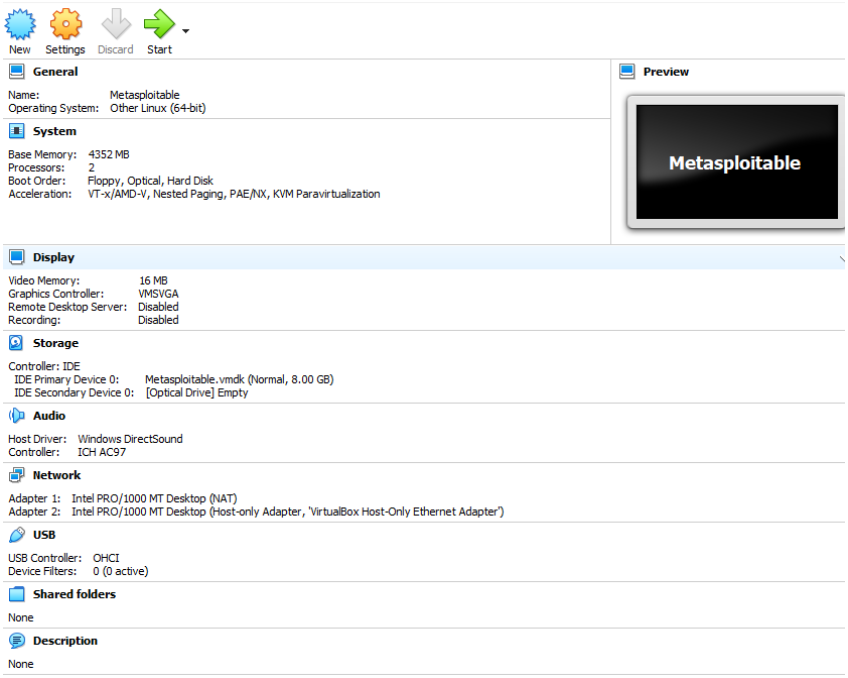
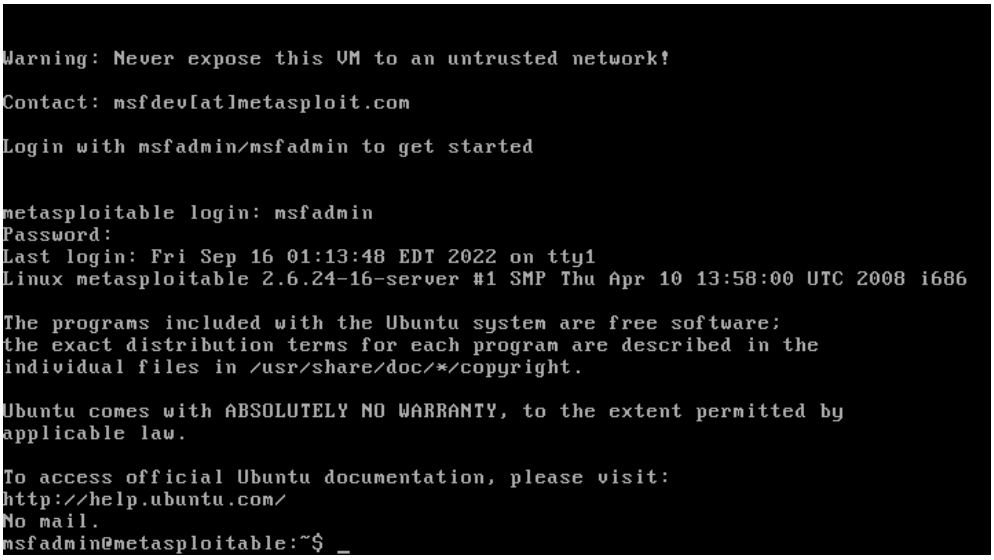
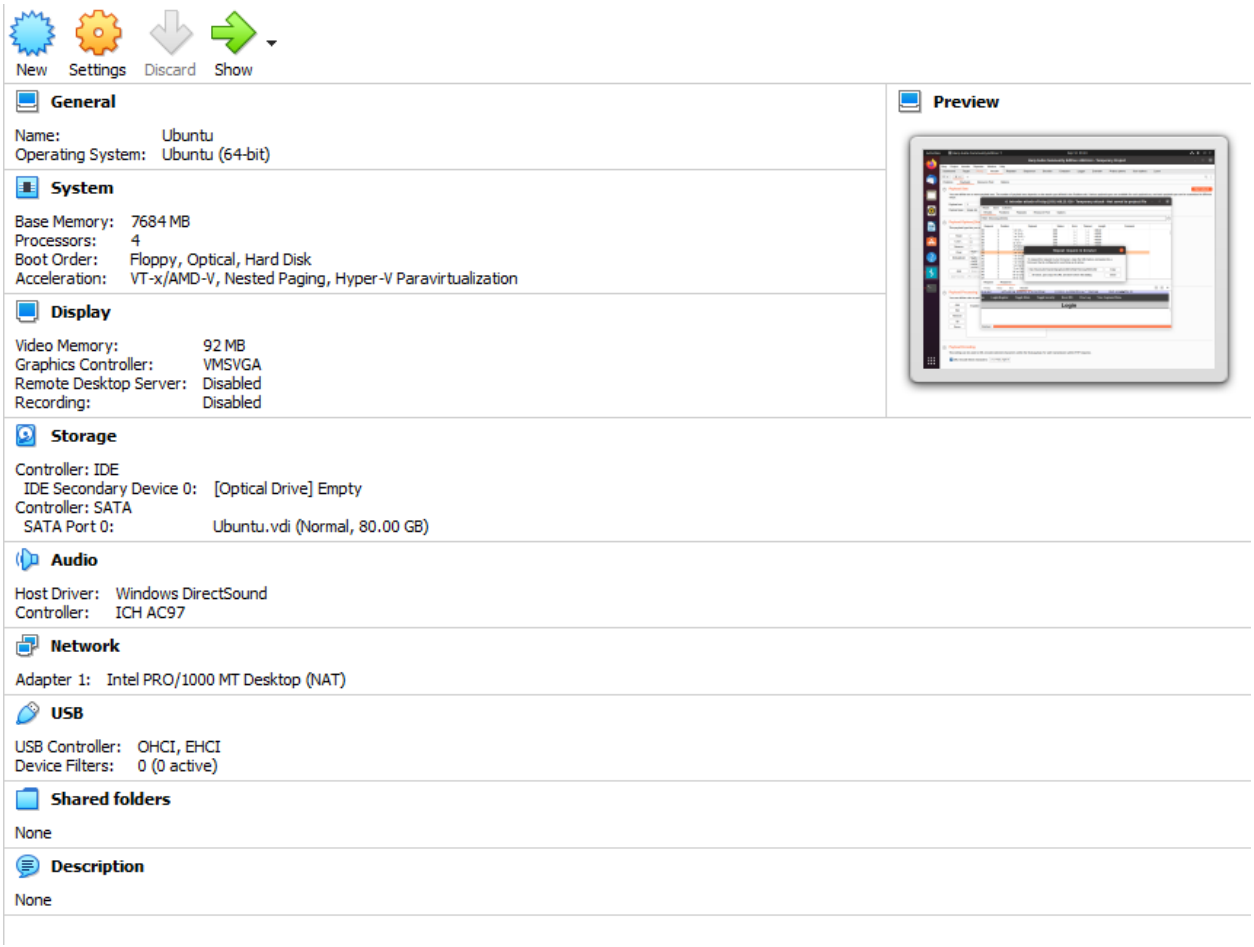
a. Objectives: I will be simulating a SQL Injection to collect usernames and passwords from a web server. I will be injecting SQL code into the username field input box on the web page to gain unauthorized access to user data. I will exploit the fact that SQL code can in put into the username input box.

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





Inaddition, 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 changed to the network adaptor.



c. Tool details:

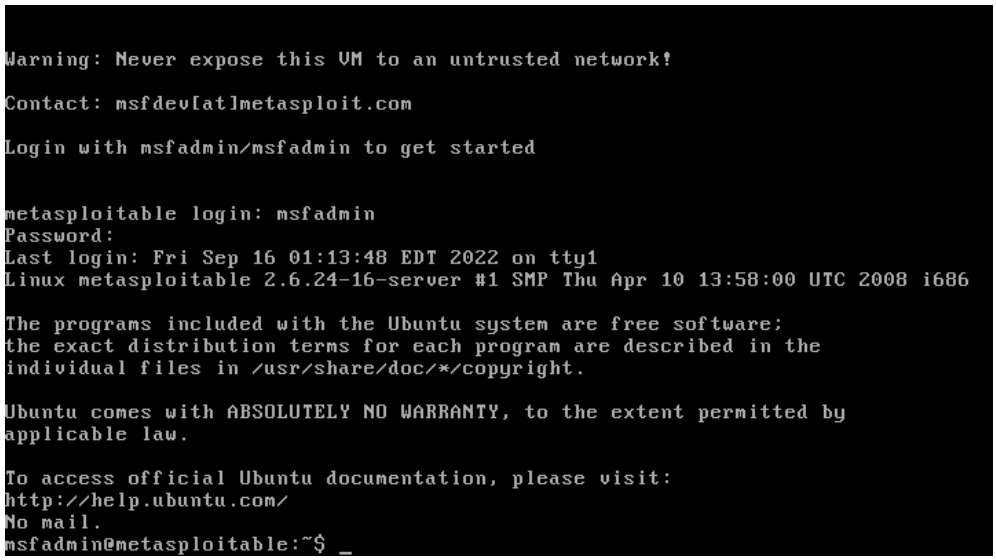
- Burpsuite community edition is from PortSwinger located at https://portswigger.net/burp/releases/professional-community-2022-8-4?requestededition=community&requestedplatform=.
- Current version is 105.0.5195.102 released on September 5, 2022
- It can run on Windows, Linux and MacOS
- Burpsuite is a 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:

