

Vulnerability Report

Vulnerability: SQL Injection

Vulnerability Information

Vulnerability Name: SQL Injection in DVWA

Location: <http://localhost/dvwa/vulnerabilities/sqli/>

Severity: High

Vulnerability Description

Summary:

The SQL Injection vulnerability allows an attacker to bypass authentication and retrieve sensitive data from the database by injecting malicious SQL queries into the user input fields.

Steps to Reproduce:

1. Go to: <http://localhost/dvwa/vulnerabilities/sqli/>
2. In the 'User ID' field, input: 1' or '1'='1
3. Click Submit.
4. Multiple user records will be displayed, confirming the SQL injection.


Proof of Concept (PoC)

Description:

The payload '1' OR '1'='1' bypasses the intended logic and returns all rows from the user table.

PoC URL: <http://localhost/dvwa/vulnerabilities/sqli/?id=1' OR '1'='1&Submit=Submit>

Vulnerability Report



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

ID: 1'='1' OR '1'
First name: admin
Surname: admin

ID: 1'='1' OR '1'
First name: Gordon
Surname: Brown

ID: 1'='1' OR '1'
First name: Hack
Surname: Me

ID: 1'='1' OR '1'
First name: Pablo
Surname: Picasso

ID: 1'='1' OR '1'
First name: Bob
Surname: Smith

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

Recommendations

Mitigation:

- Use prepared statements with parameterized queries.
- Sanitize and validate all user input.
- Suppress detailed SQL error messages in production.

Best Practices:

- Apply least privilege principle to database access.
- Implement web application firewalls.
- Conduct regular security audits.
- Train developers in secure coding.

Vulnerability: Brute Force Attack

Vulnerability Information

Vulnerability Name: Brute Force Login Attack in DVWA

Location: <http://localhost/dvwa/vulnerabilities/brute/>

Severity: Medium

Vulnerability Report

Vulnerability Description

Summary:

DVWA's login page does not limit login attempts, enabling attackers to automate password guessing using tools like Burp Suite.

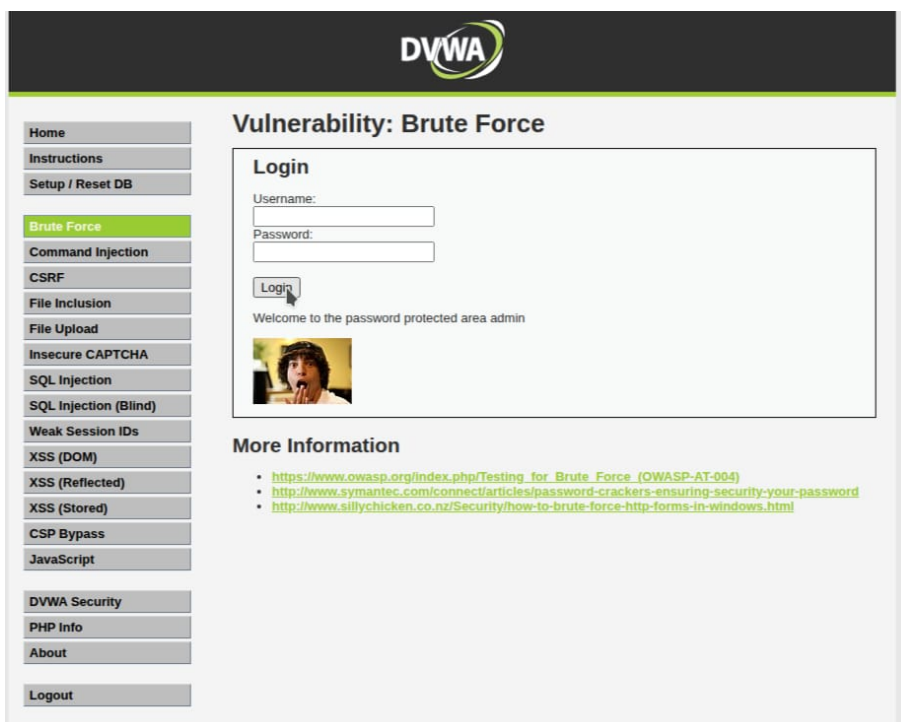
Steps to Reproduce:

1. Navigate to: <http://localhost/dvwa/vulnerabilities/brute/>
2. Use a script or tool to submit multiple username/password combinations.
3. A successful match logs in without any account lockout.

Proof of Concept (PoC)

Description:

Automated brute-force attempts with tools like Burp Suite show the login is vulnerable due to absence of rate-limiting or CAPTCHA.



Recommendations

Mitigation:

- Implement CAPTCHA or login rate limiting.

Vulnerability Report

- Lock accounts after multiple failed attempts.
- Monitor login logs for suspicious activity.

Best Practices:

- Enable multi-factor authentication.
- Use secure password policies.
- Regularly audit authentication mechanisms.

Team Member Information

Reported by: Aryan Dabhade

Reviewed by: Ved Pakhare