Web Application Security Report

1. Introduction

This report documents security testing performed on Damn Vulnerable Web Application (DVWA) using Kali Linux. The purpose is to identify common web vulnerabilities, demonstrate exploitation techniques, and highlight risks that real-world applications face. DVWA provides a safe lab environment for practicing and learning about web application security.

2. Tools Used

- DVWA (Damn Vulnerable Web Application)
- Kali Linux
- Browser (Firefox)

3. Vulnerabilities Found

SQL Injection

- Payload: ' OR '1'='1
- Result: All users listed
- Risk: Database compromise
- Explanation: Allows manipulation of backend SQL queries.

XSS (Reflected)

- Payload: <script>alert('XSS')</script>
- Result: Alert box triggered
- Risk: Session hijacking
- Explanation: Executed injected JavaScript, attacker can steal cookies.

Command Injection

- Payload: 127.0.0.1; whoami
- Result: Server responded with www-data
- Risk: Server takeover
- Explanation: Unsanitized input allows arbitrary command execution.

Web Application Security Report

4. Recommendations

- Input validation
- Prepared statements
- Output encoding
- Avoid direct system calls with user input

5. Conclusion

DVWA demonstrated critical vulnerabilities including SQL Injection, Cross-Site Scripting (XSS), and Command Injection. These findings emphasize the importance of secure coding practices, proper input validation, and regular security testing to protect web applications from exploitation.