## Name : Mukesh Kumar

CIN : FIT/FEB25/CS583

# DVWA Vulnerability Assessment Report

## 1. Introduction

This report presents the findings of a vulnerability assessment conducted on the Damn Vulnerable Web Application (DVWA). The assessment focused on Low and Medium security levels, identifying common web security flaws and their potential impact.

## 2. Scope & Methodology

The assessment was conducted using both automated and manual techniques. The following methodology was applied:  
1. Reconnaissance: Using Nmap for network enumeration.  
2. Automated Scanning : Utilizing OWASP ZAP and Burp Suite to detect vulnerabilities.  
3. Manual Testing : Exploiting vulnerabilities to confirm their impact.  
4. Risk Assessment : Evaluating the severity and likelihood of attacks.  
5. Mitigation Recommendations : Providing solutions to fix identified vulnerabilities.

## 3. Tools Used

The following security tools were employed in this assessment:

- OWASP ZAP – Web vulnerability scanner.

- Burp Suite – Web proxy for analyzing HTTP requests.

- Nmap – Network scanner for identifying open ports.

## 4. Findings

The following vulnerabilities were identified during the assessment:

### 4.1 SQL Injection (Low Security)

An SQL Injection vulnerability was found in the login form. By injecting malicious SQL statements, an attacker can bypass authentication and retrieve database information.

Proof of Concept (PoC):  
Payload used: `' OR '1'='1' --`  
Impact: Unauthorized access to user accounts.

[Insert Screenshot: SQL Injection Exploitation]

### 4.2 Cross-Site Scripting (XSS) - Medium Security

A reflected XSS vulnerability was identified in the search functionality. An attacker could inject malicious scripts that execute when a victim loads the page.

Proof of Concept (PoC):  
Payload used: `<script>alert('XSS')</script>`  
Impact: Possible session hijacking and data theft.

[Insert Screenshot: XSS Attack]

### 4.3 Security Misconfigurations

The application was found running on an outdated PHP version, which could expose it to known exploits.

Impact: Attackers could leverage unpatched vulnerabilities.

## 5. Risk Assessment

Each vulnerability was evaluated based on its severity and exploitability. The following risk levels were assigned:

- SQL Injection (Low Security) - High Risk (Direct database access possible).

- XSS (Medium Security) - Medium Risk (Potential user session hijacking).

- Security Misconfigurations - Medium Risk (Possible exploitation of outdated components).

## 6. Recommendations

1. Use Prepared Statements : Prevent SQL Injection by using parameterized queries.

2. Sanitize Inputs : Filter user inputs to prevent XSS attacks.

3. Update Software : Keep PHP and other dependencies up to date.

4. Use Web Application Firewalls (WAF) : To detect and block common attacks.

## 7. Conclusion

The assessment of DVWA's Low and Medium security levels revealed critical and moderate vulnerabilities. By implementing the recommended security measures, the risk of exploitation can be significantly reduced. Regular security audits are essential for maintaining web application security.