# VAPT Report

**Title:** PTES VAPT Report — Metasploitable2 / DVWA (192.168.132.135 / 192.168.132.130)  
**Author:** Ishan Chowdhury — VAPT Intern

**Scope & Methodology:**  
Internal lab assessment targeting Metasploitable2 network hosts and a DVWA web application at http://192.168.132.130/dvwa/index.php. Methodology followed PTES phases: Reconnaissance, Scanning, Vulnerability Analysis, Exploitation, Post‑Exploitation and Reporting using Kali toolset (Nmap, Nikto, OpenVAS, Metasploit, sqlmap, Burp Suite).

**Findings:**  
High‑impact issues discovered include vsftpd 2.3.4 backdoor (remote root), Tomcat manager authenticated deployment enabling JSP/RCE, PHP 5.2.4 source disclosure via ?-s, exposed backup/config files accessible over HTTP, an unauthenticated bindshell on port 1524, and SQL injection in DVWA. Using sqlmap against http://192.168.132.130/dvwa/index.php confirmed exploitable injection and retrievable database contents. OpenVAS enumeration recorded multiple CVE-class vulnerabilities supporting prioritization.

**Impact:**  
Exploitation of the above allows full host compromise, credential disclosure, and lateral movement. Exposed archives increase risk of key/credential leakage.

**Recommendations:**  
Immediately isolate lab hosts, remove or rotate exposed credentials and backup files, upgrade Apache/PHP/Tomcat/vsftpd, disable unnecessary services (FTP, bind shell), enforce network ACLs for admin interfaces, disable TRACE, and implement secure HTTP headers and cookie flags. Re-scan with OpenVAS/Nmap and re-test DVWA after remediation to verify fixes.