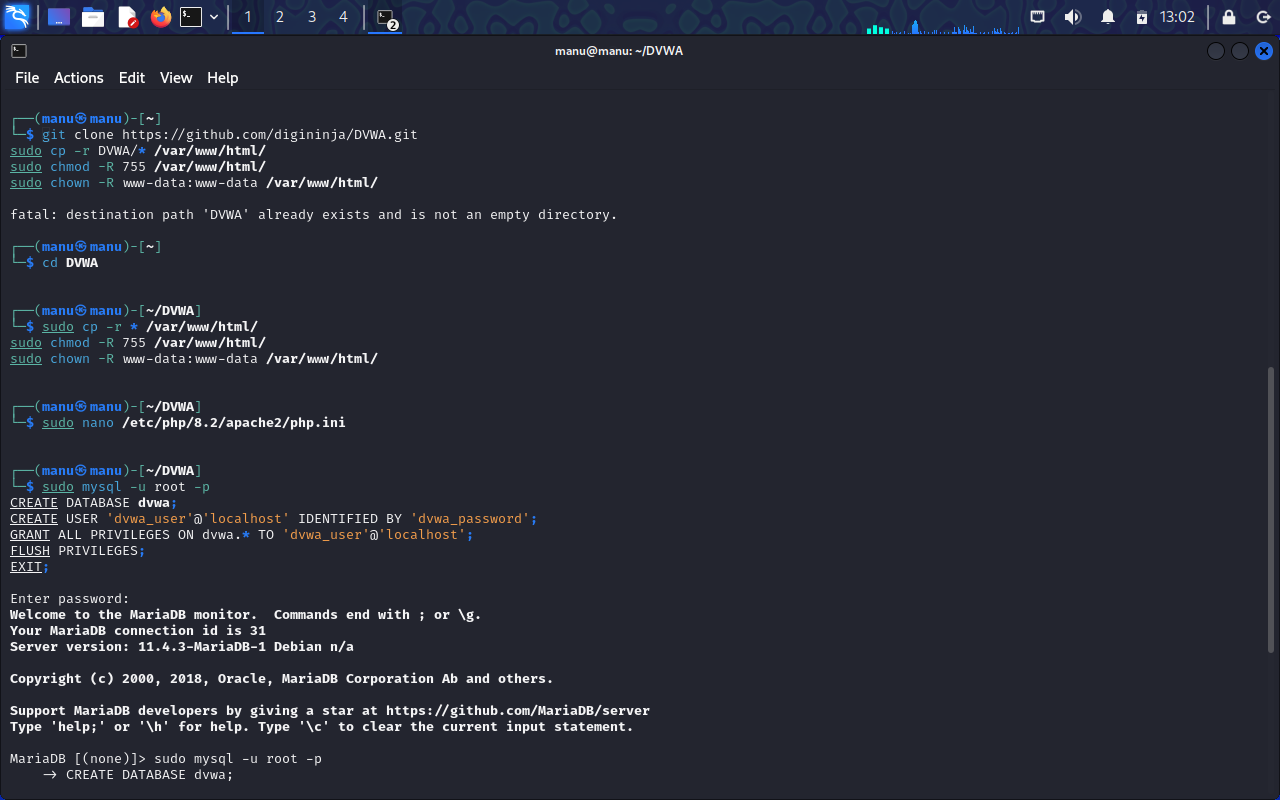


DVWA

SQL INJECTION

Manu Mohan M | CSA | 06-10-2024

# Installing DVWA

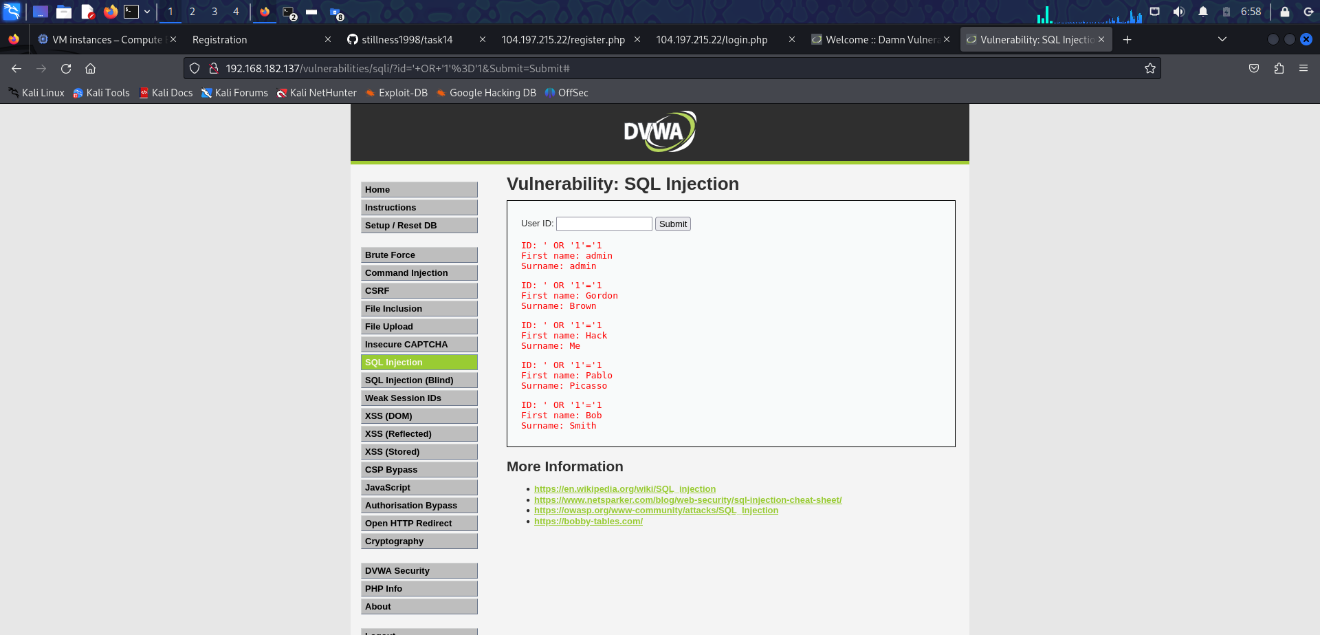


As you can see, I have already installed DVWA. I apologize for not taking screenshot of installation in the first place. This screenshot is compensation for that so that readers can understand how installation is done.

After installation, we will be directed to DVWA website. You can use admin as username and password as password.

## SQL Injection (low)

Set the DVWA security to low and go to SQL injection page. From there, you can begin.

