Web Application Security Assessment Report

Introduction

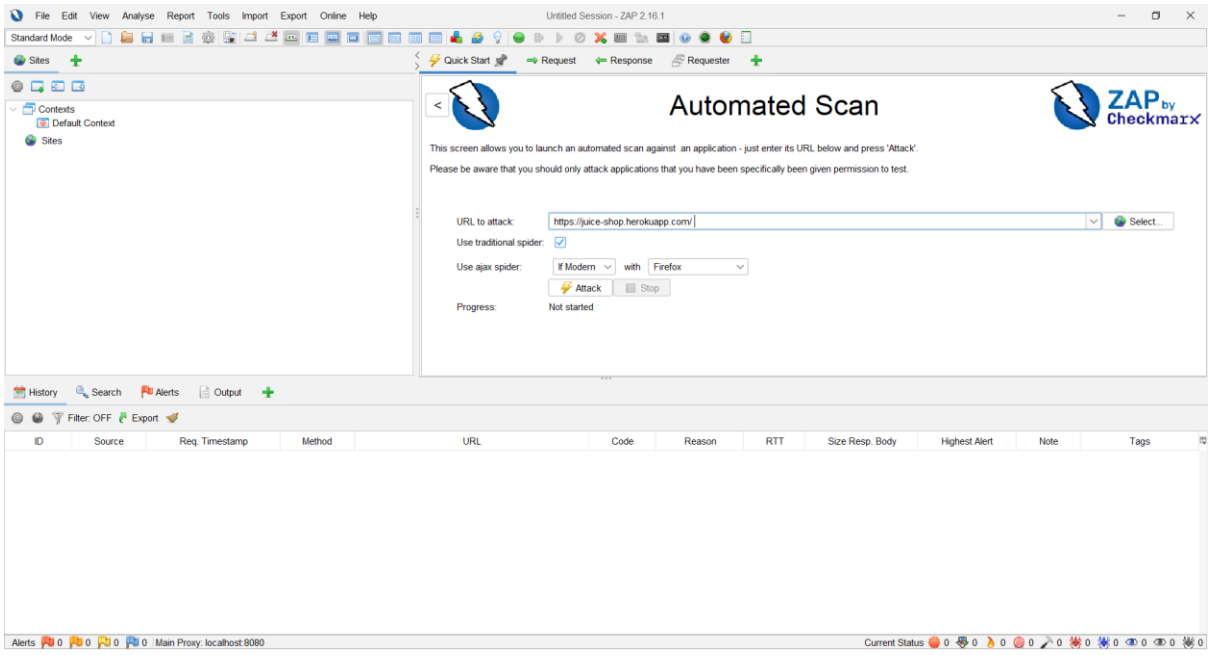
- Objective: Identify security vulnerabilities
- Application Tested: OWASP Juice Shop
- Reference: https://owasp.org/www-project-juice-shop/
- Tool Used: OWASP ZAP
- Testing Type: Automated security assessment

Methodology

- Automated Scan using OWASP ZAP
- Crawling using Spider and AJAX Spider
- OWASP Top 10 used for classification

Vulnerability Findings

The screenshot below contains the automated Zap scan



Vulnerability 1: Content Security Policy (CSP) Header Not Set

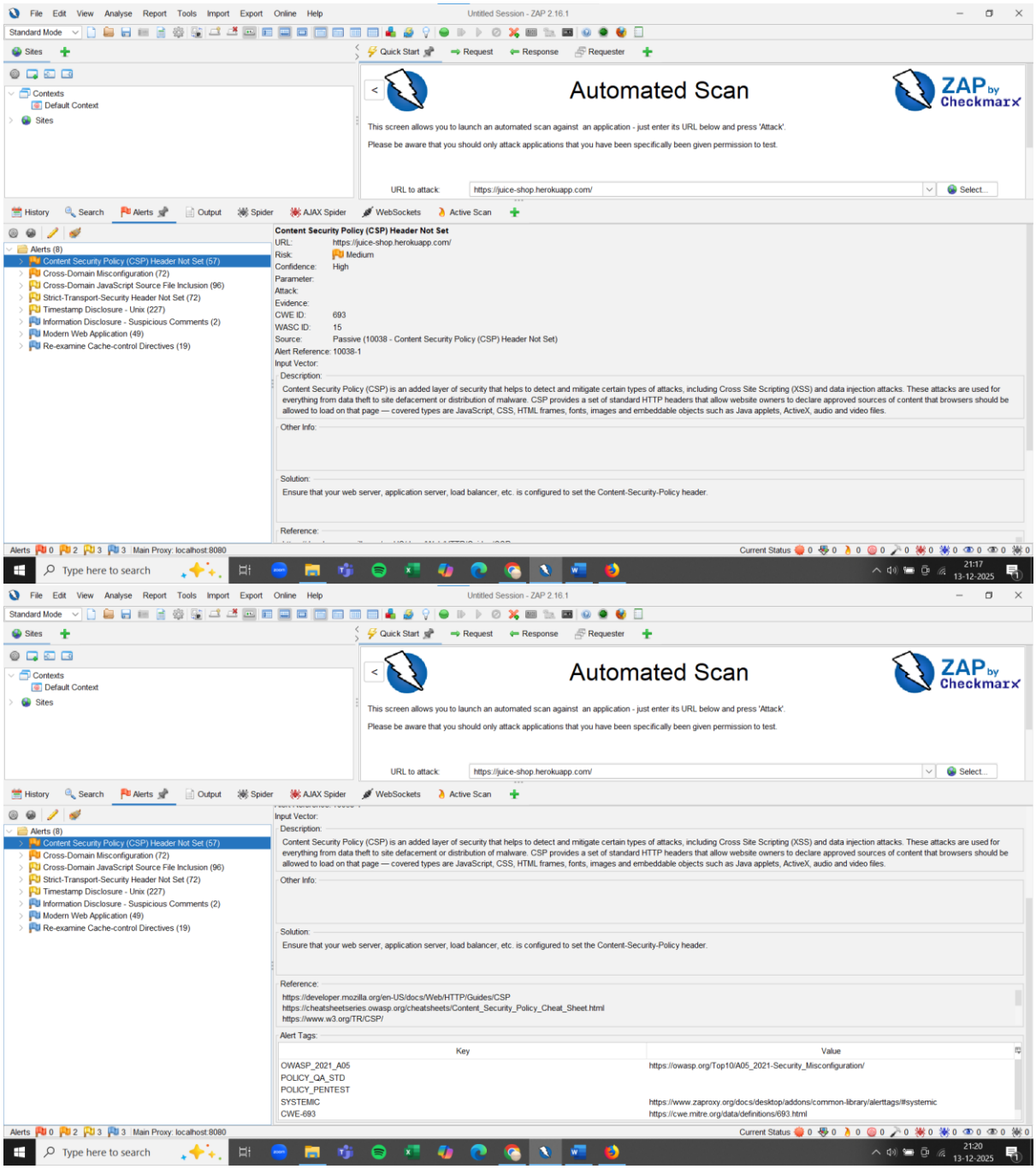
Risk Rating: Medium

Description:
The application does not define a Content Security Policy header, which may allow malicious scripts to execute.

Impact:
Attackers may inject unauthorized scripts, leading to data theft.

OWASP Category:
A05 – Security Misconfiguration

Screenshot:



Recommendation:

Implement a strict CSP header to restrict script execution.

