SQL map is a open vulnerable penetration test tool that automates the process of detecting and exploiting weaknesses in SQL injection(sqli) and taking over the server database SQL injection is a hacking technique where an attacker can insert SQL commands with a URL to be executed by the database located in the backend ,A database is a collection of information stored on a computer or a web server that is accessed by a front end client used for obtaining information from the database.

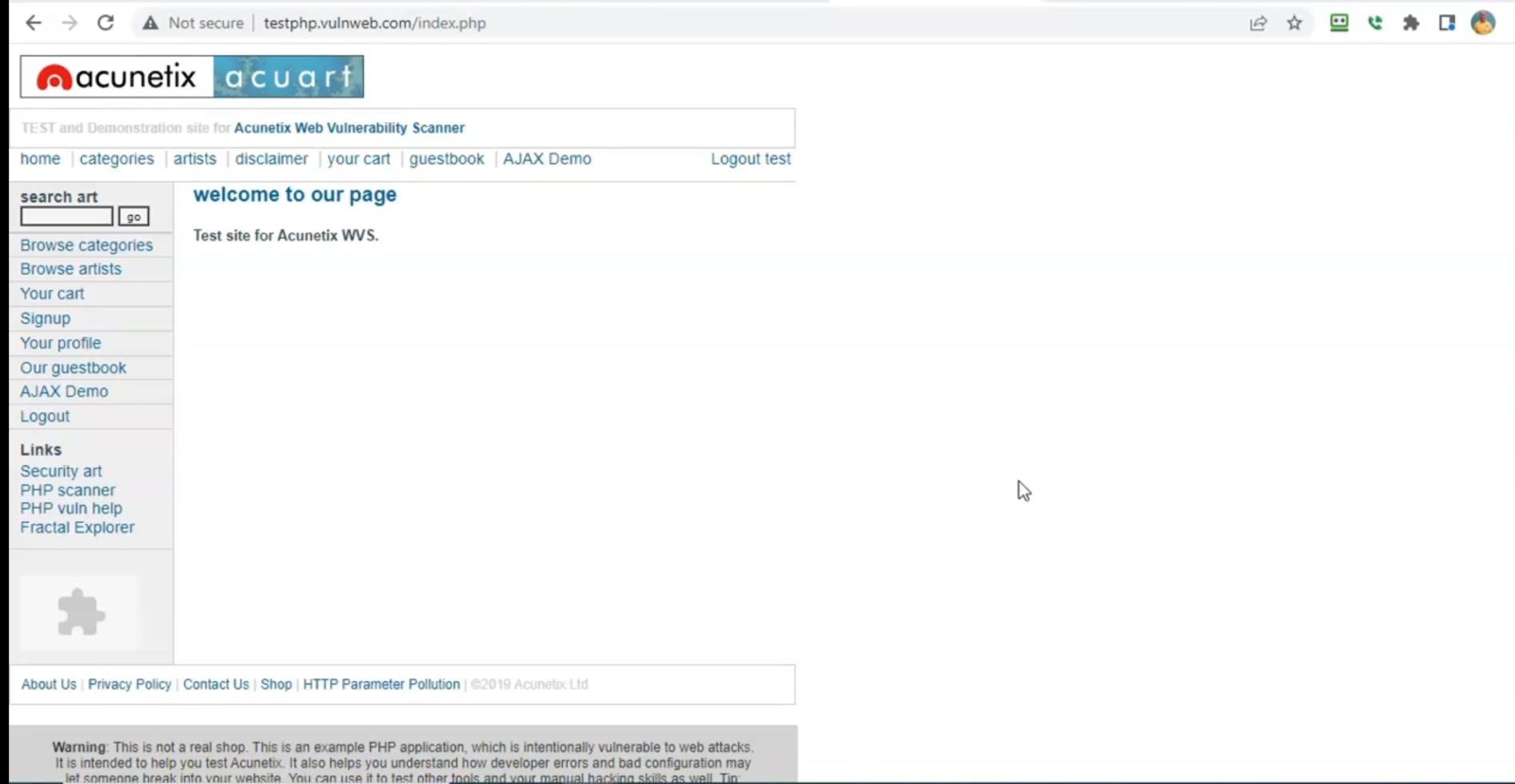
Use acunetix for web application vulnerability for SQL injection.