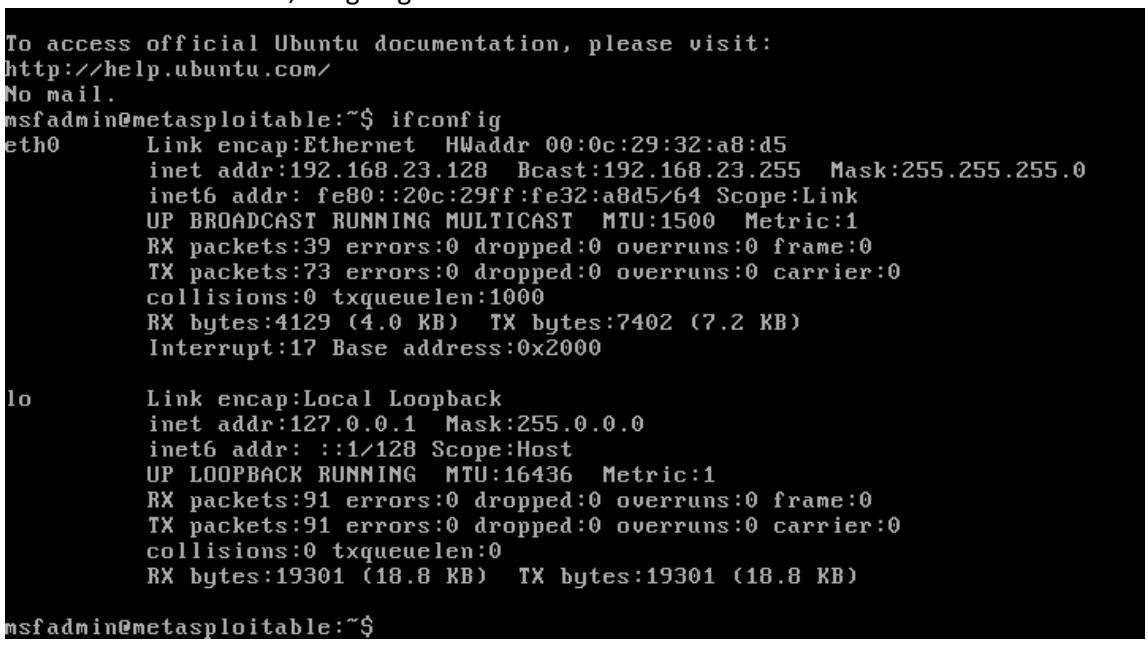
I will be attacking the Mutillidae web app in the Metasploitable VM. Burpsuite will intercept the request sent to the browser and modify the request from the webpage and insert different values to test for SQL injection. My expected outcome is the username and passwords of users in that web app's database.

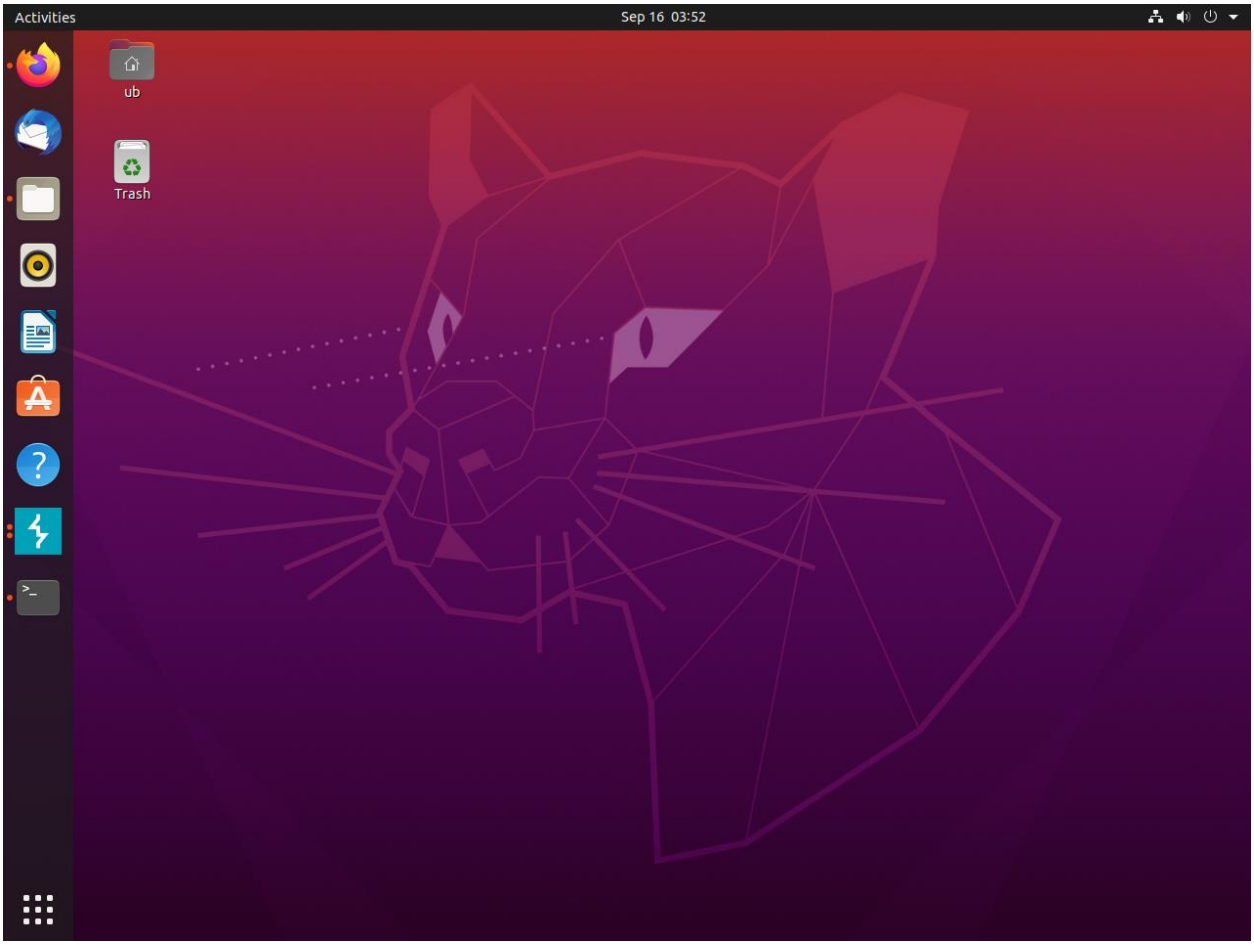
e. Experiment:

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

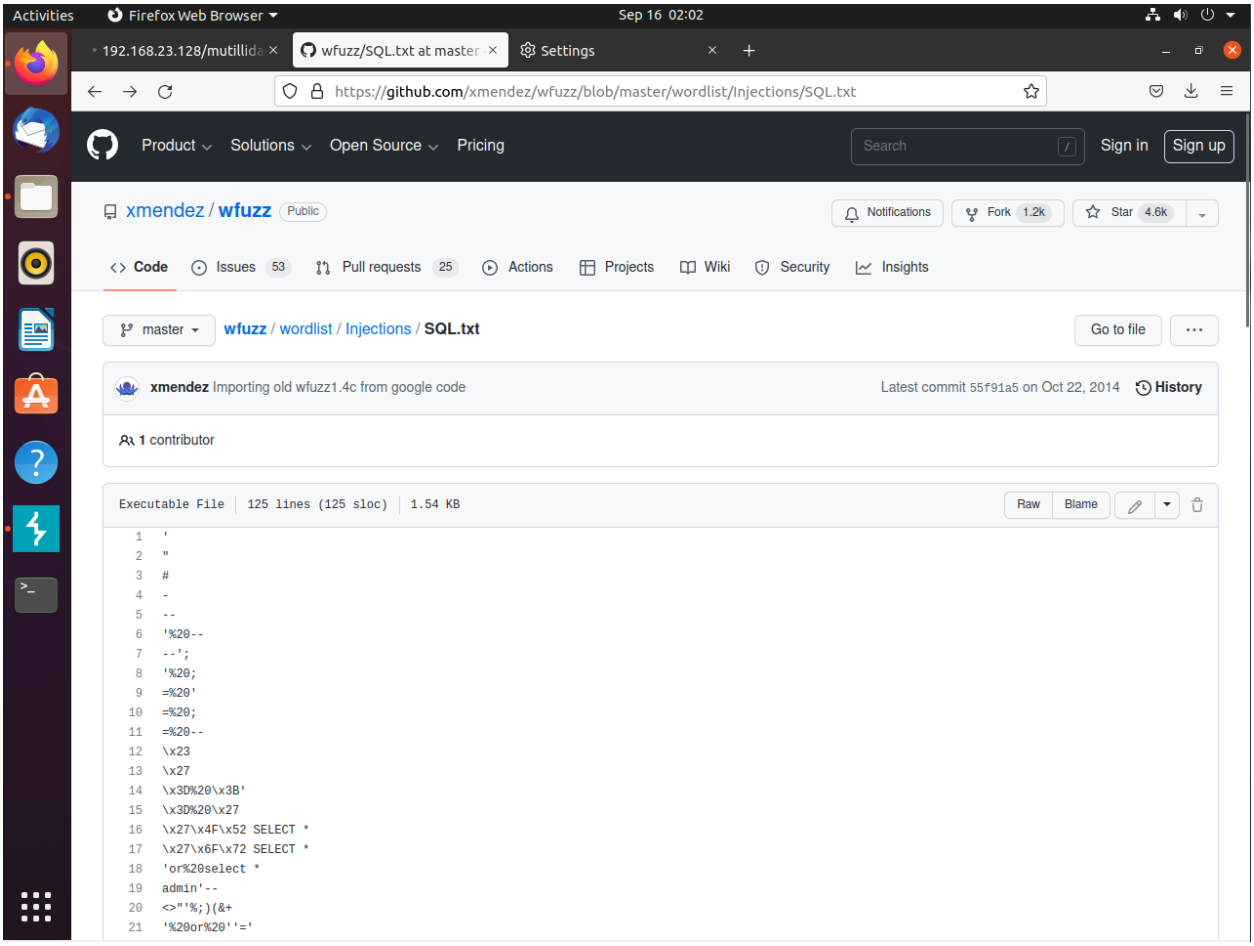


Then at the next prompt type “ifconfig” to get the IP address to connect to the web portal which is the first listed as “int addr:”, it’s going to be a 192.168.x.x IP address.



