

DVWA

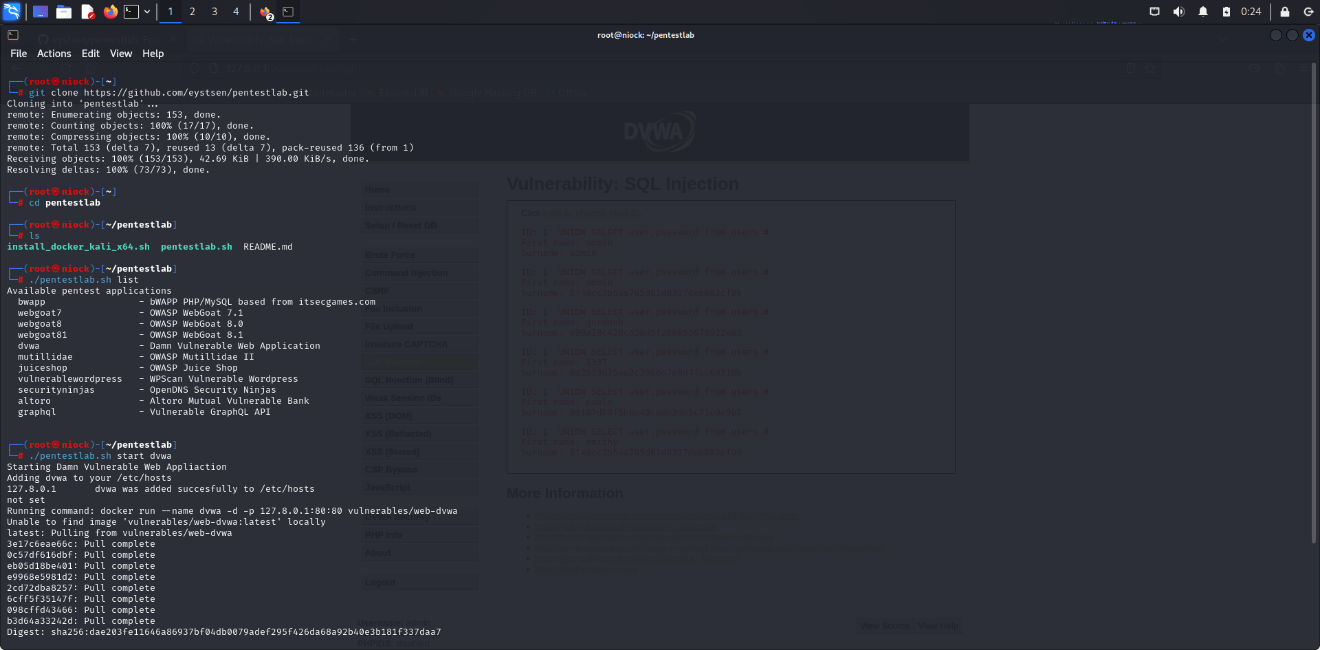
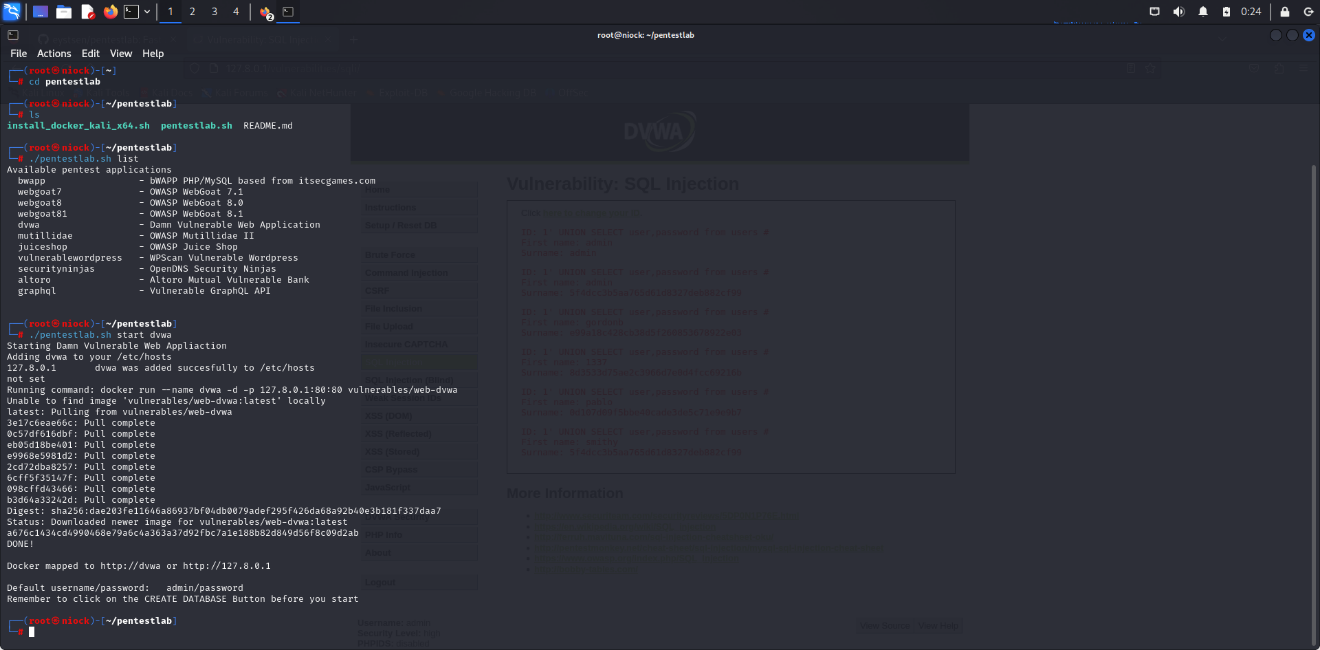
SQL INJECTION

ROHITH RD | 24-09-2024

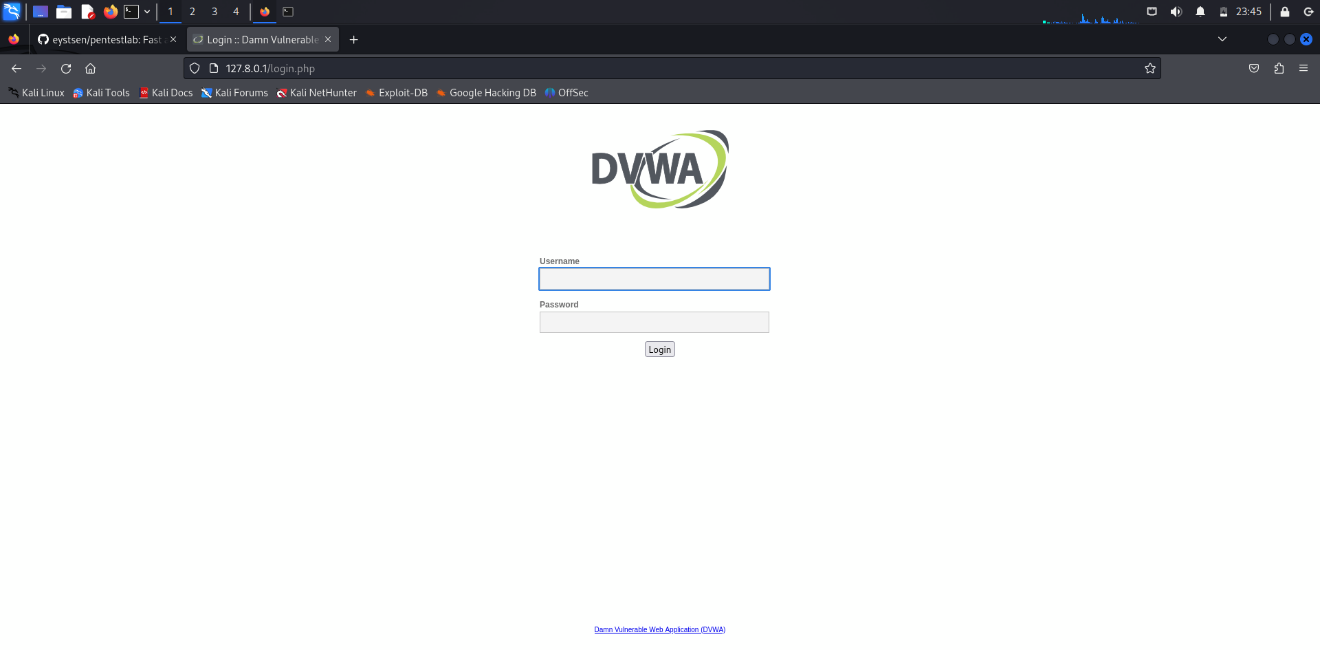
# Instaling DVWA

For installing DVWA I used docker.

