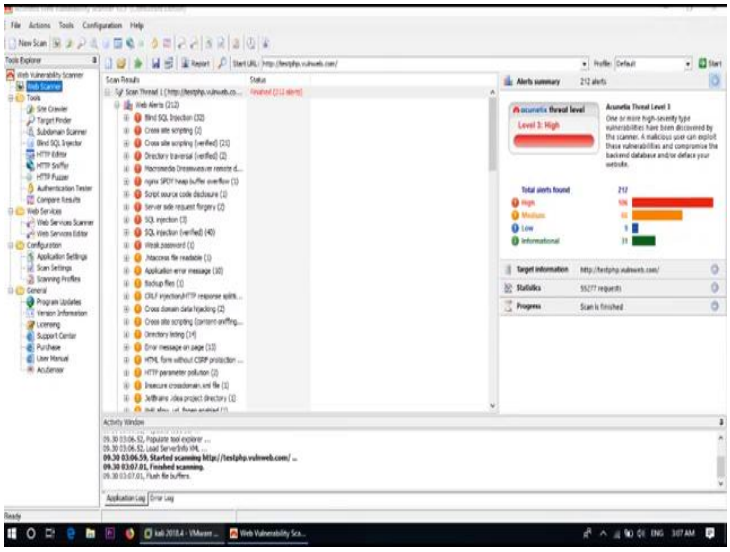
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

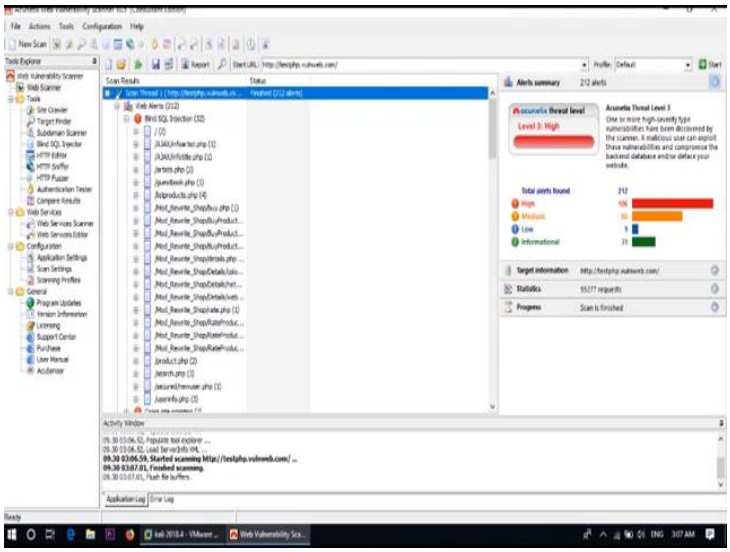
Lecture – 53
SQL MAP

(Refer Slide Time: 00:14)



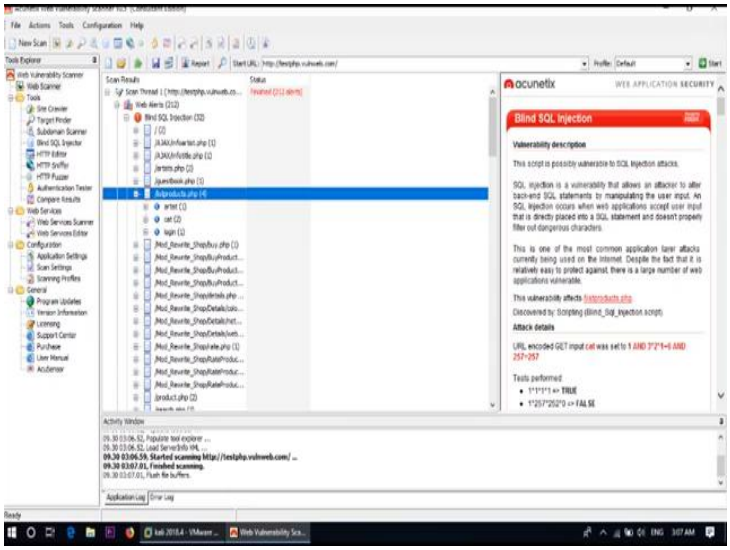
Now, in this tutorial I will show you how to perform SQL injection attack using automated tool SQLMAP from Kali Linux. Now, this is our scan result. Now, see 32 blind SQL injections are there.

