FUTURE INTERNS

Cybersecurity Internship Report (Task 1)

Security Evaluation & Testing Report

Prepared By: Philip Takyi Obese  
Email: [obesephilip25@gmail.com](mailto:obesephilip25@gmail.com)

**Table of Contents**

1. **Overview** 
   * **Purpose of the Assessment**
2. **System Configuration** 
   * **Required Tools Installation**
   * **Verifying Installation**
3. **Tools Utilized**
4. **Security Testing Approach** 
   * **Automated Scanning (OWASP ZAP)**
   * **Manual Vulnerability Testing**
5. **Findings & Observations**
6. **Conclusion**
7. **References**

**1. Overview**

This report presents the security assessment of the OWASP Juice Shop application, a deliberately vulnerable platform used for penetration testing and security research. The objective was to uncover security flaws by combining automated scanning with manual penetration testing, conducted within a controlled Windows environment.

Purpose of the Assessment:

* System Configuration: Install and deploy the OWASP Juice Shop application on a local machine. This setup includes tools such docker.
* Automated Security Scan: Use OWASP ZAP to detect vulnerabilities like missing security headers and Cross-Site Scripting (XSS).
* Manual Security Testing: Simulate attacks using developer tools to identify flaws in input validation and authentication mechanisms.
* Findings Documentation: Record vulnerabilities, analyze risks, and suggest countermeasures.

**2. System Configuration**

Before conducting security assessments, it was essential to establish a testing environment using Windows and the necessary tools.

**A. Required Tools Installation**

To prepare for testing, the following dependencies were installed:

* Docker

**Installations;**

Docker: <https://www.docker.com/products/docker-desktop/>

OWASP Juice Shop: <https://owasp.org/www-project-juice-shop/>

OWASP Zap: <https://www.zaproxy.org/download/>

**Commands;**

 Pull the official Juice Shop Docker image

****

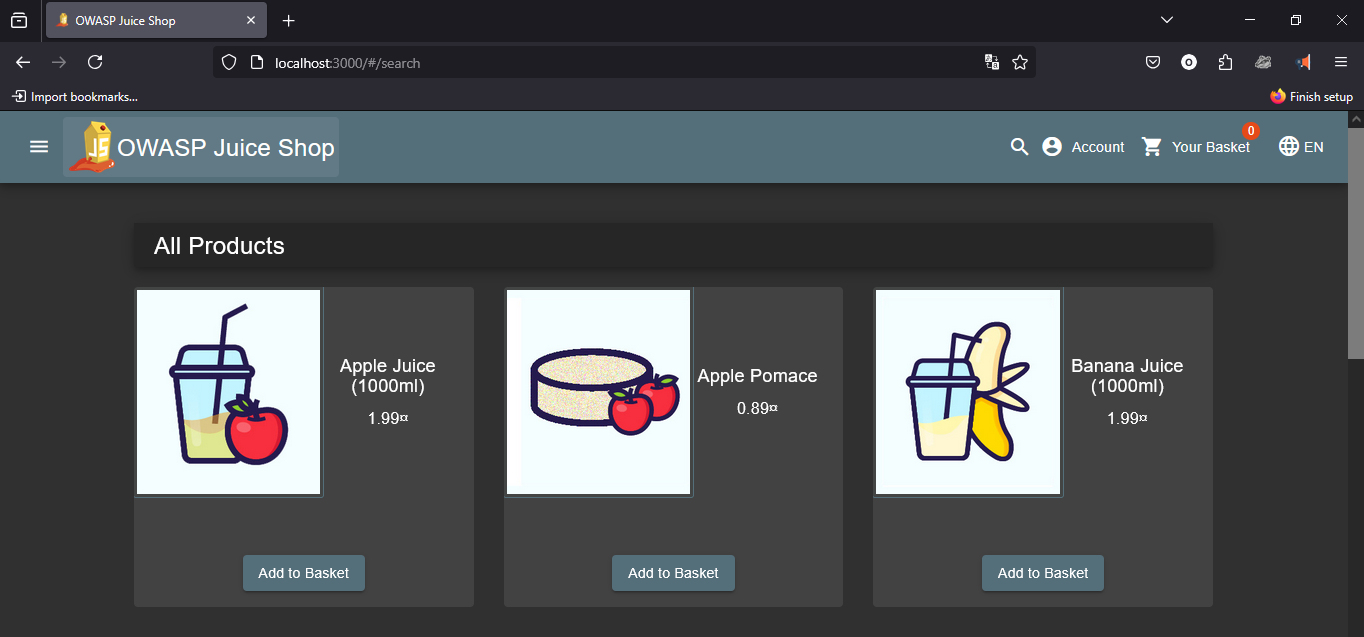
Run the Juice Shop container

****

**Verifying Installation;**

The setup was confirmed using:

* Browser Verification: Opened http://localhost:3000 to confirm access.

****

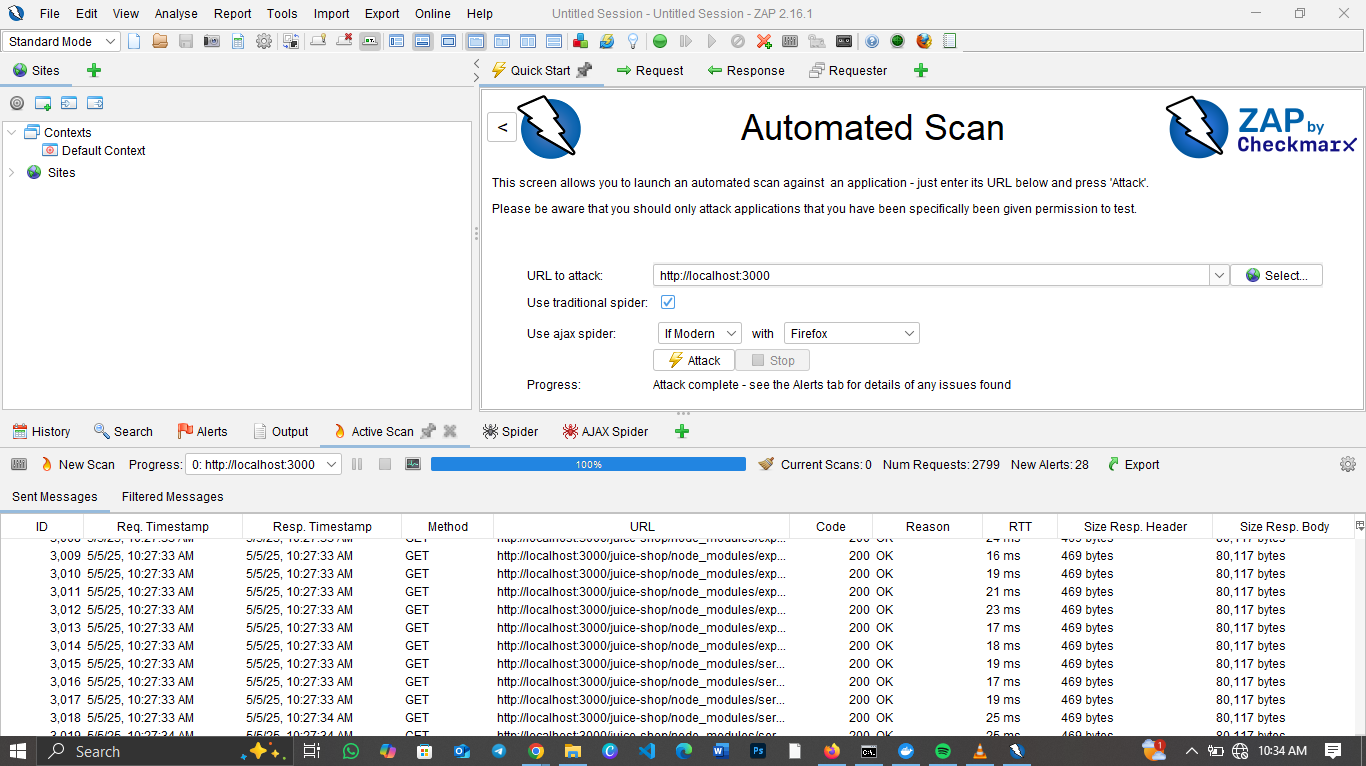
**3. Tools Utilized**

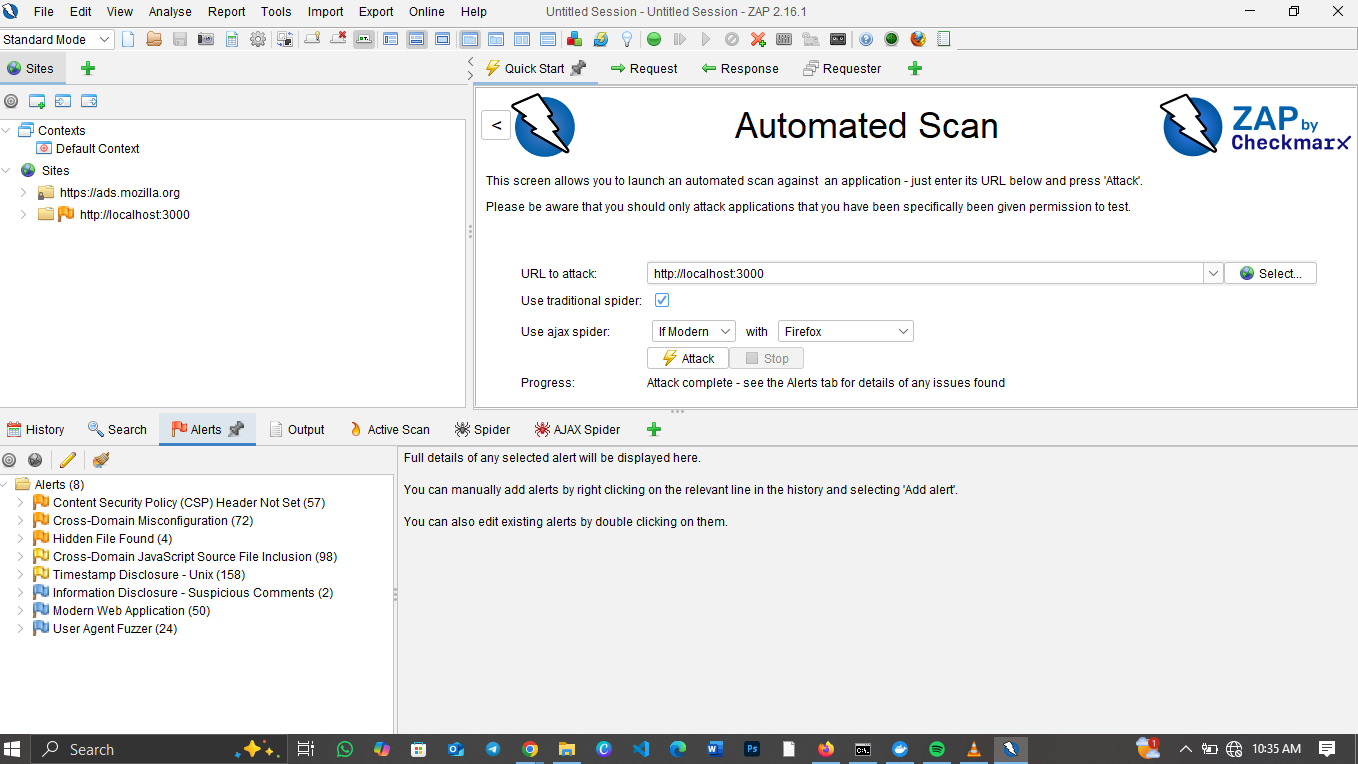
* OWASP ZAP: Conducted automated vulnerability scans**.**

**4. Security Testing Approach**

A. Automated Scanning with OWASP ZAP

* The target URL (http://localhost:3000) was set.
* A full scan was executed to detect security weaknesses.
* Vulnerabilities such as :  
  ·        SQL Injection  
  ·        Cross-domain configuration  
  ·        Cross-domain JavaScript source file inclusion  
  ·        Authentication and Session Management Flaws were logged.

****

****

**A screenshot of a computer

AI-generated content may be incorrect.**

**6. Conclusion**

The security assessment of the OWASP Juice Shop login form revealed no vulnerabilities for NoSQL Injection, or basic XSS attacks. These results suggest that proper security measures are in place. However, further assessments using more advanced attack vectors across different application components are recommended.

**7. References**

* [OWASP ZAP Documentation](https://www.zaproxy.org/)
* [OWASP Juice Shop GitHub Repository](https://github.com/juice-shop/juice-shop)