Vulnerability 2: Cross-Domain Misconfiguration

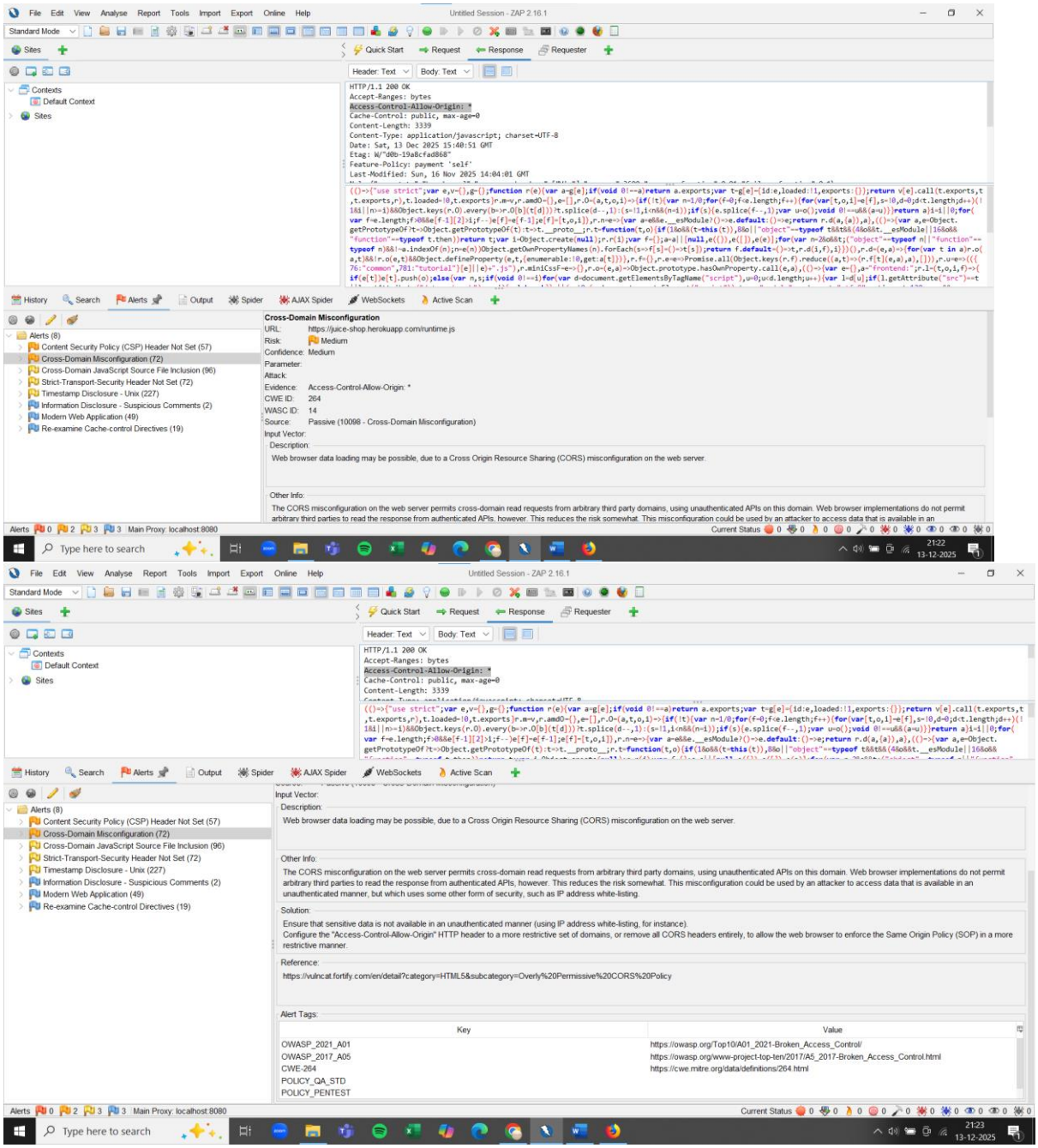
Risk Rating: Medium

Description:
The application allows cross-domain interactions without proper restrictions, which may expose sensitive resources.

Impact:
Attackers may exploit this misconfiguration to access or manipulate data from other domains.

OWASP Category:
A05 – Security Misconfiguration

Screenshot:



Recommendation:
Restrict cross-domain access by configuring proper CORS (Cross-Origin Resource Sharing) policies.