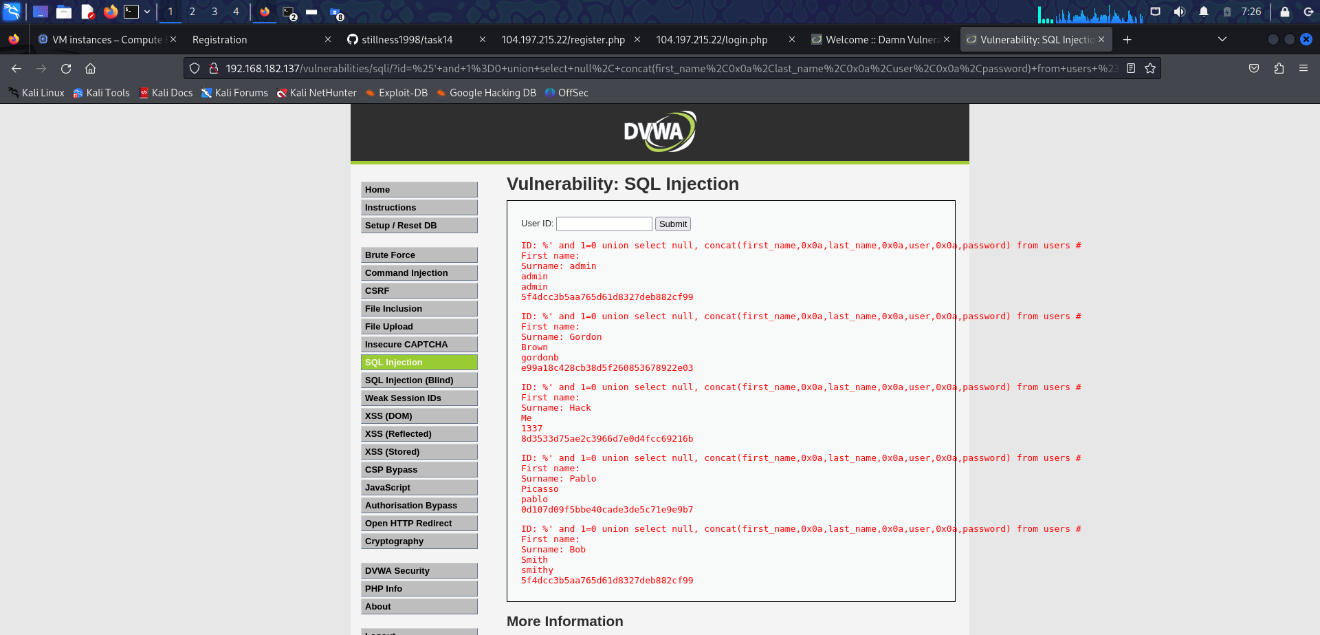


Here, it is very basic to understand and deploy. All you have to enter the following in the box that is shown in the screenshot.

' OR '1'='1

Now you see the exploited results but we’ll go a step further.

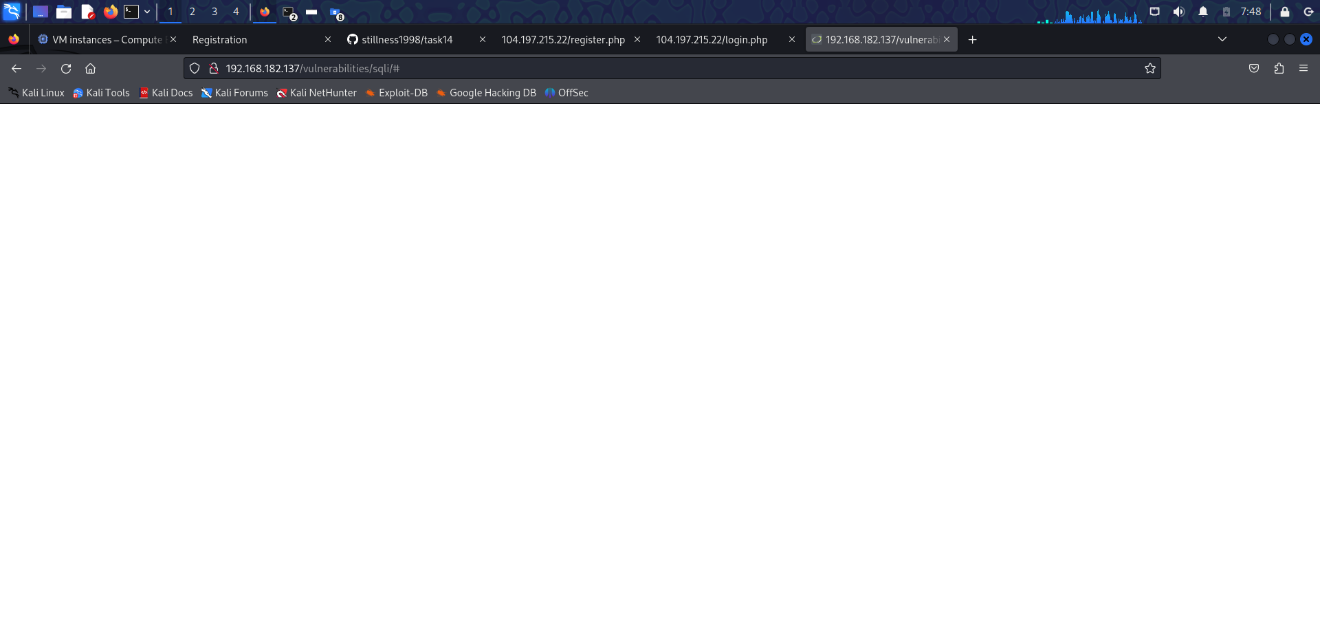
' OR 1=0 UNION SELECT NULL, CONCAT(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) FROM users #



