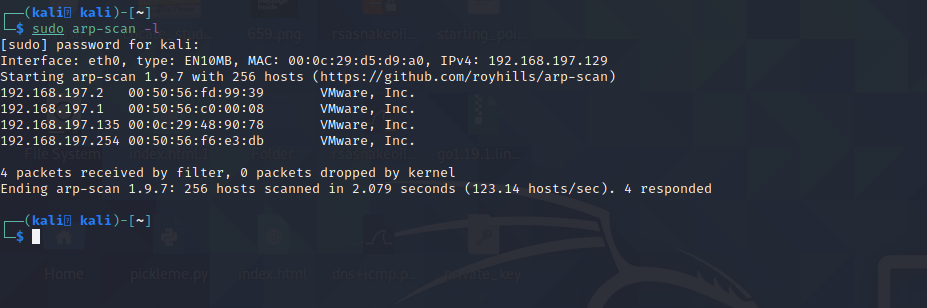
**Name: Shangirne Kharbanda**

**Registration Number: 20BAI1154**

**ISM LAB – 10**

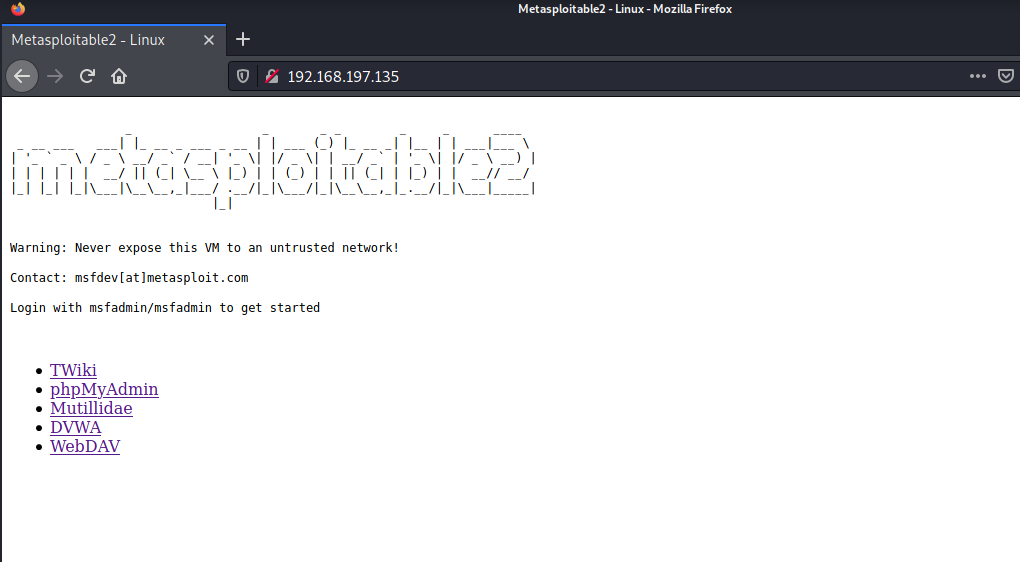
**SQL INJECTION**

We will first run an **arp scan to find out the IP of metasploitable**.



We can see that the **IP of metasploitable2 is 192.168.197.135**

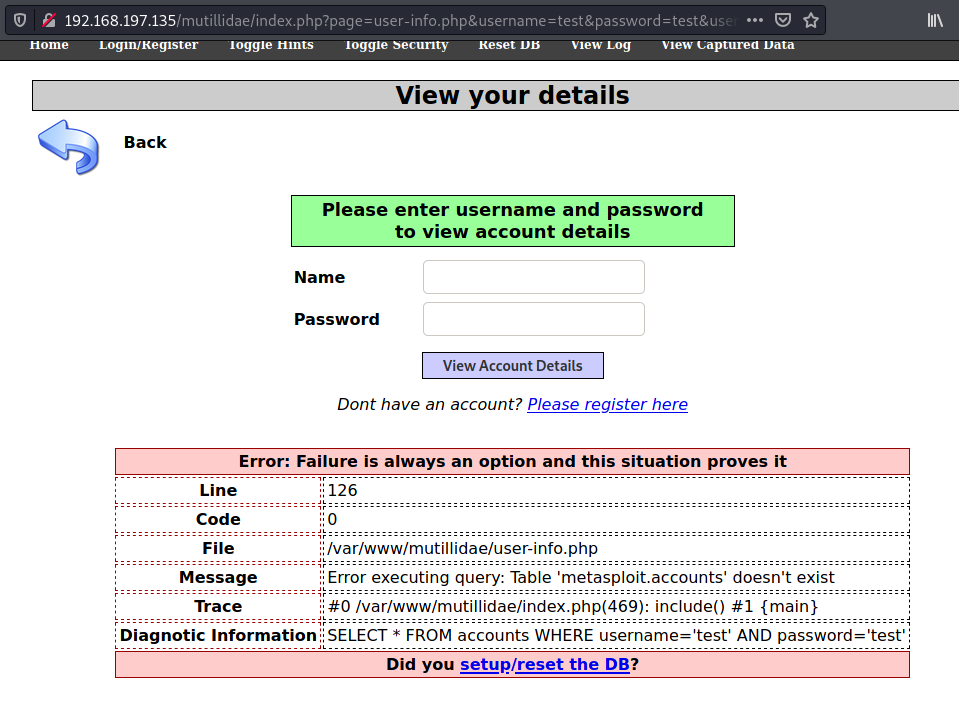
Now we type this IP in the browser of Kali.



