

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 methodology
- 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 METHODOLOGY

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



Vulnerability finding

The screenshot shows a web-based security tool interface. At the top, there are tabs for History, Search, Alerts, Spider, AJAX Spider, Active Scan, and a plus sign icon. Below the tabs, there are icons for Home, Refresh, and a pencil. A sidebar on the left lists 'Alerts (9)' with various items, some of which are expanded to show detailed information. The main panel displays a specific alert: 'Content Security Policy (CSP) Header Not Set'.

Content Security Policy (CSP) Header Not Set

URL: <https://demo.owasp-juice.shop/sitemap.xml>
Risk: Medium
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)
Alert Reference: 10038-1
Input Vector:
Description:
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross-Site Scripting (XSS), Clickjacking, and Data Theft. It provides a set of standard HTTP headers that allow websites to specify what content is allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, and iframes.

Below this, another section shows a detailed view of the 'Content Security Policy (CSP) Header Not Set' vulnerability for the URL <https://demo.owasp-juice.shop/ftp>. The details are identical to the first one, except for the URL.

At the bottom of the interface, there are status indicators for alerts (0), errors (2), warnings (4), and info (3), followed by the text 'Main Proxy: localhost:8080'.

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

Content Security Policy (CSP) Header Not Set

URL: <https://demo.owasp-juice.shop/ftp/package.json.bak>
Risk: Medium
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)
Alert Reference: 10038-1
Input Vector:
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow you to specify what resources are allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects.

Alerts: 0 Critical, 2 High, 4 Medium, 3 Low | Main Proxy: localhost:8080

Server Leaks Version Information via "Server" HTTP Response Header Field

URL: https://demo.owasp-juice.shop/ftp/coupons_2013.md.bak
Risk: Low
Confidence: High
Parameter:
Attack:
Evidence: Apache/2.4.6 (Ubuntu)
CWE ID: 497
WASC ID: 13
Source: Passive (10036 - HTTP Server Response Header)
Alert Reference: 10036-2
Input Vector:
Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information can be used to exploit known vulnerabilities your web/application server is subject to.

Alerts: 0 Critical, 2 High, 4 Medium, 3 Low | Main Proxy: localhost:8080

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 configuration 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.

..

Content Security Policy (CSP) Header Not Set
URL: https://demo.owasp-juice.shop
Risk: Medium
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 683
WASC ID: 15
Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)
Alert Reference: 10038-1
Input Vector:
Description:
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. Owners can declare approved sources of content that browsers should be allowed to load on that page — o

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!
