TASK 15

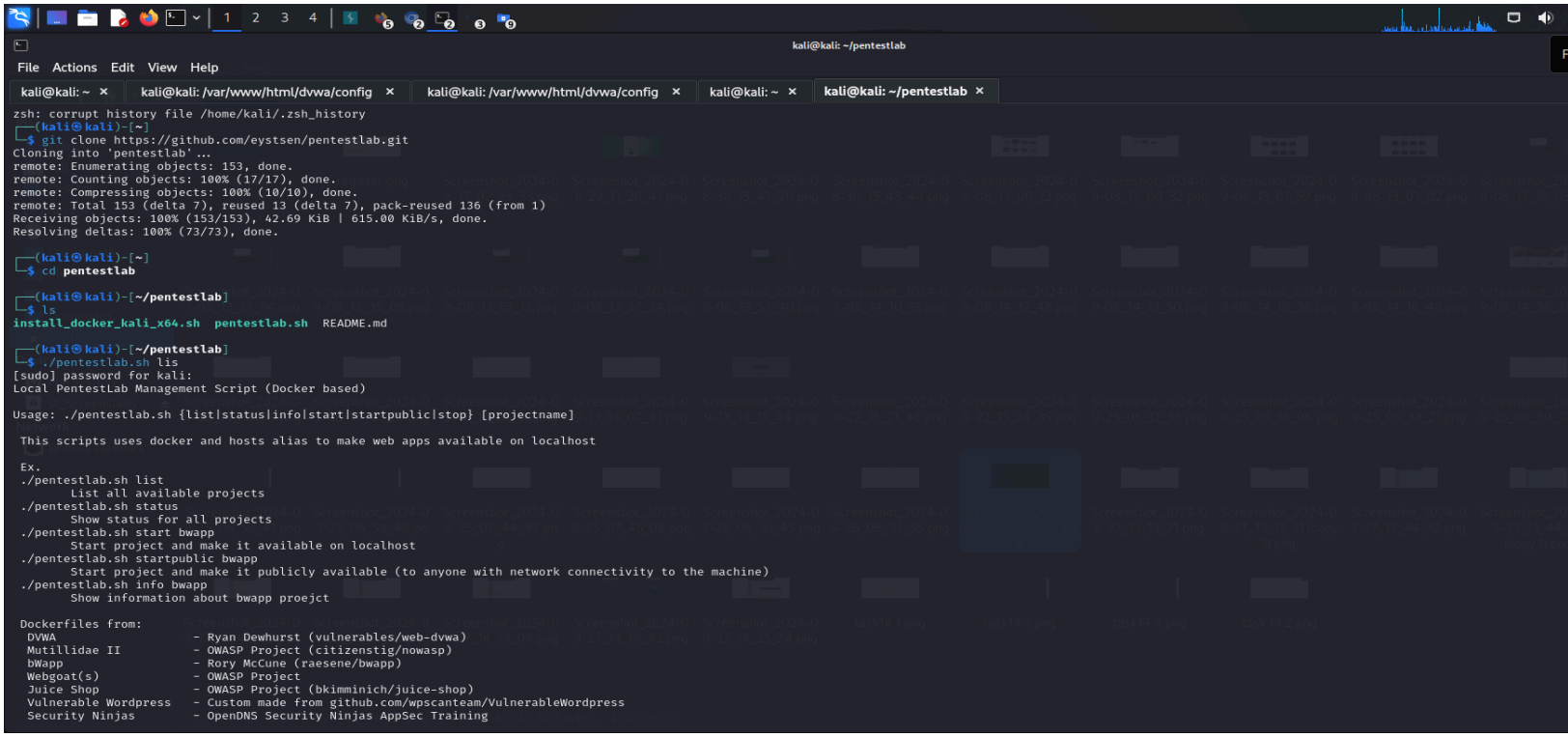
DVWA

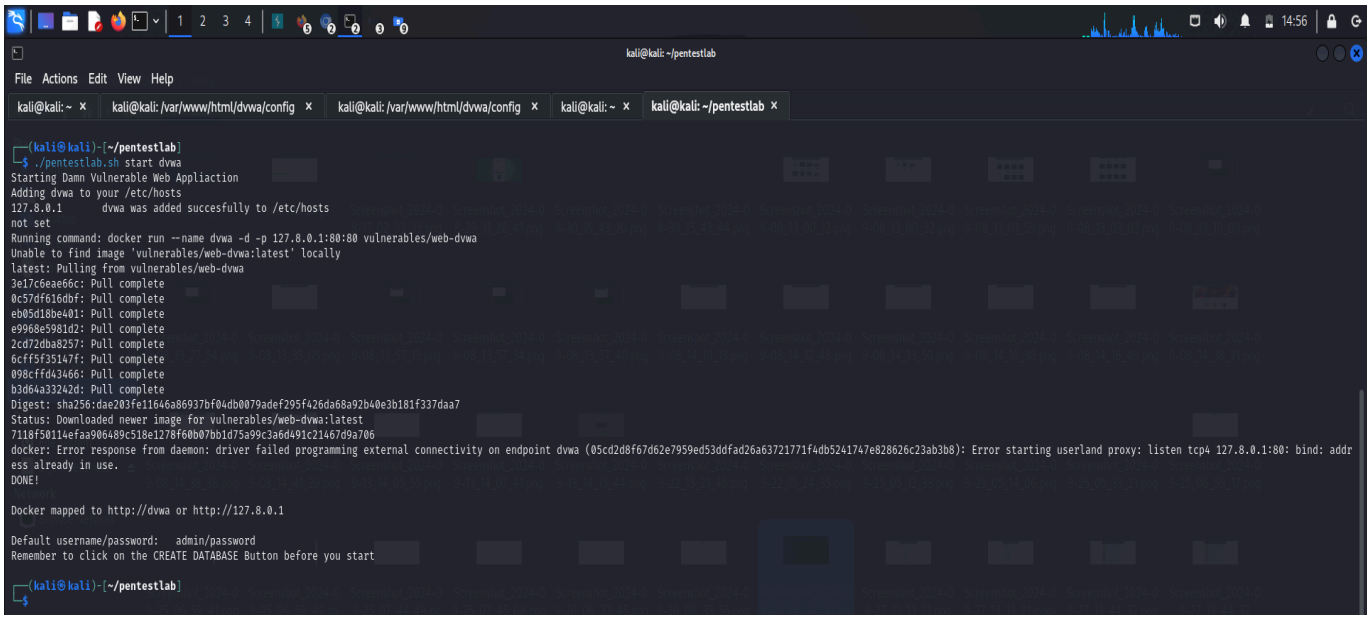
SQL INJECTION

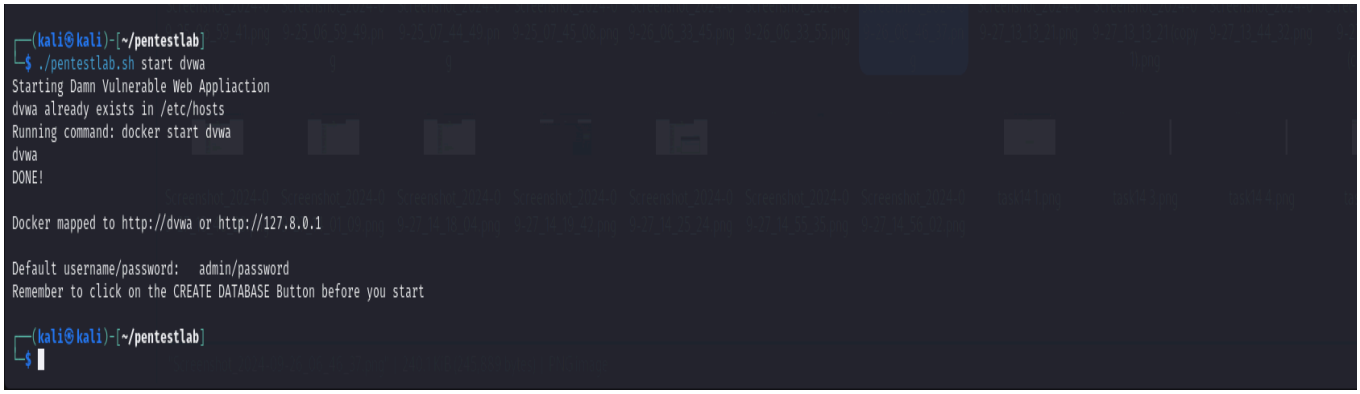
VARSHA M

INSTALL DVWA