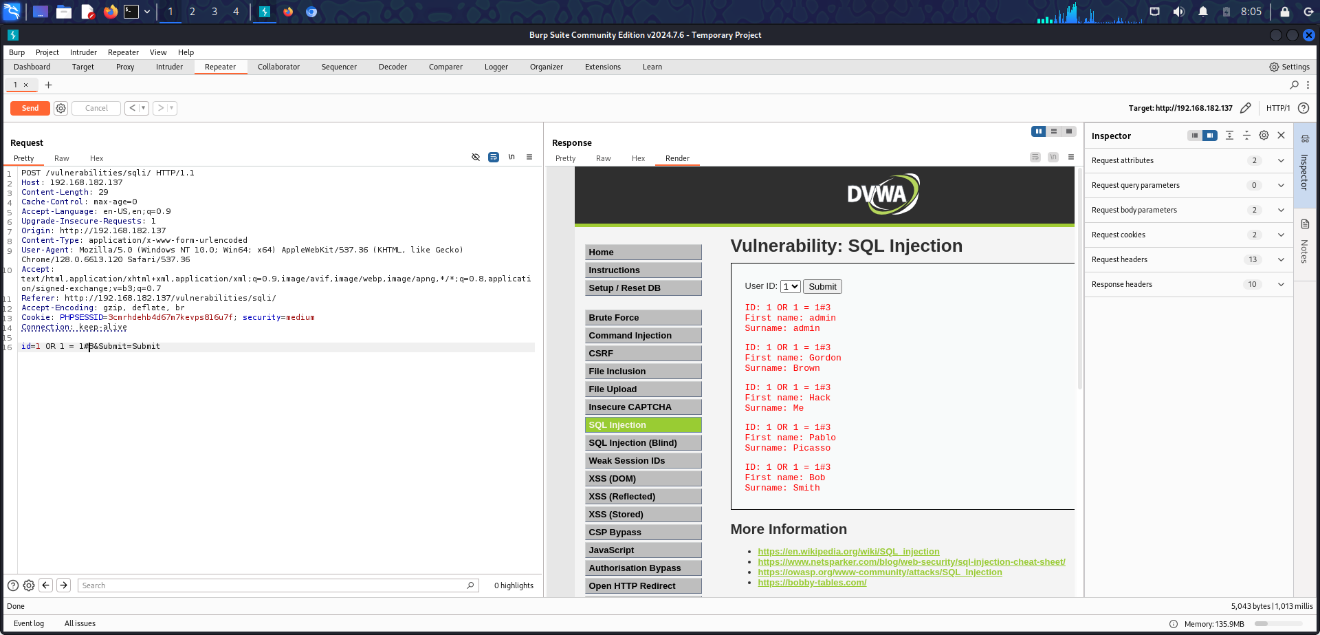
# SQL Injection (Medium)

Set low to medium in DVWA Security and we shall begin.

While trying to exploit, unfortunately, the site crashed. So, I used burp suite.



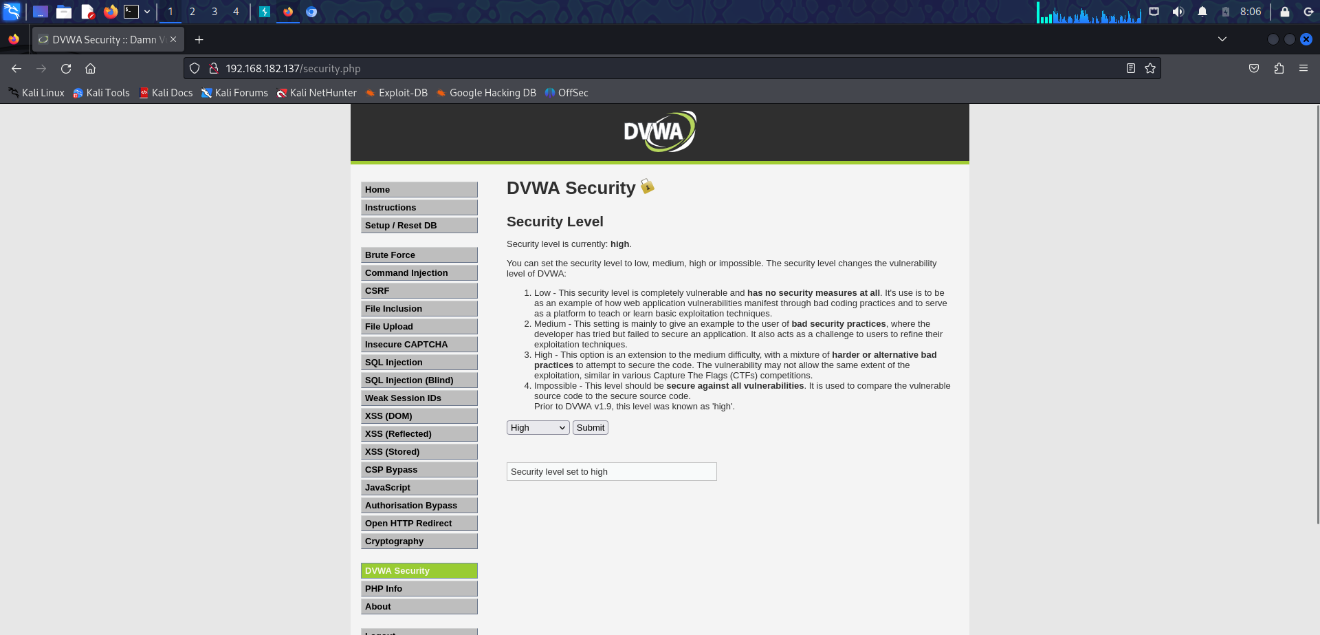
While using burp suite, I looked into request and saw id parameter. Then decided to exploit. Left click and click on the “send to repeater”.

