Cyber Security Internship Report – Task 2

Name: Kabsha Farooq

University: University of Engineering and Technology, Taxila

Department: Telecommunication Engineering

Internship Organization: Digital Empowerment Network

Task Title: Vulnerability Scanning using OWASP ZAP

Task No.: 2

# Task Overview

In Task 2 of my cybersecurity internship, I conducted a vulnerability scanning assessment of the OWASP Juice Shop web application using the OWASP ZAP tool. The objective was to identify security weaknesses in the application and generate actionable insights.

# Tools Used

• OWASP ZAP (Zed Attack Proxy)  
• Java JDK 17 (to run ZAP)  
• Operating System: Windows 10

# Steps Performed

1. Installed OWASP ZAP and configured Java JDK 17.
2. Opened ZAP and selected 'Manual Explore'.
3. Loaded target URL: https://juice-shop.herokuapp.com into ZAP's browser.
4. Clicked around the Juice Shop site to ensure page discovery.
5. Right-clicked on the loaded site in the 'Sites' tab and initiated an Active Scan.
6. Monitored progress via the Alerts tab and site structure.
7. Collected and reviewed vulnerability alerts flagged by the scan.

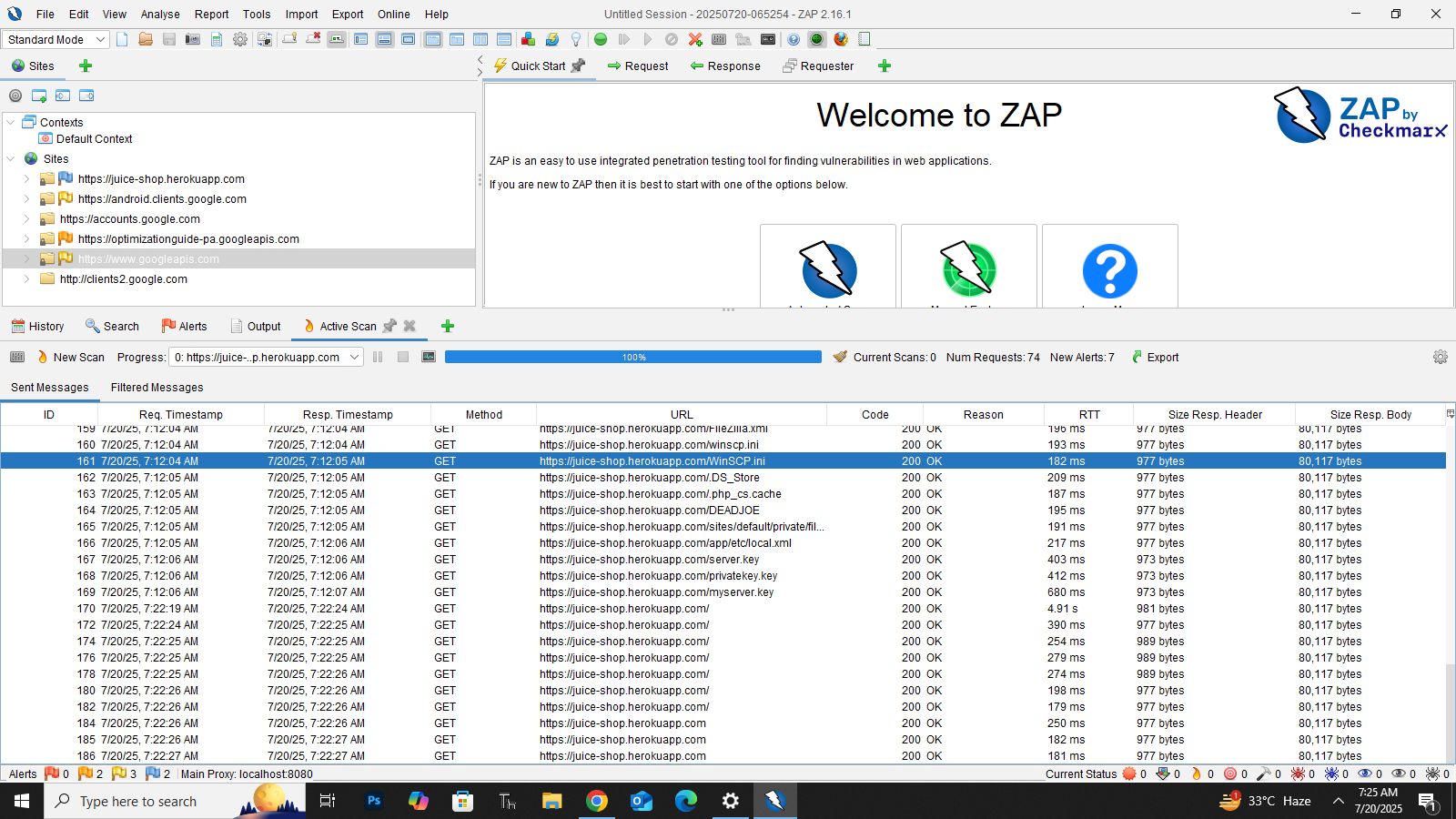
# Vulnerabilities Identified

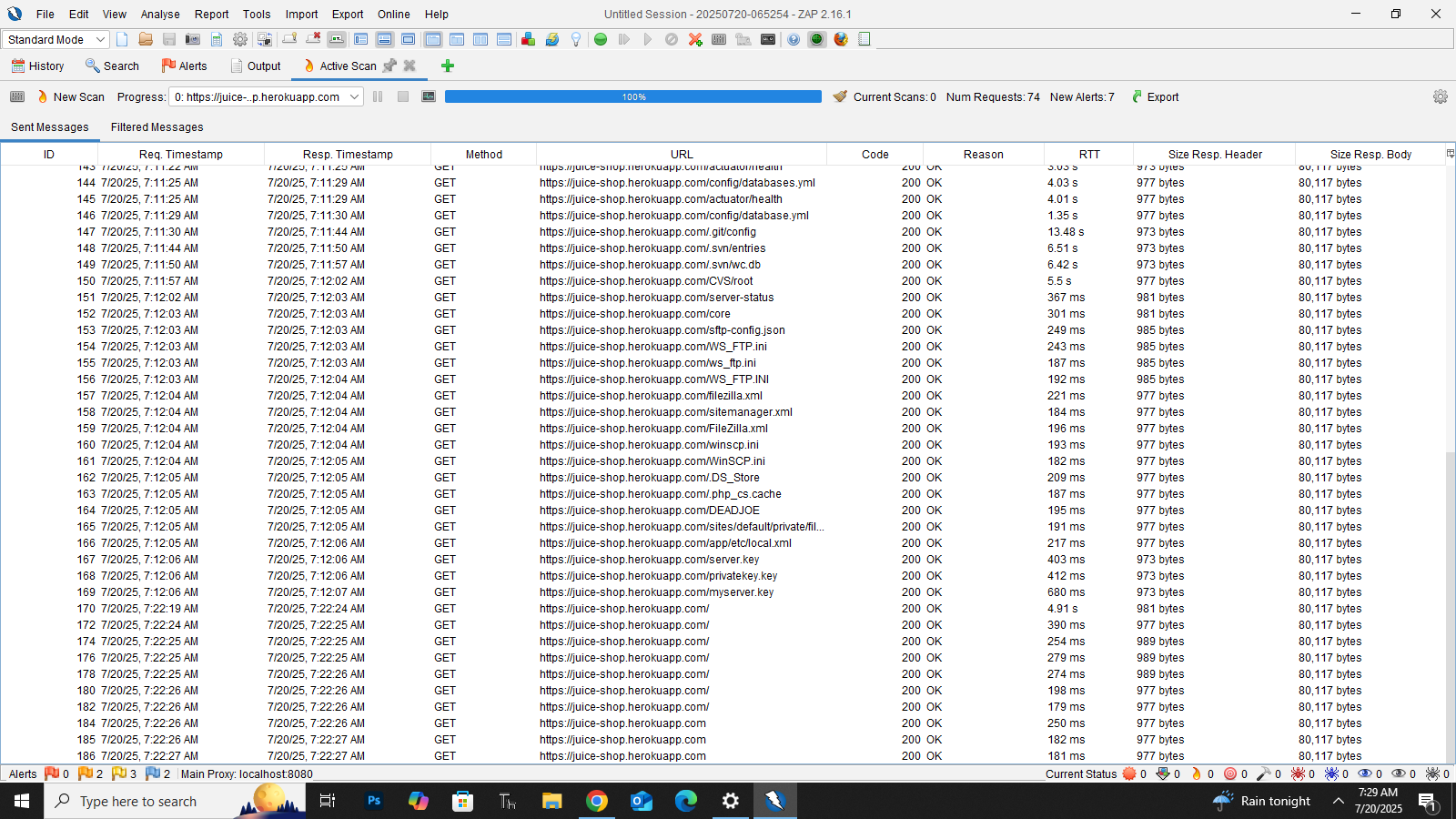
|  |  |  |
| --- | --- | --- |
| Severity | Vulnerability | Description |
| Low | Cookie without Secure Flag | Cookies were not marked Secure, making them vulnerable to MITM attacks. |
| Medium | X-Content-Type-Options Header Missing | May allow MIME sniffing vulnerabilities. |
| Medium | X-Frame-Options Header Missing | Can allow clickjacking via framing by other sites. |