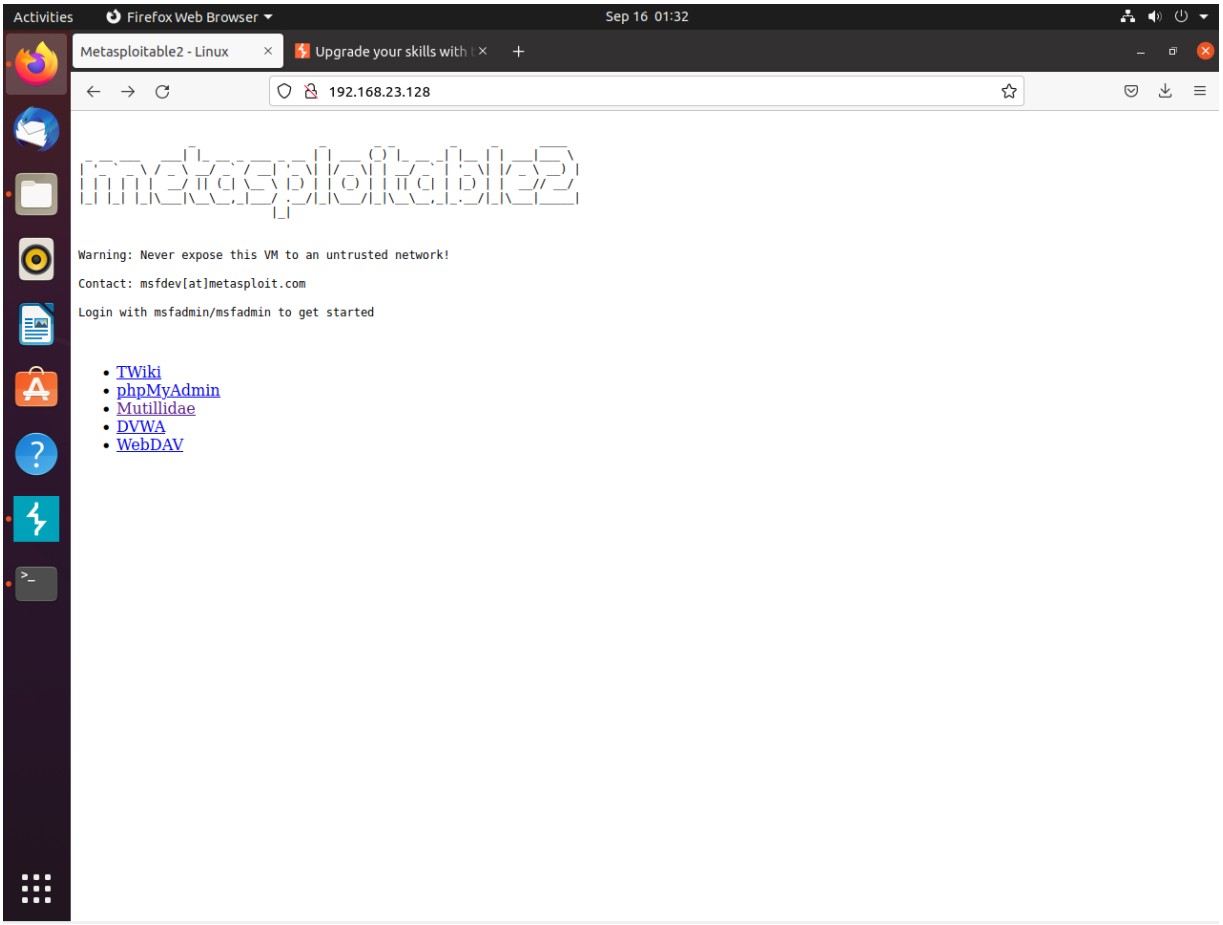


Then, launch the Ubuntu VM and login into the user account.

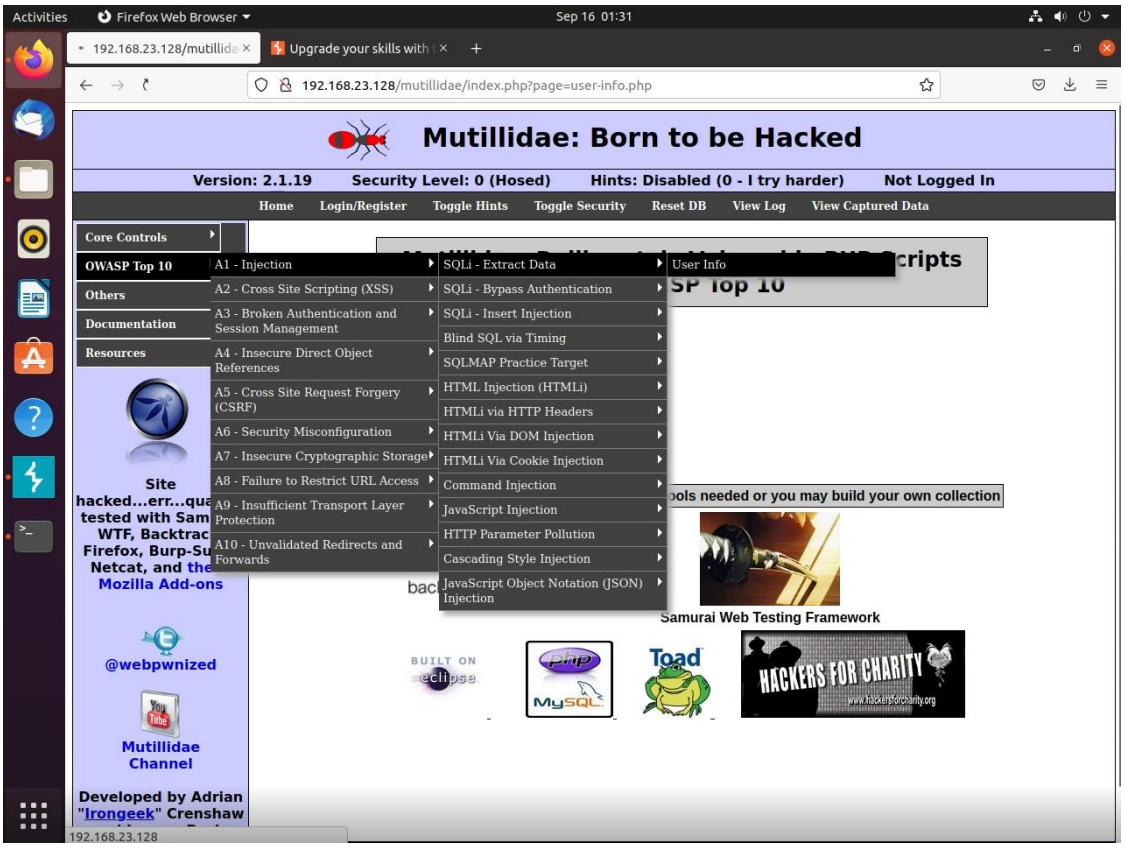


Open Firefox web browser and go to https://github.com/xmendez/wfuzz/blob/master/wordlist/Injections/SQL.txt and copy this list of wordlists. Next, paste the list into a text editor and save it as “SQL.txt”. This is the same wordlist from Kali OS specifically for testing SQL injection vulnerabilities

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

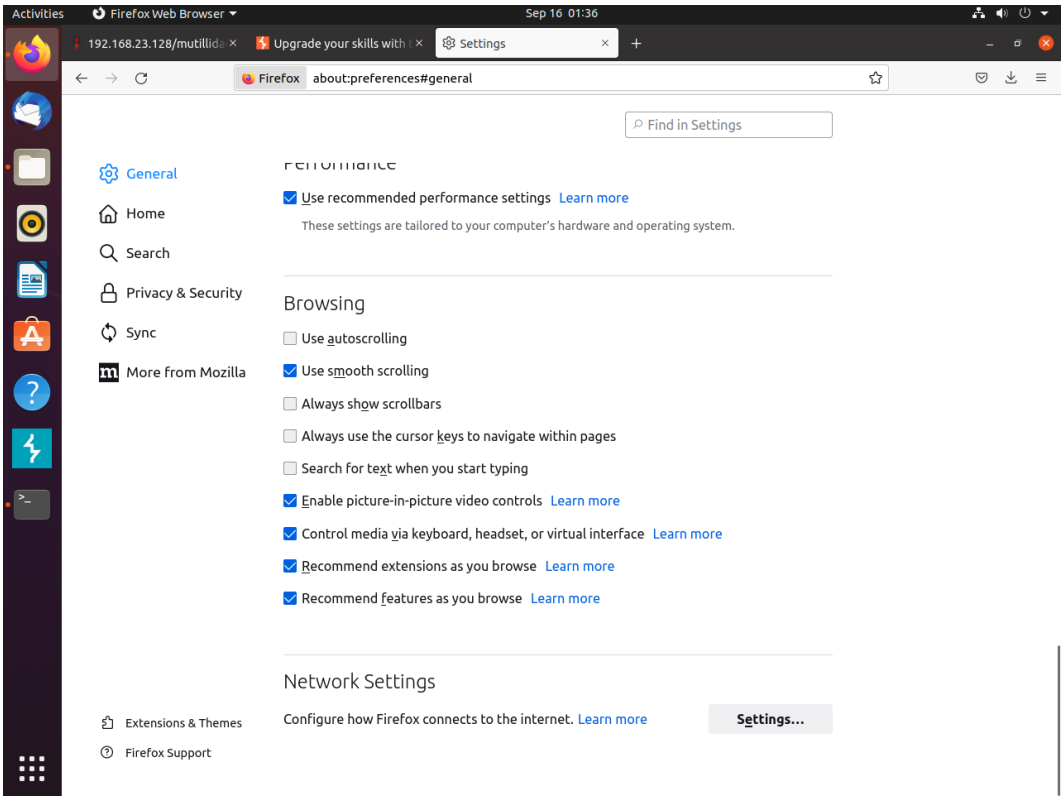


Click on “Mutillidae” in the bulleted list to continue.

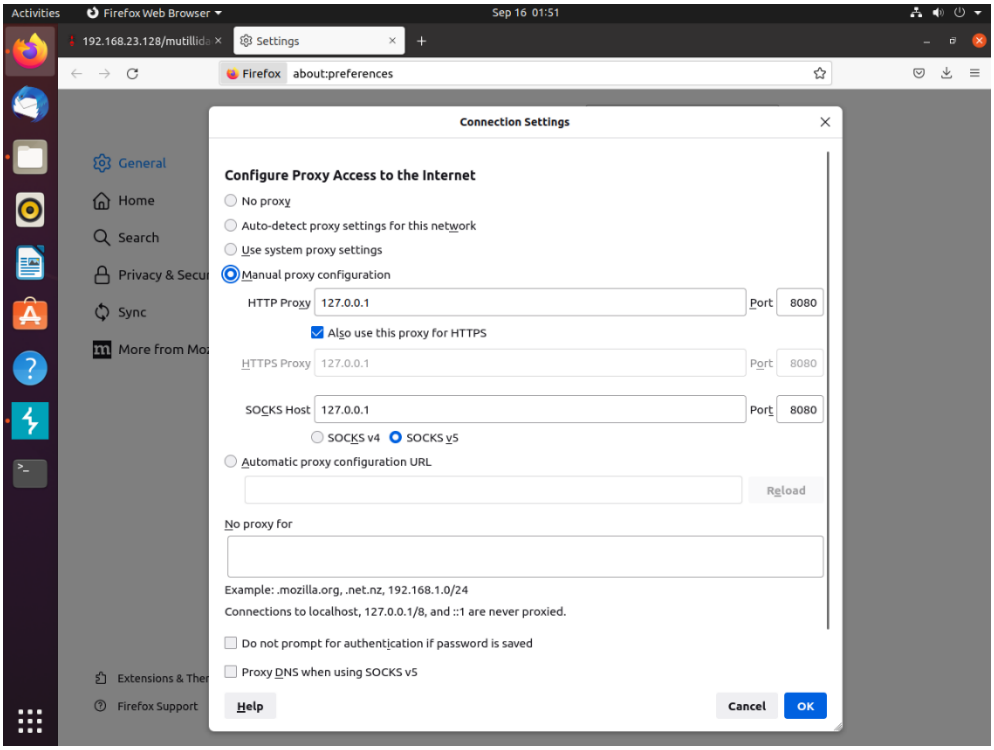


Then, navigate the directory on the left side of the page to "OWASP Top 10." Then, select "Injection", followed by "Extract Data", then "User Info." You will be greeted with a login screen.