Here, we need to change id parameter from 1 to 

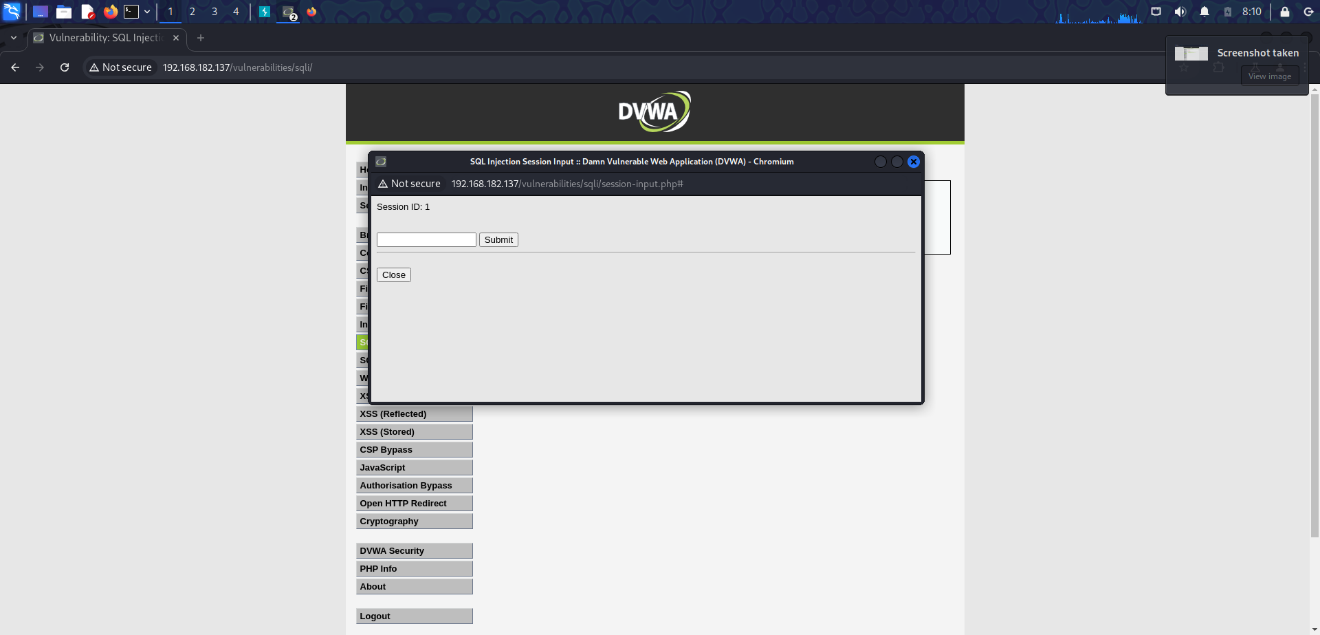
1 OR 1=1#

We successfully exploited.

