Technical Report

Executive Summary: During the authorized penetration test of DVWA application conducted on August 22, 2025, I identified and successfully exploited four critical vulnerabilities that could lead to complete system compromise. The application's current security posture presents significant risk to data confidentiality, integrity, and availability. Immediate remediation is required to prevent potential breaches.

Methodology: Testing followed PTES methodology including reconnaissance, scanning, enumeration, exploitation, and post-exploitation phases. Both automated tools (sqlmap, OpenVAS) and manual testing techniques were employed to ensure comprehensive coverage.

Critical Findings:

1. SQL Injection allowing complete database access
2. Command Injection enabling remote code execution
3. Unrestricted file upload leading to web shell deployment
4. Cross-site scripting vulnerabilities affecting user sessions

Remediation Recommendations:

- Implement parameterized queries for all database interactions
- Validate and sanitize all user inputs
- Restrict file upload types and implement content verification
- Deploy Web Application Firewall (WAF)
- Conduct regular security assessments
- Provide secure coding training for development team

Risk Rating: CRITICAL - Immediate action required

Non-Technical Summary

My security testing revealed serious vulnerabilities in the web application that could allow attackers to steal sensitive data, take control of the system, and disrupt operations. Think of it like finding unlocked doors and windows in a building that should be secure. These issues are similar to leaving passwords written on sticky notes or having no security cameras. We successfully demonstrated how an attacker could exploit these weaknesses to access confidential information. Immediate fixes are needed, including better password protection, input checking, and system monitoring. Regular security reviews should be scheduled to prevent future vulnerabilities.