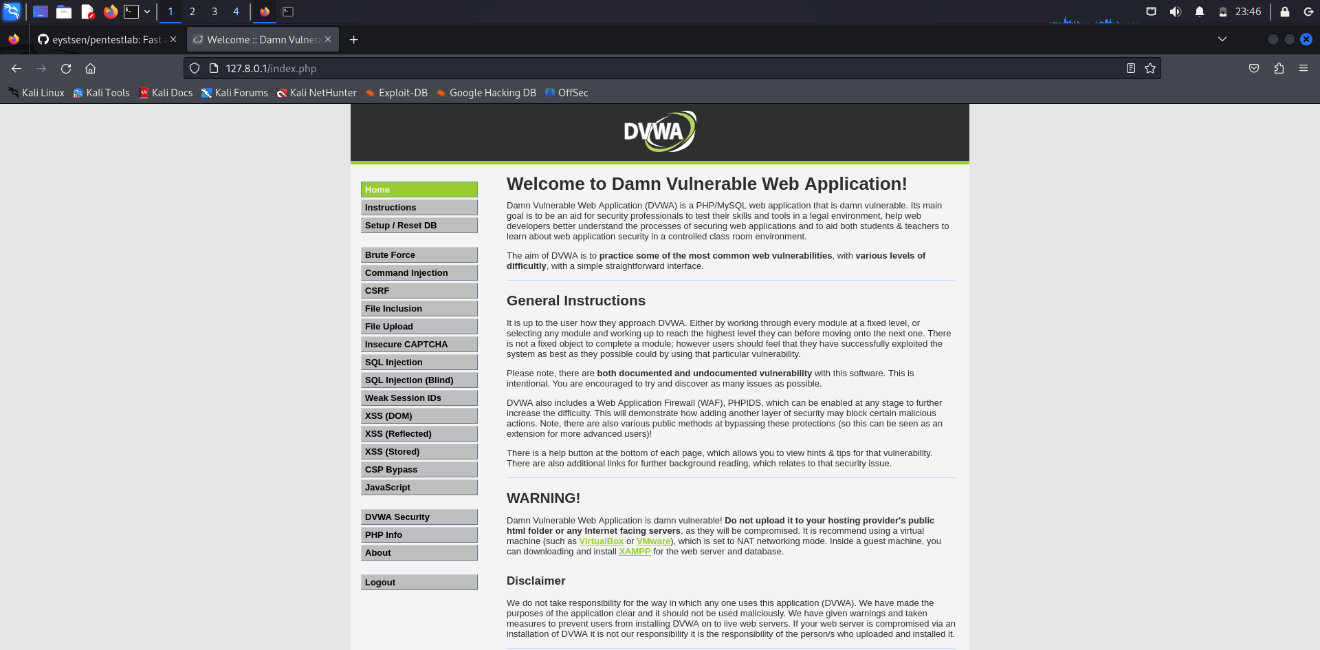
Then i went to pentestlab.github. I am sharing my screenshots for better understanding. These are the step by step process I went through, starting from git clone……



After the complete installation of DVWA we will get automatically redirected to the webpage.



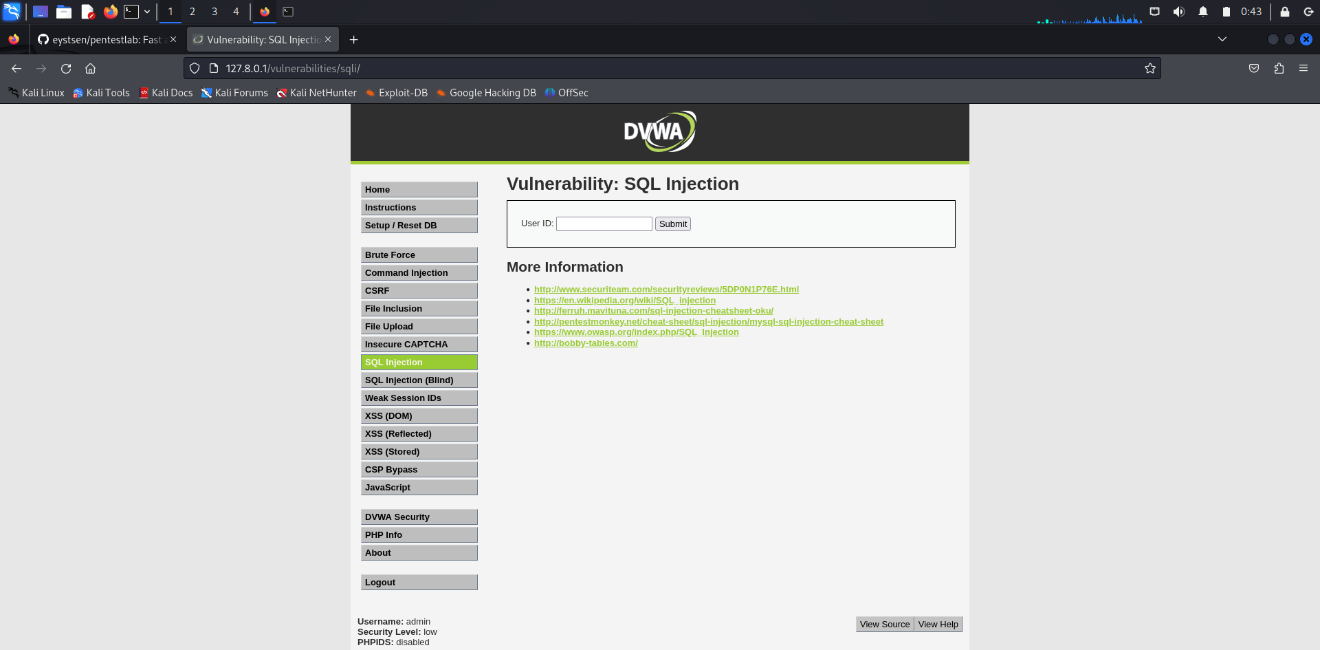
The default username is admin and password is password. Then in the next page you should be asked for reset your database(forgot to take that screenshot). Click that button. Installation complete. Then once again you will be redirected to login page, use the default credentials again. Then you will get to see this page