Cloned pentestlab.github .For installing DVWA docker is used

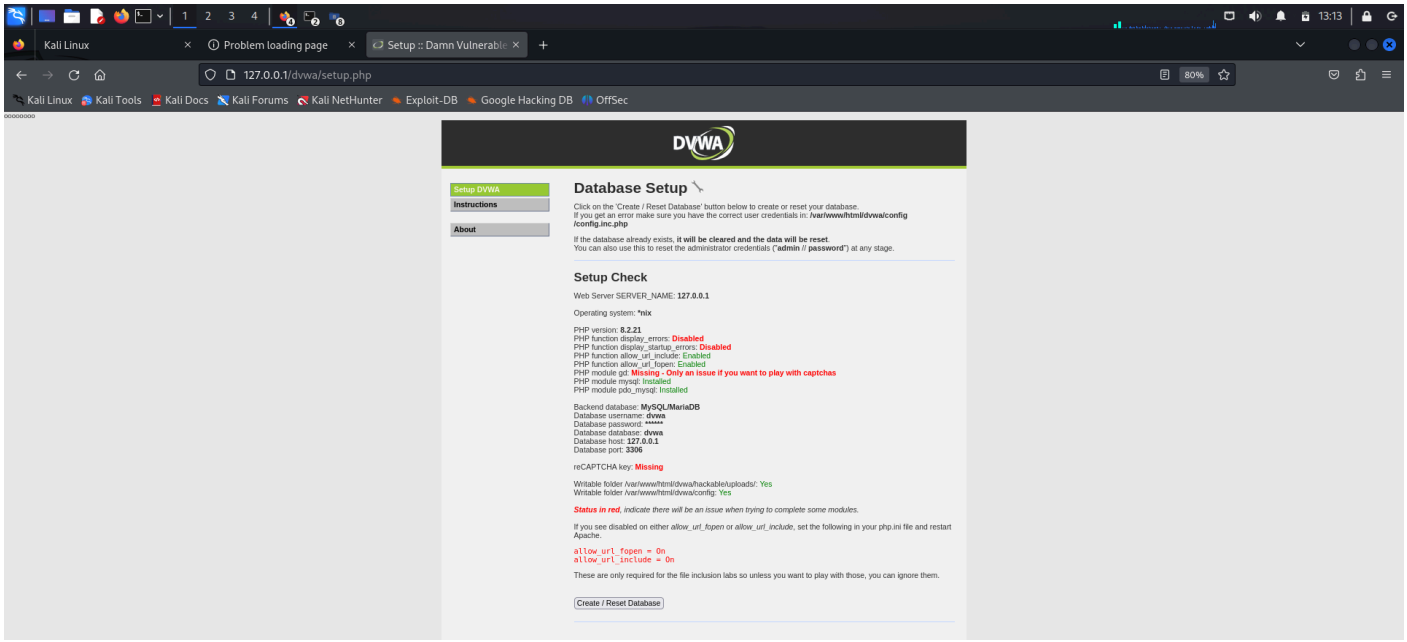




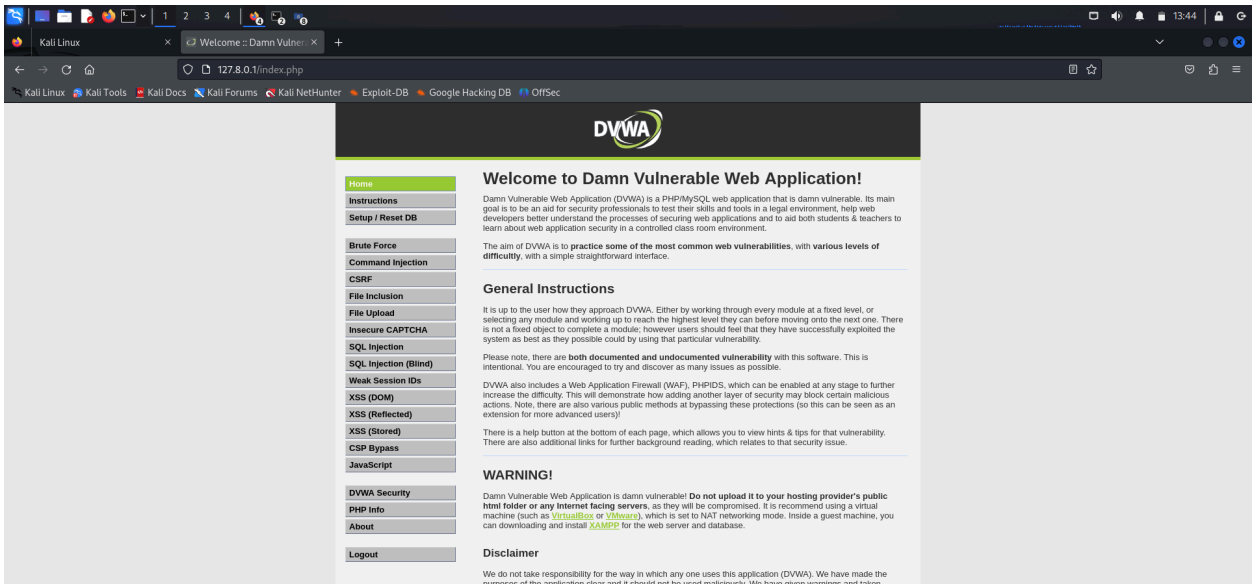


Now we can access it via web browser at:

- http://dvwa
- http://127.8.0.1



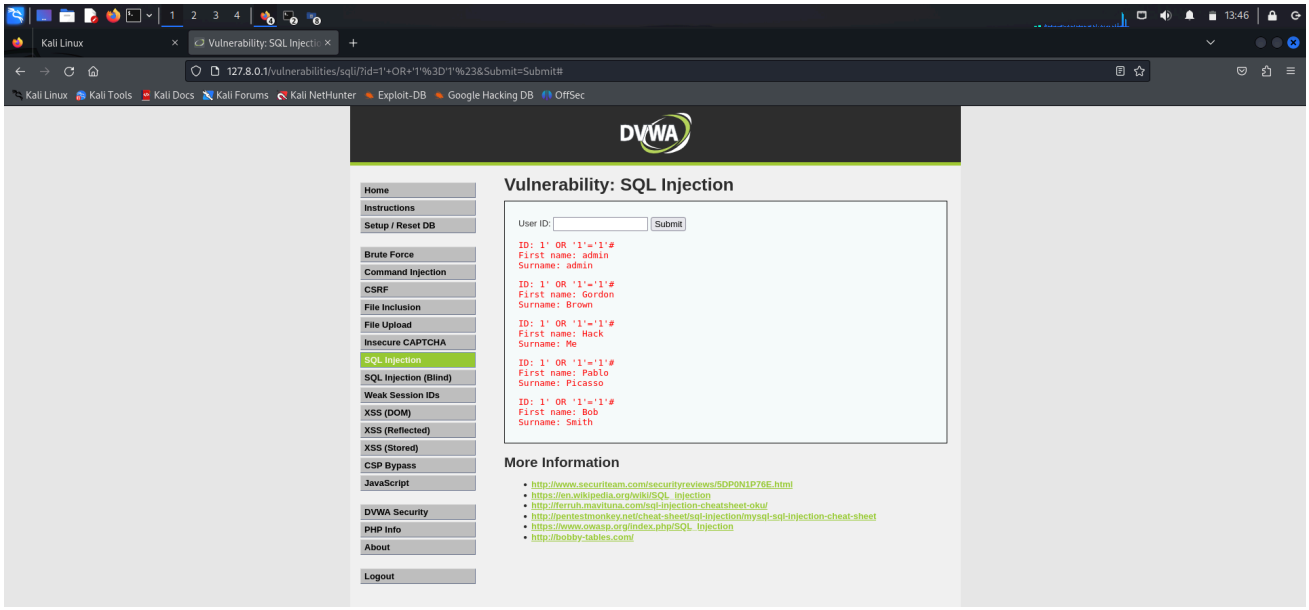
The default username is admin and password is password. Then in the next page you should be asked for reset your database. Click that button. Installation complete.



Then once again you will be redirected to login page, use the default credentials again. Then you will get to see this page.

