SECURITY ASSESSMENT REPORT

WEB APPLICATION SECURITY ASSESSMENT REPORT

Intern Name: rishika joshi
Internship Program: Cyber Security Internship – Future Interns
Task: – Web Application Security Testing
Target Application: OWASP Juice Shop

Target URL: https://demo.owasp-juice.shop
Assessment Type: Vulnerability Assessment
Tool Used: OWASP ZAP
Date: 18-12-2025

A G E N D A

- Introduction
- scope of testing
- tools and methadology
- Vulnerability Findings
- conclusion
- disclaimer

INTRODUCTION

This project focuses on performing a vulnerability assessment of a deliberately vulnerable web application, OWASP Juice Shop. The objective of this assessment is to identify common web application security vulnerabilities using ethical hacking tools and to map the findings to OWASP Top 10 security risks.

The assessment simulates a real-world client engagement where web applications used by startups, SaaS platforms, and e-commerce companies must be tested and secured against potential cyber threats..

SCOPE OF TESTING

in scope

Target website:
https://demo.owasp-juice.shop
All publicly accessible pages
and directories

out of scope

External domains (Google,
GitHub, CDN links, social media)
Third-party services

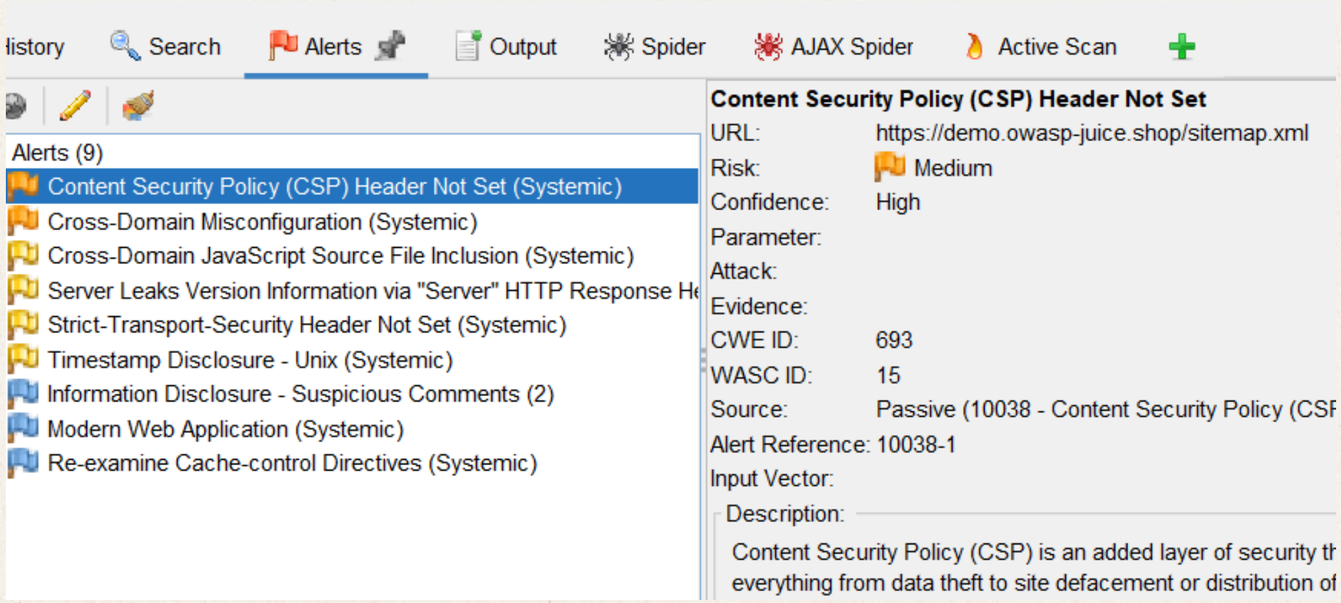
TOOLS AND METHADOLOGY

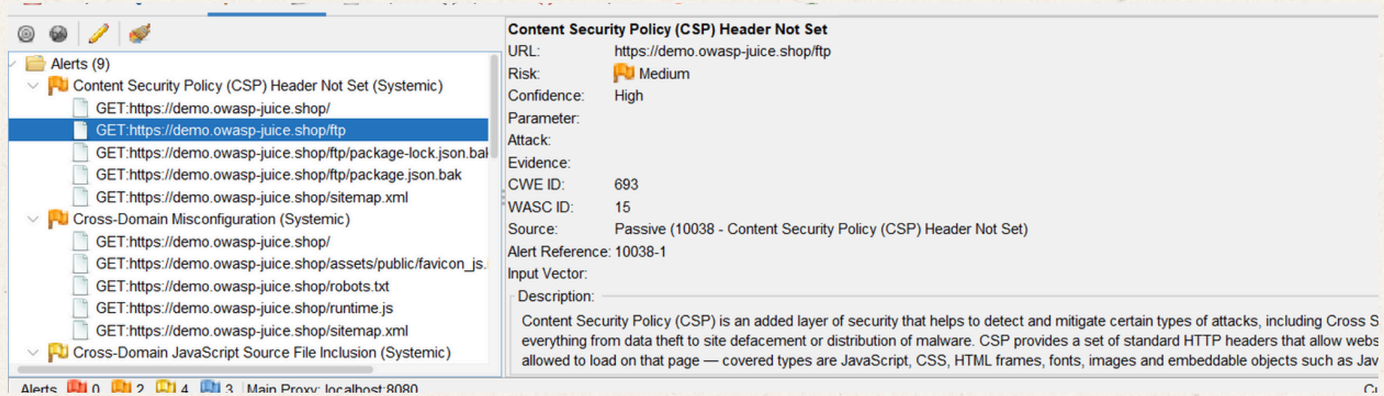
Tools Used:

OWASP ZAP – Automated vulnerability scanning and analysis
Web Browser – Manual verification
WPS office – Documentation

Methodology:

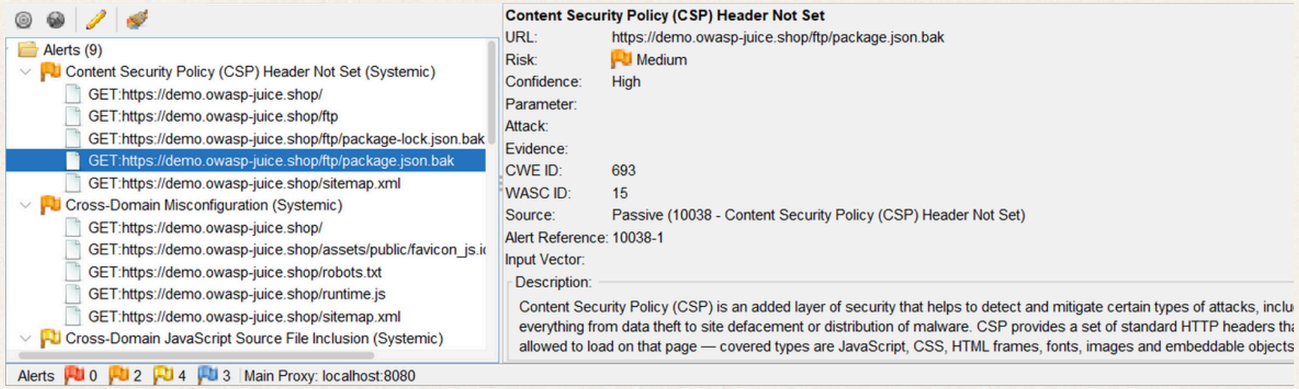
1. Automated scan using OWASP ZAP
2. Identification of Medium-risk vulnerabilities
3. Manual verification using browser
4. Mapping vulnerabilities to OWASP Top 10
5. Documentation with screenshots and remediation steps





vernability finding

Vulnerability 1:
Directory Browsing Enabled
Risk Level: Medium
OWASP Top 10 Category:
A05 – Security Misconfiguration
Description:
The application allows directory browsing, which exposes internal directories and files to unauthorized users. This allows attackers to gain insight into the application's internal structure.
Affected URL:
https://demo.owasp-juice.shop/ftp/
Impact:
An attacker can view, download, or analyze internal files, which may contain sensitive information and assist in further attacks.
Disable directory listing on the server
Restrict access to sensitive directories
Apply proper access control rules



Vulnerability 2:

Sensitive File Exposure

Risk Level: Medium

OWASP Top 10 Category:

A05 – Security Misconfiguration

Description: :

Sensitive files such as backup files (.bak), documentation files, and configurationrelated
files were publicly accessible through the FTP directory

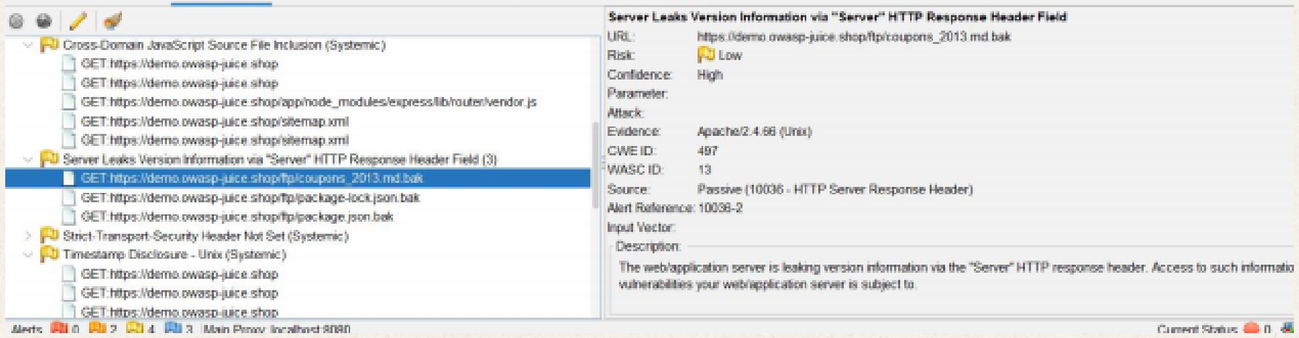
Examples of Exposed Files:

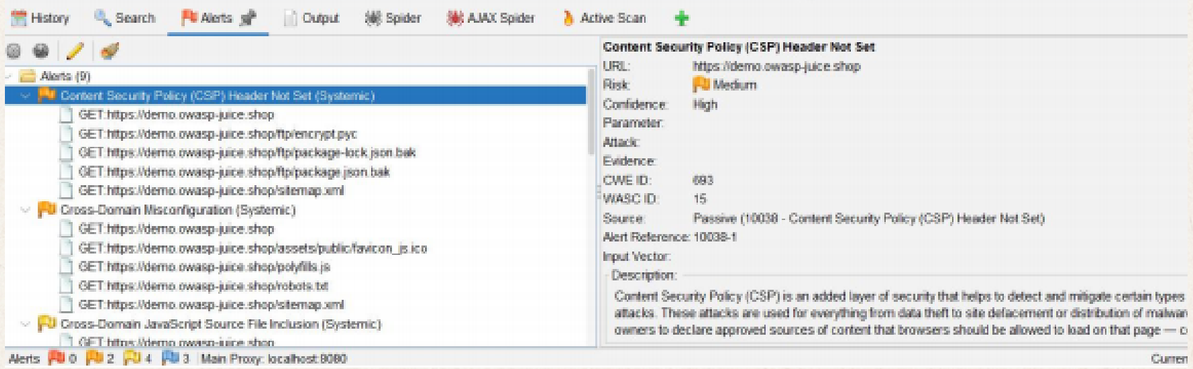
coupons_2013.md.bak

package.json.bak

Impact:

Exposure of sensitive files may lead to information disclosure, credential leakage, or further system compromise





Vulnerability 3:

Missing Security Headers

Risk Level: Medium

OWASP Top 10 Category:

A05 – Security Misconfiguration

Description:

The application does not implement important HTTP security headers, which are used to protect against common web attacks .

Missing Headers Include:

X-Frame-Options

X-Content-Type-Options

Content-Security-Policy

Impact:

The absence of these headers increases the risk of clickjacking, MIME-type attacks, and cross-site scripting. ..

OWASP TOP 10 MAPPING SUMMARY

Vulnerability OWASP Top 10

Directory Browsing A05 – Security Misconfiguration
Sensitive File Exposure A05 – Security Misconfiguration
Missing Security Headers A05 – Security Misconfiguration
Information Disclosure A01 – Broken Access Control

CONCLUSION

The vulnerability assessment identified multiple medium-risk security issues primarily related to security misconfiguration and information disclosure. Although the application is intentionally vulnerable for learning purposes, similar issues in realworld applications could lead to serious security breaches.

Implementing proper access controls, removing exposed files, and applying recommended security headers would significantly improve the application's security posture.

DISCLAIMER

This assessment was conducted solely for educational purposes on an intentionally
vulnerable application. No unauthorized testing was performed on real-world
production systems.

Thank you!