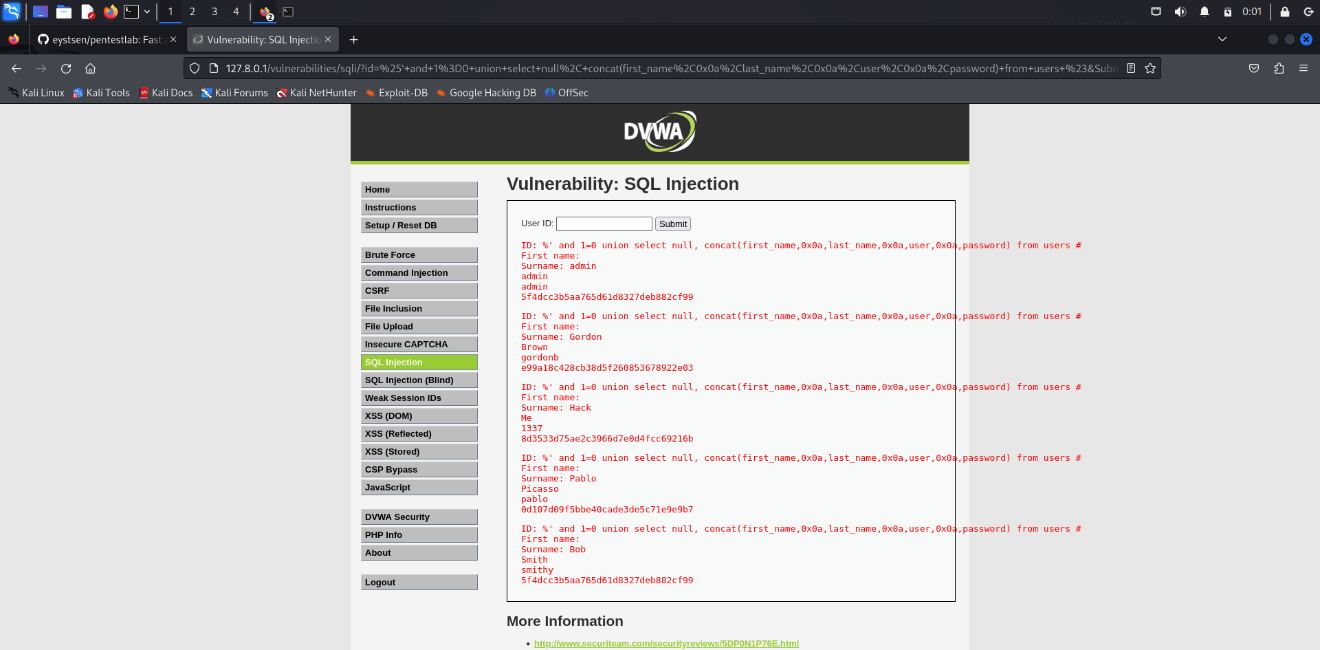
The whole set up is complete.

# SQL injection(low)

First I got to see the page and thought of how to inject the code(no problem for finding the place to inject).



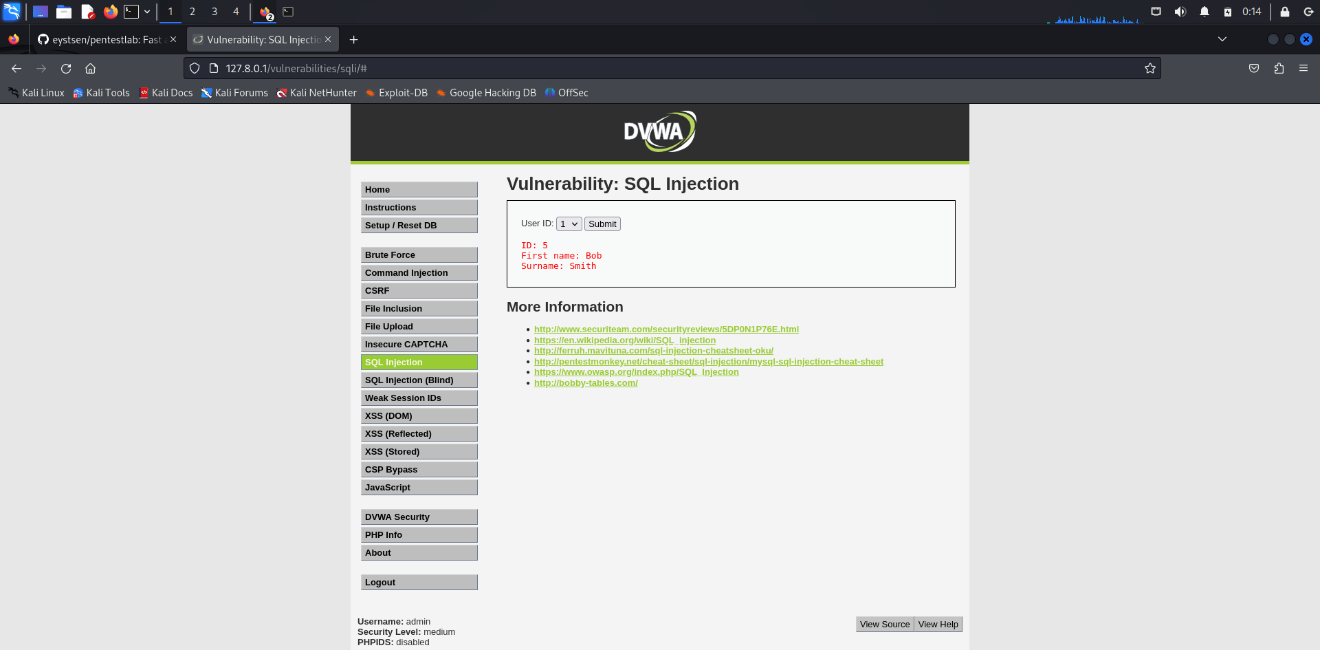
First I used simple one’s but that was not helpful to getting inside the database. Went through many websites and at last I used **%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #** which I got from portswigger cheatsheet.

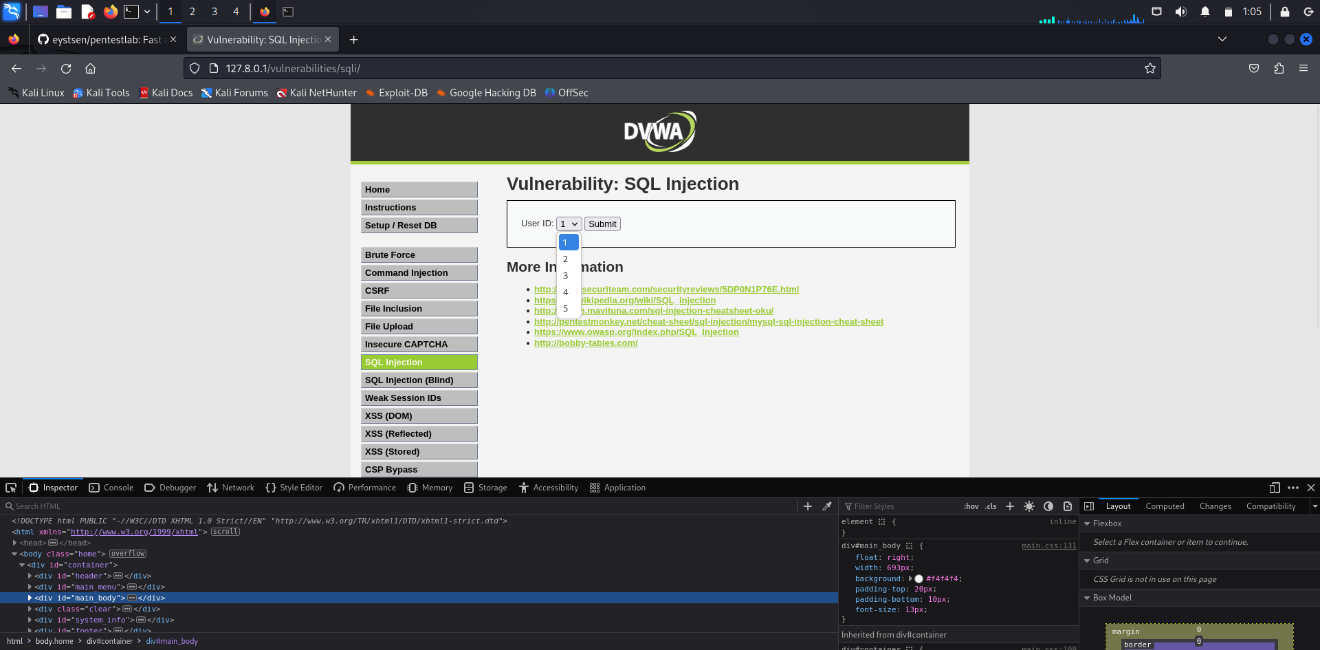


After executing the above mentioned code, this was the result. Got the first and last names and cookies of the users.

# SQL injection(medium)

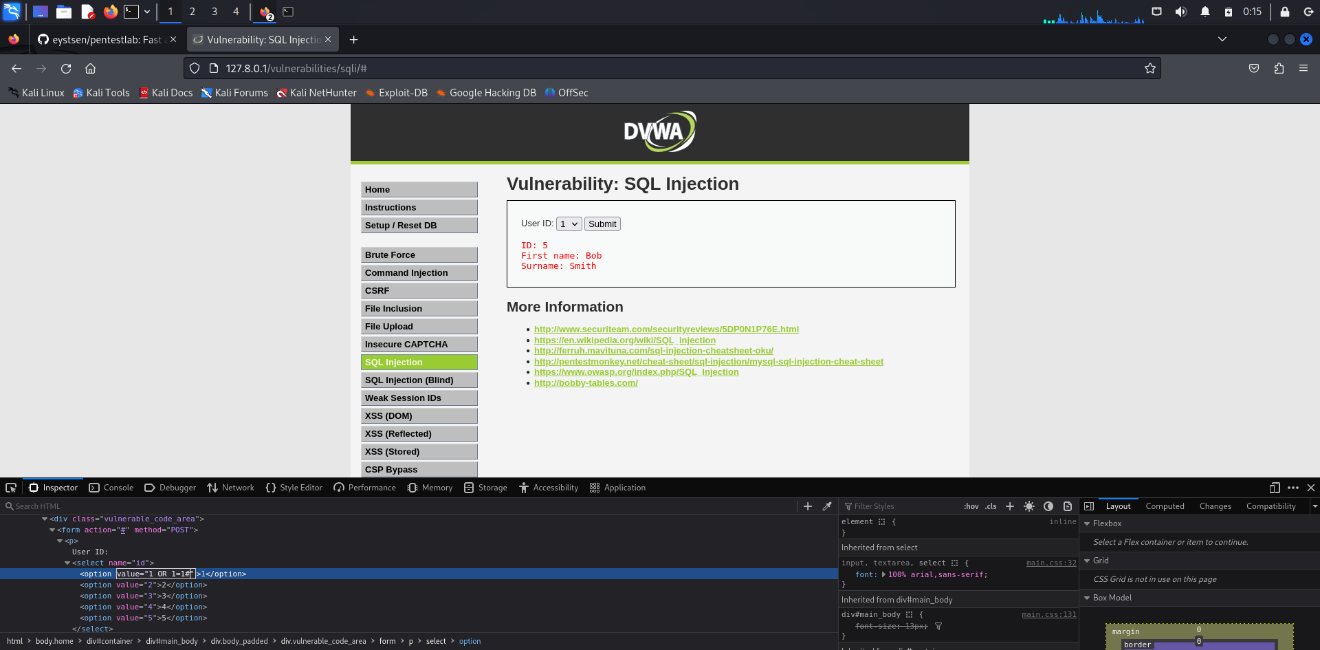
After changing the setting to medium, sqli page was slight different.



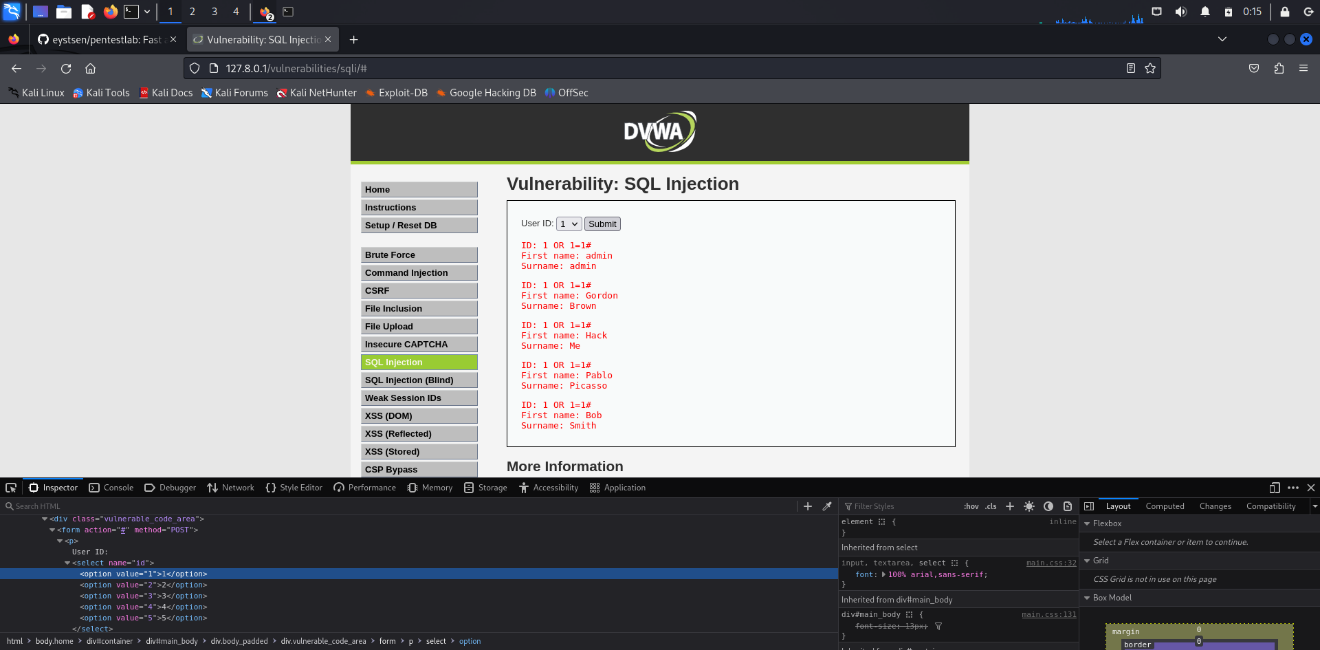
There was only buttons of navigating userid and submit, no comment options to inject then I tried some codes from port swigger cheatsheet and medium articles and injected them in URL that was also unsuccessful. Later then went to developer tools hoping that i’ll get an idea.