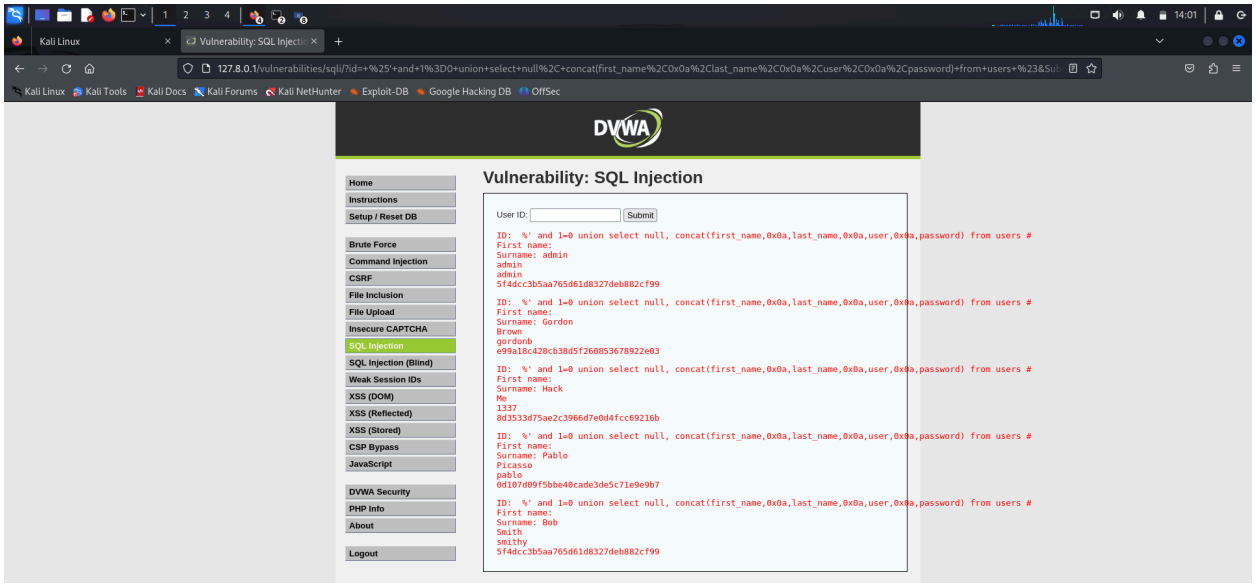
SQL injection(low)

We can easily inject the code in the user ID form.



Using 1' OR '1'='1'# , it is able to see first name and surname.

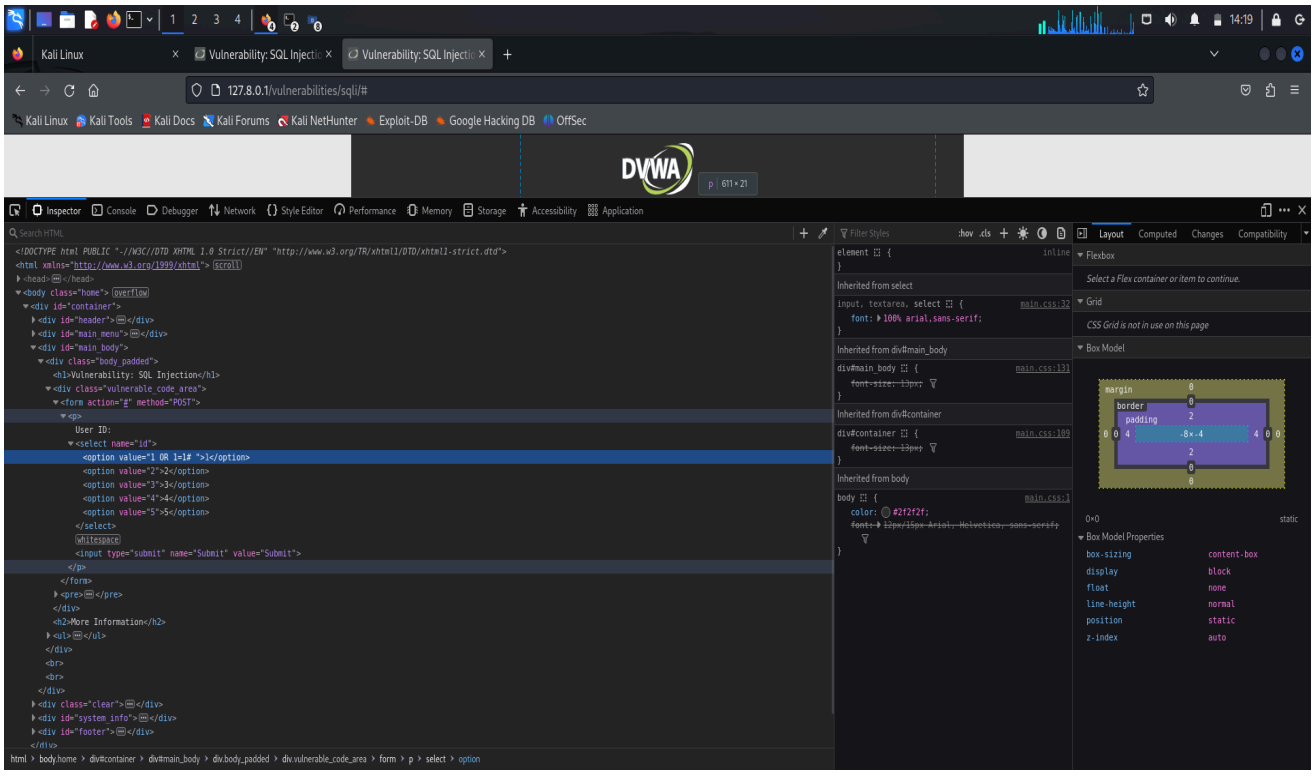
Using %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users # , Got the first and last names and cookies of the users.



