OWASP Juice Shop Security Assessment

Date: 25/02/25
Tools Used: OWASP ZAP, Docker, OWASP Juice Shop

Introduction:
This report analyzes the security of OWASP Juice Shop, an intentionally vulnerable web application. The test was conducted using OWASP ZAP to identify security vulnerabilities from the OWASP Top 10 list.

Goals:

-Practical understanding of OWASP vulnerabilities

-Penetration Testing

-Ethical hacking

Methodology:
To conduct this security assessment:

-OWASP ZAP installed to perform an automated vulnerability scan.

-Set up OWASP Juice Shop using Docker to run the application locally.

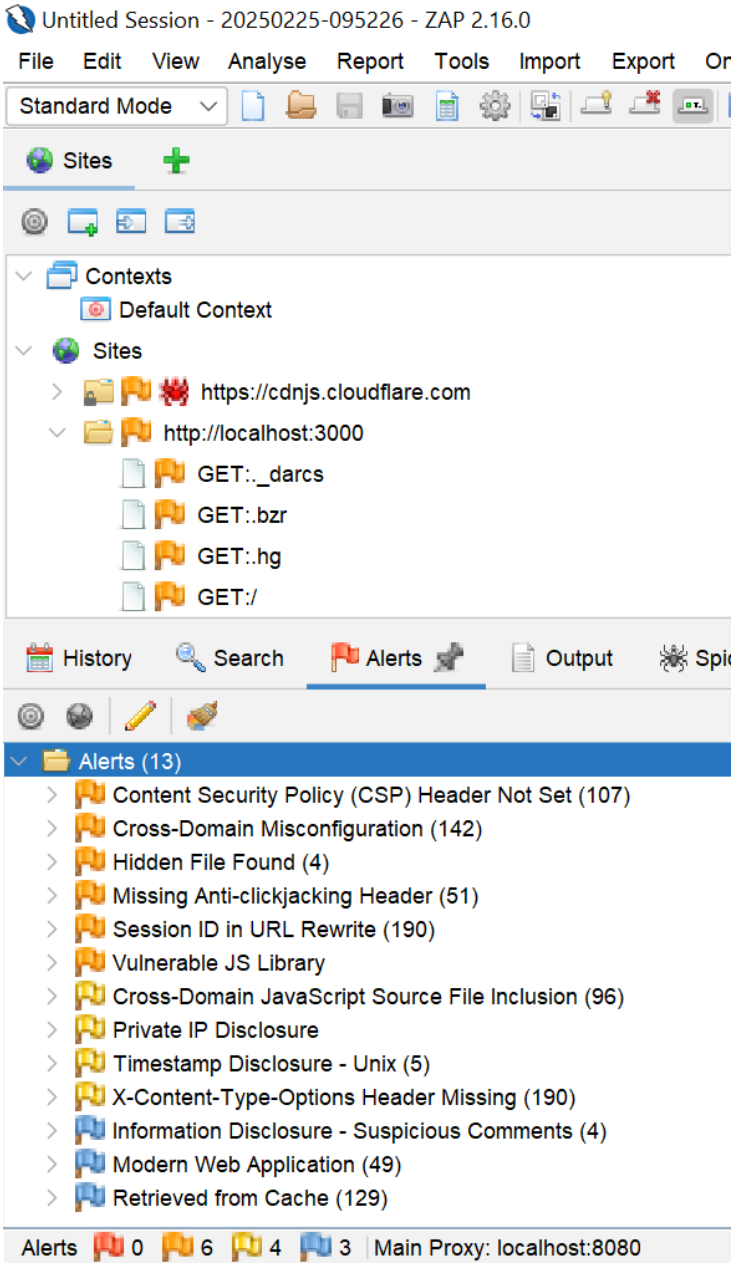
-Configured Windows Subsystem for Linux (WSL) with Ubuntu Linux to manage the Docker environment.

-Executed the security scan in OWASP ZAP, targeting http://localhost:3000.

Security Findings:

Vulnerability	Category	Description	Risk Level	Recommendation
Content Security Policy (CSP) header not set	Security Misconfiguration	-Prone to data injection attacks of malicious content to the website -Allows for XXS attacks, Cross-Site Scripting	Medium	Configure the Content-Security-Policy header into all servers.
Cross-Domain Misconfiguration	Security Misconfiguration	-This is a Cross-Origin Resource Sharing misconfiguration. -This means any website can	Medium	-Allow only trusted websites. -Use proper authentication for API requests.

		request data from this site without prior authentication.		-Ensure that sensitive data is not available in an unauthenticated manner.
Hidden File Found	Sensitive Data Exposure	-A sensitive file was identified as accessible. -This may leak administrative, configuration, or credential information.	Medium	-Ensure access to the file requires appropriate authentication and authorization. -Limit exposure to internal systems.
Missing Anti-clickjacking Header	Security Misconfiguration	-An attacker can embed the website inside an invisible iframe on their malicious site.	Medium	-Enable CSP to allow embedding only from trusted sites.
Cross-Domain JavaScript Source File Inclusion	Security Misconfiguration & Cross-Site Scripting (XSS Risk)	-The page includes one or more script files from a third-party domain.	Low	-Ensure JavaScript source files are loaded from only trusted sources. -Ensure end users of the application can't control the sources.
Timestamp Disclosure - Unix	Information Disclosure	-Exposure of time stamp which allows for a risk of more data being exposed through social engineering	Low	-Manually confirm that the timestamp data is not sensitive.
Information Disclosure – Suspicious Comments	Information Disclosure	-Exposure of sensitive information, which allows for a risk of more data being exposed through social engineering	Informational	-Remove all comments that return information that may help an attacker. -Fix any underlying problems they refer to.



Conclusion:

This assessment identified thirteen security vulnerabilities in OWASP Juice Shop. The major threats were Injection, Security Misconfiguration and Cross-Site Scripting. Implementing the recommended fixes will significantly improve the security of the test application.

References:

1.OWASP Top 10 Vulnerabilities And Preventions - GeeksforGeeks

2.OWASP ZAP Documentation