Note: Vulnerabilities may vary by scan — these were most common during my analysis.

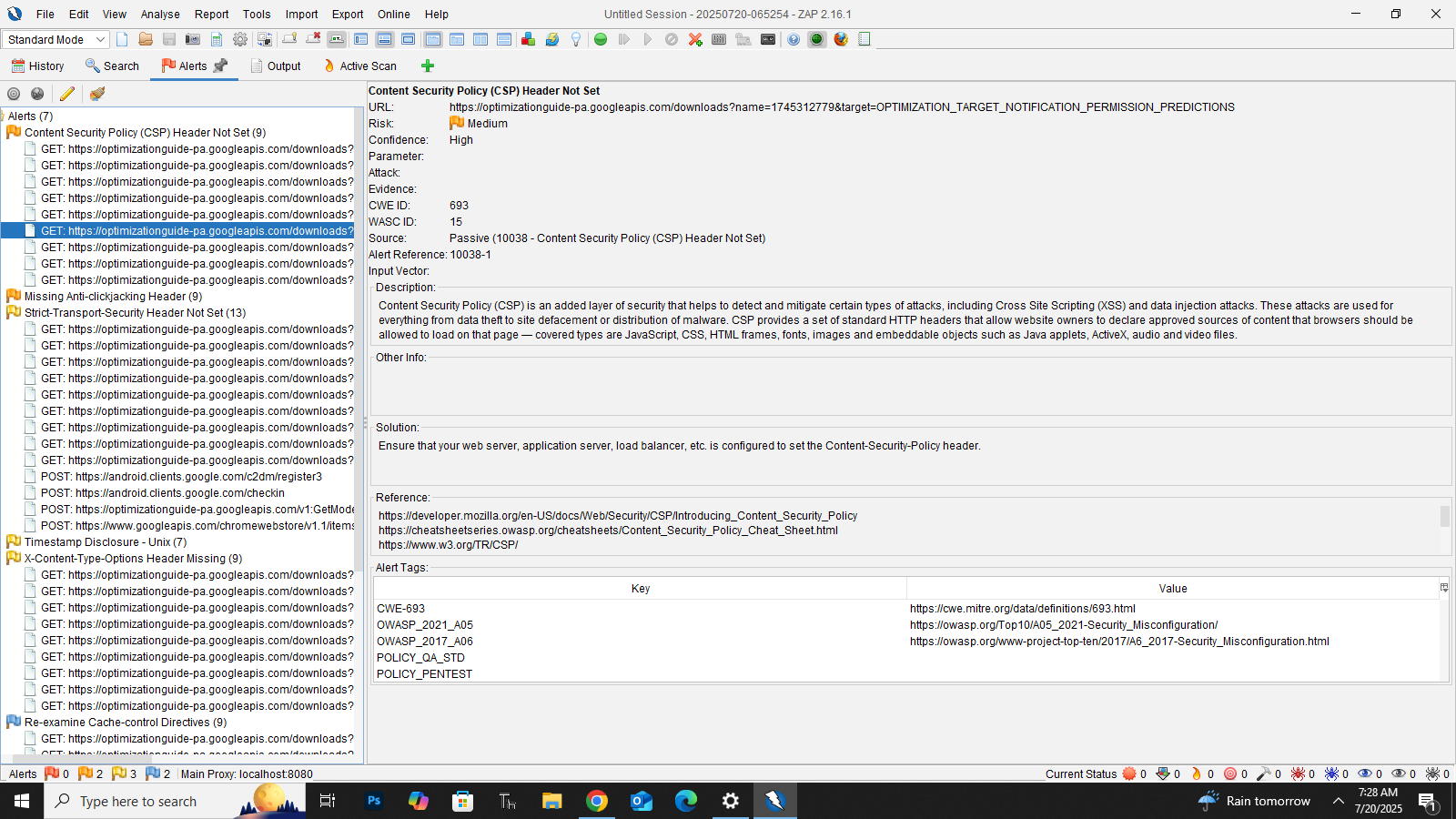