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.

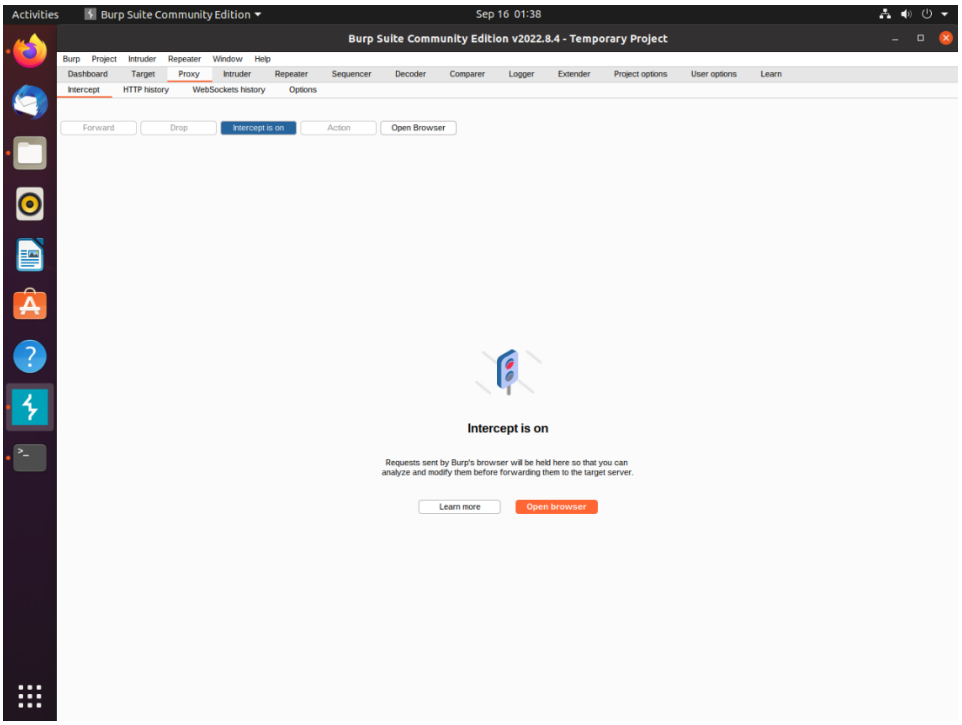


Next, scroll down to the bottom of the page to find the “Network Settings” and click on that “Settings” button.

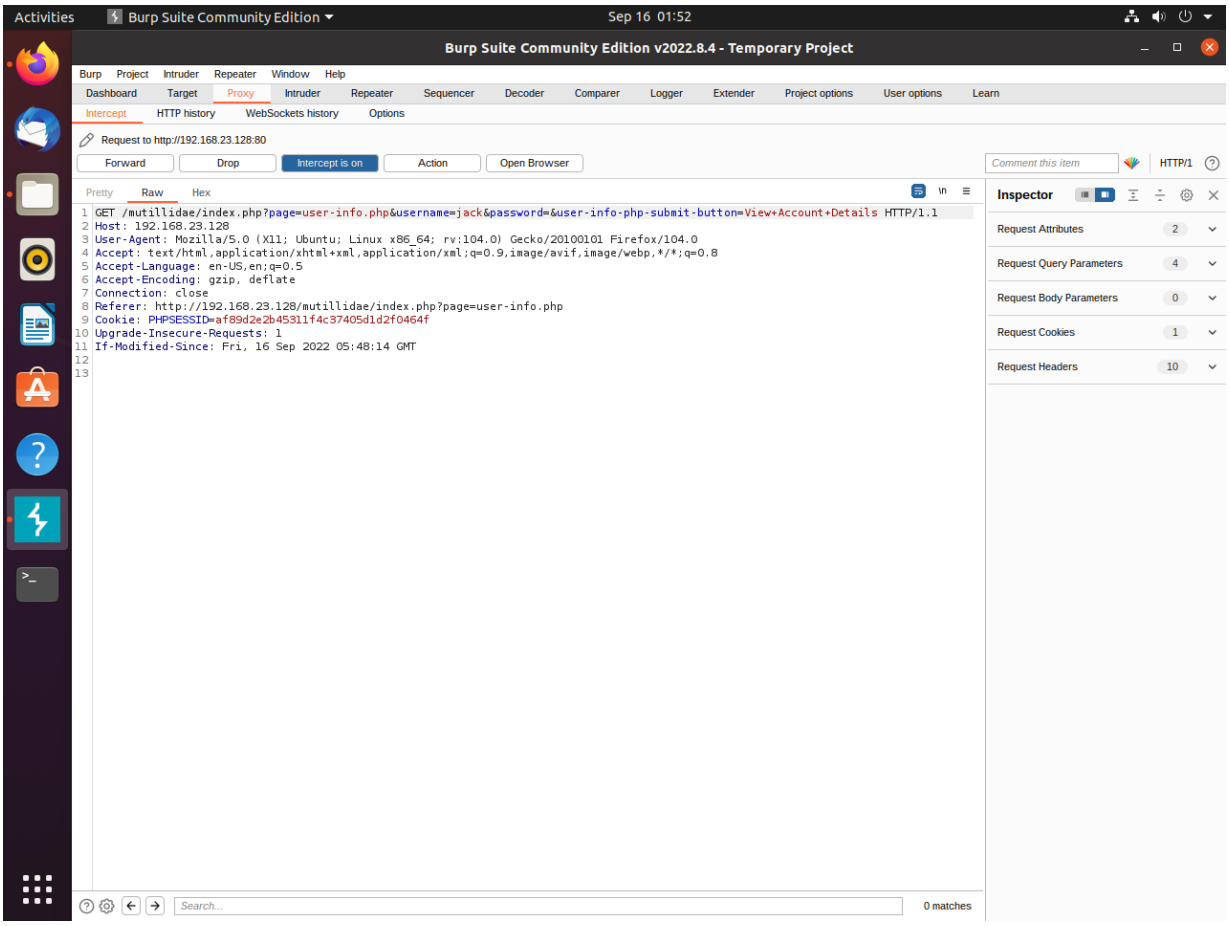


Next, make sure the top radial button is set to "Manual proxy configuration" and enter 127.0.0.1 as the HTTP Proxy and 8080 as the Port. Next, check "Also use this proxy for HTTPS", also and enter 127.0.0.1 as the SOCKS Host and 8080 as the Port, make sure the radial button is set to " SOCKS v5" make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

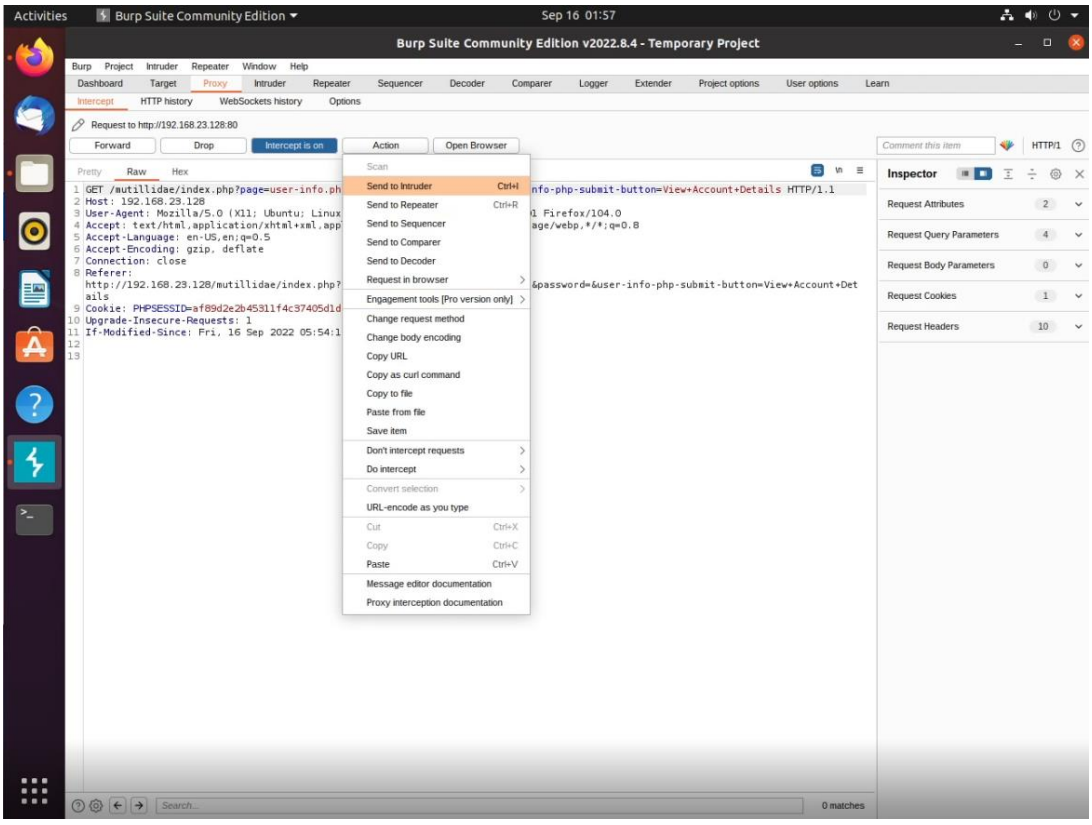
Next, Launch Burpsuite and create a Temporary Project then click “Next”, on the next window “use Burp defaults”, then click "Start Burp”



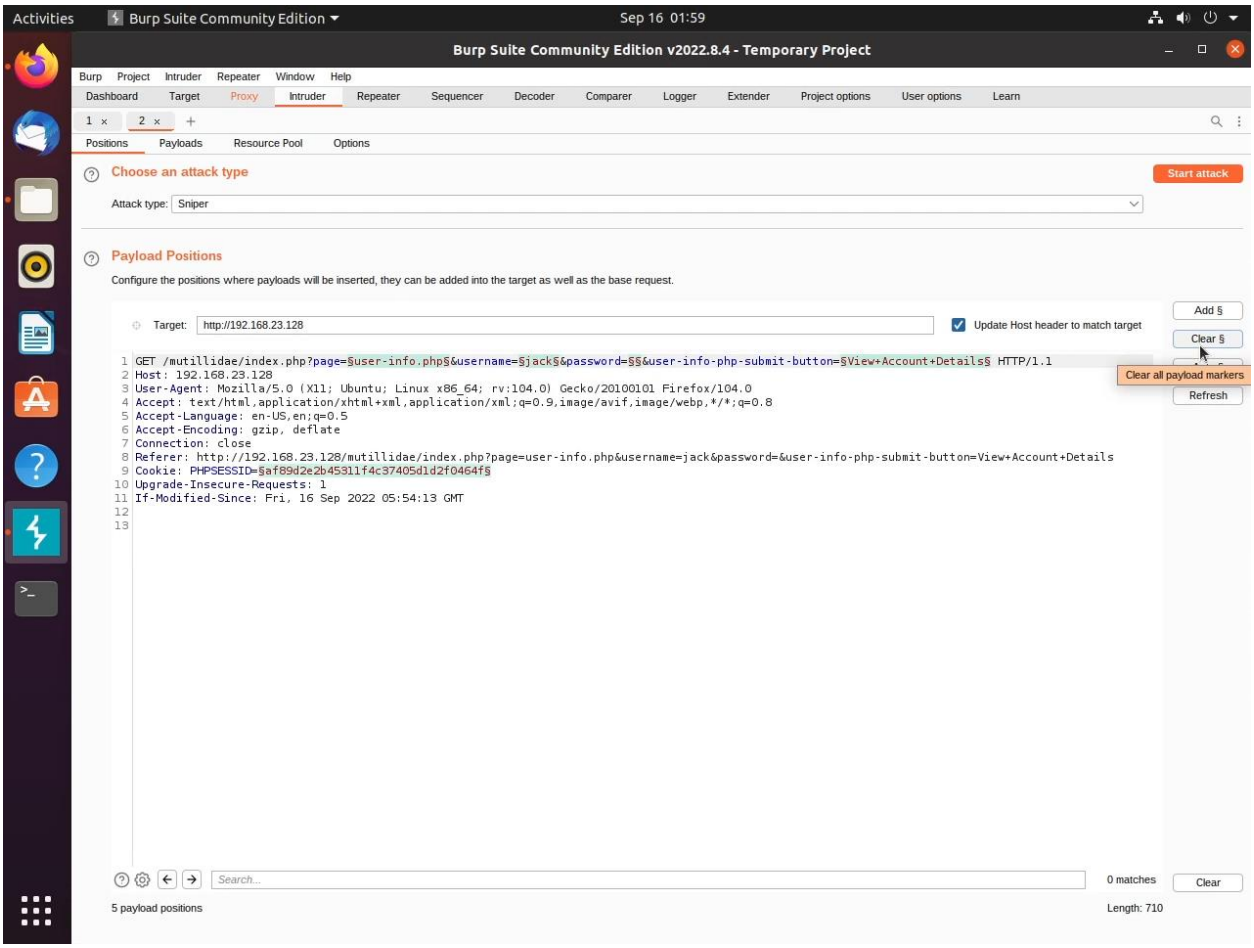
When it finishes loading click on the “Proxy” tab then the “Intercept” tab and make sure Intercept is on. Next, enter text in the “name” and “password” text field and submit uses the Enter key or clicking the “View Account Details” button.



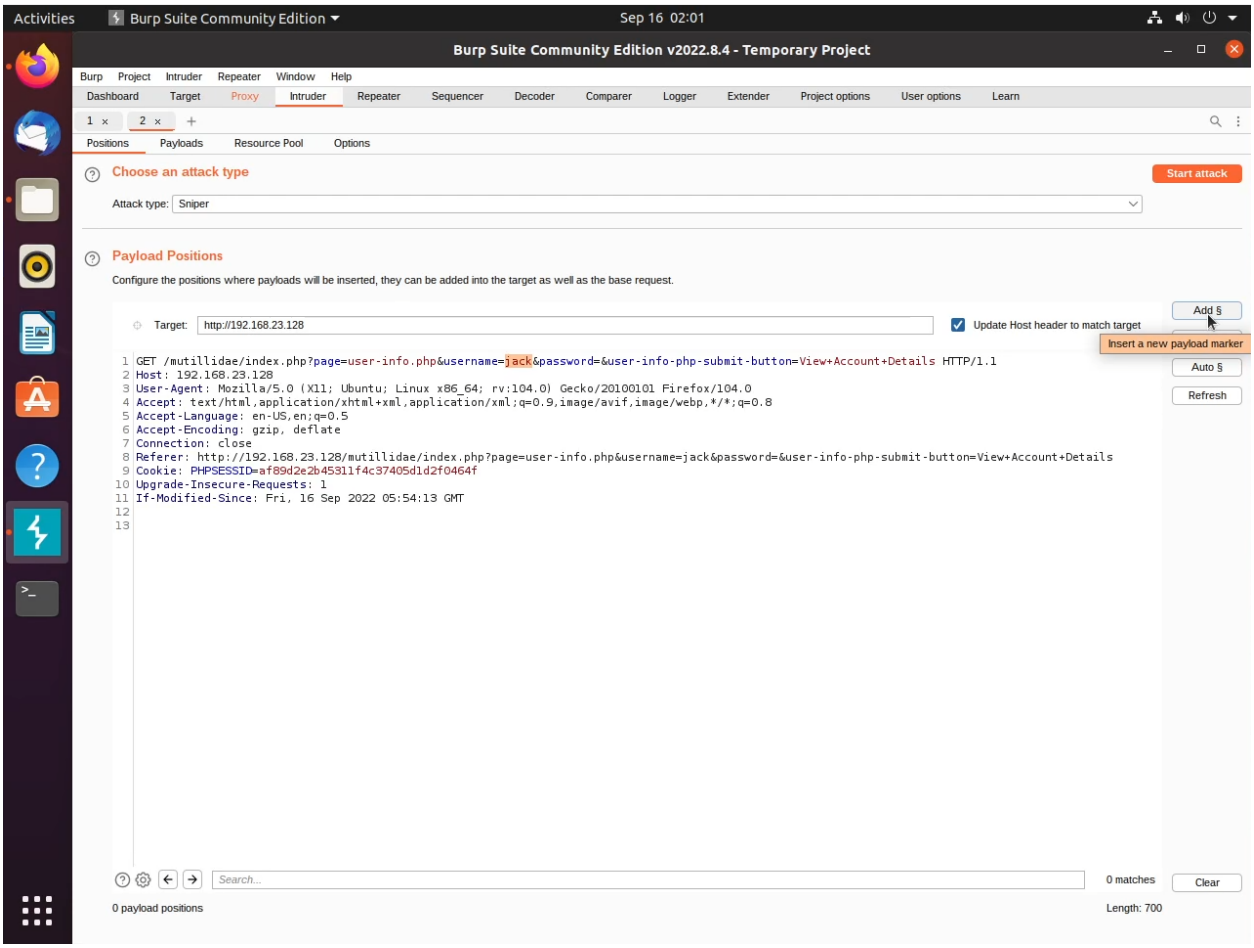
Next, go back to Burpsuite.



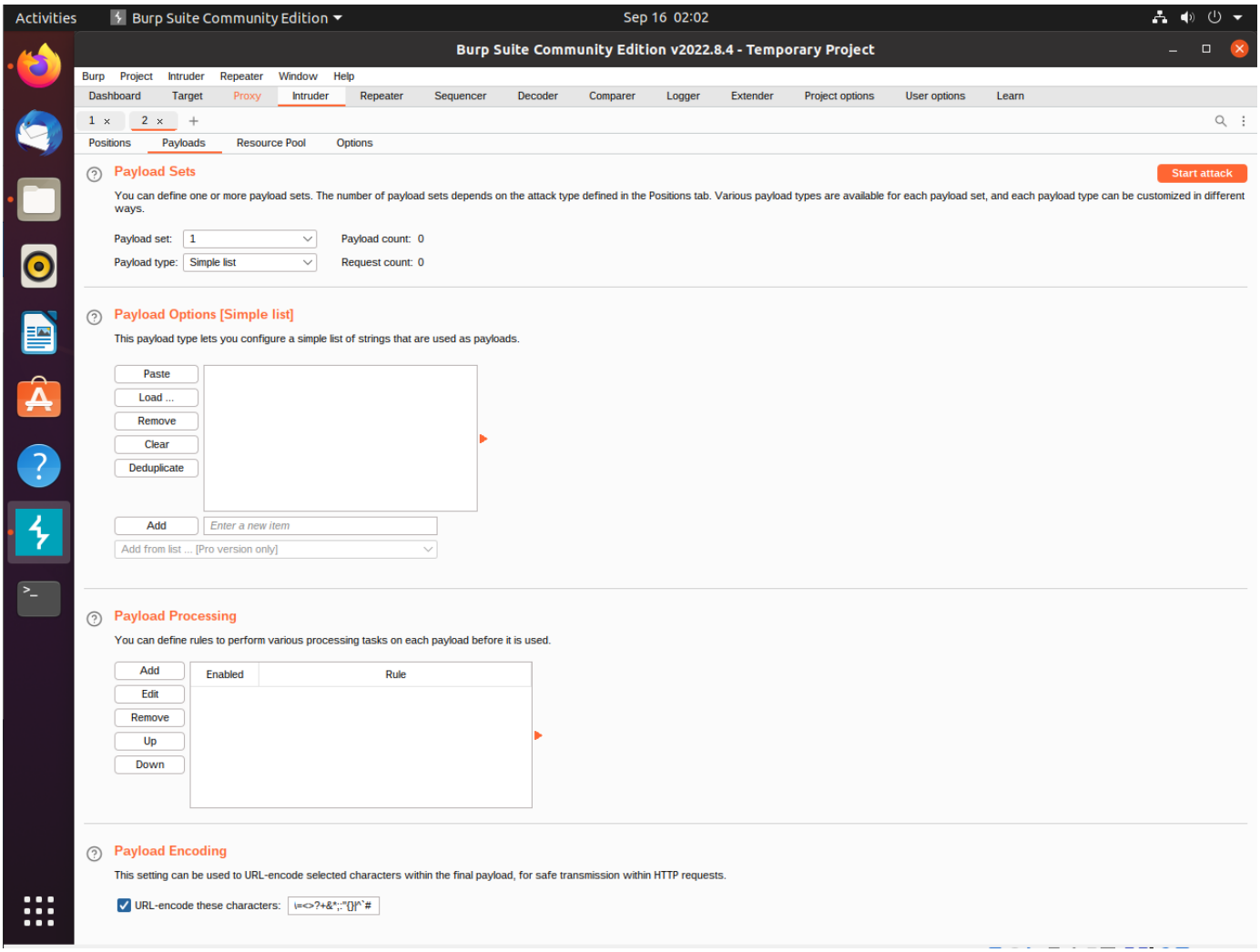
Next, click the “Action” button, then click “Send to Intruder”. Change the tab from Proxy to the “Intruder” tab.



