# Reporting & Stakeholder Communication Lab

Author: Harshal Harekar

Date: 14/10/2025

## Executive Summary

This assessment targeted the DVWA application hosted on a vulnerable test environment to simulate OWASP Top 10 exploitation. Systematic testing revealed critical vulnerabilities including SQL Injection and Reflected Cross-Site Scripting (XSS). These flaws allow unauthorized access to sensitive data and client-side script execution. Exploits were successfully demonstrated using Burp Suite. Immediate remediation is recommended to prevent real-world exploitation and improve application security posture.

## Findings

* SQL Injection was identified in the id parameter of the SQLi module. Malicious input allowed unauthorized database queries and data exposure.
* Reflected XSS was found in the name parameter of the XSS (Reflected) module. Unsanitized input was reflected in the response, enabling script execution in the browser.

## Remediation Plan

* Implement strict input validation and parameterized queries to prevent SQL Injection.
* Apply output encoding and input sanitization to mitigate XSS risks.
* Upgrade DVWA to a hardened version for training or isolate it from production networks.
* Conduct regular code reviews and automated security scans.

## Findings Table

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Vulnerability | CVSS Score | Remediation |
| 1 | SQL Injection | 9.1 | Input validation |
| 2 | XSS Reflected | 7.5 | Output encoding & sanitization |

## Diagram

A diagram of a network

AI-generated content may be incorrect.

## Briefing

During a controlled security test of the DVWA training environment, we identified two critical vulnerabilities: SQL Injection and Reflected Cross-Site Scripting. These flaws allow attackers to extract sensitive data and execute malicious scripts in users’ browsers. Exploits were successfully demonstrated using Burp Suite, confirming the risk. While DVWA is a deliberately vulnerable app, these findings highlight common weaknesses in real-world systems. We recommend implementing input validation, output encoding, and isolating training environments from production. Addressing these issues will reduce exposure and strengthen our overall security posture.