testphp.vulnweb.com/index.php

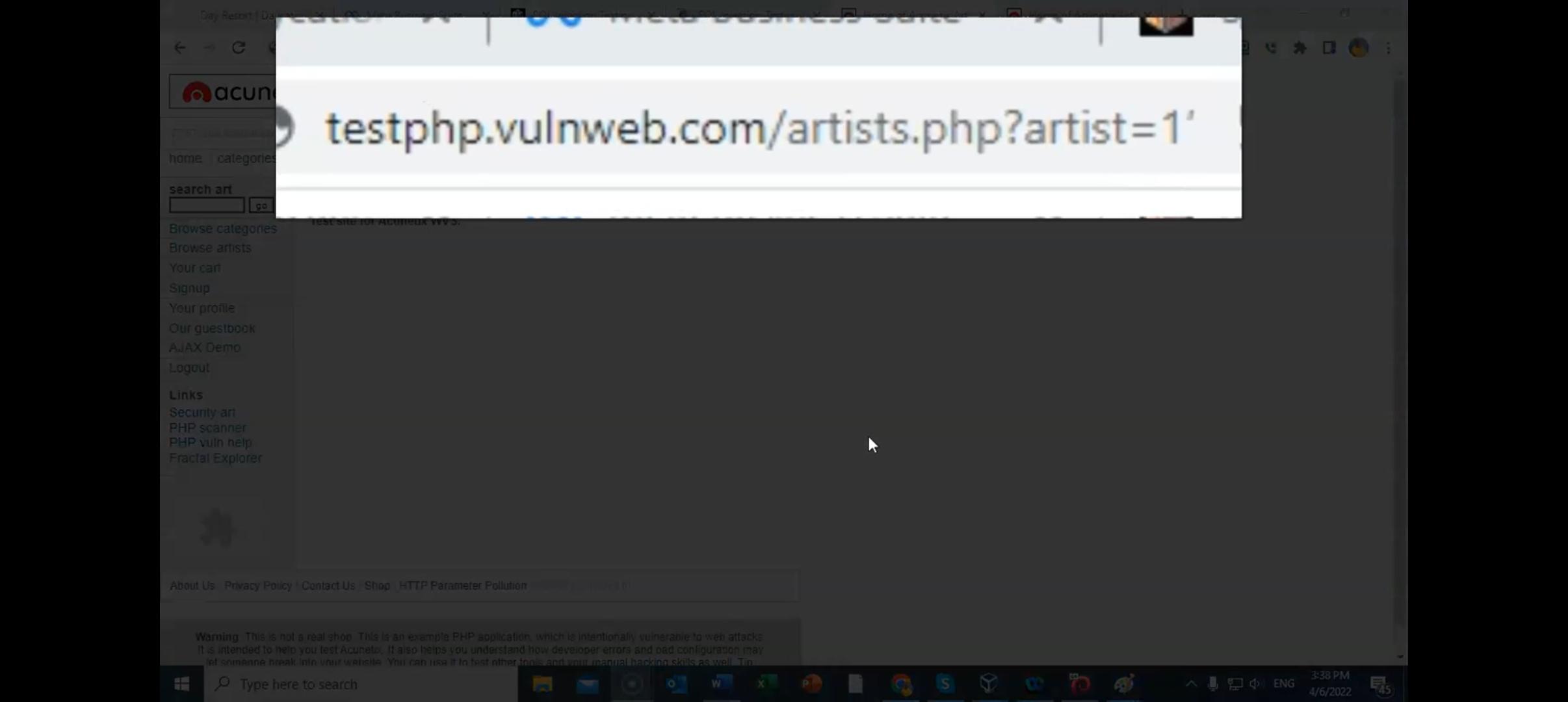
Type sqlmap -h in kali linux terminal

Now you can see all the different switches that you can use with sqlmap and since we know that acunetix website is vulnerable to a sql injection we can now attempt to find the databases ,what is and how many sql type are running on the server.

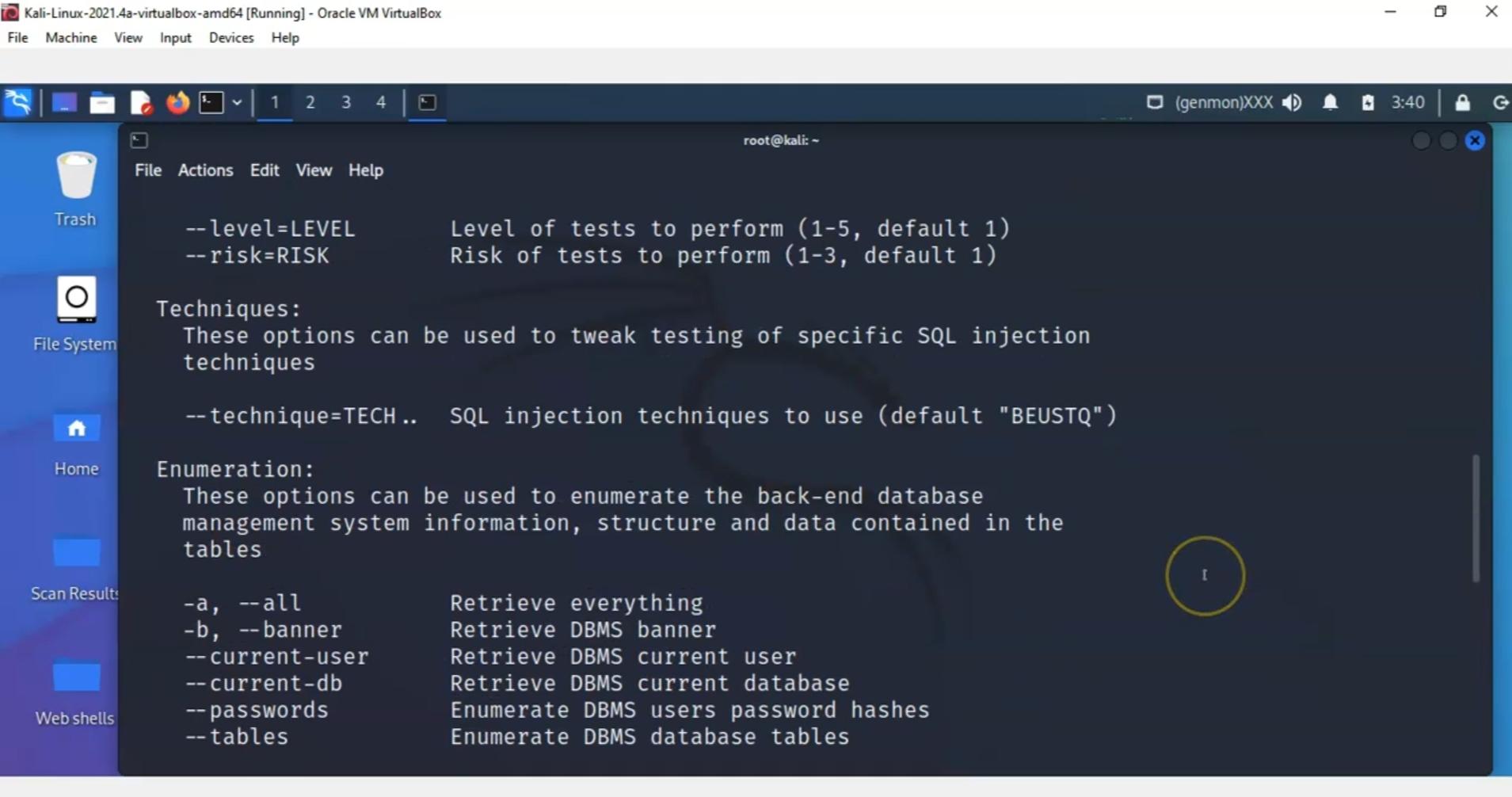
1.