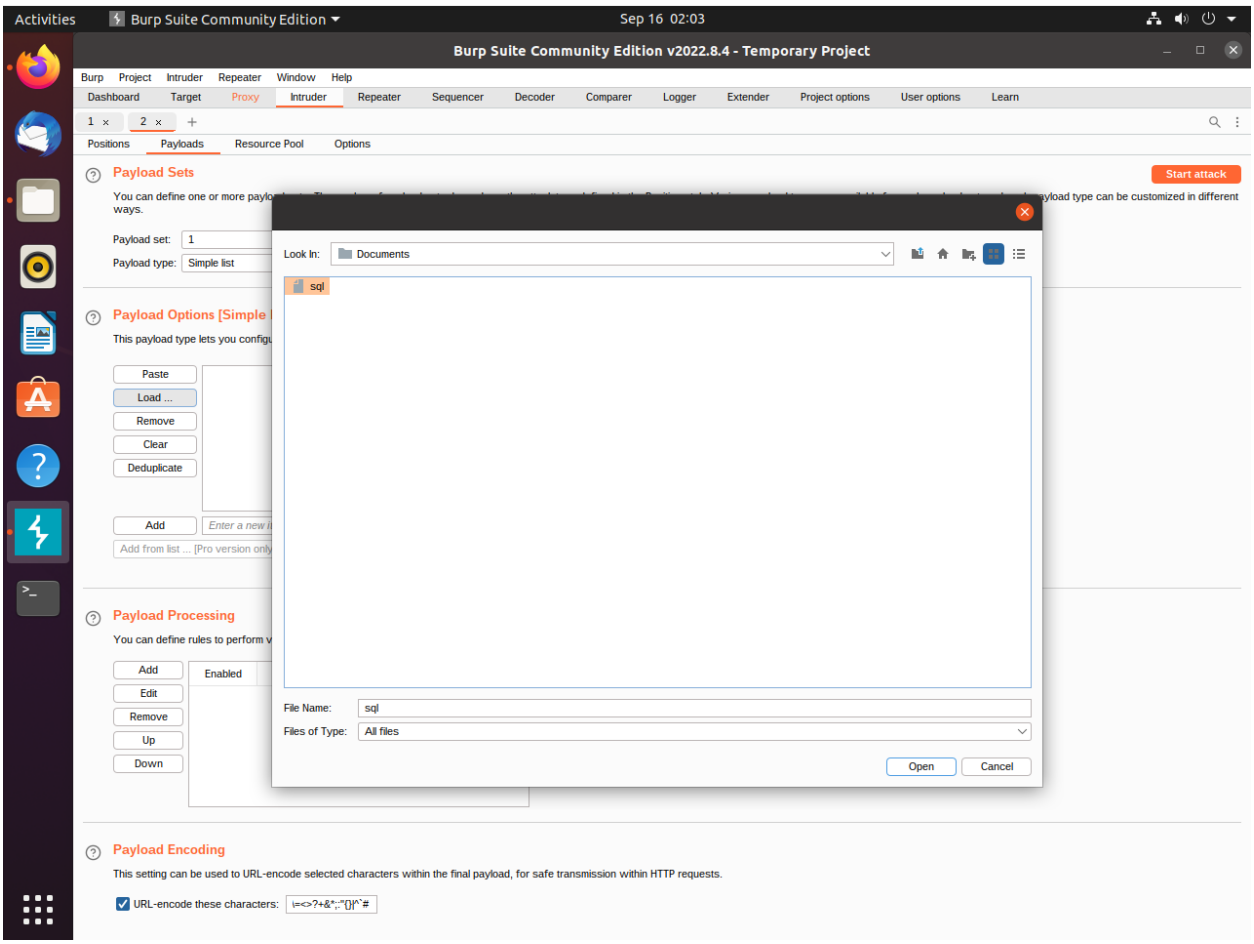
Next click on "Positions". Burpsuite automatically configures the positions where payloads are inserted when a request is sent to intruder, but we one need the name text field. Then, click the “Clear $” button on the right to Clear all payload markers.



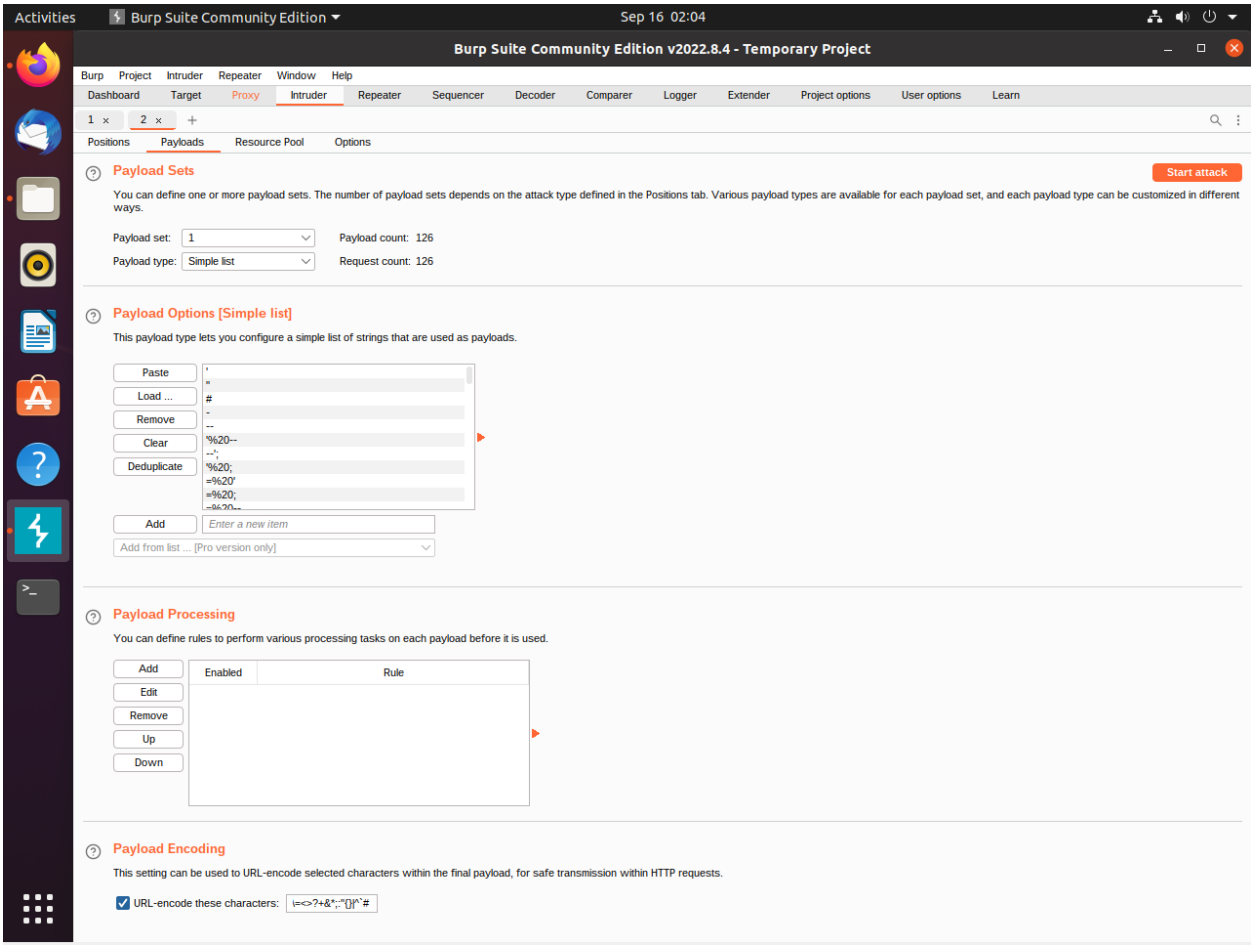
Next, double click the value you entered into the name field and click the “Add $” button to add payload markers to that field. We will use the "Sniper" attack type which will run through a list of values in the payload and try them one at a time.



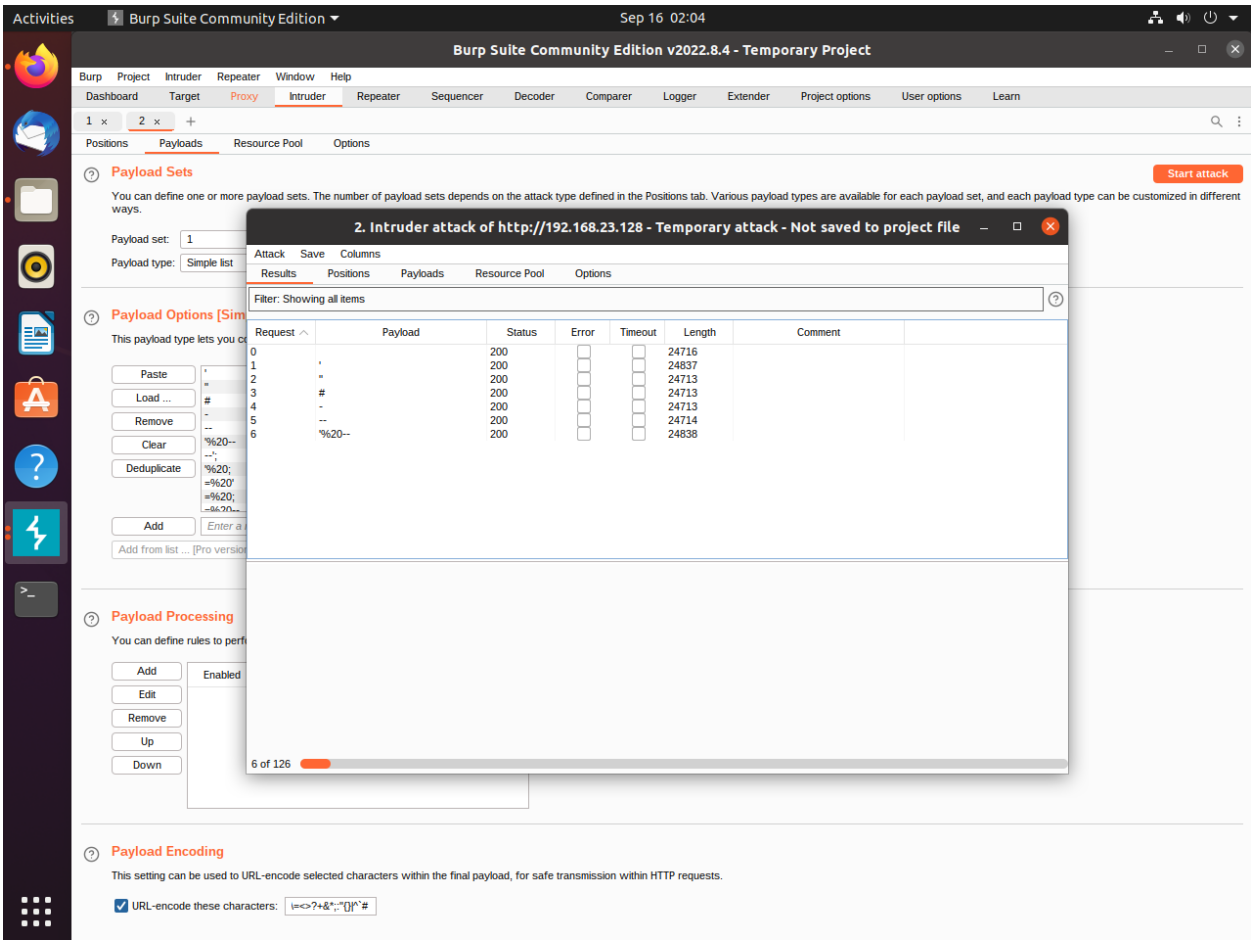
Next, click on the "Payloads" tab and we will use all the default values.



