03 REPORTING PRACTICE

1. EXECUTIVE SUMMARY

A security assessment was conducted on the Damn Vulnerable Web Application (DVWA) hosted on Metasploitable2 to identify OWASP Top 10 vulnerabilities. The application intentionally contained exploitable flaws, confirming multiple high and critical risks, including SQL Injection and File Upload/XXE. Medium-severity issues such as Cross-Site Scripting (XSS), Security Misconfiguration, and outdated components were also identified. Testing utilized Burp Suite, SQLMap, and Nmap. Recommended remediations include parameterized queries, strict file validation, output encoding, and server hardening.

2. TECHNICAL FINDINGS

F001 — SQL INJECTION (CRITICAL)

Target URL: http://192.168.96.128/dvwa/vulnerabilities/sqli/

How Found: Manual payloads (1' OR '1'='1, 1') in Burp Repeater confirmed data extraction and time-based response delays. SQLMap enumeration verified database contents.

Impact: Full database disclosure including usernames and passwords; potential system compromise.

Recommendation: Implement parameterized queries, enforce input validation, and restrict database privileges.

F002 — FILE UPLOAD / XXE (HIGH)

Target URL: http://192.168.96.128/dvwa/vulnerabilities/upload/

How Found: Upload form tested with altered filenames and content-types via Burp Suite. XML payload with external entity accessed local files (/etc/passwd).

Impact: Disclosure of sensitive files; possible remote code execution via malicious upload or XML entity abuse.

Recommendation: Restrict file types, validate file names, store uploads outside webroot, disable XML external entities, and block directory traversal (..).

F003 — CROSS-SITE SCRIPTING (XSS) (MEDIUM)

Target URL:

- Reflected: http://192.168.96.128/dvwa/vulnerabilities/xss_r/
- Stored: http://192.168.96.128/dvwa/vulnerabilities/xss_s/

How Found: Injected payloads <script>alert(1)</script> and <script>alert('xss')</script> executed in the browser without sanitization.

Impact: Session hijacking, cookie theft, and CSRF chaining possible.

Recommendation: Contextual output encoding, input validation, and implementation of a strong Content Security Policy (CSP).

F004 — SECURITY MISCONFIGURATION (MEDIUM)

Target URL: http://192.168.96.128/dvwa/

How Found: HTTP headers exposed Server and X-Powered-By banners; Nikto found default files and directory listing enabled.

Impact: Increased fingerprinting and exposure of outdated components.

Recommendation: Hide version info, disable directory listing, remove default files, and apply secure configuration settings.

F005 — OUTDATED COMPONENTS (INFORMATION)

Target: 192.168.96.128

How Found: nmap -sV and HTTP headers revealed outdated Apache/PHP versions.

Impact: Vulnerable to known CVEs in outdated components.

Recommendation: Regularly update software, apply security patches, and monitor CVE feeds for vulnerabilities.

3. REMEDIATION PLAN

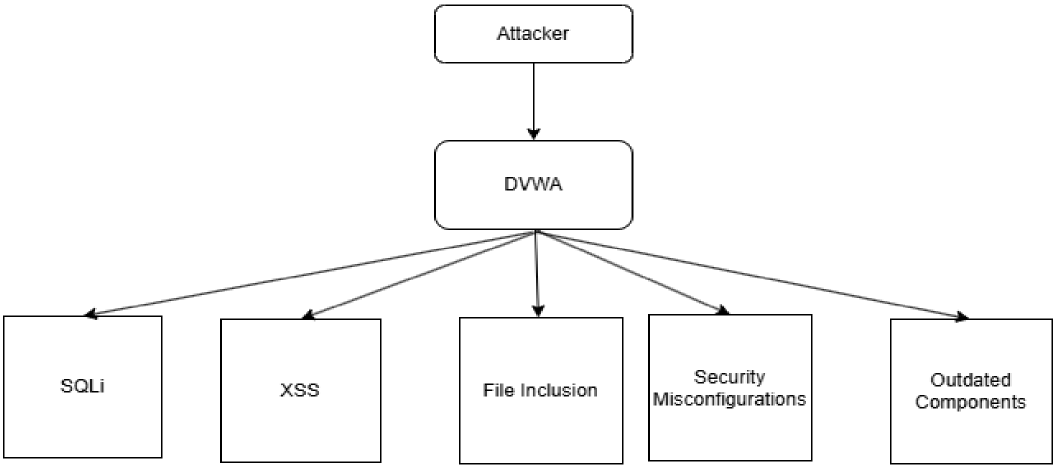
Priority	Area	Recommended Actions
Critical	Database Security	Implement prepared statements, sanitize inputs, and minimize DB privileges.

Priority	**Area**	**Recommended Actions**
High	File Handling	Validate file uploads, restrict file types, and disable XML external entities.
Medium	Application Logic	Encode outputs, validate inputs, and enforce CSP.
Medium	Server Configuration	Remove version banners, default files, and disable directory listings.
Medium	Patch Management	Update and maintain all web server components regularly.

4. FINDINGS TABLE

Finding ID	**Vulnerability**	**CVSS Score**	**Remediation Summary**
F001	SQL Injection	9.1	Parameterized queries, input validation
F002	File Upload / XXE	8.3	Restrict file types, disable XXE
F003	Cross-Site Scripting	6.5	Encode outputs, enforce CSP
F004	Security Misconfiguration	6.0	Harden configuration, hide version info
F005	Outdated Components	5.0	Apply patches and version updates

5. VISUALIZATION



6. CONCLUSION

The DVWA instance displayed multiple high-impact vulnerabilities aligned with OWASP Top 10 categories. SQL Injection and File Upload/XXE represent the highest risks due to data disclosure and possible remote execution. Medium-severity issues (XSS, misconfiguration) compound exposure. Remediation should prioritize secure coding practices, configuration hardening, and regular patch cycles. Post-remediation verification and periodic assessments are recommended to maintain security posture.

7. NON-TECHNICAL SUMMARY

A simulated penetration test of the DVWA web application revealed several weaknesses that could allow unauthorized data access or system compromise. The most critical issues were flaws in how the application handles database queries and file uploads. These weaknesses could let attackers extract sensitive information or execute malicious code. Fixing them involves strengthening input checks, controlling file uploads, and keeping the system updated. With proper fixes and regular reviews, these vulnerabilities can be fully mitigated, significantly improving the web application’s overall security.