# Screenshots

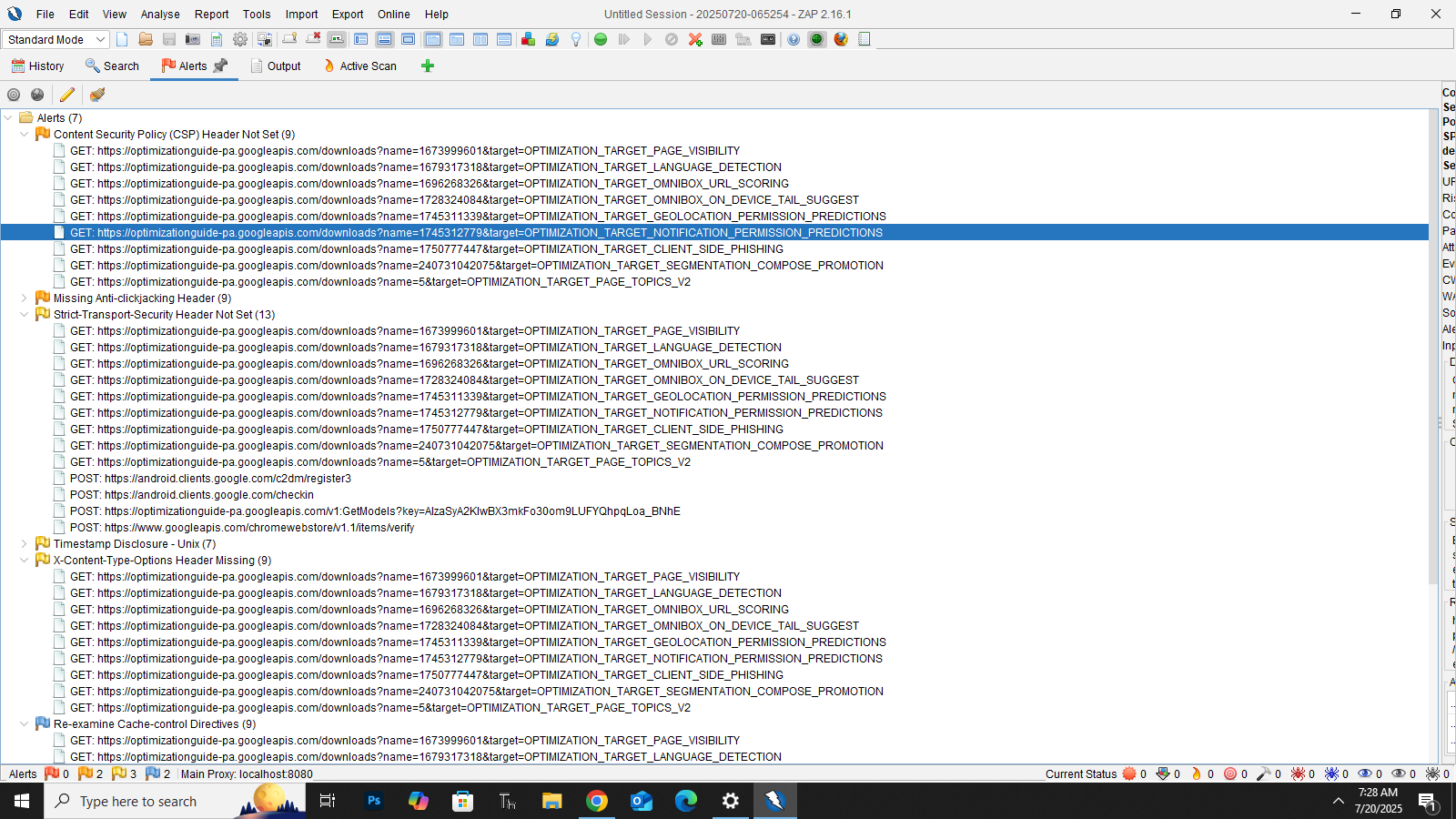
1. zap-scan-progress.png – Active scan in progress