Then I went to research for sql injection through developer tools contents and used pentestGPT.

PentestGPT gave OR 1=1# command to use this on any value of the userID button and then I clicked submit.



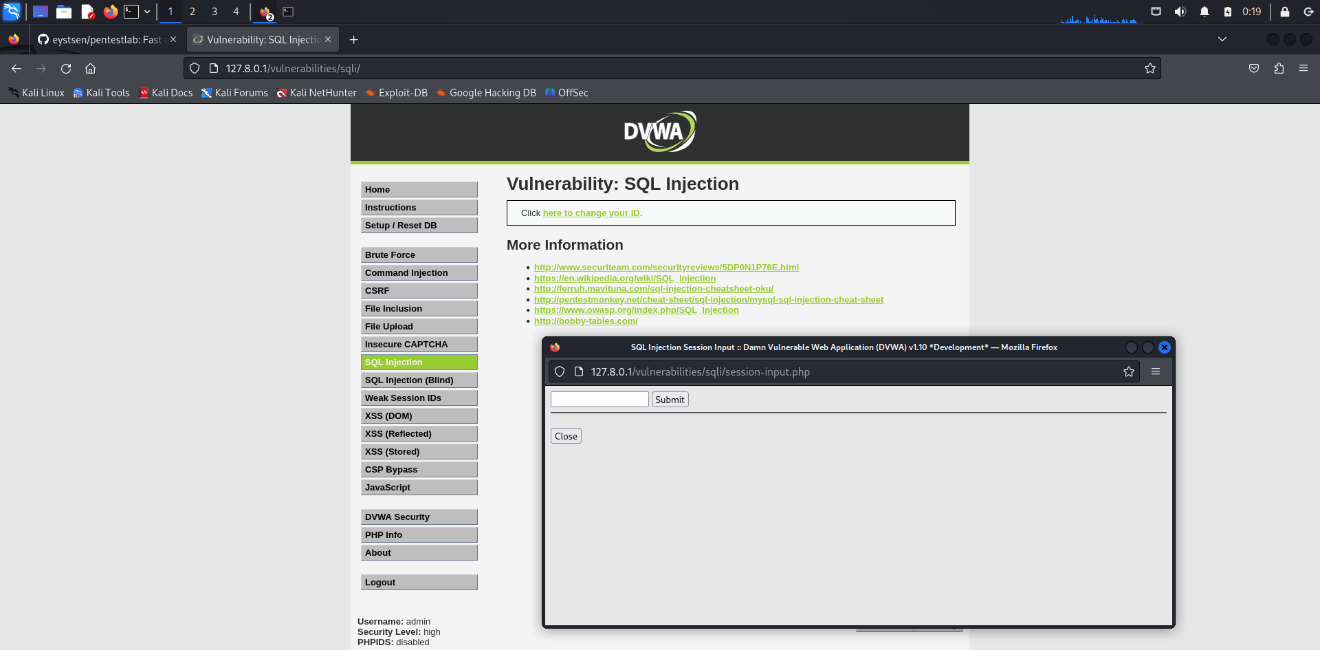
Then on the next page…….