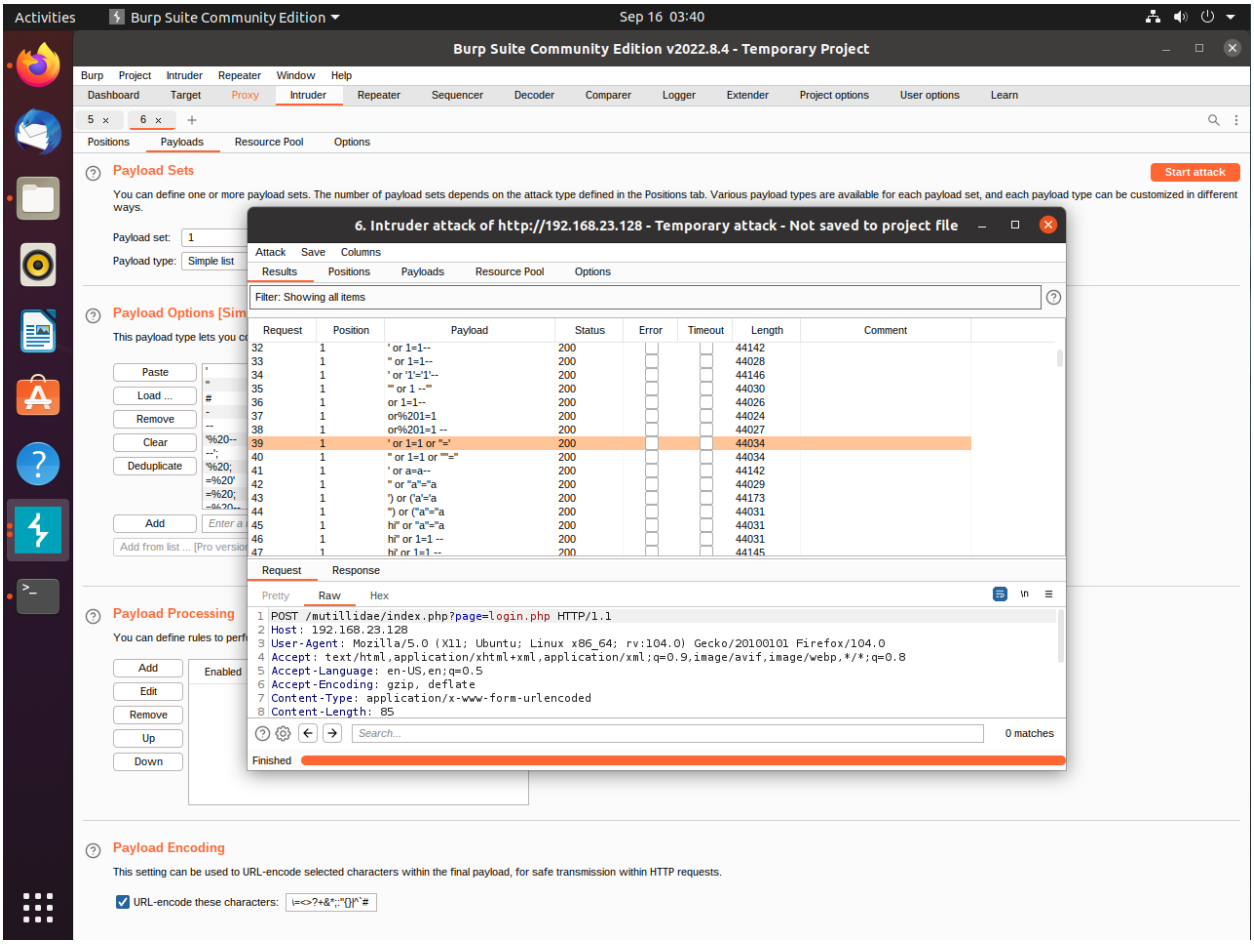
Next, we will enter our payloads into the "Payload Options [simple list]" by either adding them one by one or loading an existing list. Click the "Load" button and find the "SQL.txt" file and click the "Open" button.



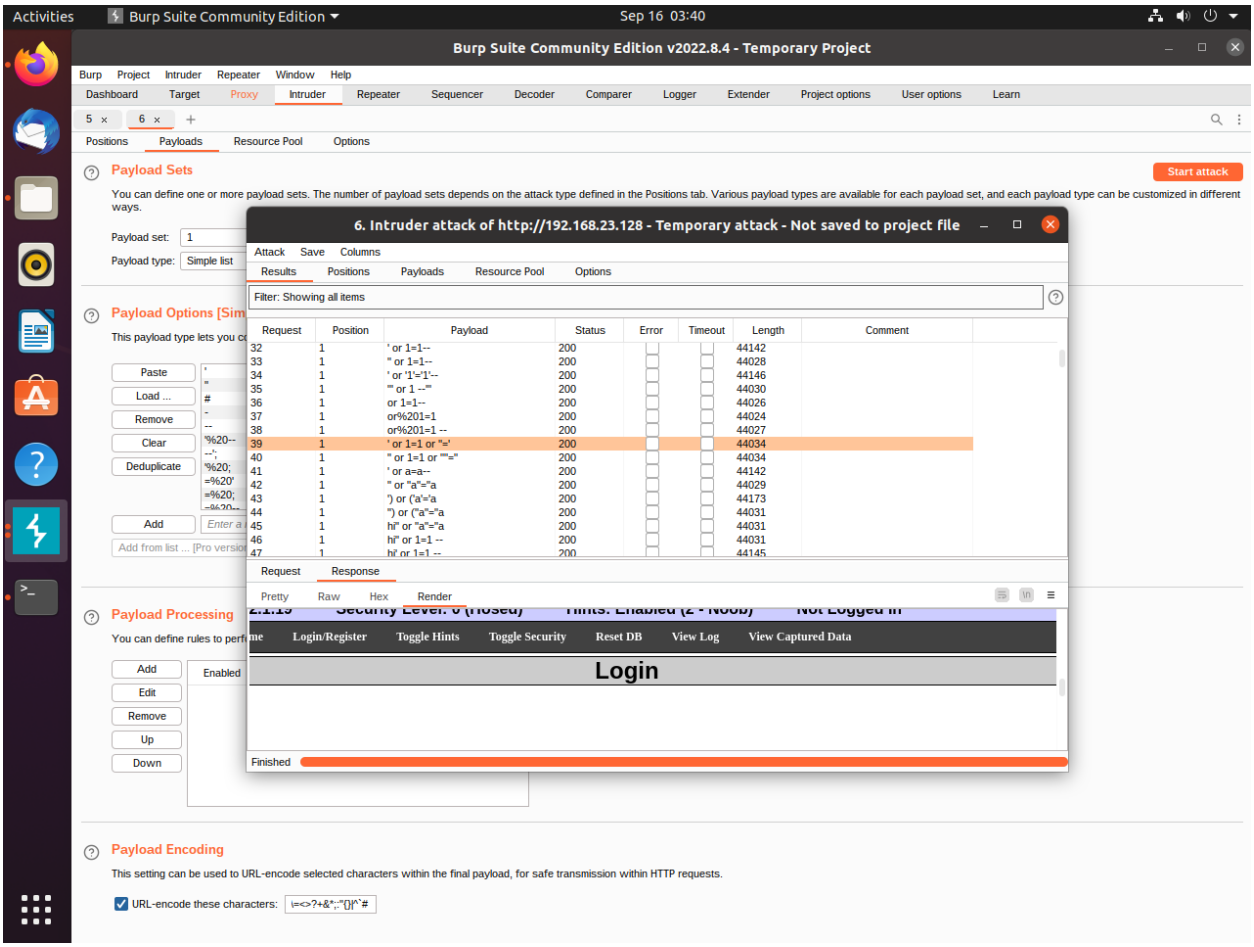
Now it is time to run an Intruder Attack. This is done by click the "Start attack" button, and a new window will pop up showing the intruder attack.