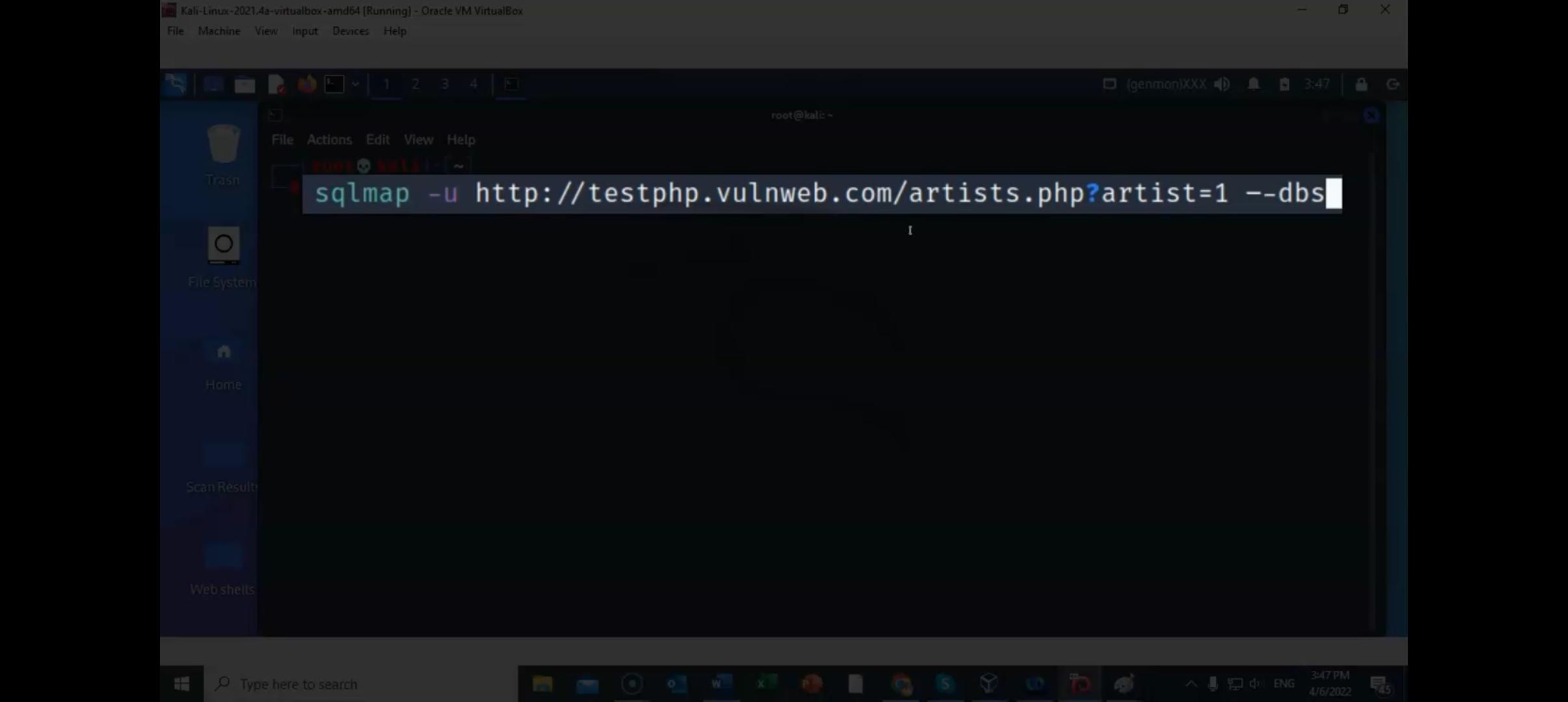
2.



3. Type sqlmap -h, It will list all the available services.



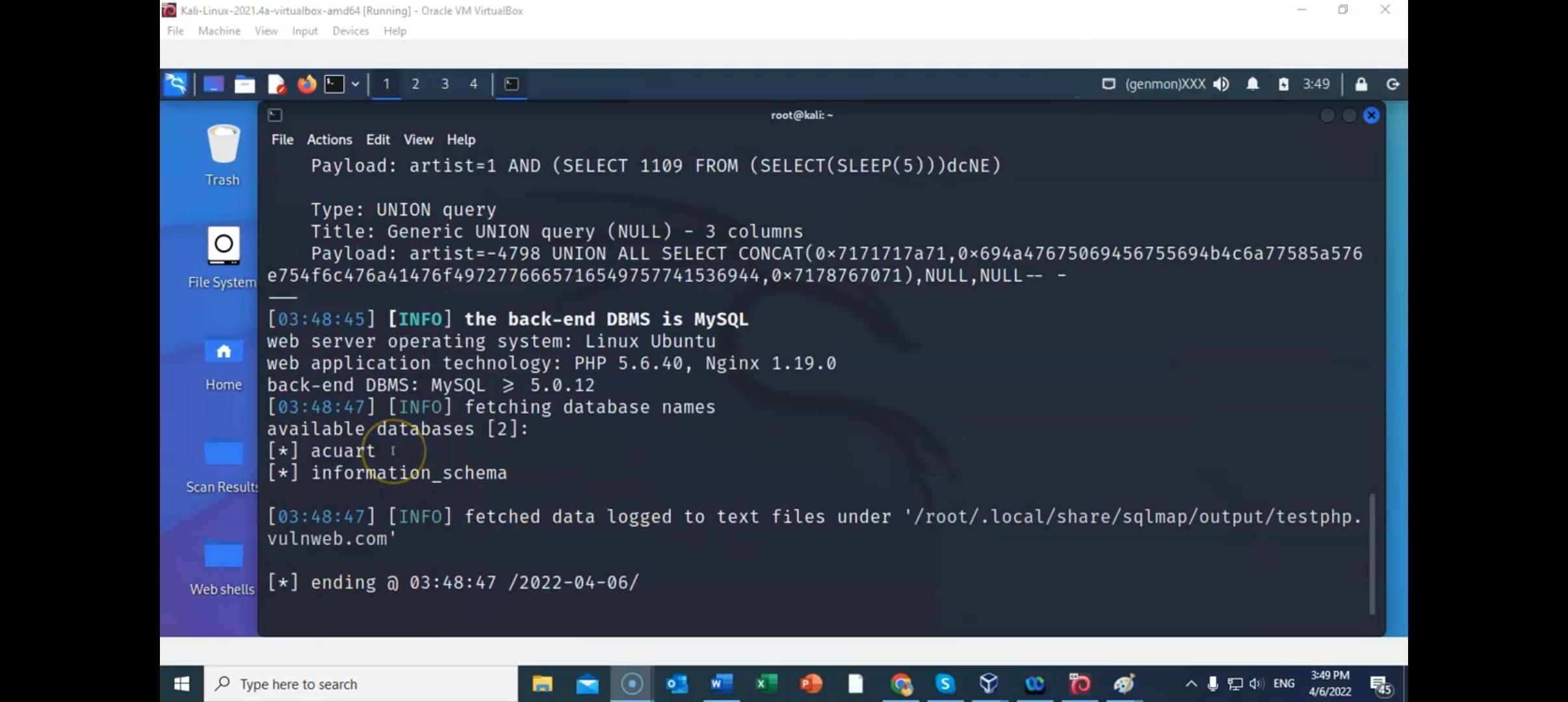
4. For accessing database type this command.