Now we will open Mutillidae, go to OWASP Top 10, Injection and click on SQLi – Extract data.

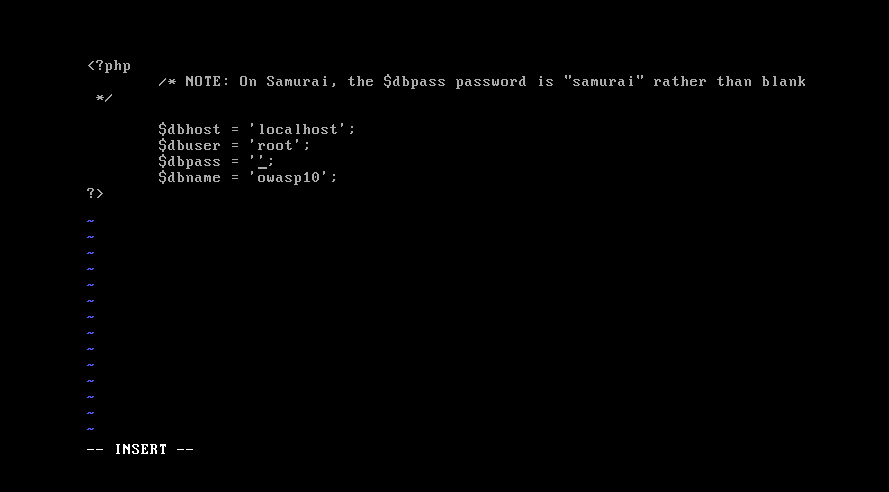


We will type in the default name and password of “test” and “test”.

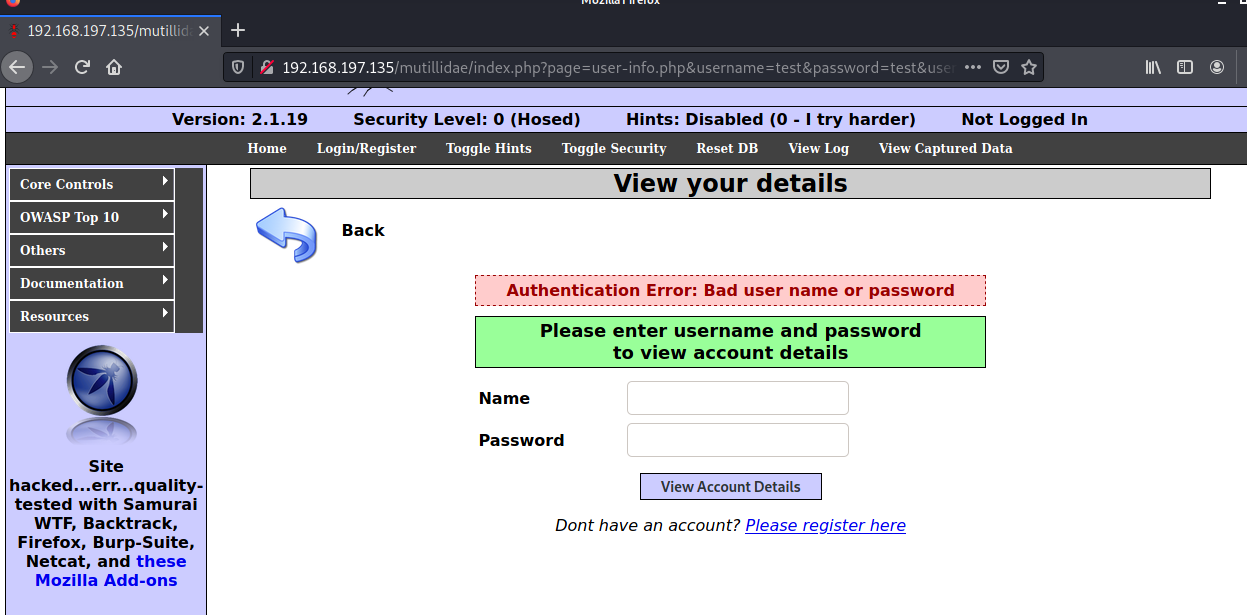


We need to setup the db in Metasploitable2 now.

