Vulnerability Assessment Report

Report created by: Supreet BS Shetty

LinkedIn-Profile: 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

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

Email: supreetsadashiv123@gmail.com

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.

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.

Email: supreetsadashiv123@gmail.com