(Refer Slide Time: 00:37)



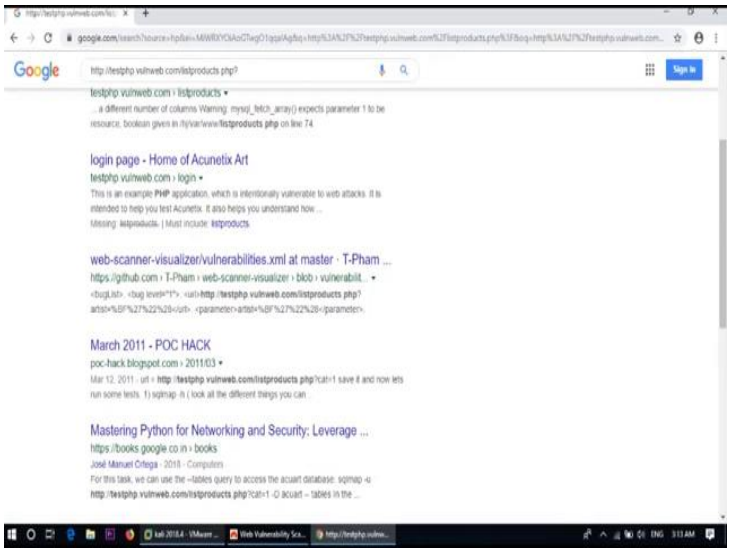
So, here is all the details page of the blind SQL injection vulnerable.

(Refer Slide Time: 00:53)



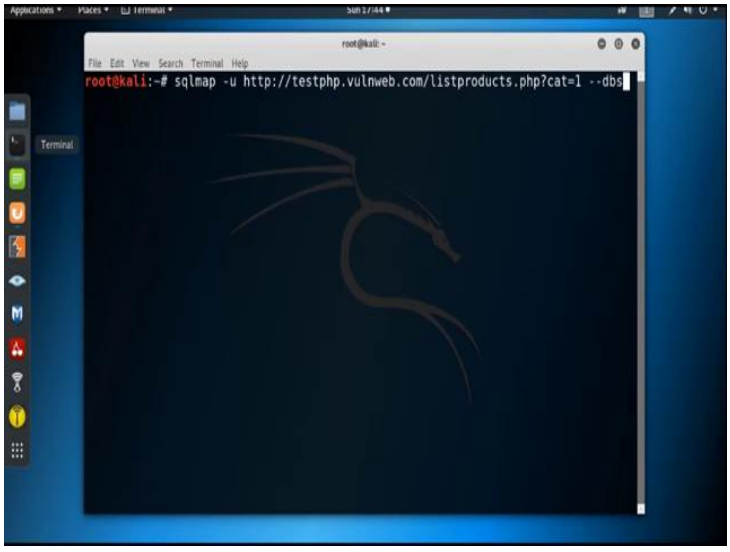
So, now start with the page **listproducts.php**. Now, we need to find out the attack page address by using the Google doc.

(Refer Slide Time: 01:16)



So, now go to on Google and search that particular URL. The URL is **http://testphp.vulnweb.com/listproducts.php?**, **listproducts.php?cat=1**. So, we can use this URL for further attack. So, go to Kali Linux and open the terminal to use the SQLMAP.

(Refer Slide Time: 02:38)



So, the command is **sqlmap -u** specify the URL. URL is **http://testphp.vulnweb.com/ listproducts.php?cat=1 - - dbs**.

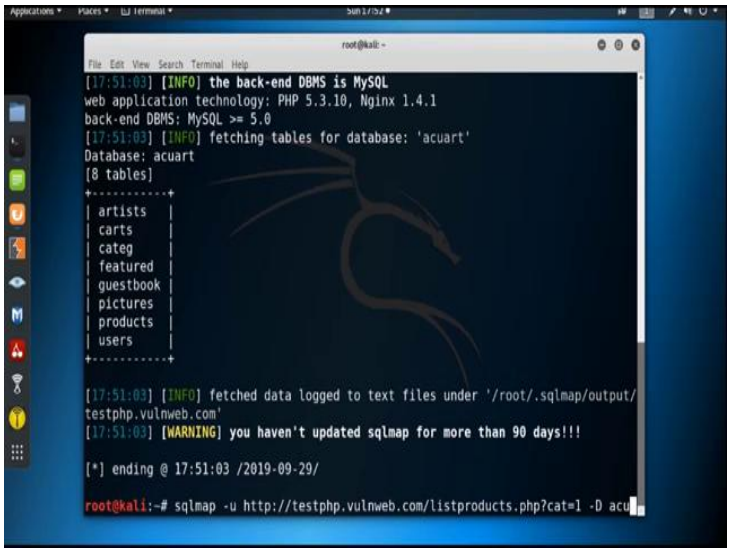
(Refer Slide Time: 03:32)

So, we got the database. There are two available database are there acuart and information_schema. information_schema is the common database; the acuart is the database where it stores all the tables. So, for further search we need to use this database. So, from database now we need to search the table name.

(Refer Slide Time: 04:12)

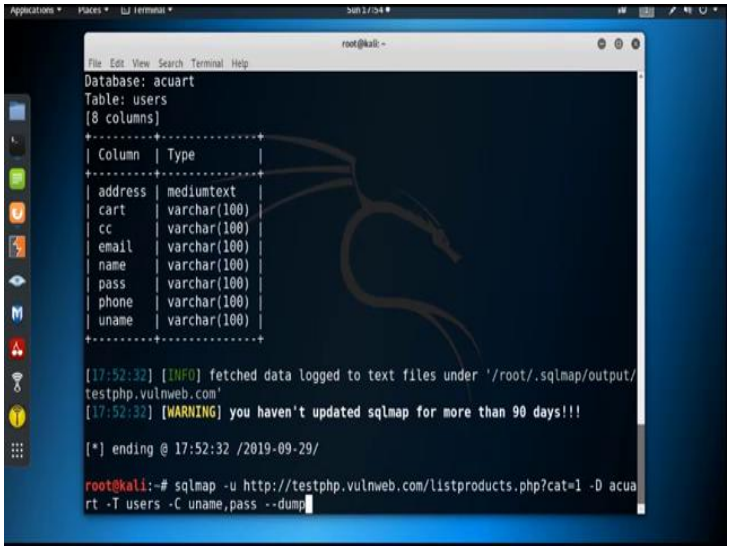
So, the command is **sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart - - tables**. Find out all the tables from that particular database. So, here is the table name. Now, suppose we want to find out next the columns in a particular table.

(Refer Slide Time: 05:11)



So, the command is **sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D** specify the database name is **acuart** then **-T** specify the table name. Suppose, we are going to find out the columns of the table users and then **- - columns**; find out all the columns in that particular table users.

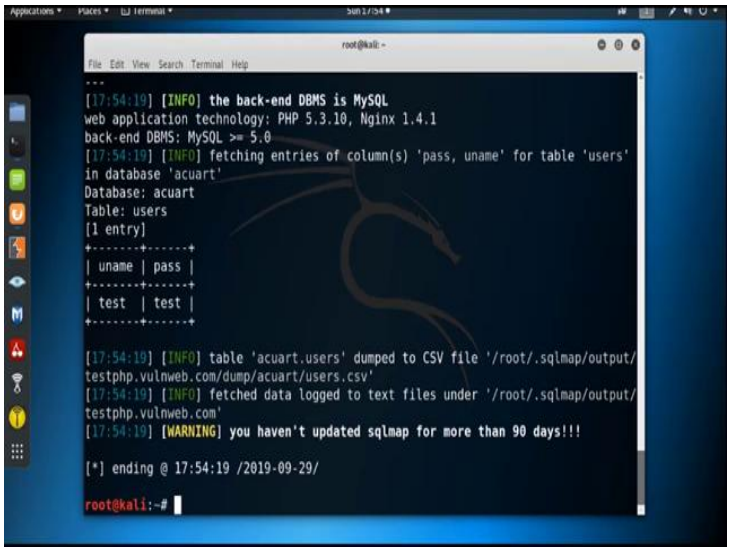
(Refer Slide Time: 06:11)



So, we got all the columns. Now, suppose we want to dump the value of the uname and password, it is pass. The **sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D** specify database name **acuart**. Then, **-T** specify the table name **users**, then **-C**

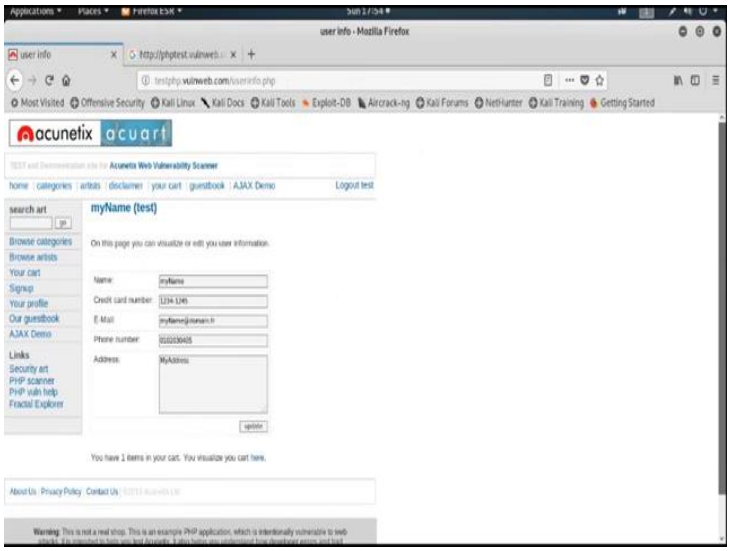
specify the column name. So, to get the data of multiple column name use the multiple column name separated by comma. So, **uname, pass** then to dump the values use **- - dump**.

(Refer Slide Time: 08:16)



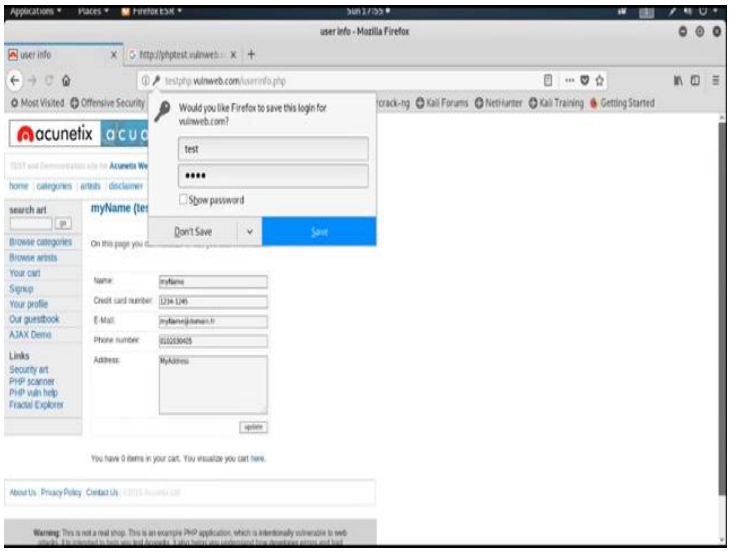
See uname is test and password is also test. So, now, we can use this valid credential to login inside that particular web application also.

(Refer Slide Time: 08:35)



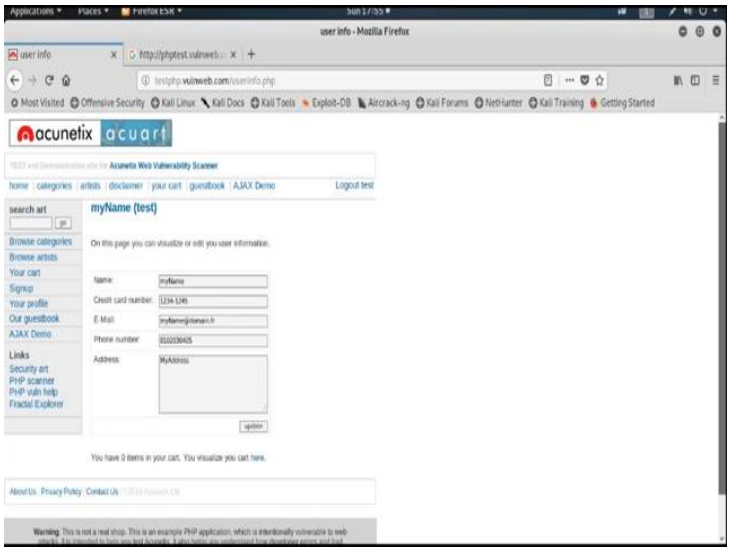
So, go here.

(Refer Slide Time: 08:40)



So, now go to sign up and use username as test and password is also test then enter, login.

(Refer Slide Time: 09:01)



Now, see it go inside the web application as a valid user. So, this way we can use the tool SQLMAP to find out all the information from the database by using SQL injection attack.

Thank you.