# Vulnerability Assessment Report

Future Interns – Cyber Security Internship
Task 1: Vulnerability Assessment

# Introduction

This report presents the results of a vulnerability assessment conducted on a legally permitted demo web application. The objective is to identify common web security issues, assess risk levels, and provide remediation recommendations in a clear and business-friendly manner.

# Scope & Methodology

Due to system restrictions, advanced security tools could not be installed. A browser-based manual testing approach was used, including input validation testing, reflected XSS checks, HTTP security header analysis, and cookie inspection.

# Tools Used

- Web Browser (Chrome/Edge)
- Browser Developer Tools
- OWASP Top 10 Reference
- Manual Testing Techniques

# Vulnerability Summary

| Vulnerability | Risk Level |
|---|---|
| SQL Injection | High |
| Cross-Site Scripting (XSS) | Medium |
| Insecure Cookies | Medium |
| Missing Security Headers | Low |
| Server Information Disclosure | Low |

# 1. SQL Injection (High)

The application does not properly validate user input, allowing manipulation of backend database queries. This can lead to unauthorized data access and full database compromise.

# 2. Cross-Site Scripting (XSS) (Medium)

User input is reflected without proper encoding, allowing malicious scripts to execute in the browser.

# 3. Insecure Cookies (Medium)

Session cookies lack Secure and HttpOnly attributes, increasing the risk of session hijacking.

# 4. Missing Security Headers (Low)

Important HTTP security headers are missing, exposing users to browser-based attacks.

# 5. Server Information Disclosure (Low)

Server version and technology details are exposed, aiding attacker reconnaissance.

# Conclusion

The assessment identified multiple security weaknesses. Addressing these issues will significantly improve the overall security posture of the application.

# Disclaimer

This assessment was conducted strictly for educational purposes on a legal demo website.