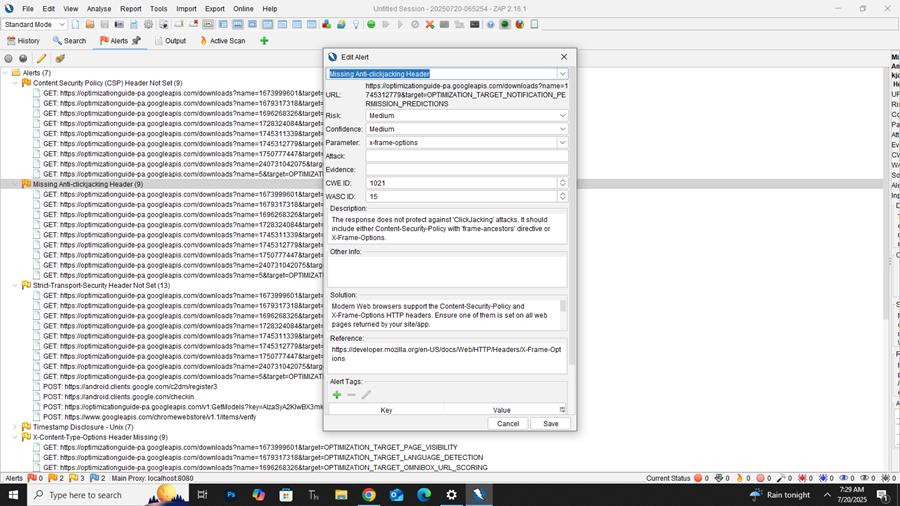


1. zap-alerts.png – Summary of detected vulnerabilities





1. zap-vuln-detail.png – Example detail of one issue



# Conclusion

This task helped me understand the basics of automated vulnerability scanning and interpreting web application security flaws. OWASP ZAP proved to be a beginner-friendly yet powerful tool for real-world assessments.