Title: VAPT Report — Lab Assessment  
**Author:** Ishan Chowdhury  
**Date:** 14-10-2025  
**Scope:** Authorized assessment of lab hosts (192.168.132.130 — DVWA; 192.168.132.135 — Metasploitable2)

## Executive Summary

This authorized assessment of lab hosts identified critical application-level and configuration issues that could allow data exfiltration and system compromise. Immediate remediation of high-risk items (SQL injection, insecure uploads, weak authentication) is recommended.

## Technical Findings

**Finding F001 — SQL Injection**

**Target:** http://192.168.132.130/dvwa/vulnerabilities/sqli/?id=

**Impact:** Data exfiltration, credential exposure.

**Evidence:** dvwa-sqlmap\_1.txt, dvwa-sqlmap\_2.txt, ~/lab/evidence/msf2/dvwa-users-YYYY-MM-DD\_HHMMSS.txt.

**Reproduction (brief):** Parameter id accepted injection vectors (boolean/error/union/time-based).

**Finding F002 — Weak Password**

**Target:** Credentials discovered/used on services (e.g., phpMyAdmin, FTP).

**Impact:** Unauthorized access to services.

**Evidence:** Authentication attempts logs, nmap service list msf2-services.txt.

**Reproduction (brief):** Common lab credentials allowed login.

**Finding F003 — Reflected XSS**

**Target:** http://192.168.132.130/dvwa/vulnerabilities/xss\_r/?name=

**Impact:** Session theft, CSRF escalation.

**Evidence:** dvwa-screenshots (contains reflected marker Hello TEST).

**Reproduction (brief):** Input reflected unencoded in response.

**Finding F004 — Exposed/Outdated Services**

**Target:** 192.168.132.135 (ftp, ssh, tomcat, distccd, etc.)

**Impact:** Increased attack surface; potential service exploits.

**Evidence:** msf2-services.txt (Nmap output).

**Reproduction (brief):** Nmap service/version enumeration.

## Remediation Plan

**SQL Injection (Priority: High)** — Use parameterized queries or stored procedures; enforce server-side input validation; apply WAF rules to block common injection patterns.

**Authentication & Passwords (Priority: High)** — Enforce strong password policy, rotate default credentials, implement account lockout and MFA where feasible.

**Reflected XSS (Priority: Medium)** — Output-encode user-supplied content, implement a strict Content Security Policy, and sanitize inputs server-side.

**File Uploads / Image Processing (Priority: High if present)** — Validate MIME and magic bytes, restrict extensions, store uploads outside webroot, run processing in isolated sandboxes.

**Service Hardening (Priority: Medium)** — Patch/upgrade services, disable unnecessary daemons, reduce version exposure, and apply host-based firewall rules.

**Verification** — After remediation, perform rescan (Nmap/OpenVAS) and retest the specific endpoints to confirm fixes.

## Findings Table

Finding ID | Vulnerability | CVSS Score | Remediation

-----------|---------------------|------------|-----------------------------

F001 | SQL Injection | 9.1 | Implement parameterized queries; input validation

F002 | Weak Password | 7.5 | Enforce complexity; rotate default creds; enable MFA

F003 | Reflected XSS | 6.1 | Output-encode; input sanitization; Content Security Policy

F004 | Exposed Services | 5.0 | Patch services; disable unnecessary daemons; firewall