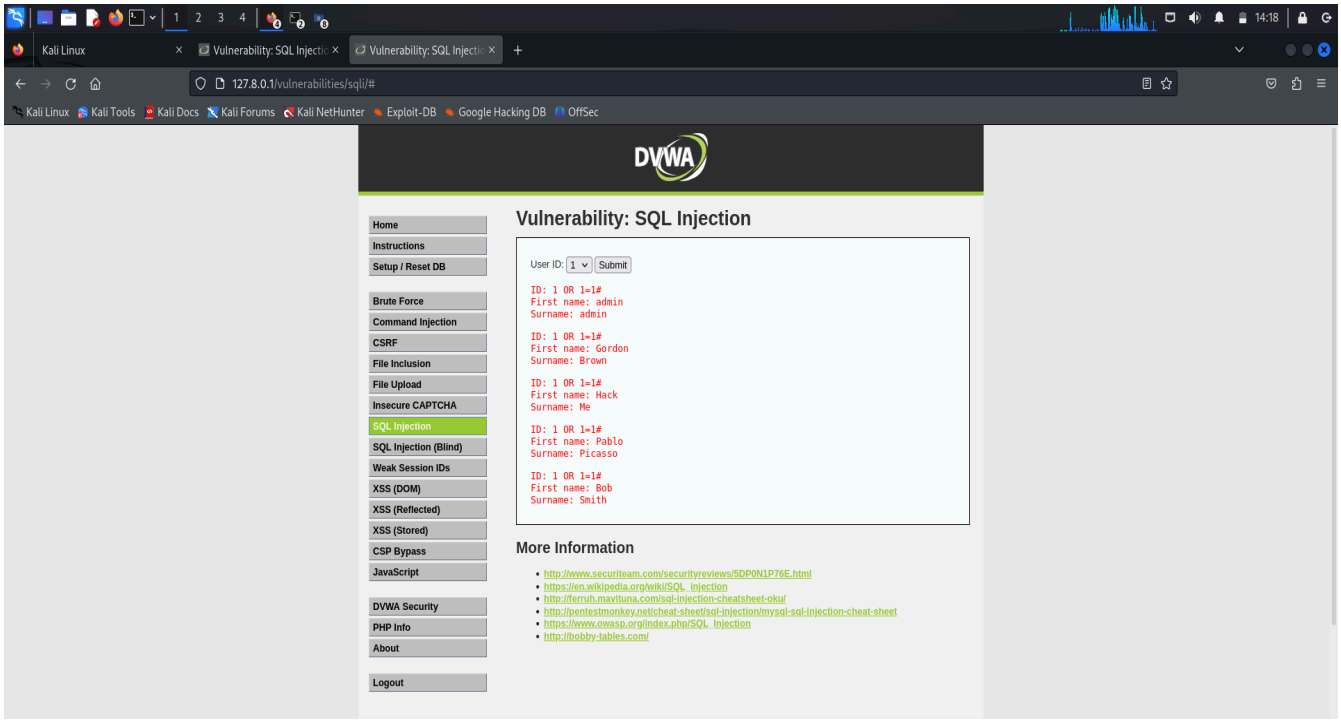
SQL injection(medium)

No comment options to inject in medium level.