Now we open Metasploitable 2 and change the configuration file to change the DB name to owasp10.



We will now check if we get an authentication error or not.

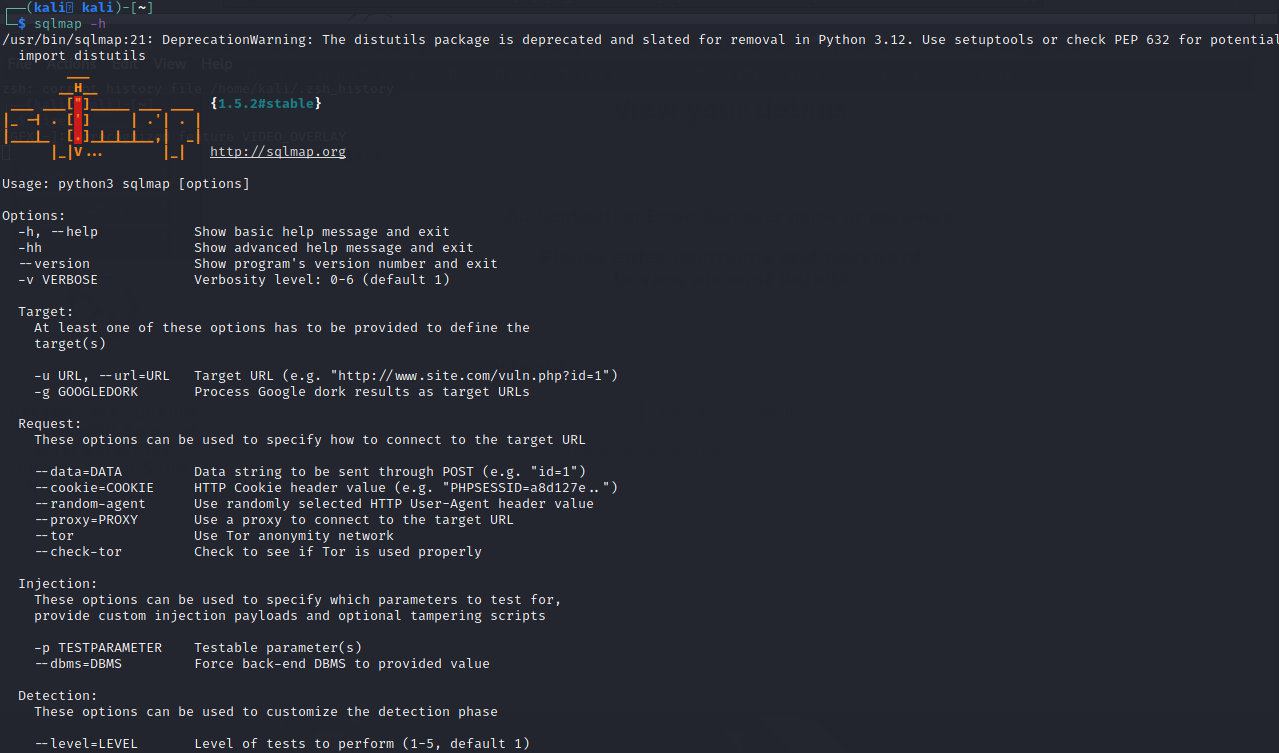


We are getting an authentication error now.