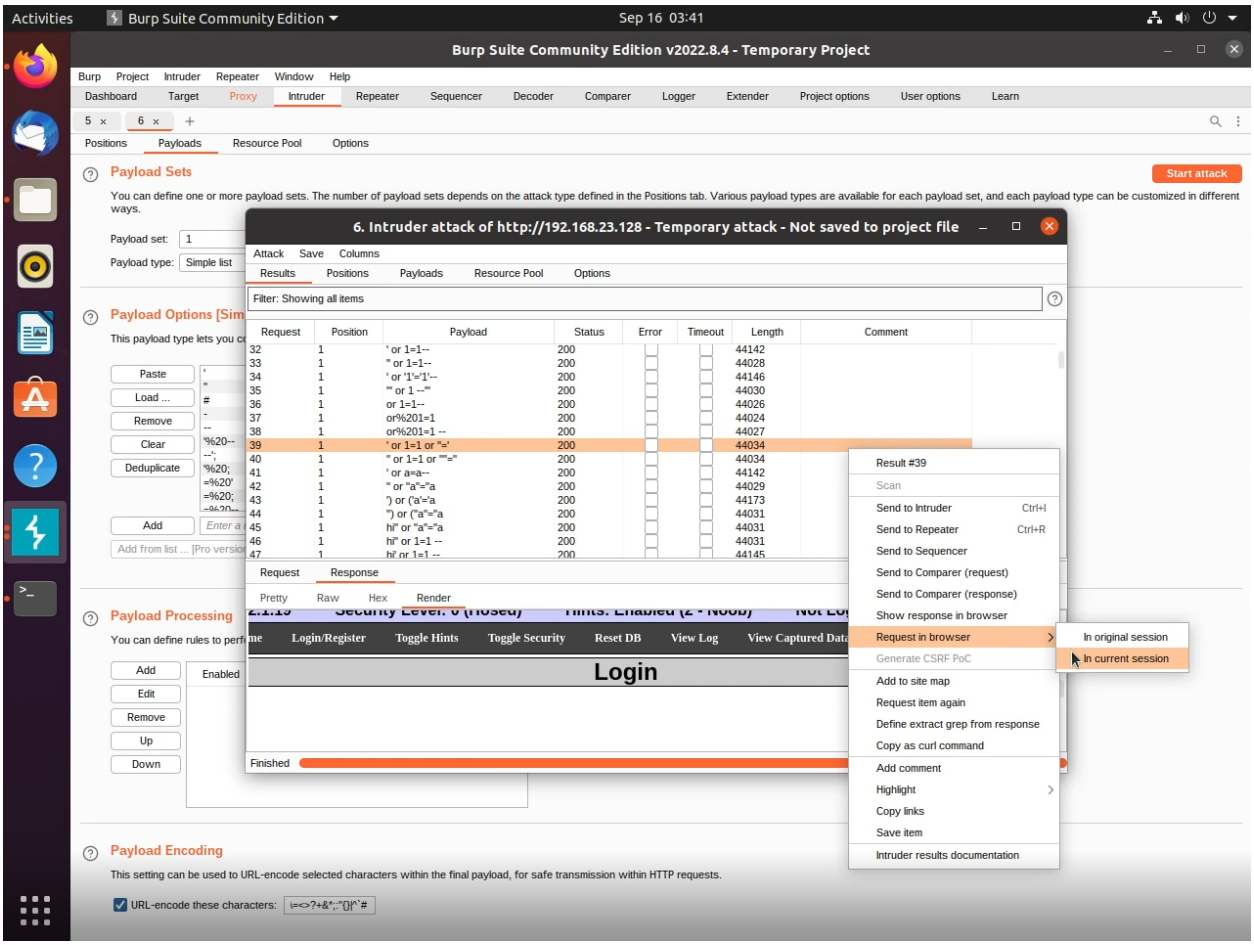
This Window shows you the progress of the requests plus their payload and status. This can take quite some time to complete depending on the length of the list.



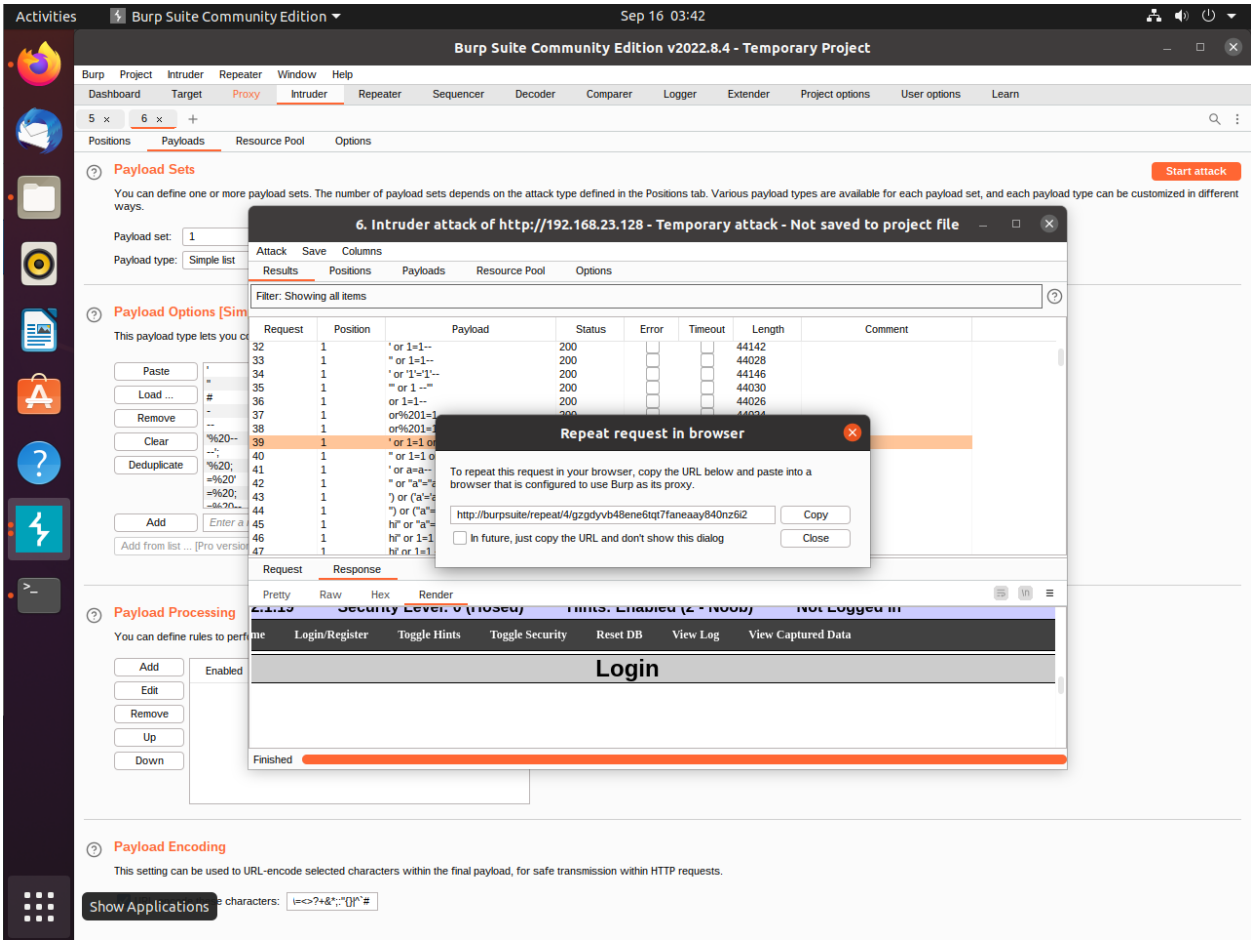
Once any intruder is finished, you can view the details of any request simply by clicking on it. The Response that is seen here is the raw HTTP request that was sent to the database.



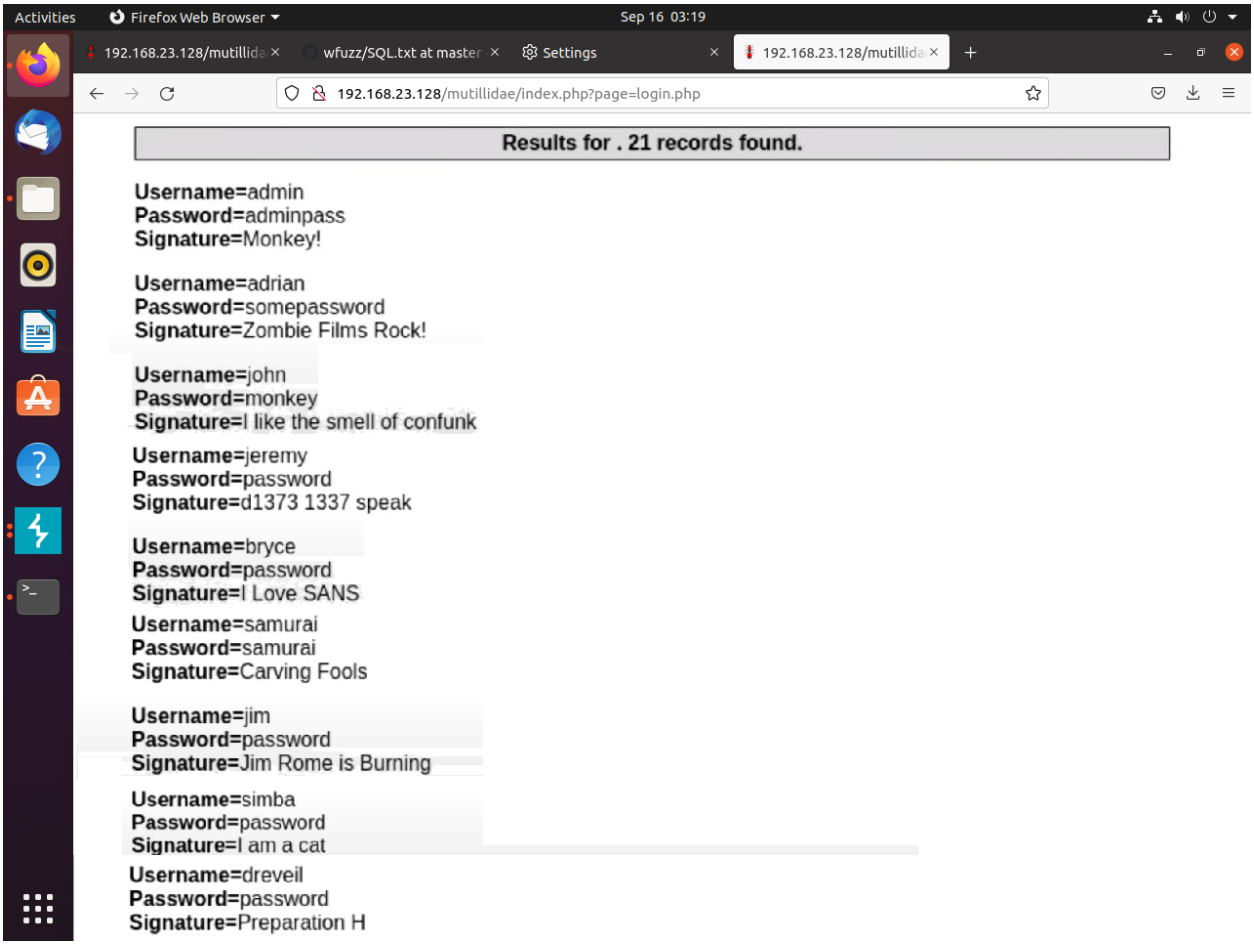
Every single request that was made returned a status code 200 response, but sometimes when a payload is successful you will see a different code. Another way to tell if a query succeeded is if the length of the response is noticeably different from the others usually around 1000 more than the rest of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



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.



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.