# SQL Injection (High)

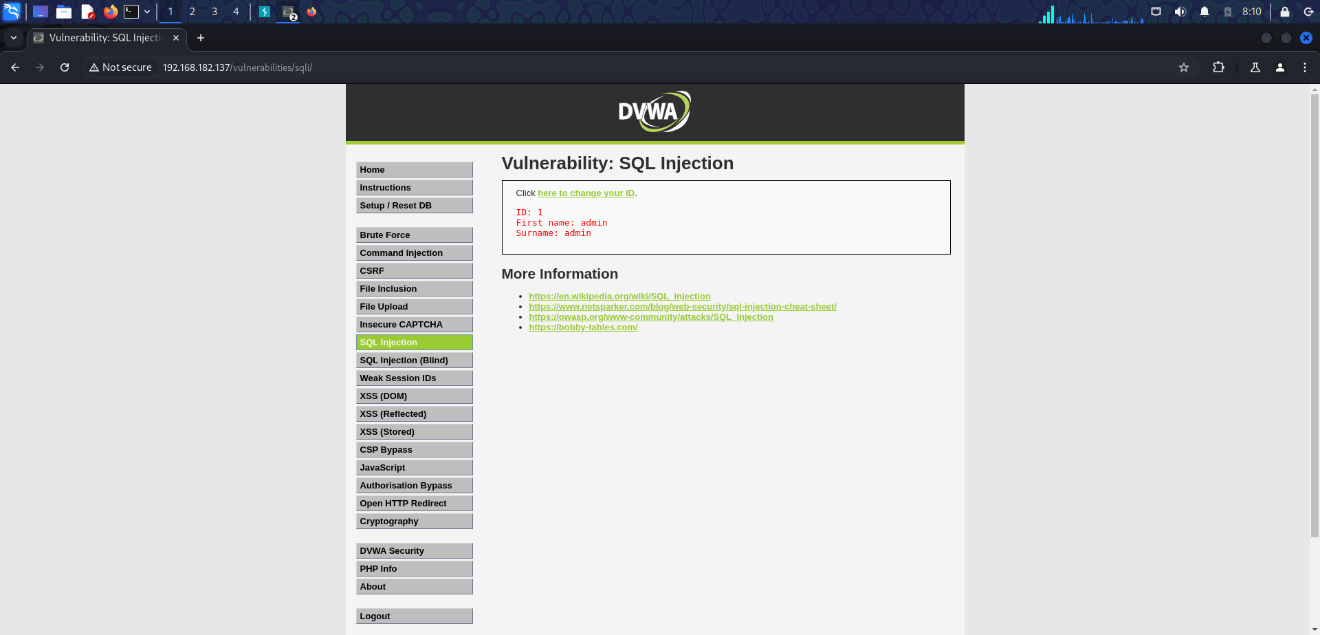


Set medium to high in DVWA security and here we begin.