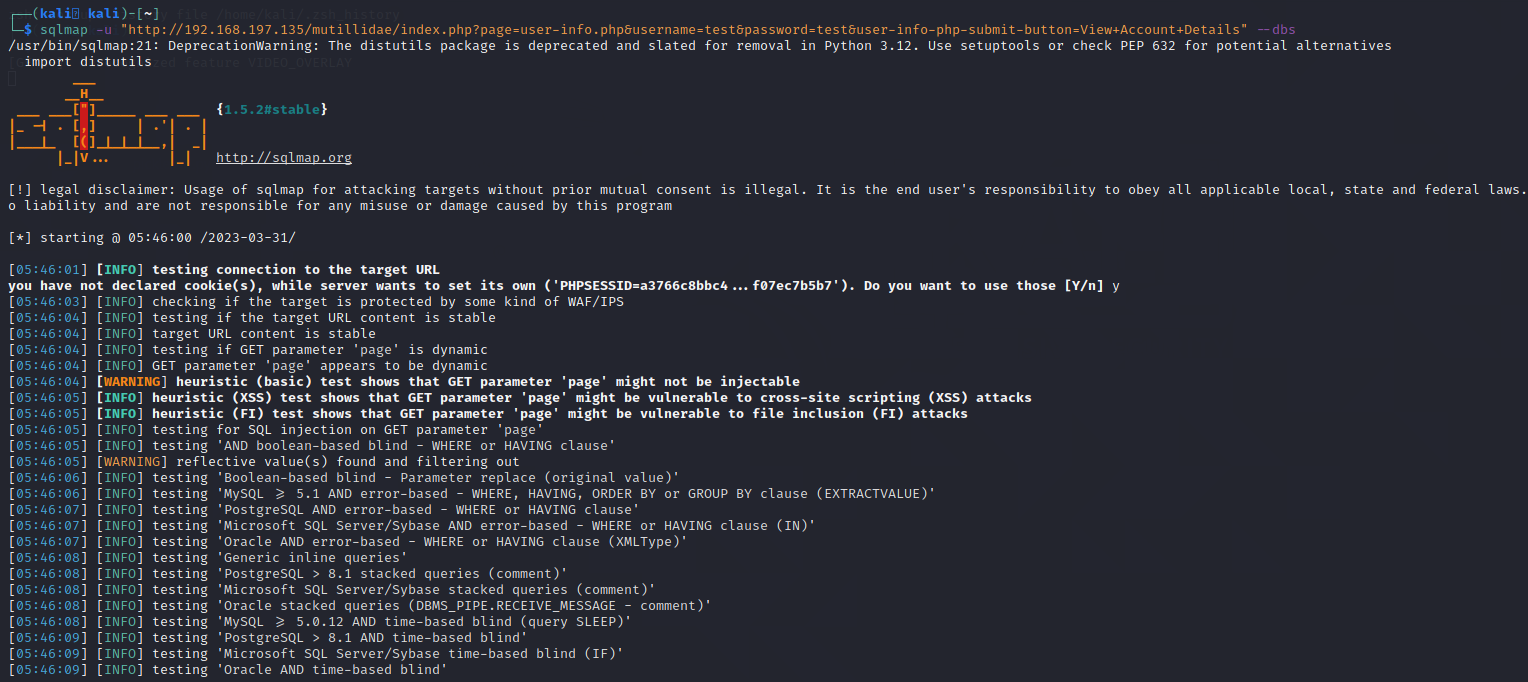
So we will now use **Sqlmap** to get information on the databases in the URL and potentially dump everything in it.

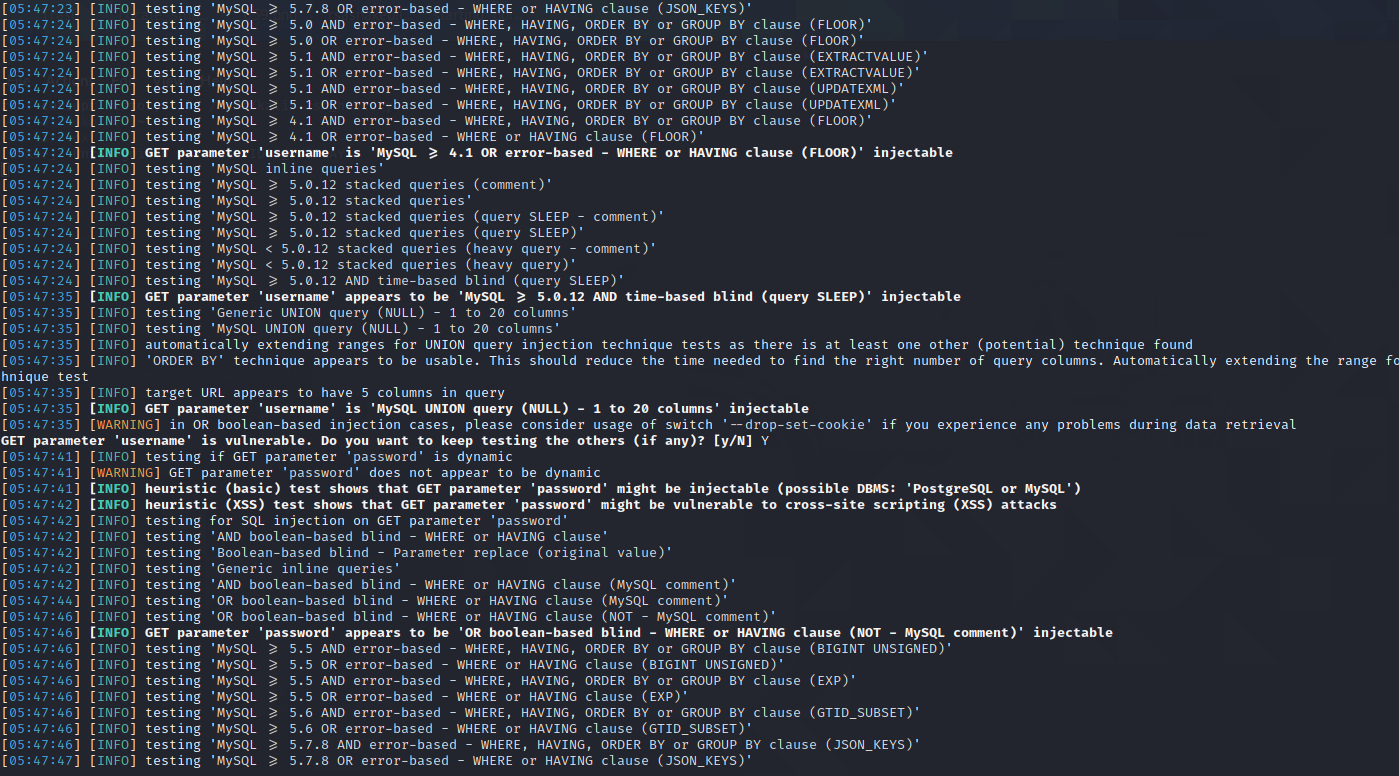
Now we will open sqlmap.

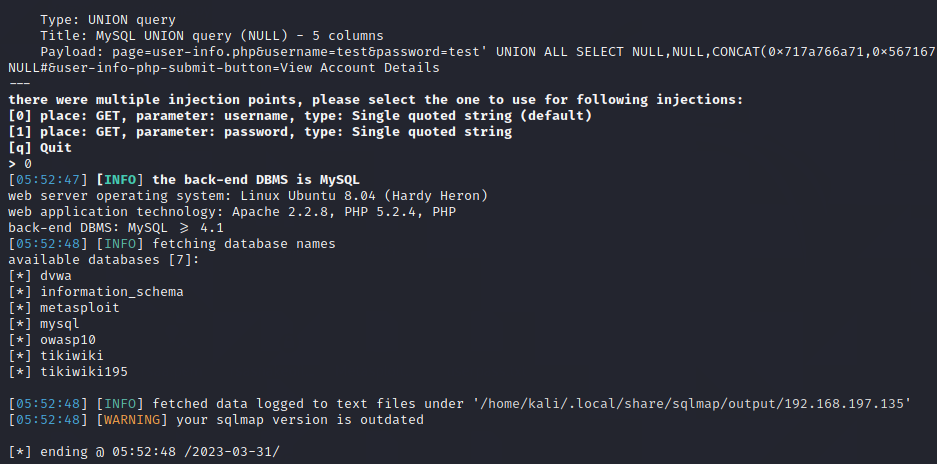
To get help with this tool, we will type sqlmap –h and explore our options.



To view databases inside the URL, we will type in the following command shown in the screenshot below.

