Website Security Audit Report

Target: Metasploitable2 (Deliberately Vulnerable Lab Environment)
Target IP: 192.168.1.4
Assessment Type: Website & Web Application Security Audit
Date: 29 January 2026
Auditor: Sumit

---

1. Executive Summary

A comprehensive website security assessment was conducted against a deliberately vulnerable web application hosted on the Metasploitable2 virtual machine. The objective of this assessment was to identify common web application vulnerabilities, demonstrate real-world attack scenarios, and provide actionable remediation guidance.

The assessment identified multiple **critical and high-risk vulnerabilities**, including remote code execution, SQL injection, and insecure authentication mechanisms. Exploitation of these issues could allow an attacker to fully compromise the application, underlying server, and sensitive data.

Immediate remediation is strongly recommended before deploying similar configurations in production environments.

---

2. Scope of Assessment

In Scope: - Web services hosted on Metasploitable2 - DVWA (Damn Vulnerable Web Application) - HTTP-based application endpoints

Out of Scope: - Denial-of-Service attacks - Physical security - Social engineering

Testing Environment: - Attacker Machine: Kali Linux - Target Machine: Metasploitable2 - Network Type: Isolated lab environment

---

3. Methodology

The assessment followed industry-standard web security testing practices inspired by the OWASP Web Security Testing Guide (WSTG):

1. Reconnaissance and service enumeration
2. Authentication and access control testing
3. Input validation and injection testing

4. File handling and upload testing
5. Client-side vulnerability testing (XSS)
6. Manual verification of findings

---

4. Tools Used

- Nmap – Network and service discovery
- Web Browser (Manual Testing)
- DVWA built-in vulnerable modules
- Linux command-line utilities

---

5. Findings Summary

ID	Vulnerability	Severity
F-01	Default Credentials	Critical
F-02	OS Command Injection	Critical
F-03	SQL Injection	High
F-04	Blind SQL Injection	High
F-05	Insecure File Upload (RCE)	Critical
F-06	Reflected Cross-Site Scripting	Medium
F-07	Stored Cross-Site Scripting	High

---

6. Detailed Findings

F-01: Default Credentials

Severity: Critical
Affected Component: DVWA Login

Description: The application allows authentication using well-known default credentials (`admin / password`).

Impact: An attacker can gain administrative access without any exploitation.

Remediation: - Enforce strong password policies - Remove default credentials before deployment

---

F-02: OS Command Injection

Severity: Critical
Affected URL: `/dvwa/vulnerabilities/exec/`

Description: User input is passed directly to system-level commands without sanitization.

Proof of Concept:

```
127.0.0.1; whoami
```

Impact: Allows arbitrary command execution on the server.

Remediation: - Avoid system calls with user input - Implement strict input validation

---

F-03: SQL Injection

Severity: High
Affected URL: `/dvwa/vulnerabilities/sqli/`

Description: Improper input handling allows attackers to manipulate SQL queries.

Proof of Concept:

```
1' OR '1'='1
```

Impact: Unauthorized access to database records.

Remediation: - Use prepared statements - Parameterized queries

---

F-04: Blind SQL Injection

Severity: High
Affected URL: `/dvwa/vulnerabilities/sqli_blind/`

Description: The application is vulnerable to blind SQL injection using boolean-based logic.

Proof of Concept:

```
1' AND '1'='1
1' AND '1'='2
```

Impact: Attackers can extract database information without visible errors.

Remediation: - Parameterized queries - Strict input validation

---

F-05: Insecure File Upload (Remote Code Execution)

Severity: Critical
Affected URL: `/dvwa/vulnerabilities/upload/`

Description: The application allows unrestricted file uploads and executes uploaded files from a web-accessible directory.

Proof of Concept: Uploaded file:

```
test.php
```

Accessed at:

```
/dvwa/hackable/uploads/test.php
```

Impact: Full remote code execution and server compromise.

Remediation: - Restrict file types - Store uploads outside web root - Disable script execution in upload directories

---

F-06: Reflected Cross-Site Scripting (XSS)

Severity: Medium
Affected URL: `/dvwa/vulnerabilities/xss_r/`

Description: User input is reflected without output encoding.

Proof of Concept:

```
<script>alert('XSS')</script>
```

Impact: Session hijacking and phishing attacks.

Remediation: - Output encoding - Input validation

F-07: Stored Cross-Site Scripting (XSS)

Severity: High
Affected URL: `/dvwa/vulnerabilities/xss_s/`

Description: Malicious scripts are stored and executed for all users.

Proof of Concept:

```
<script>alert('Stored XSS')</script>
```

Impact: Persistent client-side attacks affecting all users.

Remediation: - Output encoding - Content Security Policy (CSP)

---

7. Overall Risk Rating

Overall Risk Level: Critical
Multiple vulnerabilities allow full compromise of the application and server.

---

8. Recommendations

- Follow secure coding practices
- Implement OWASP Top 10 controls
- Conduct regular security assessments
- Use automated and manual testing

---

9. Conclusion

The assessment demonstrates how common misconfigurations and insecure coding practices can lead to severe security risks. Addressing the identified vulnerabilities is essential before deploying similar applications in production.

This report is intended for educational and portfolio demonstration purposes within a controlled lab environment.

End of Report