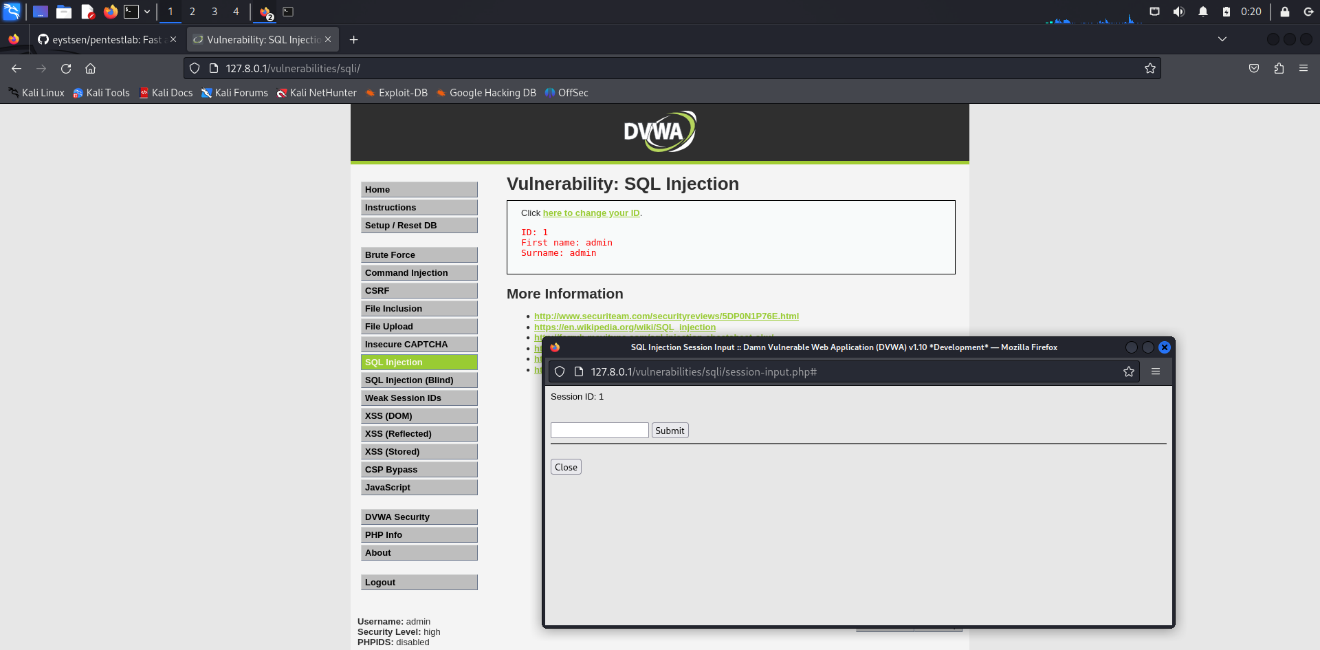


I got the first and last name of every user.

# SQL injection(High)

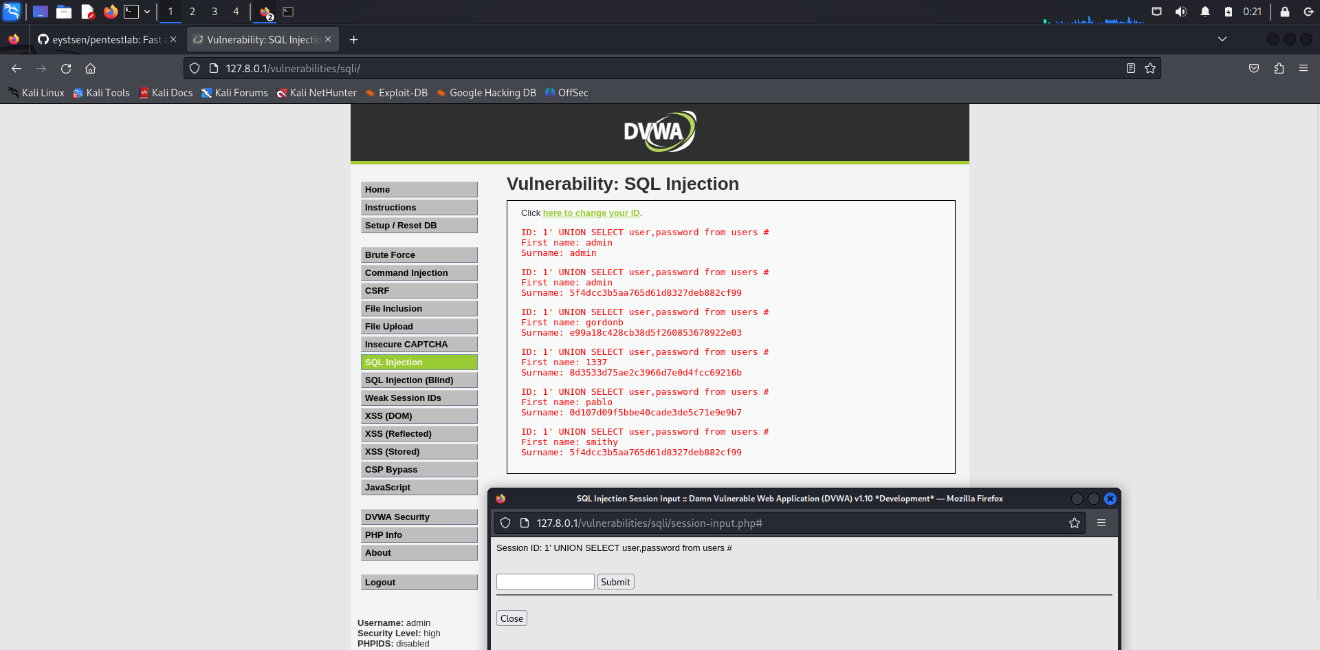
In SQLi high mode the interface different. There was a hyperlink texting click here to change your id. After clicking that link another window showed up.



In that window there was a box to text session id. I enter 1 and gave the first and surnames of user number 1.

Then I again went for researching for what to do in this snenario.

**1' UNION SELECT user,password from users #** i got this command from medium article of Kamal S and said to use this command after the execution of session id.



After entering that command I got the first names and session cookies of the users.