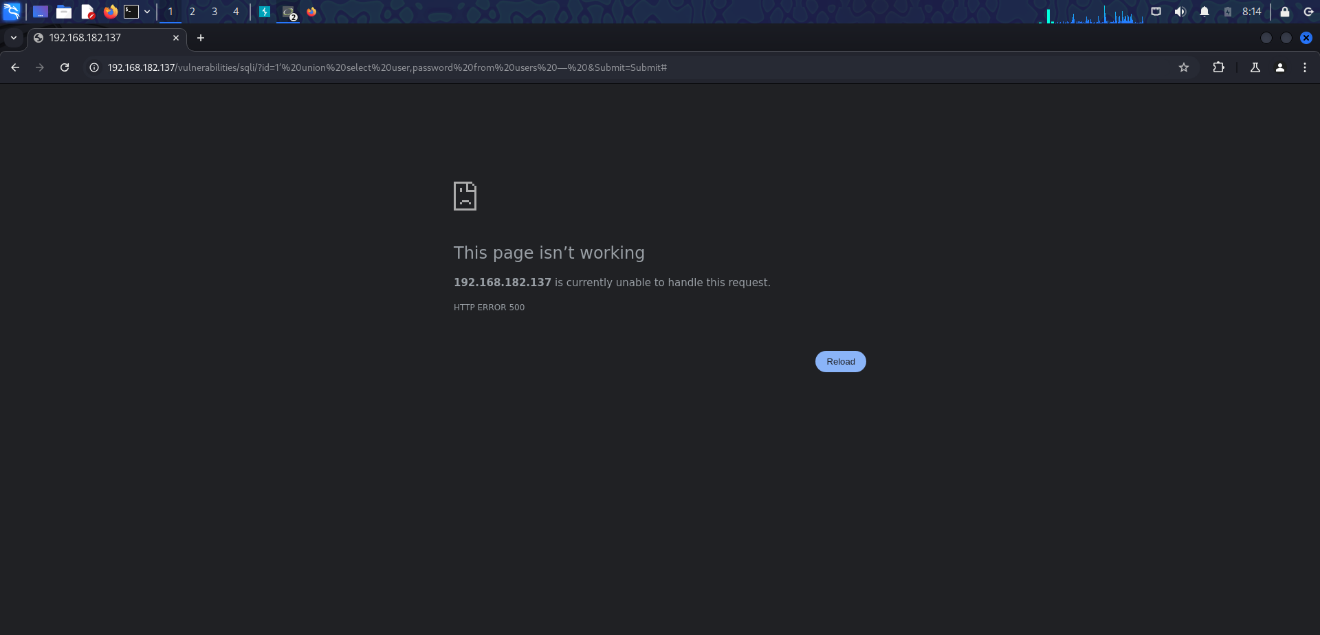


After clicking on the link and submitting value 1,

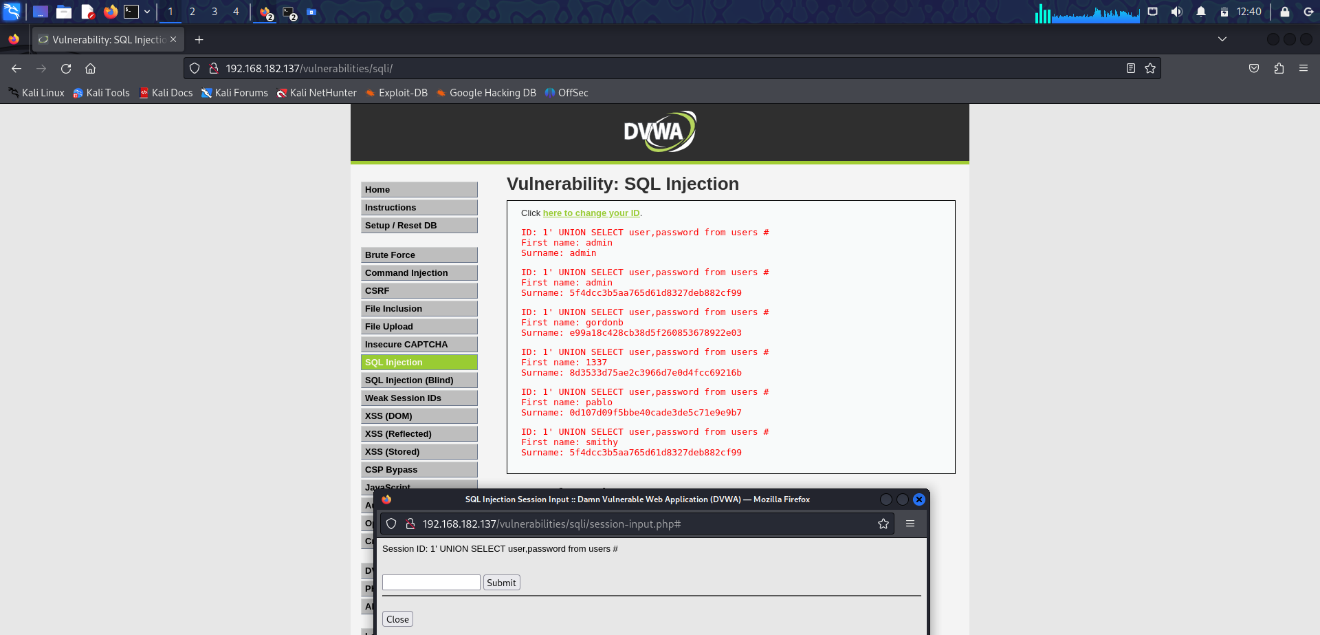
We get,



So, we understand that exploitation is basically same as medium. You can use burp suite or SQL map to exploit but they can be tedious and time consuming. Not to mention, risking crashes like I got



What we need to do is this,



1’ UNION SELECT user,password from users #

Finally, we have got the results of the exploitation.