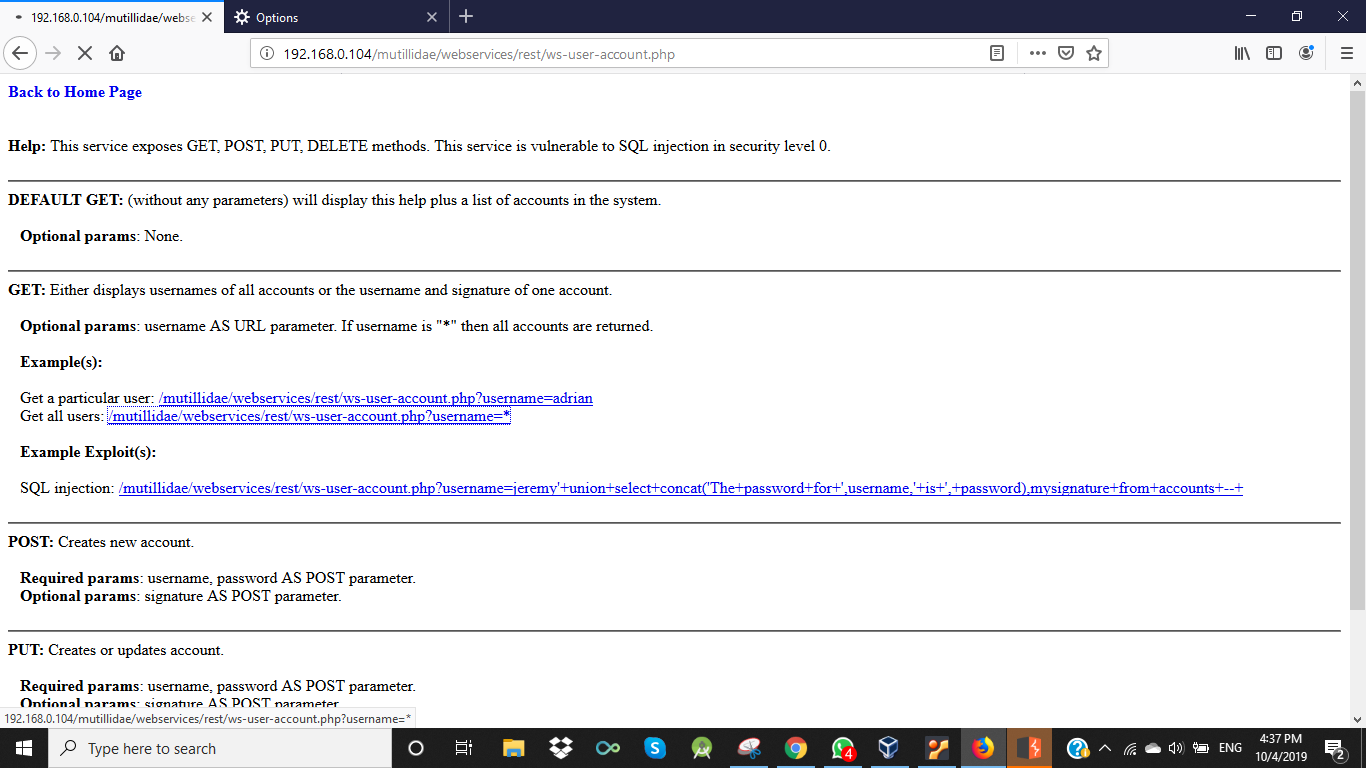


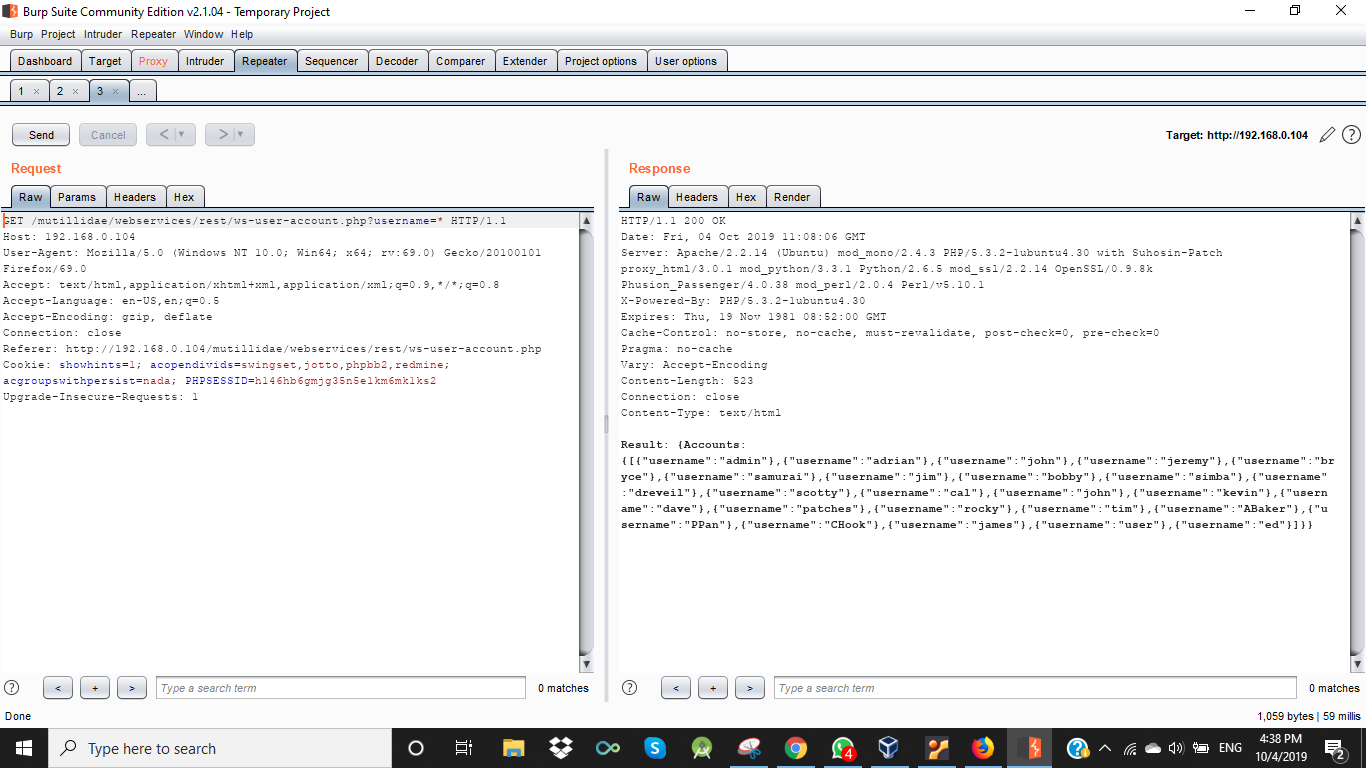
Space was added in the request (SQL injection)



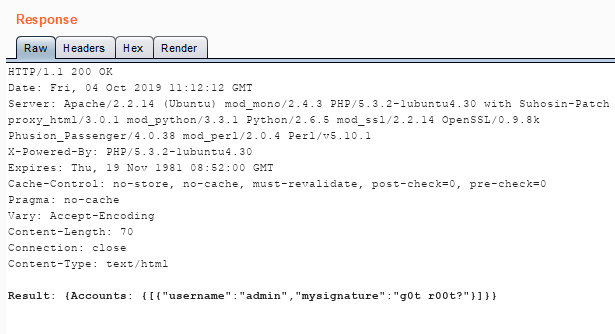
Lastly REST:







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

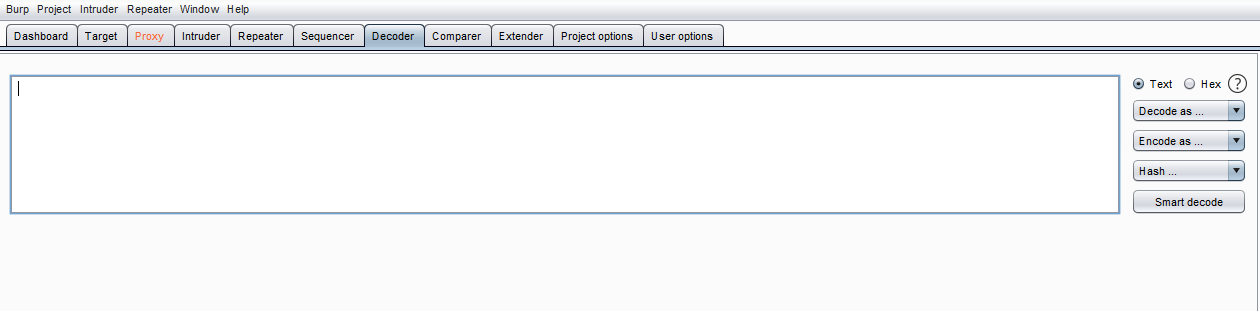
base64

Binary

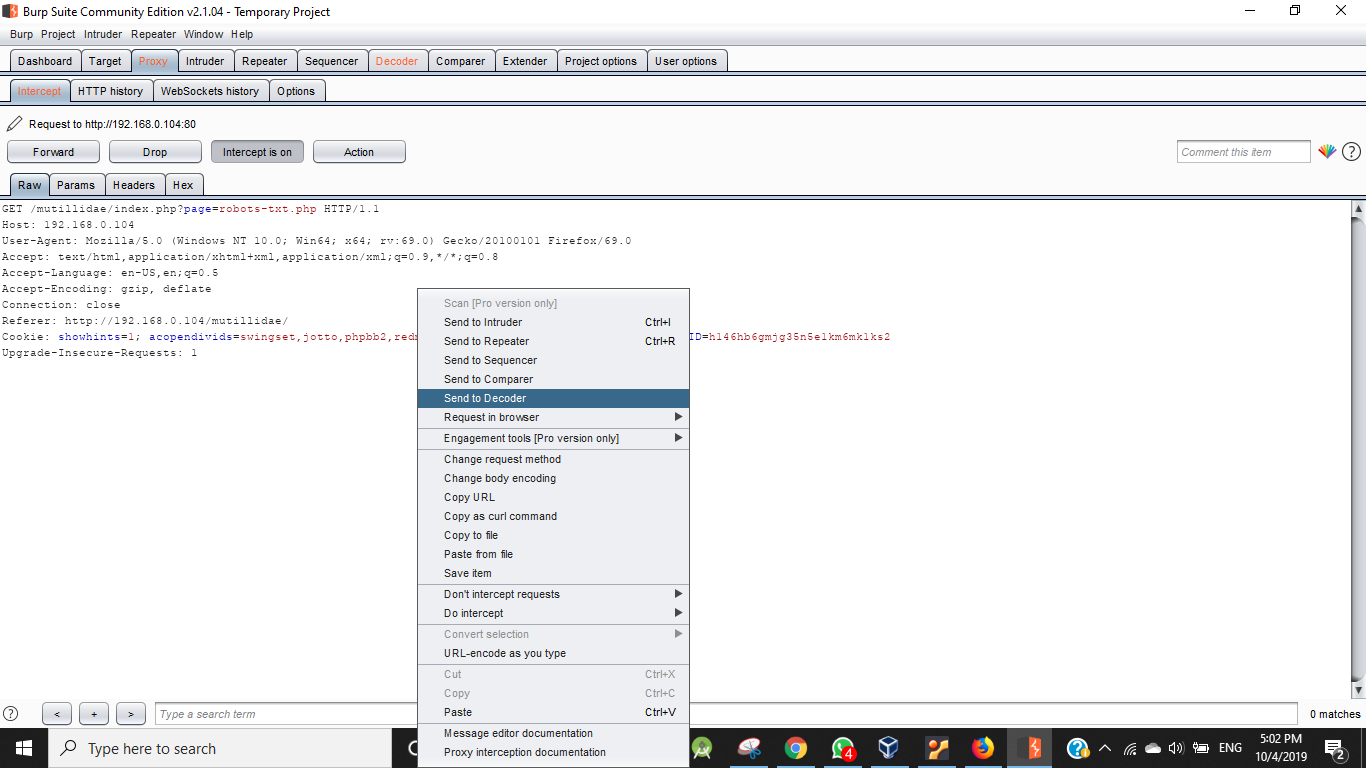
MD5 Hash

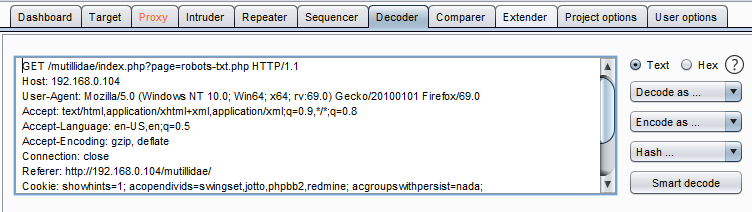
SHA 256 Hash

The decoder tab is as:

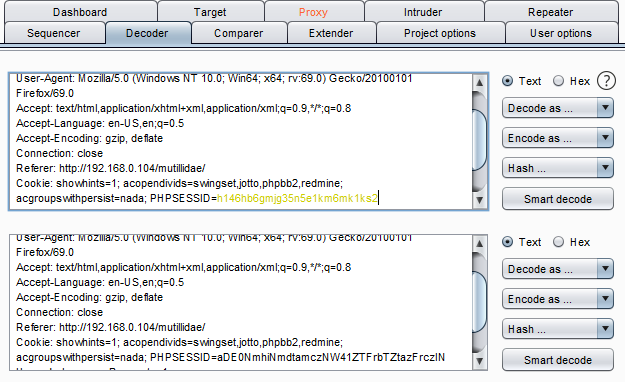




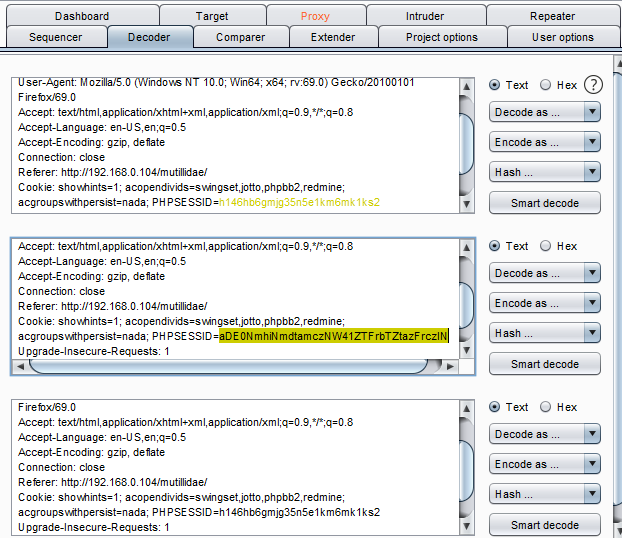


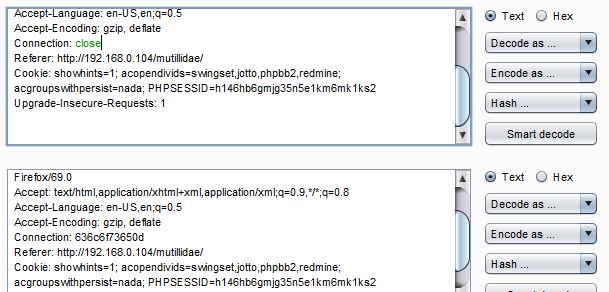


Encoding PHPSESSID into Base64



Decoding it back



 Encoding close to ASCII hex

SHA-256 hash of HELLO