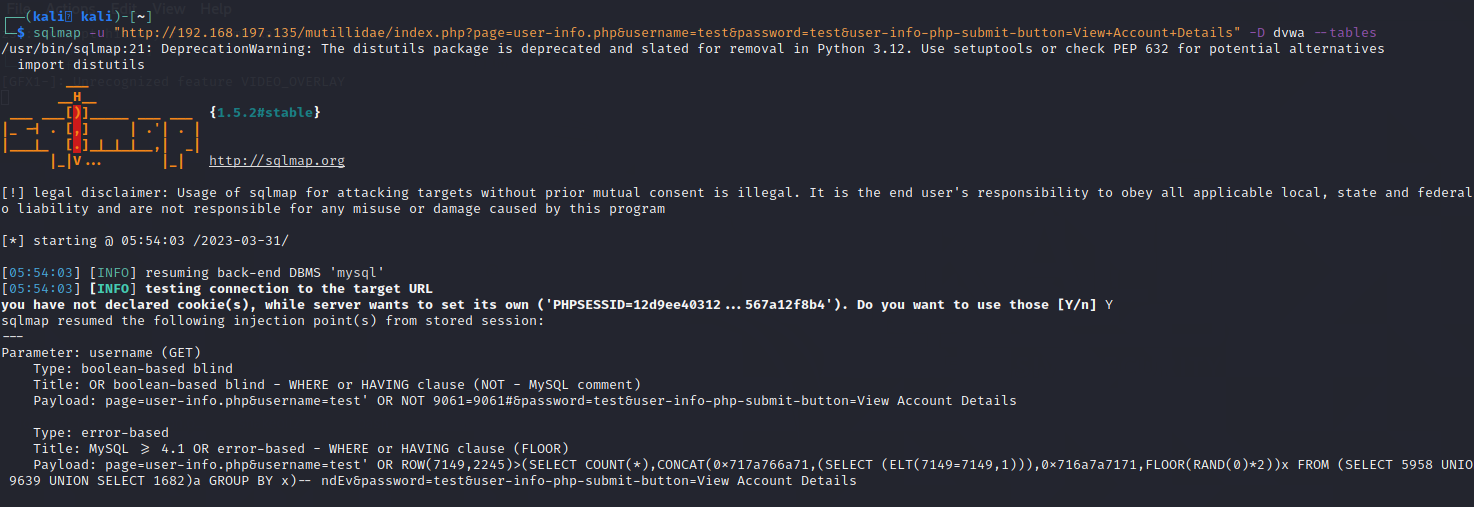


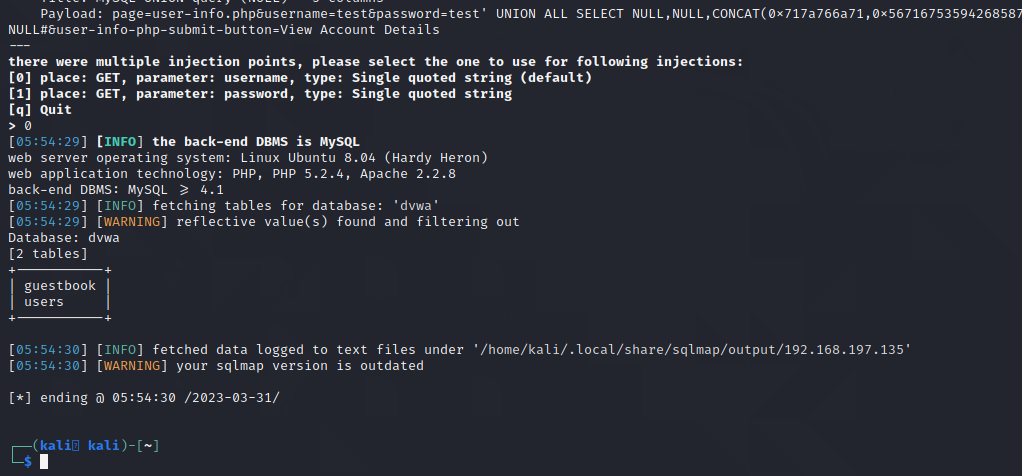




There are 7 databases as shown in the screenshot above.

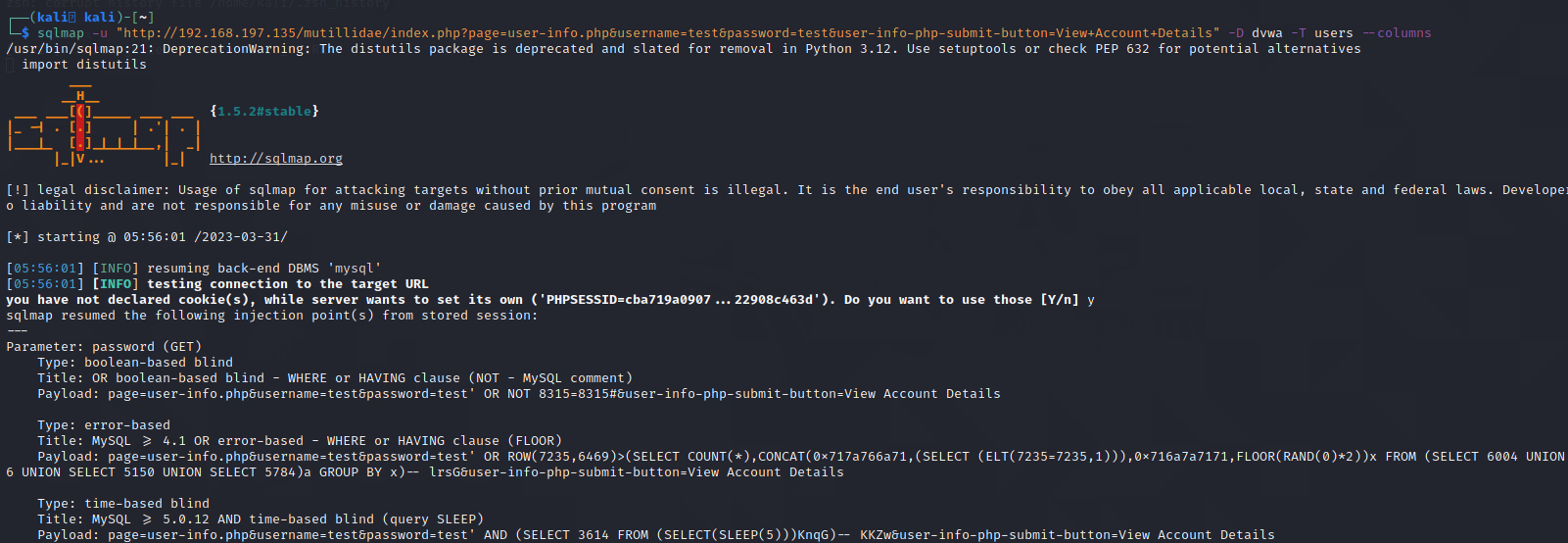
Now we will view tables inside the DVWA database by using sqlmap.

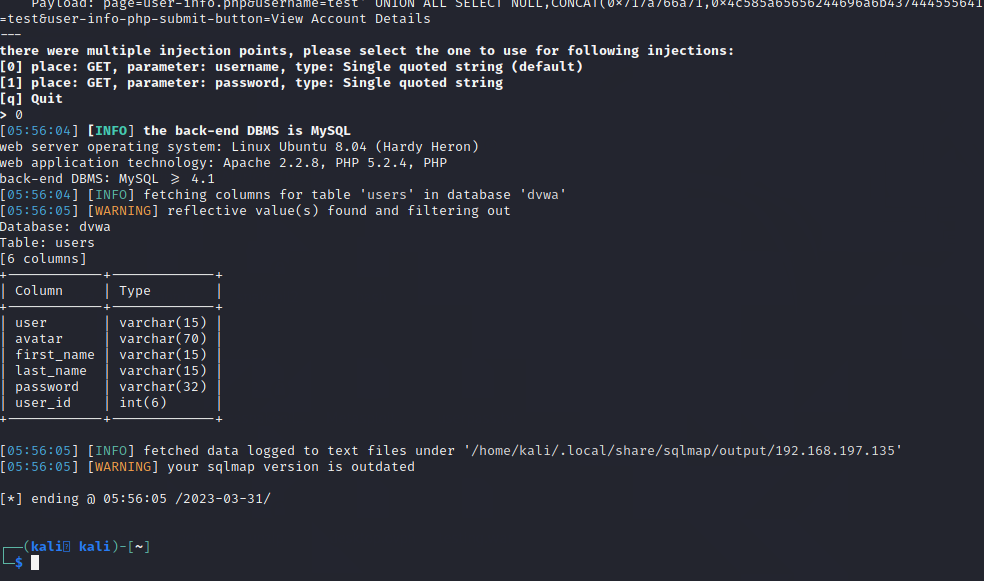




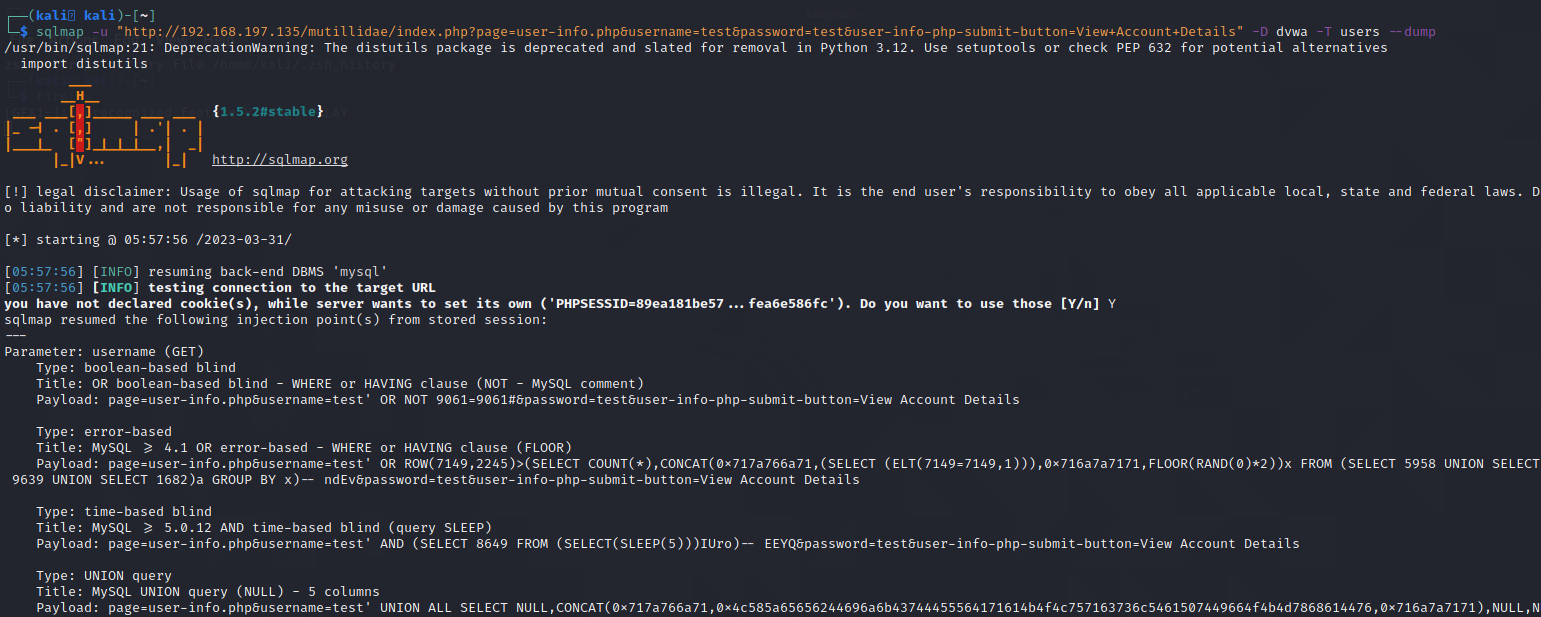
There are two tables in the DVWA database namely “guestbook” and “users”.

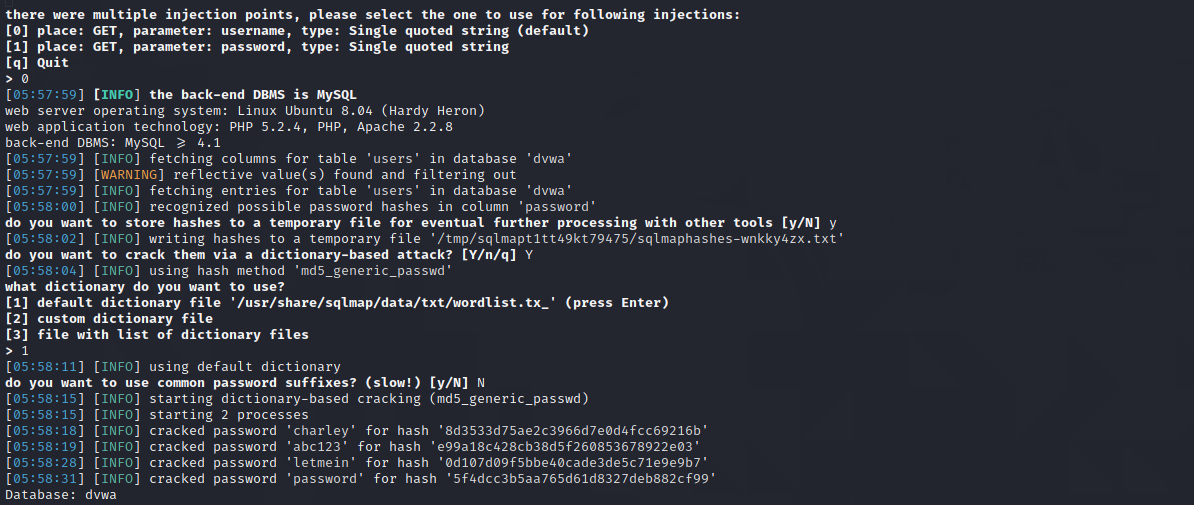
We will now use sqlmap to view columns inside the users table by typing in the command shown in the following screenshot.

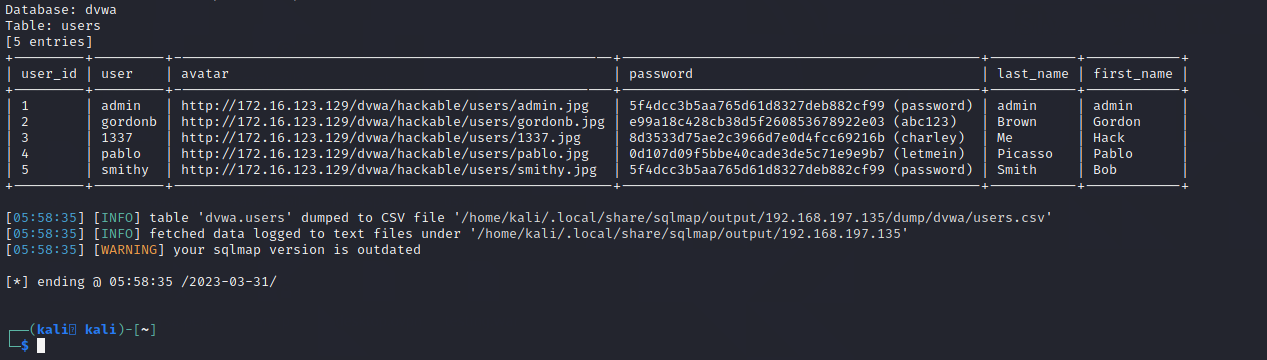




To view all data inside the users table, we will again use sqlmap and type in the following command.







We got all the information in the users table and the tool sqlmap even cracked the hashes for us by using a dictionary attack.

**Thus, we have gotten all the information in the users table using the SQL injection tool sqlmap. Lab successfully completed.**