Then i inspect the page after submitting the User ID as 1.Then injected OR 1=1#



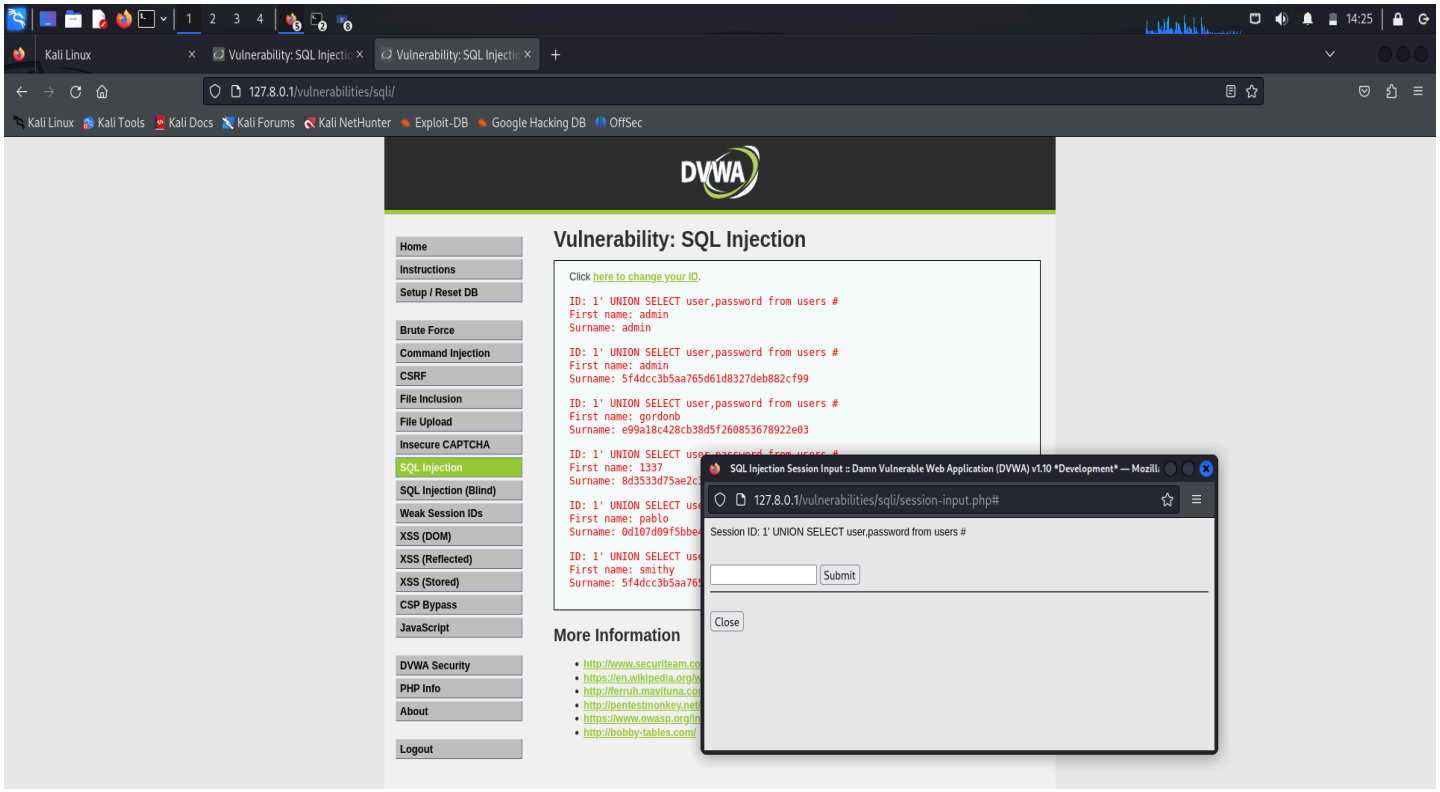
command on any value of the userID button and then I clicked submit.



Able to see other users first name and last name.

SQL injection(High)

In this phase clicking the link another window of a box to text session id is available.



Injecting 1' UNION SELECT user,password from users # in the box.I got the first names and session cookies of the users.