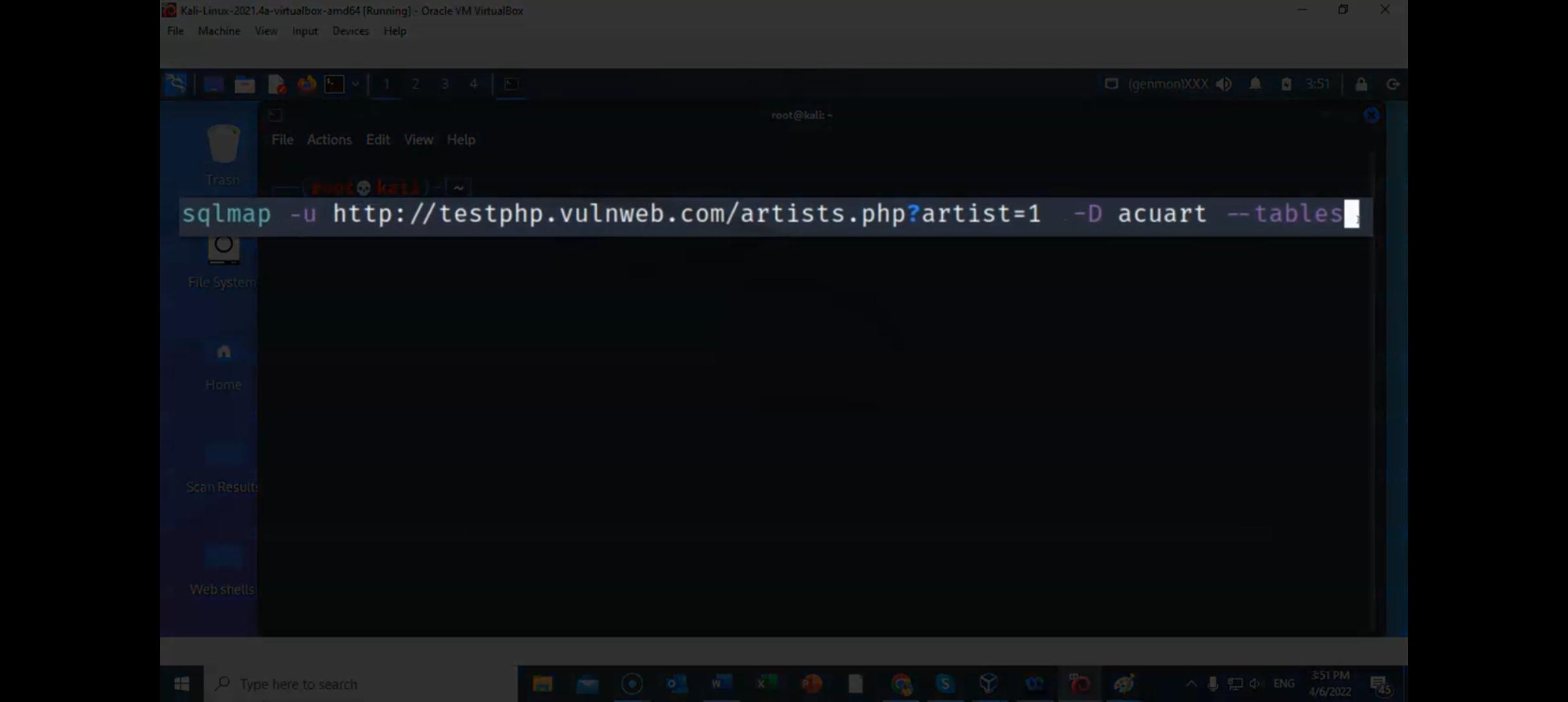
5. It will show 2 databases

1. acurat

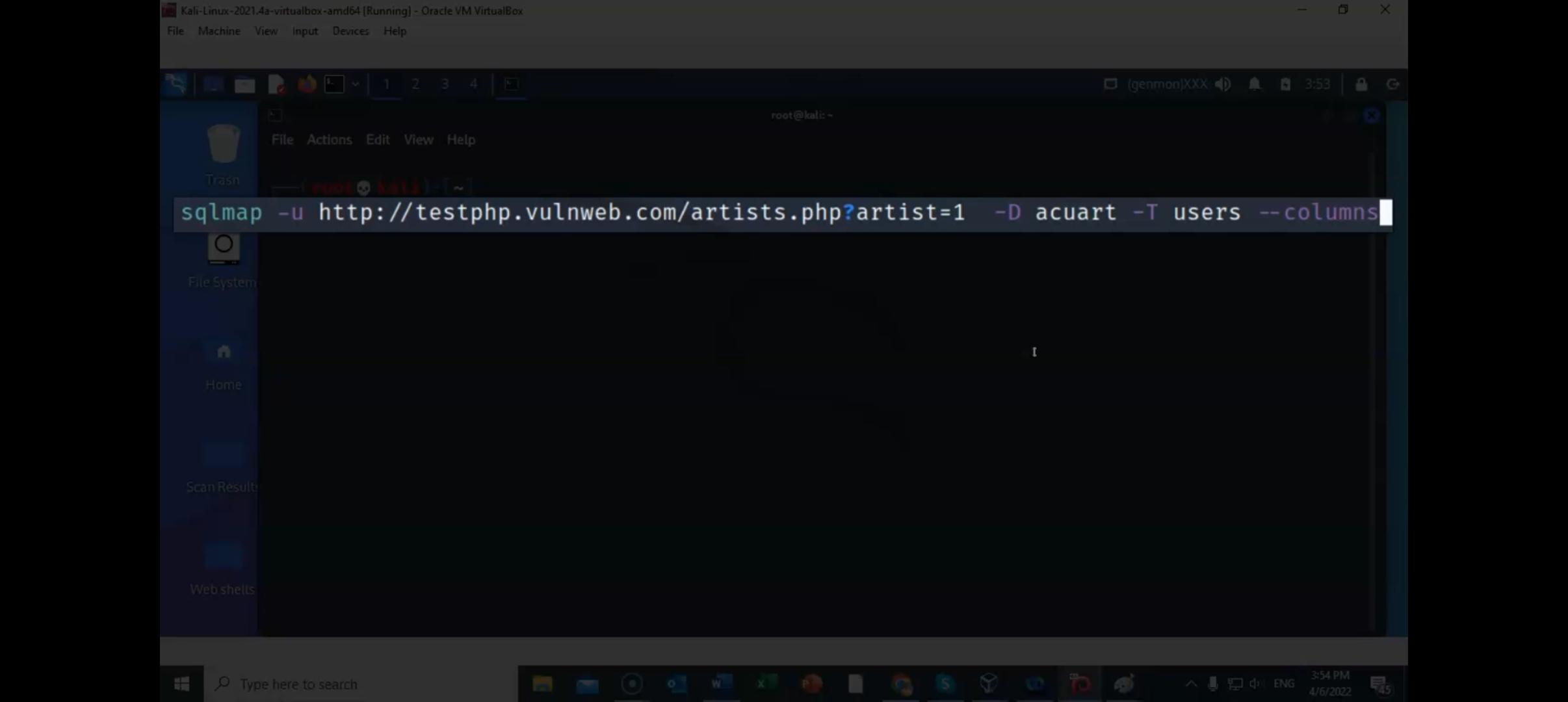
2. Information\_schema



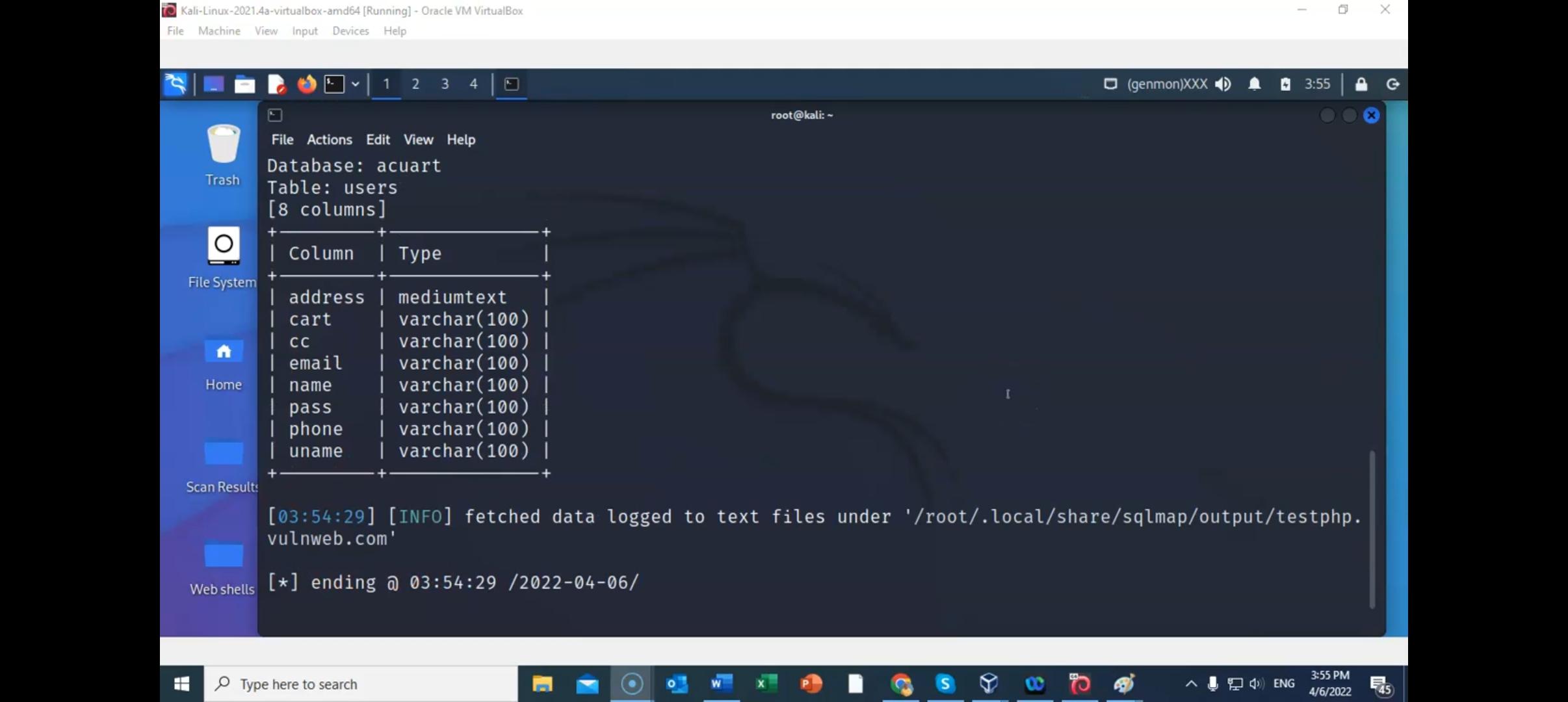
6. For accessing tables in database



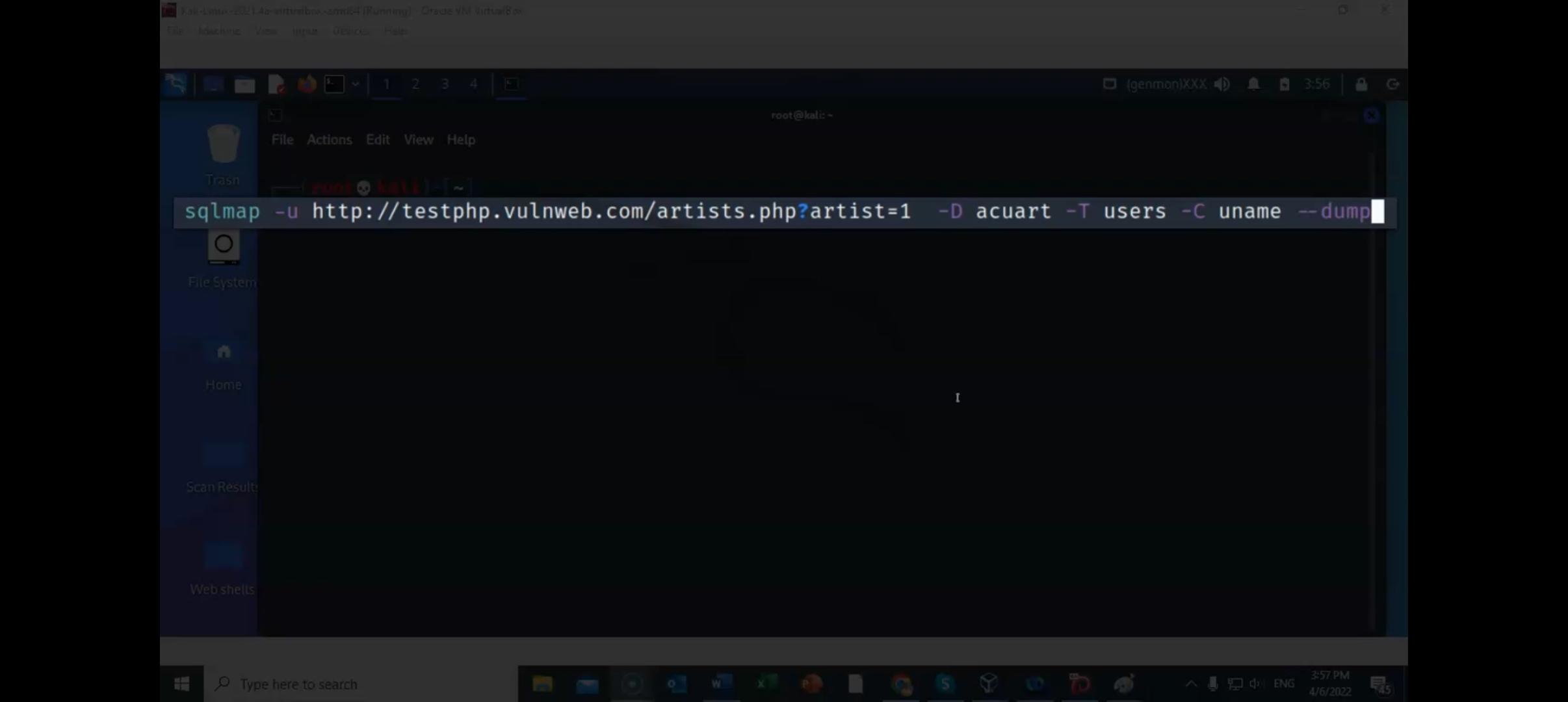
7. For accessing column in database we have following command



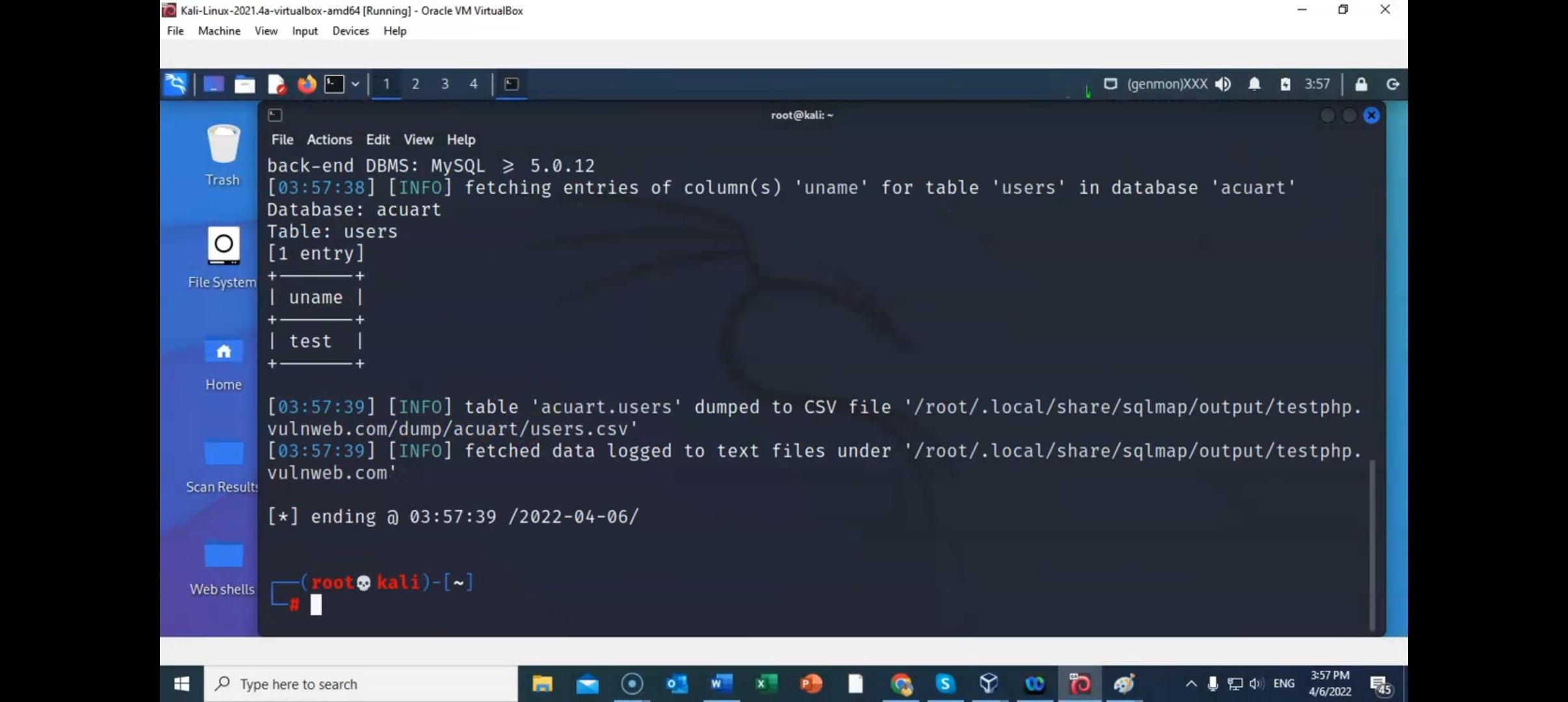
It will show all the present columns.



