**SQL Injection Testing using SQLmap**

Group Members:

Harshal Sawant

Ishan Prabhune

Pratik Darade

Aniket Singh

Raj Dedhia

Step 1: Install SQLmap.



Figure command for installation

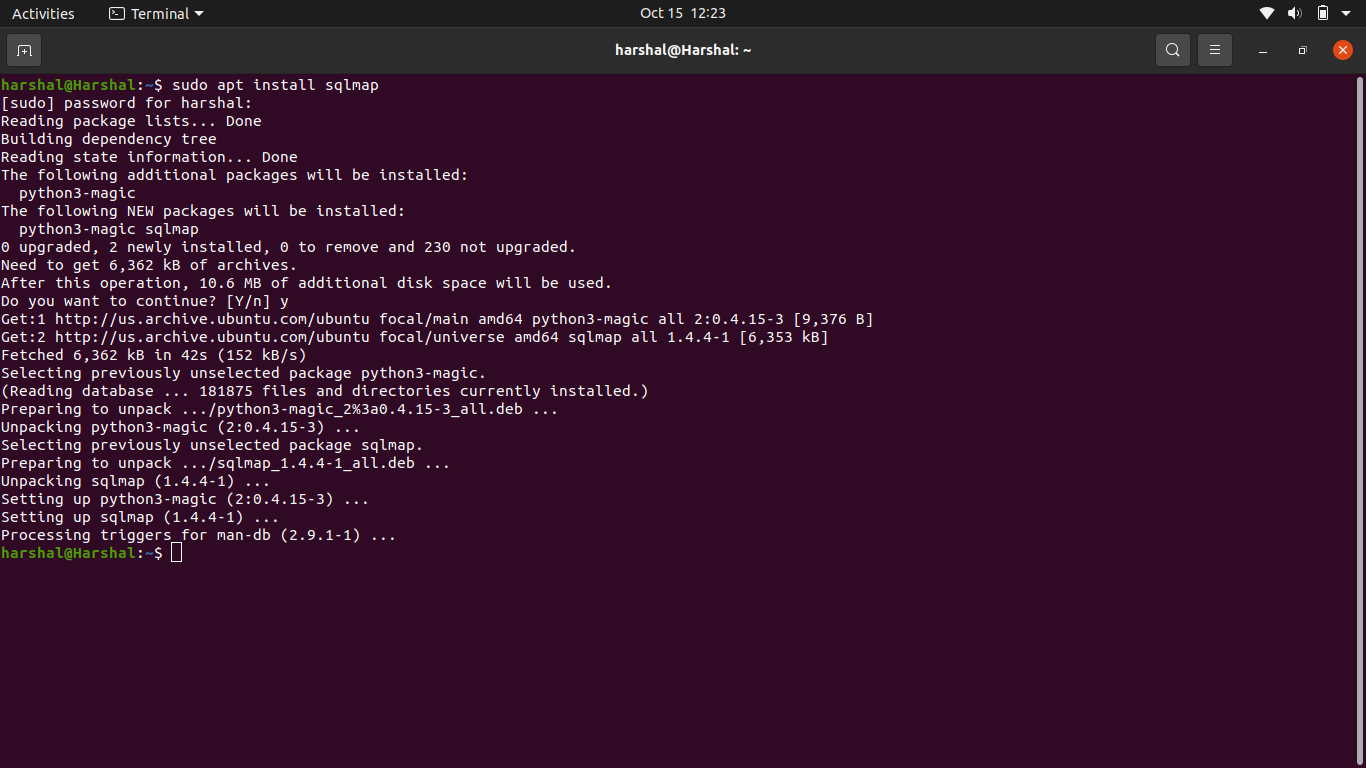


Figure SQLmap Installation complete

Step 2: Run SQLmap.

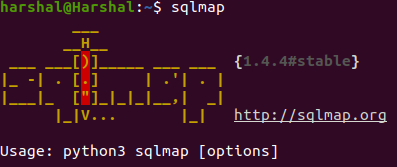


Figure Run SQLmap

The SQLmap installed is 1.4.4 stable version.

Step 3: Target URL Website.

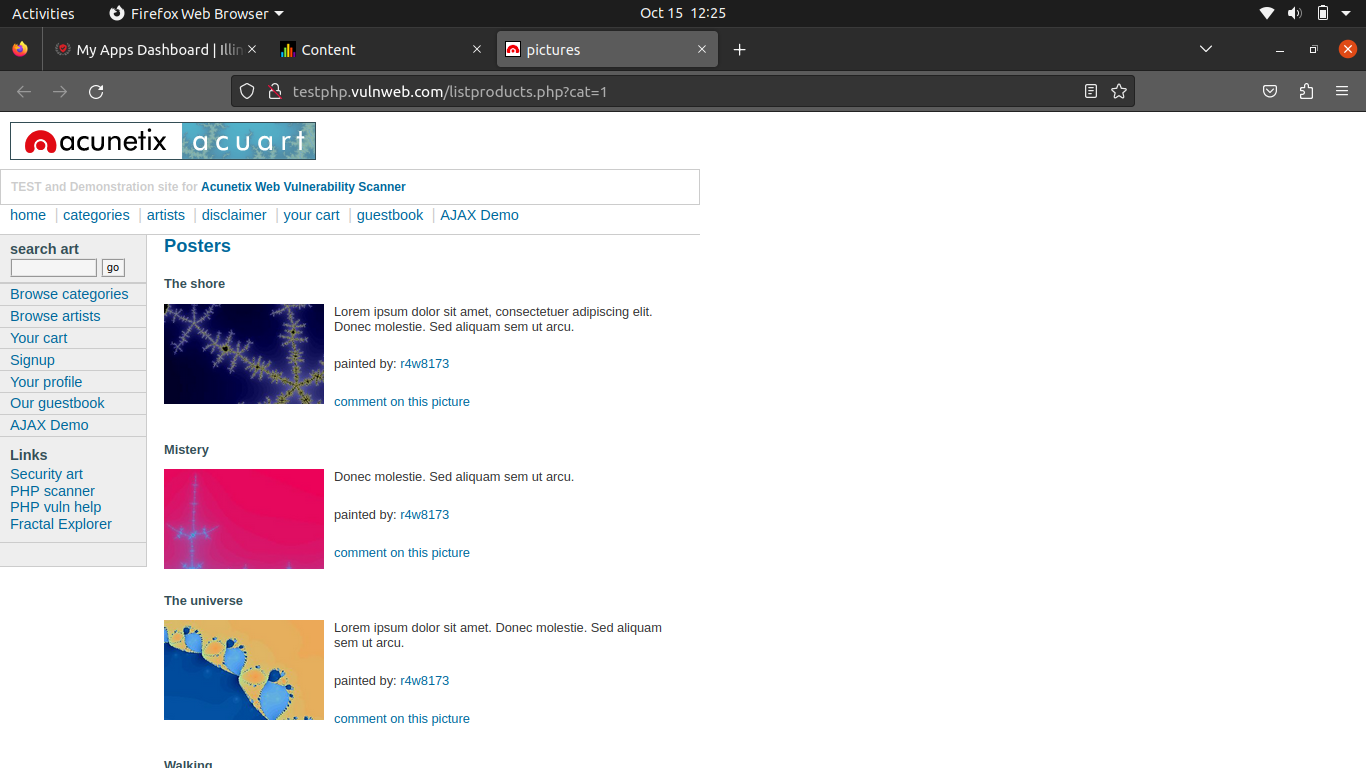


Figure Target URL Website

SQLmap unauthorized testing on websites is illegal and unethical, so we can use it for educational purpose through testing on own website or on sample website such as above website provided by acunetix.

Step 4: Analyze the target URL.



Figure command to analyze target URL using SQLmap

In SQLmap, the ‘-u’ is used to specify the target URL that you want to test for SQL Injection vulnerabilities which will then be analyzed by SQLmap for potential SQL Injection vulnerabilities.

Step 5: Results from SQLmap.



Figure Cat parameter is vulnerable

So, after we analyze, here we got the parameter which is cat and the database is mysql, so these are the vulnerabilities found by SQLmap.

Step 6: Check databases listed in Target URL.



Figure Command for listing databases

‘dbs’ stands for databases

Step 7: Output of databases.

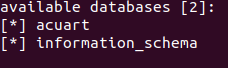


Figure Databases available

There are two databases available. We will select acuart database as the other database is the information\_schema is a generic or default db.

Step 8: Listing tables in the database.



Figure Tables listed in the db

Step 9: Tables listed in acuart

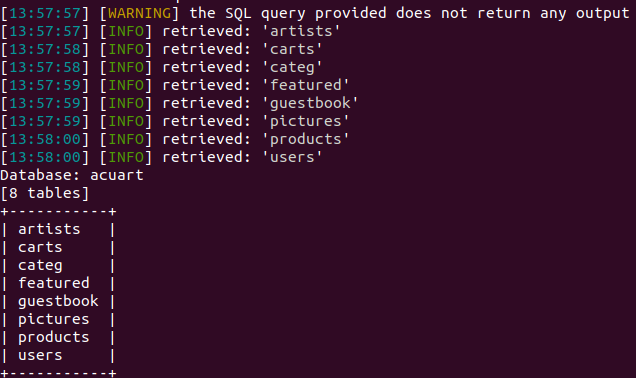
Step 10: Display columns in table

Figure Output of tables in Acuart database



In this, ‘-D’ is database, ‘-T’ is table, --columns lists columns of the selected table.

Out of tables displayed we will choose users table as it may contain user information.

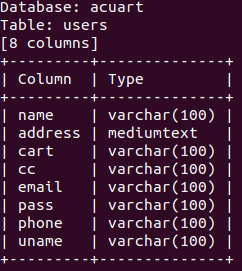


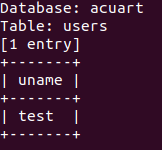
Figure Output of users

Step 10: Displaying the usernames in table users.



Figure Command to display usernames

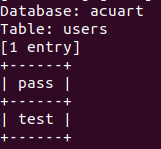
Here ‘-C’ is for column name, ‘—dump’ is to dump or make the data visible on the terminal.



This is the output from username.

Step 11: Displaying the passwords in table.

Figure Command to display password

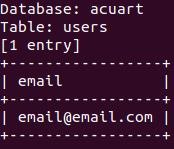


This is the output from password.

Step 12: Displaying email id in the table.



Figure Command for display email



This is output from email.

Step 13: Display credit card info from table.

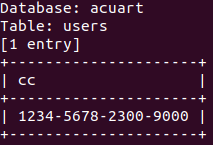
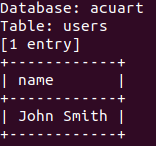


Figure Command to list credit card information

This is output from credit card.

Step 14: Display name from table.

Figure Command to list name



This is output from name.

Step 15: Login to TargetURL website using retrieved credentials from SQLmap.

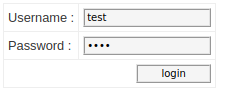


Figure Login screen

Step 16: Profile screen on TargetURL.

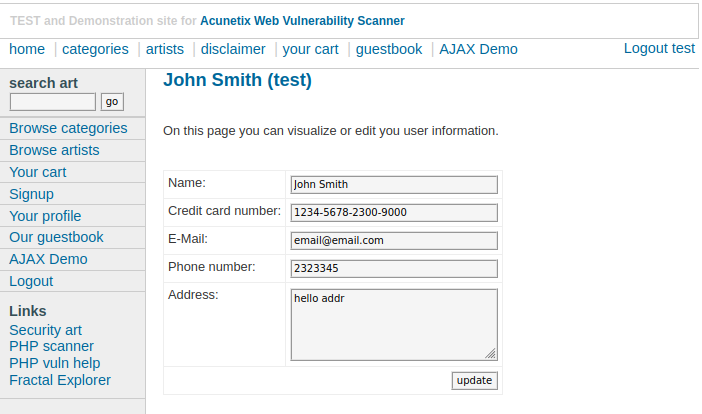
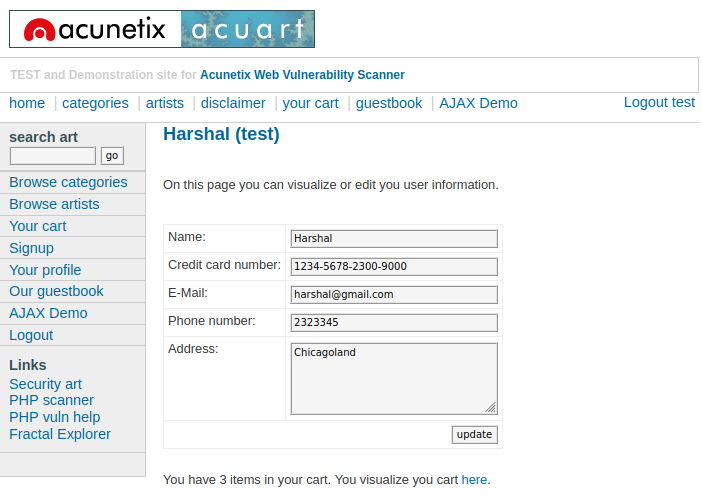


Figure Profile Screen

User profile screen on website which shows all the data of the user.

Step 17: Modifying the user data on TargetURL:

Figure Modifying the user data



Step 18: The cart data can also be modified.

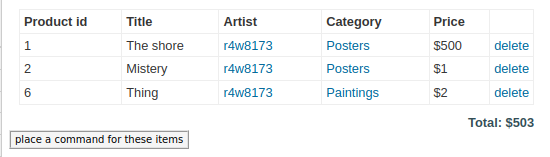


Figure Cart