Vulnerability 3: Strict-Transport-Security (HSTS) Header Not Set

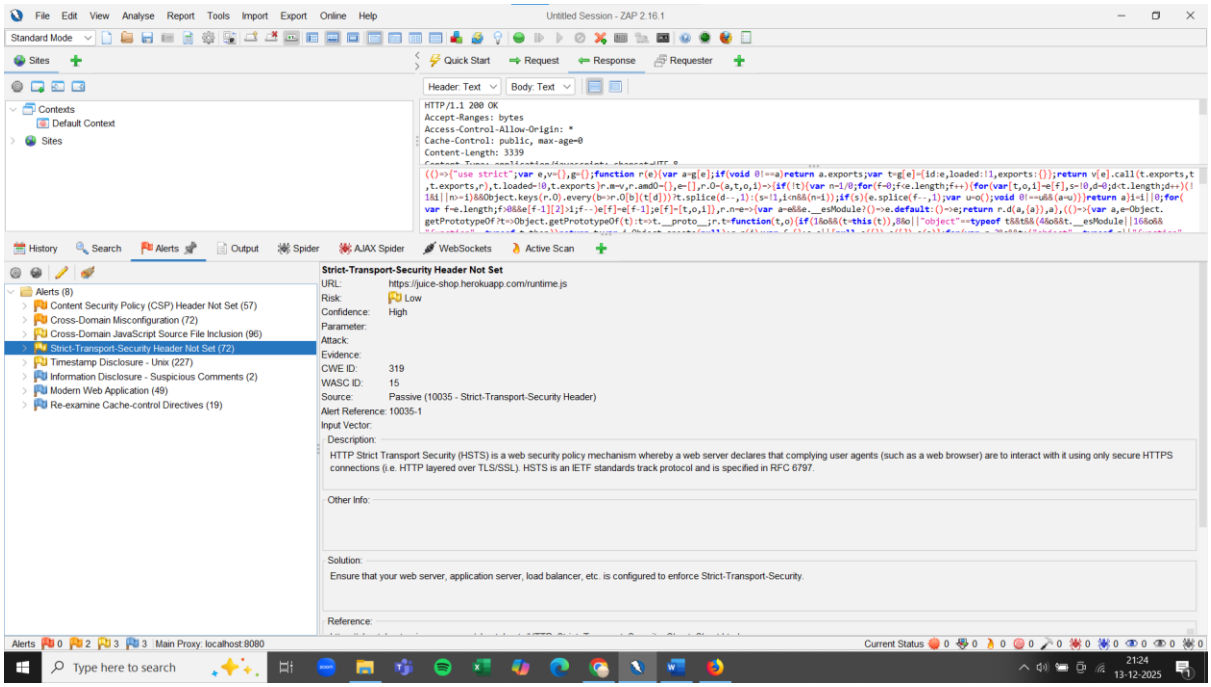
Risk Rating: Medium

Description:
The application does not include the HTTP Strict Transport Security (HSTS) header, allowing browsers to communicate over insecure HTTP connections.

Impact:
An attacker could perform man-in-the-middle attacks and intercept sensitive data.

OWASP Category:
A02 – Cryptographic Failures

Screenshot:



Recommendation:
Enable the HSTS header to ensure all communications occur over HTTPS.