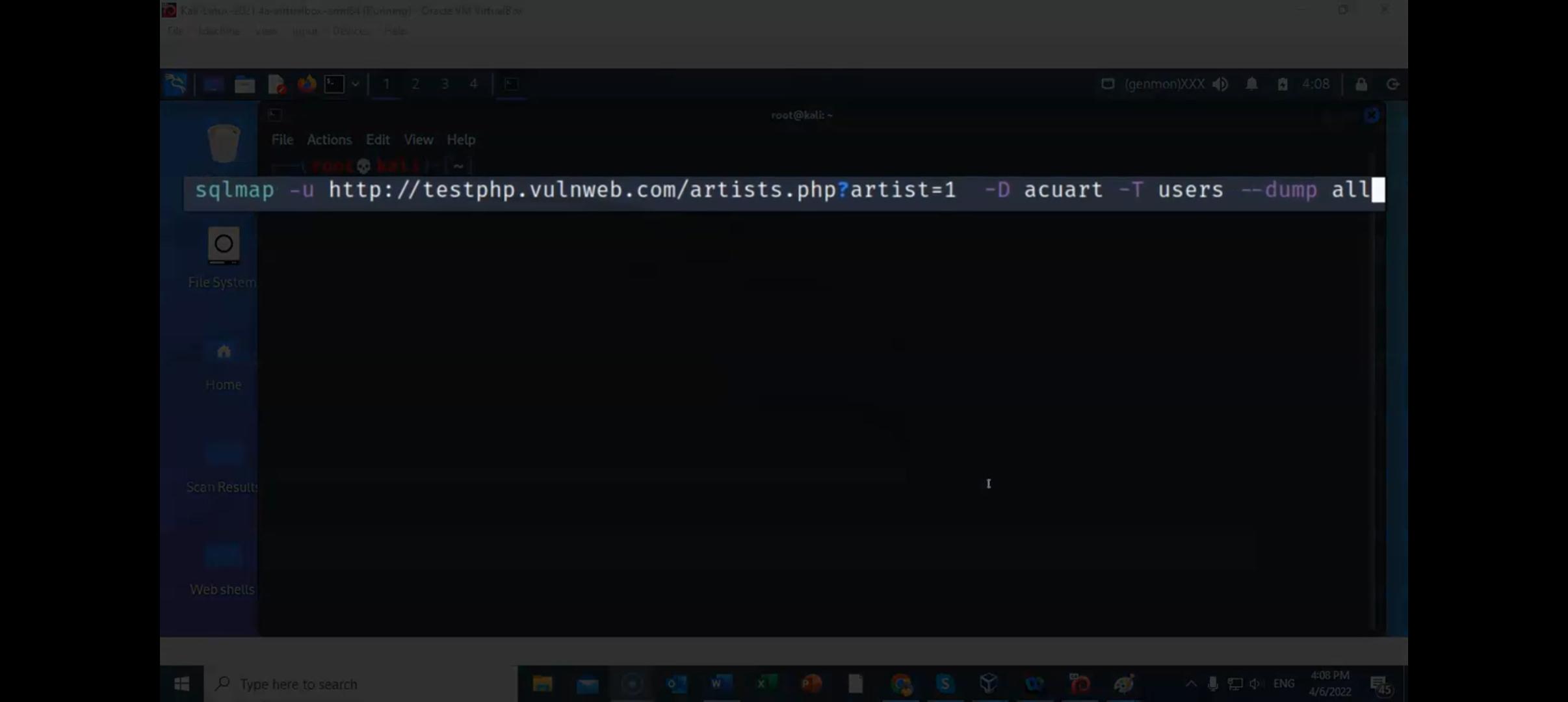
Now I want to change some particular column name



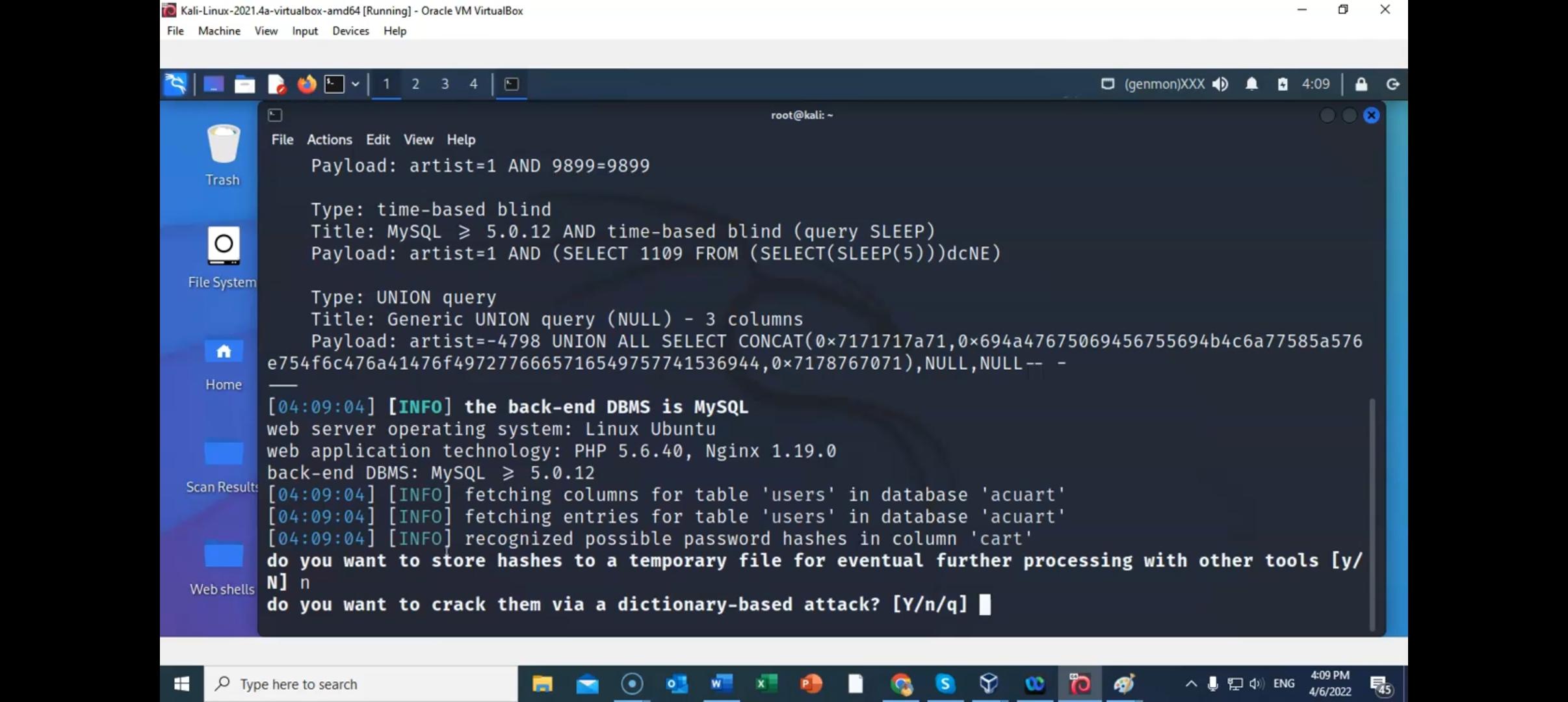
It will show the entry in uname column



For altering the complete table



Choose No for this question.



Then after accessing the table you will get the access of complete database, password is also available so you can exploit the vulnerability.

