🛡️ Web Application Security Assessment Report – Task 1

👤 **Author:** Odai wahib
🗓️ **Date of Scan:** August 6, 2025
💉 **Tool Used:** OWASP ZAP
🎯 **Target Application:** http://localhost

📝 Introduction

This report presents the results of a security assessment conducted on a locally hosted web application as part of **Task 1** in a cybersecurity learning program. The primary objective was to identify common vulnerabilities using automated scanning techniques and document the results in a professional format.

The scanning was performed using **OWASP ZAP**, an open-source security tool widely used for web application penetration testing. The focus was on evaluating HTTP response headers, content security policies, and information exposure.

📜 Overview

This assessment highlights key security issues discovered during the scan. The vulnerabilities are categorized based on their risk level and include issues related to Content Security Policy (CSP), missing headers, and information leakage.

🚨 Security Findings

⚠️ Medium Risk Vulnerabilities

1. **CSP: Failure to Define Directive with No Fallback**
   The Content Security Policy (CSP) does not include default fallback directives, which may lead to unintentional content execution.
2. **CSP: Wildcard Directive (*)**
   The use of wildcards in CSP (e.g., default-src: *) permits content from any origin, weakening security enforcement.
3. **CSP: script-src 'unsafe-inline'**
   Allows execution of inline JavaScript, increasing susceptibility to XSS attacks.

4. **CSP: style-src 'unsafe-inline'**
   Permits inline CSS, which could allow style injection vulnerabilities.
5. **CSP Header Not Set**
   The absence of a CSP header leaves the application unprotected from script injection.
6. **Missing Anti-clickjacking Header**
   The X-Frame-Options header is missing, exposing the application to potential clickjacking attacks.
7. **X-Frame-Options Defined via <meta> Tag**
   The anti-clickjacking policy is set using a <meta> tag, which is not a secure or reliable implementation.

🟡 Low Risk Vulnerabilities

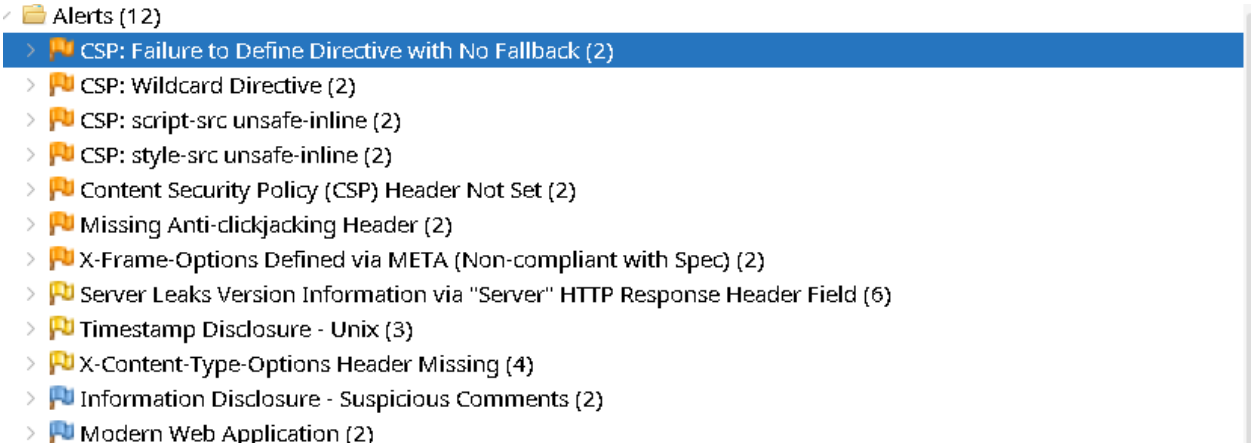
1. **Server Version Disclosure**
   The Server response header reveals backend server version details.
2. **Timestamp Disclosure - Unix Format**
   Unix timestamps are visible in the page, which may leak timing or session details.
3. **Missing X-Content-Type-Options Header**
   The nosniff header is not present, potentially allowing content type confusion.
4. **Information Disclosure via Comments**
   HTML or JavaScript comments contain information that could be leveraged in targeted attacks.

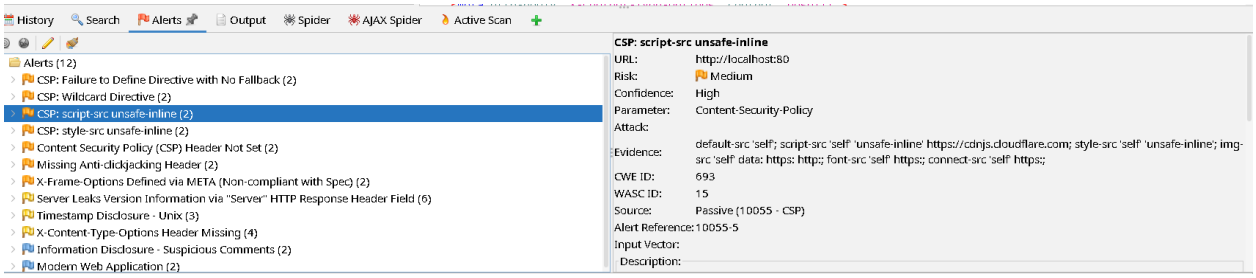
ℹ️ Informational Observations

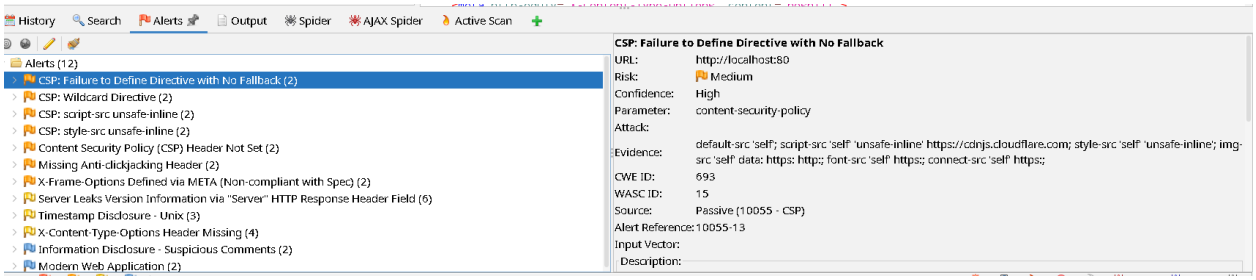
- **Modern Web Application Stack Detected**
  The scan identified technologies consistent with a modern web application architecture. This is informational only and not a vulnerability.

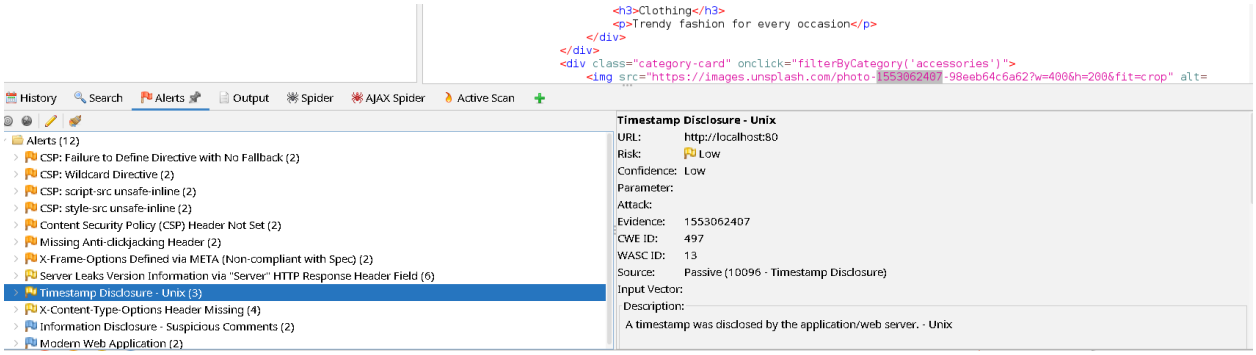
📸 Key Screenshots

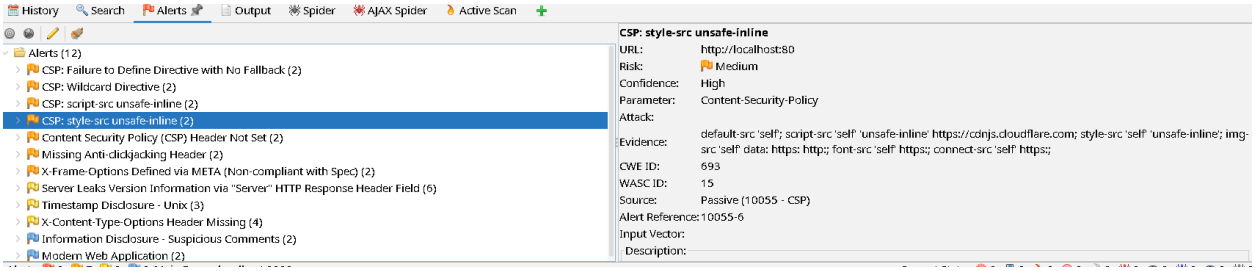
All findings are visually documented using screenshots captured during the scanning process. These images are included in the full report and provide contextual clarity for each vulnerability detected.

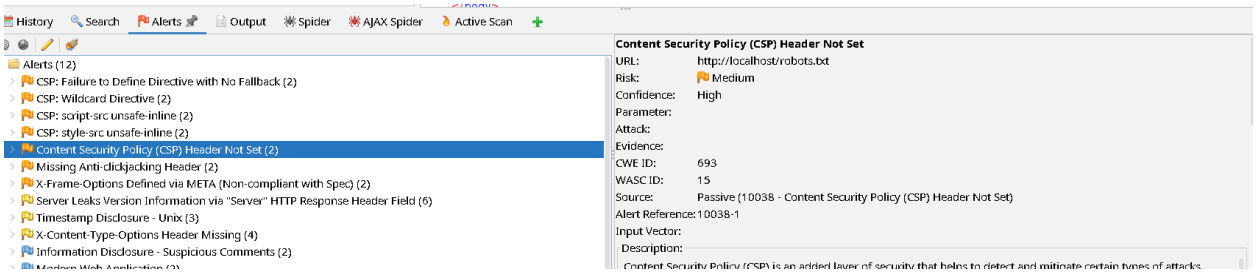


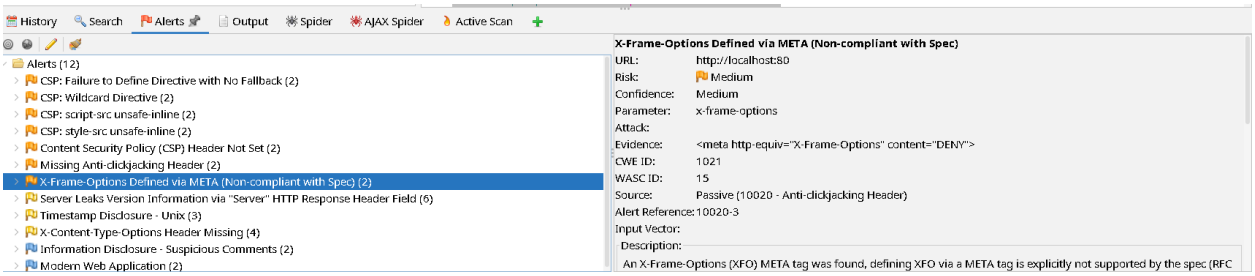


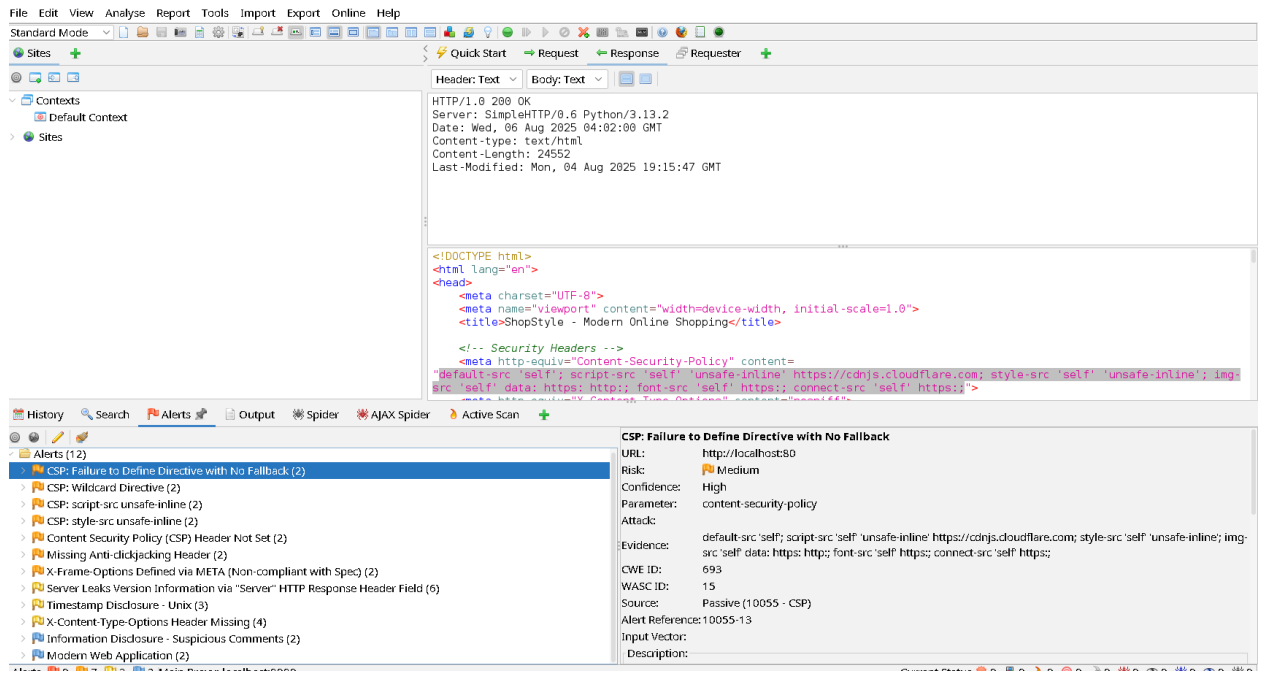





History Search Alerts Output Spider AJAX Spider Active Scan
Alerts (12)
CSP: Failure to Define Directive with No Fallback (2)
CSP: Wildcard Directive (2)
CSP: script-src unsafe-inline (2)
CSP: style-src unsafe-inline (2)
Content Security Policy (CSP) Header Not Set (2)
Missing Anti-clickjacking Header (2)
X-Frame-Options Defined via META (Non-compliant with Spec) (2)
Server Leaks Version Information via "Server" HTTP Response Header Field (6)
Timestamp Disclosure - Unix (3)
X-Content-Type-Options Header Missing (4)
Information Disclosure - Suspicious Comments (2)
Modern Web Application (2)
CSP: style-src unsafe-inline
URL: http://localhost:80
Risk: Medium
Confidence: High
Parameter: Content-Security-Policy
Attack:
Evidence: default-src 'self'; script-src 'self' 'unsafe-inline' https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline'; img-src 'self' data: https: http:; font-src 'self' https:; connect-src 'self' https:;
CWE ID: 693
WASC ID: 15
Source: Passive (10055 - CSP)
Alert Reference: 10055-6
Input Vector:
Description:


History Search Alerts Output Spider AJAX Spider Active Scan
Alerts (12)
CSP: Failure to Define Directive with No Fallback (2)
CSP: Wildcard Directive (2)
CSP: script-src unsafe-inline (2)
CSP: style-src unsafe-inline (2)
Content Security Policy (CSP) Header Not Set (2)
Missing Anti-clickjacking Header (2)
X-Frame-Options Defined via META (Non-compliant with Spec) (2)
Server Leaks Version Information via "Server" HTTP Response Header Field (6)
Timestamp Disclosure - Unix (3)
X-Content-Type-Options Header Missing (4)
Information Disclosure - Suspicious Comments (2)
Content Security Policy (CSP) Header Not Set
URL: http://localhost/robots.txt
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:


History Search Alerts Output Spider AJAX Spider Active Scan
Alerts (12)
CSP: Failure to Define Directive with No Fallback (2)
CSP: Wildcard Directive (2)
CSP: script-src unsafe-inline (2)
CSP: style-src unsafe-inline (2)
Content Security Policy (CSP) Header Not Set (2)
Missing Anti-clickjacking Header (2)
X-Frame-Options Defined via META (Non-compliant with Spec) (2)
Server Leaks Version Information via "Server" HTTP Response Header Field (6)
Timestamp Disclosure - Unix (3)
X-Content-Type-Options Header Missing (4)
Information Disclosure - Suspicious Comments (2)
Modern Web Application (2)
X-Frame-Options Defined via META (Non-compliant with Spec)
URL: http://localhost:80
Risk: Medium
Confidence: Medium
Parameter: x-frame-options
Attack:
Evidence: <meta http-equiv="X-Frame-Options" content="DENY">
CWE ID: 1021
WASC ID: 15
Source: Passive (10020 - Anti-clickjacking Header)
Alert Reference: 10020-3
Input Vector:
Description:
An X-Frame-Options (XFO) META tag was found, defining XFO via a META tag is explicitly not supported by the spec (RFC


File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start Request Response Requester
Header: Text Body: Text
Contexts
Default Context
Sites
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.13.2
Date: Wed, 06 Aug 2025 04:02:00 GMT
Content-type: text/html
Content-Length: 24552
Last-Modified: Mon, 04 Aug 2025 19:15:47 GMT
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>ShopStyle - Modern Online Shopping</title>
<!-- Security Headers -->
<meta http-equiv="Content-Security-Policy" content=
"default-src 'self'; script-src 'self' 'unsafe-inline' https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline'; img-src 'self' data: https: http:; font-src 'self' https:; connect-src 'self' https:;">
History Search Alerts Output Spider AJAX Spider Active Scan
Alerts (12)
CSP: Failure to Define Directive with No Fallback (2)
CSP: Wildcard Directive (2)
CSP: script-src unsafe-inline (2)
CSP: style-src unsafe-inline (2)
Content Security Policy (CSP) Header Not Set (2)
Missing Anti-clickjacking Header (2)
X-Frame-Options Defined via META (Non-compliant with Spec) (2)
Server Leaks Version Information via "Server" HTTP Response Header Field (6)
Timestamp Disclosure - Unix (3)
X-Content-Type-Options Header Missing (4)
Information Disclosure - Suspicious Comments (2)
Modern Web Application (2)
CSP: Failure to Define Directive with No Fallback
URL: http://localhost:80
Risk: Medium
Confidence: High
Parameter: content-security-policy
Attack:
Evidence: default-src 'self'; script-src 'self' 'unsafe-inline' https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline'; img-src 'self' data: https: http:; font-src 'self' https:; connect-src 'self' https:;
CWE ID: 693
WASC ID: 15
Source: Passive (10055 - CSP)
Alert Reference: 10055-13
Input Vector:
Description: