TITLE – Found SQL Injection in Government website

Submitted by:- Himanshi

Basic Introduction –

The objective of this assignment is to give a vast arena of knowledge about SQL INJECTION. SQLi (SQL Injection) is an old technique where hacker executes the malicious SQL statements to take over the website.

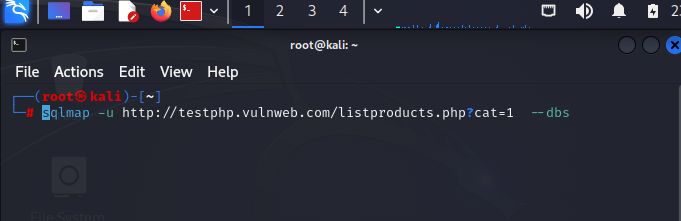
SQL Injection (SQLi) is a widely known and potentially devastating technique used by hackers to exploit vulnerabilities in web applications. By executing malicious SQL statements, attackers can gain unauthorized access to a website's database and manipulate its contents. This type of attack is classified as a high severity vulnerability due to the severe consequences it can inflict. When successful, SQL injection allows attackers to bypass security measures and retrieve data that would otherwise be inaccessible. This may include sensitive information belonging to other users or any data within the application's reach. Moreover, attackers can modify or delete data, leading to persistent changes in the application's behavior or content. SQL injection attacks typically require significant bandwidth and involve sending large amounts of data. As a result, they have become one of the most common and concerning security threats, posing a serious risk to systems and the confidentiality of sensitive data.

Steps –

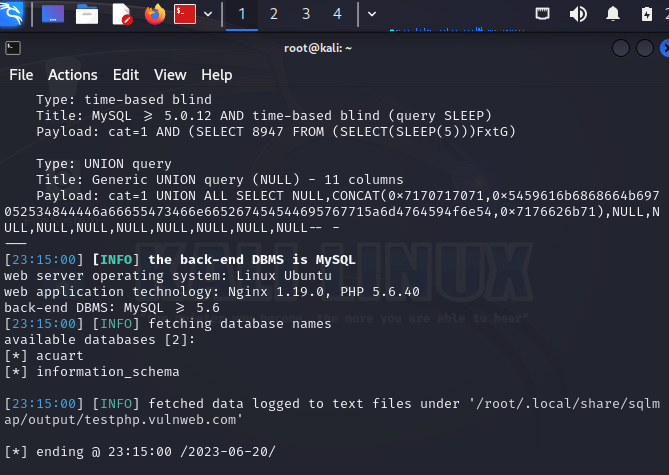
1. Get database names

Syntax- sqlmap -u URL –dbs

Command:



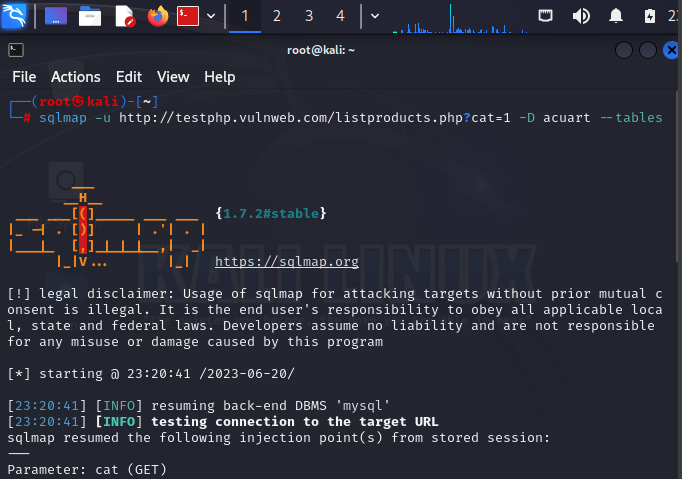
Output-



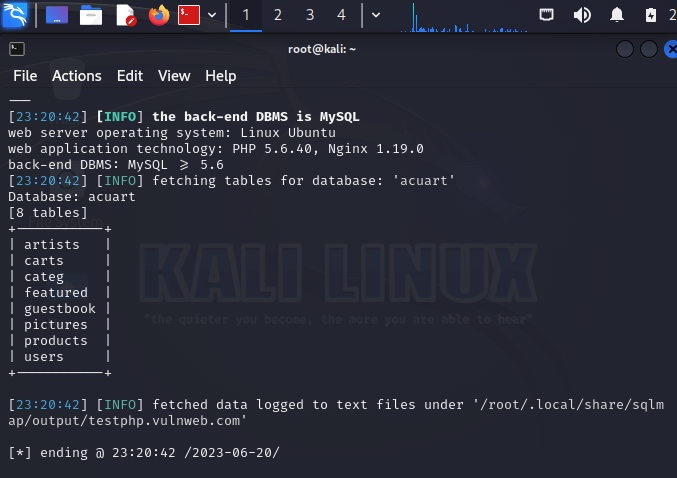
1. Get table names from Database

Syntax : sqlmap -u URL -D database –tables

Command:



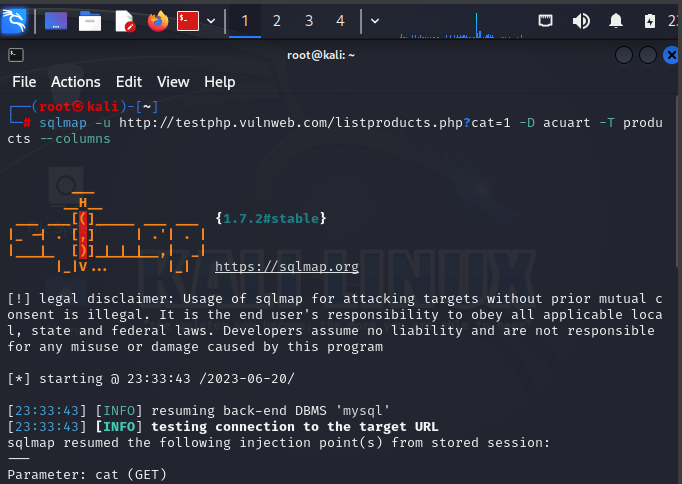
Output -



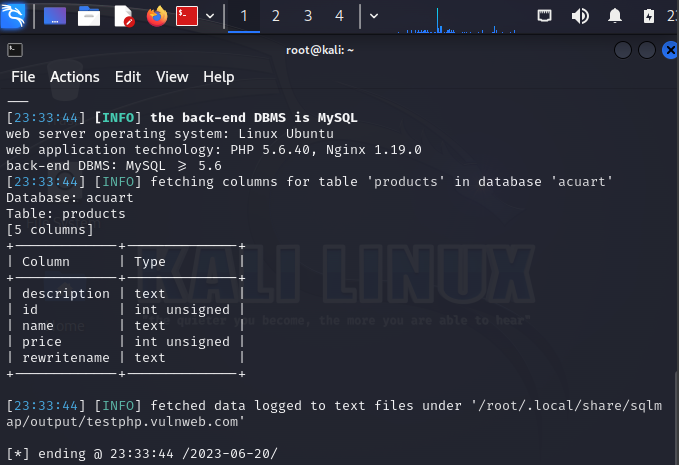
1. Get column names from tables

Syntax : sqlmap -u URL -D database -T tables –columns

Command:



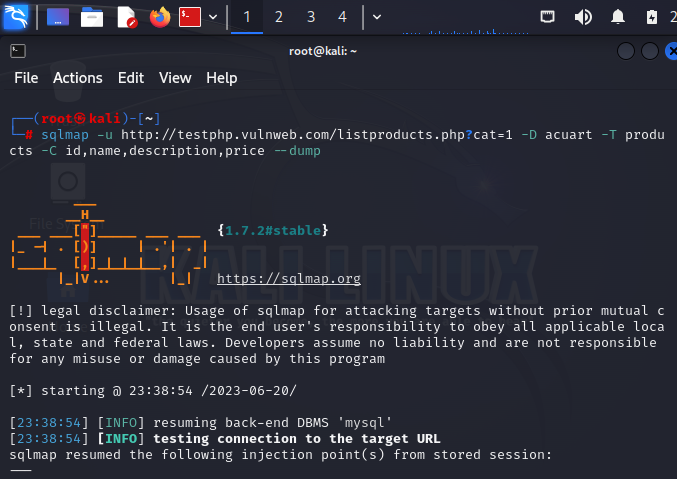
Output –



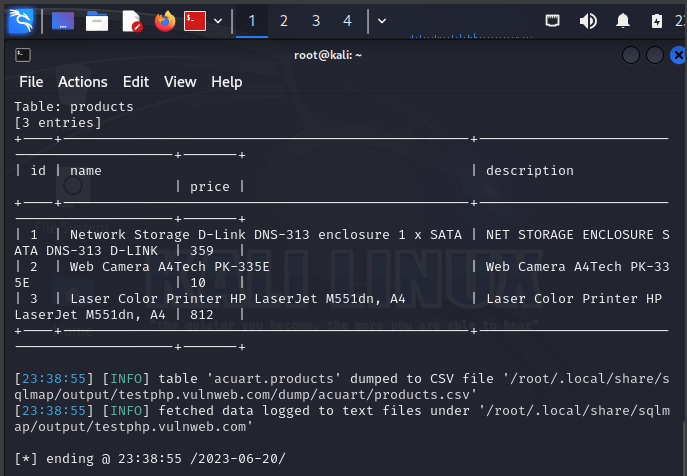
4)Dump the data

Syntax: sqlmap -u URL -D database -T table name -C column names –dump

Command:



Output-



Conclusion-

So this is how we can inject in a sql database and can dump it.So you can utilise all the sensitive database and you can get all the sensitive user data and passwords. The above information is prepared on my own desktop using the testing link because I don’t have the authentication to access the government website . I used the tested website. I have made all the above in my own laptop using kali linux software. As it is illegal to access government website I hope you will check my assignment because I have completed all this on my own.