VULNERABILITY ASSESSMENT REPORT

Internship: Cyber Security – Future Interns
Task: Task 1 – Vulnerability Assessment Report
Prepared By: Dishant
Date:

1. Introduction

This report presents the results of a vulnerability assessment conducted on a live website as part of the Cyber Security Internship. The objective is to identify common security vulnerabilities, classify their risks, and provide remediation steps in simple business-friendly language.

2. Scope of Assessment

Target Website: Demo/Test Website
Assessment Type: Passive, Non-intrusive
Tools Used: Nmap, OWASP ZAP (Passive), Browser Developer Tools
Out of Scope: No exploitation or data modification

3. Vulnerability Findings

Vulnerability 1: Missing Security Headers
Risk Level: Medium
Description: Important HTTP security headers are missing.
Impact: May allow clickjacking or script injection attacks.
Remediation: Implement recommended HTTP security headers.

Vulnerability 2: Open Ports Detected
Risk Level: Low
Description: Unnecessary open ports were identified using Nmap.
Impact: Increased attack surface.
Remediation: Close unused ports and apply firewall rules.

Vulnerability 3: Insecure Cookie Flags
Risk Level: Low
Description: Cookies missing Secure and HttpOnly flags.
Impact: Cookies may be exposed to client-side attacks.
Remediation: Enable Secure and HttpOnly flags.

4. Risk Summary

Vulnerability	Risk Level
Missing Security Headers	Medium
Open Ports	Low
Insecure Cookies	Low

5. Conclusion

The assessment identified low to medium risk vulnerabilities. Applying the recommended fixes will improve the overall security posture of the website.

Disclaimer: This report is created for educational purposes only.