Web Application Security Assessment Report (TASK 1)

Prepared by: Harshika Haresh Gangan (Cybersecurity Intern)

Date: June 24, 2025

# Executive Summary

An automated and manual security assessment was conducted on the DVWA application using tools like OWASP ZAP, Burp Suite, and SQLMap. Multiple security vulnerabilities were found across various OWASP Top 10 categories, including injection flaws, missing security headers, and server misconfigurations. These issues, if left unaddressed, could lead to data breaches, unauthorized access, and service disruption.

# Identified Vulnerabilities

## SQL Injection in Login Form [High Risk]

OWASP Mapping: A03:2021 - Injection

Tools Used: Burp Suite (Manual Testing)

Description: SQL Injection vulnerability was identified in the login form using manual payloads.

Mitigation: Use parameterized queries (prepared statements) and input validation.

## Content Security Policy (CSP) Header Not Set [Medium Risk]

OWASP Mapping: A05:2021 - Security Misconfiguration

Tools Used: OWASP ZAP

Description: The application lacks CSP headers which help prevent XSS and injection attacks.

Mitigation: Configure the server to include a proper Content-Security-Policy header.

## Directory Browsing Enabled [Medium Risk]

OWASP Mapping: A05:2021 - Security Misconfiguration

Tools Used: OWASP ZAP

Description: Users can browse directories and access source files.

Mitigation: Disable directory listing in server configuration.

## Hidden File Accessible (/server-status) [Medium Risk]

OWASP Mapping: A05:2021 - Security Misconfiguration

Tools Used: OWASP ZAP

Description: The /server-status page exposes server status and traffic information.

Mitigation: Restrict access or remove this file from production environments.

## Missing Anti-Clickjacking Header [Medium Risk]

OWASP Mapping: A05:2021 - Security Misconfiguration

Tools Used: OWASP ZAP

Description: No X-Frame-Options or CSP frame-ancestors header is set.

Mitigation: Add 'X-Frame-Options: DENY' or use CSP to control iframe embedding.

# OWASP Top 10 Coverage

A01:2021 - Broken Access Control: Covered (e.g., insecure cookie settings)

A03:2021 - Injection: Covered (SQL injection in login)

A05:2021 - Security Misconfiguration: Covered (CSP, directory listing, clickjacking)

A06:2021 - Vulnerable/Outdated Components: Covered (Apache/PHP version exposed)

A07:2021 - Identification & Authentication Failures: Covered (session token & cookie leakage)