FUTURE INTERNS

CYBERSECURITY
TASK-1

PREPARED BY

ANUSHA PEDDAPALLI

INTRODUCTION

This report shares the results of a security check performed on a public demo website (OWASP Juice Shop) using tools like Nmap and OWASP ZAP. The purpose of this assessment is to find common security weaknesses in a simple, read-only way and explain why they matter. The findings are grouped by risk level and followed by clear, practical recommendations that a business can understand and act on.

SCOPE OF THE ASSESSMENT

This assessment was performed on a public demo website (OWASP Juice Shop) using a read-only approach. The testing focused on identifying exposed services, checking basic security controls, and finding common web application security issues.

Tools Used:

- Nmap – Used to identify open ports, running services, and service versions on the target system.
- OWASP ZAP – Used to scan the web application for security issues.
- ZAP Spider – Used to discover URLs and application pages.
- ZAP AJAX Spider – Used to crawl dynamic and JavaScript-based content for deeper coverage.

NMAP TOOL RESULTS

What Was Found:
The scan shows that the target system is online and has two open ports: 80 (HTTP) and 443 (HTTPS), both handled by heroku-router. All other ports are filtered.

Risk Level
Medium Risk – Publicly exposed web services increase the attack surface and can be targeted if misconfigured or outdated.

Recommended Fixes:
Keep only required ports open
Keep the server and services updated
Use a firewall/WAF and limit information disclosure

ZAP SCAN RESULTS

1) Content Security Policy (CSP) Header Not Set :
Found: No CSP header is used.
Risk: Increases chance of XSS and malicious script injection.
Fix: Add a CSP header to allow content only from trusted sources.

2) Session ID in URL:
Found: Session identifier appears in the URL.
Risk: Session hijacking via logs, history, or shared links.
Fix: Use cookies for session management, not URLs.

3) Vulnerable JavaScript Library
Found: Outdated JS library detected.
Risk: Known vulnerabilities can be exploited.
Fix: Update to the latest secure version or remove unused libraries.