Vulnerability 4: Information Disclosure – Suspicious Comments

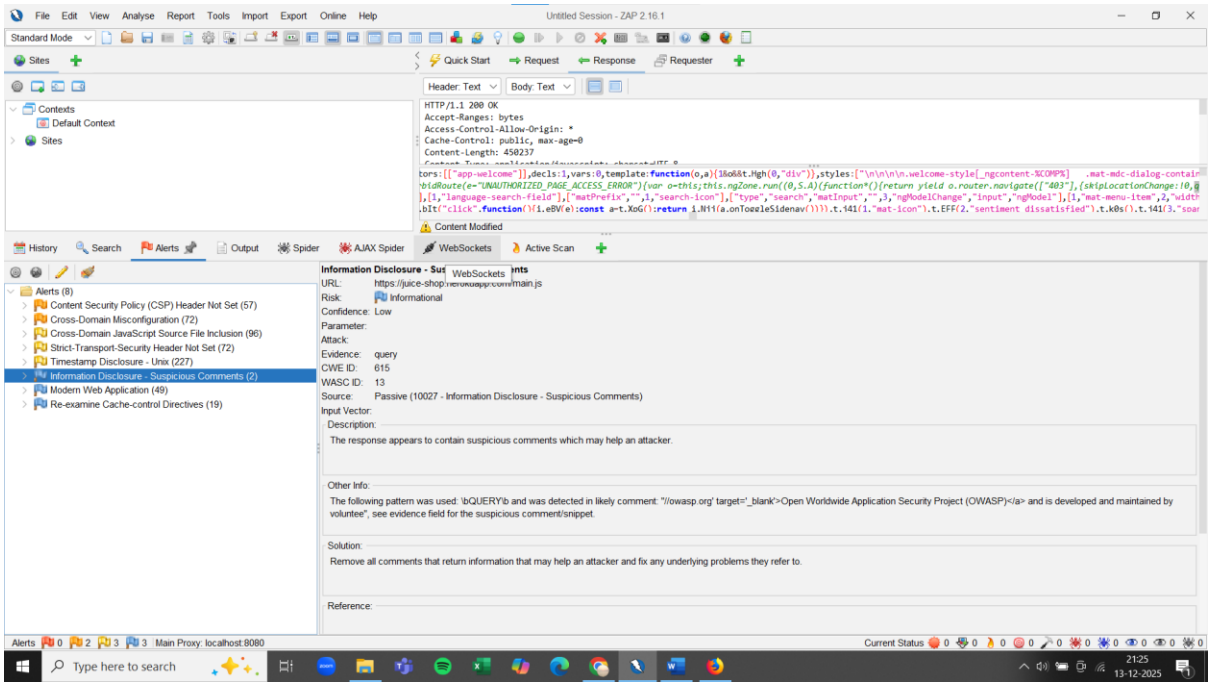
Risk Rating: Low

Description:
The application contains suspicious comments in the source code that may reveal internal implementation details.

Impact:
Attackers could use this information to understand the application structure and plan further attacks.

OWASP Category:
A01 – Broken Access Control

Screenshot:



Recommendation:
Remove all unnecessary comments from production code before deployment.

Vulnerability 5: Timestamp Disclosure – Unix

Risk Rating: Low

Description:

The application discloses Unix timestamps in server responses, which may reveal system information.

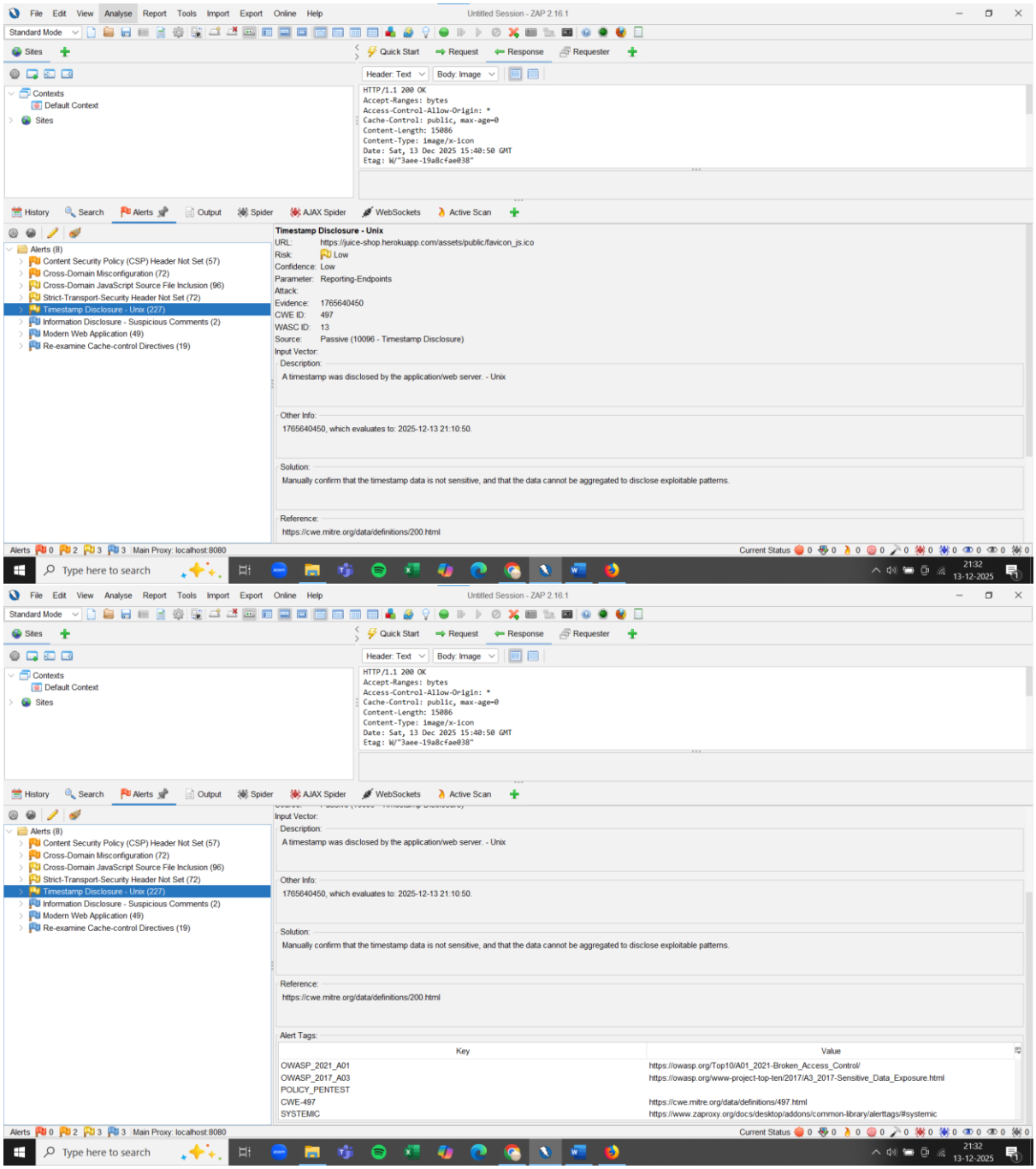
Impact:

Attackers could use timing information to analyse server behaviour or plan targeted attacks.

OWASP Category:

A01 – Broken Access Control

Screenshot:



Recommendation:

Avoid exposing internal timestamp information in responses unless required.

OWASP Top 10 Category mapping

OWASP Top 10 Category	**Status**
A01: Broken Access Control	Issues Found in vulnerabilities 5,4
A02: Cryptographic Failures	Issues Found in vulnerabilities 3
A03: Injection	Not found
A04: Insecure Design	Not found
A05: Security Misconfiguration	Issues Found in vulnerabilities 1,2
A06: Vulnerable and Outdated Components	Not found
A07: Identification and Authentication Failures	Not found
A08: Software and Data Integrity Failures	Not found
A09: Security Logging and Monitoring Failures	Not found
A10: Server Side Requested Forgery	Not found

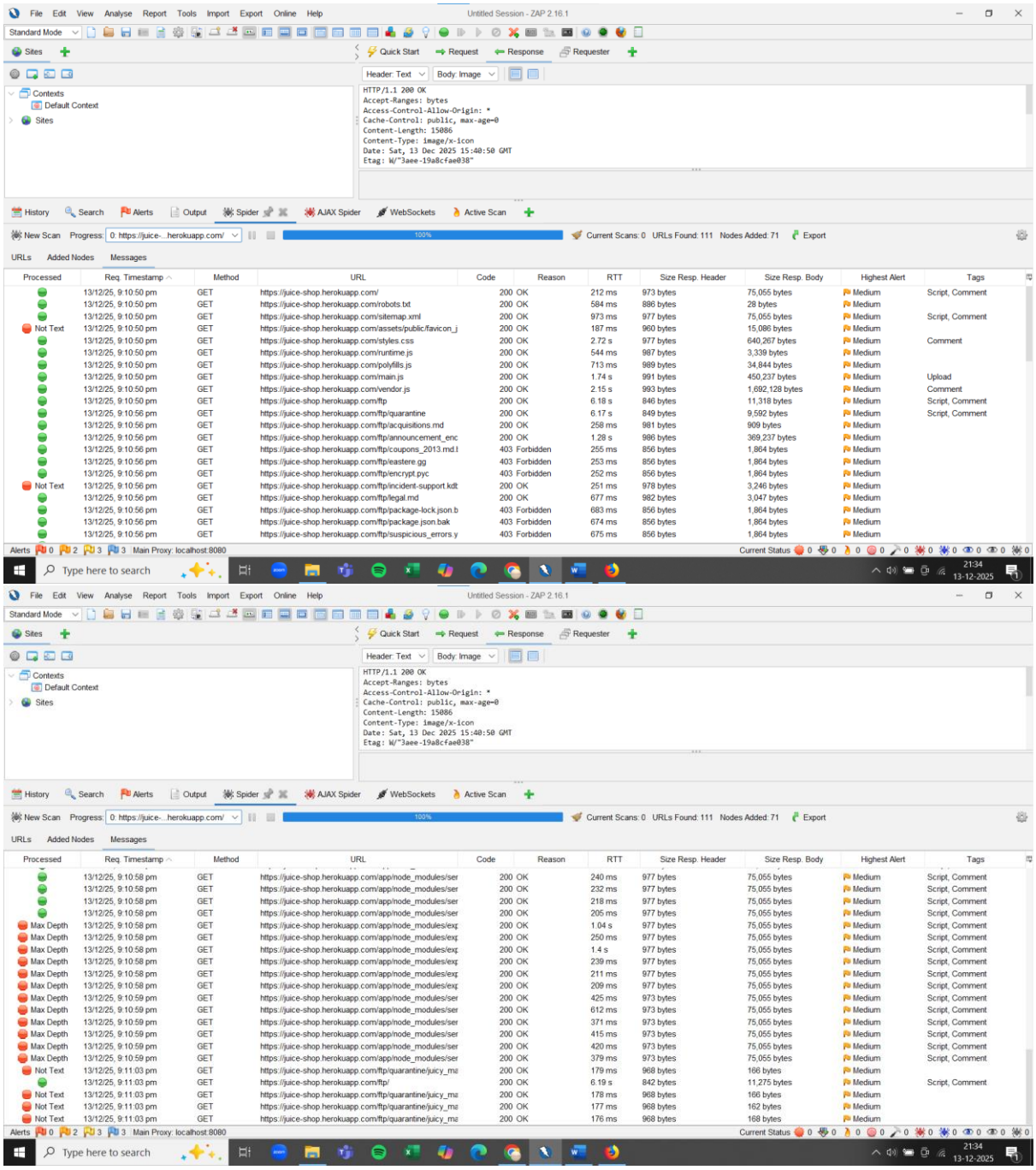
Tool logs:

ZAP scan report:

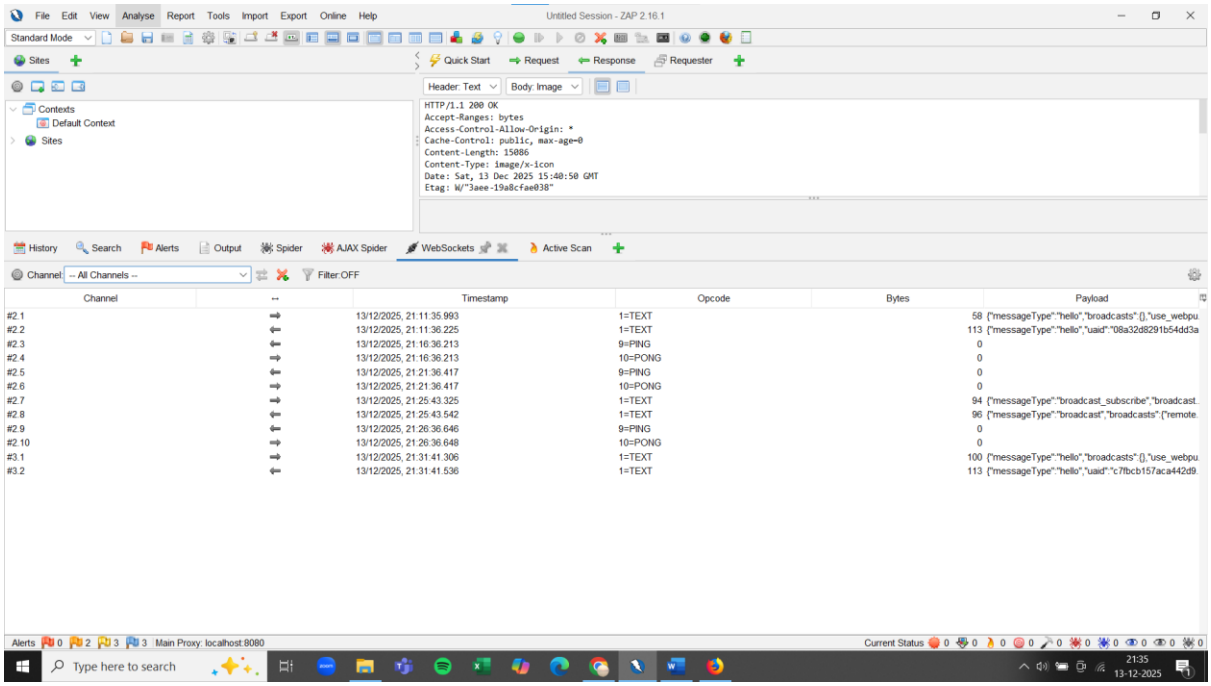
ZAP by Checkmarx Scanning Report

Additional screenshots:

Spider running:



Websockets:



Active scan: