Vulnerability Assessment using OWASP ZAP

1. Introduction

This report documents the process of conducting a vulnerability assessment on a target website using OWASP ZAP. The assessment includes installation of required tools, execution of an active scan, and analysis of the results.

2. Tools Used

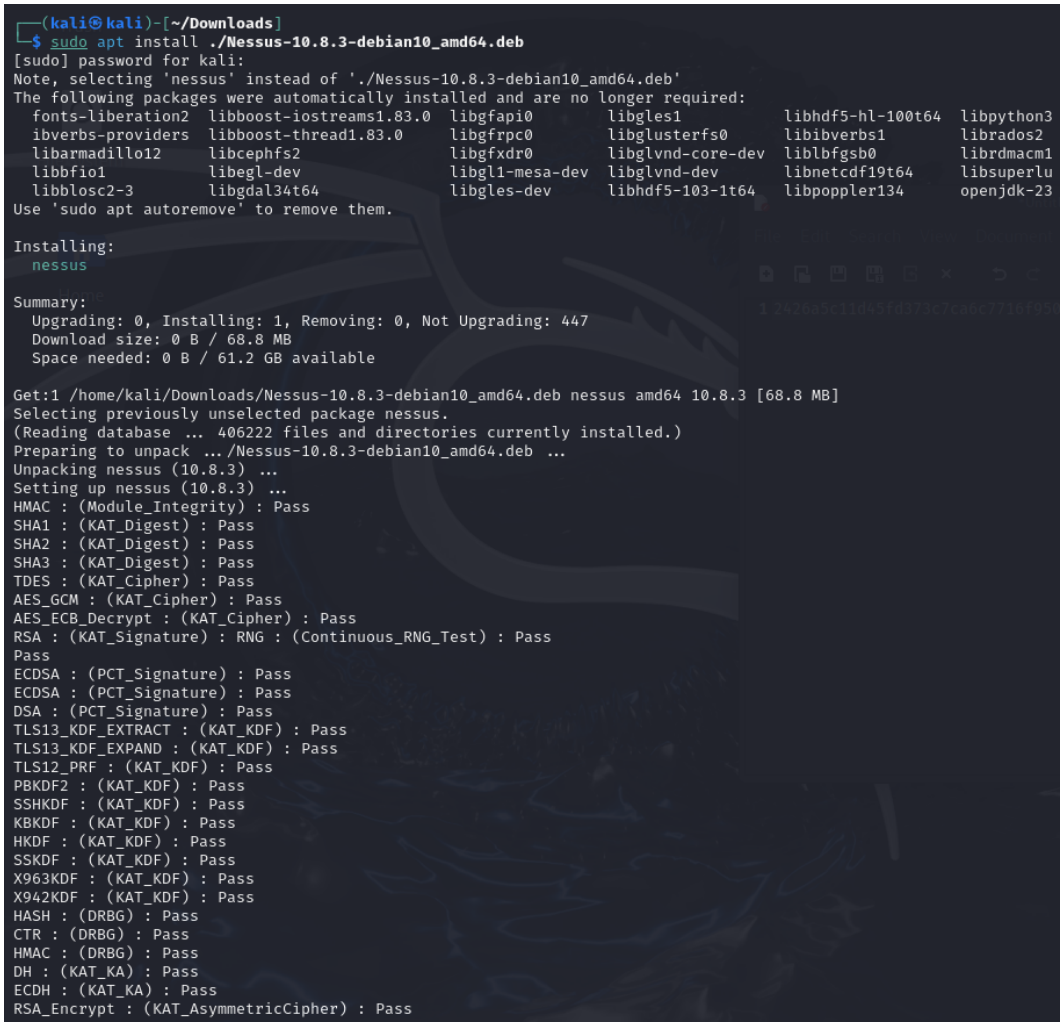
- Nessus – Installed for general vulnerability scanning purposes.

- OWASP ZAP (Zed Attack Proxy) – Used to run a security scan on the target web application.

3. Steps Performed

Step 1: Installed Nessus on a Kali Linux system.

Screenshot of installation:



Step 2: Downloaded and installed OWASP ZAP.

Step 3: Performed an active scan on the target: http://www.itsecgames.com.

4. ZAP Scan Report Summary

Spider Scan:

• Total URLs Found: 62

• New Nodes Added: 43

Active Scan:

• Total Requests Sent: 121

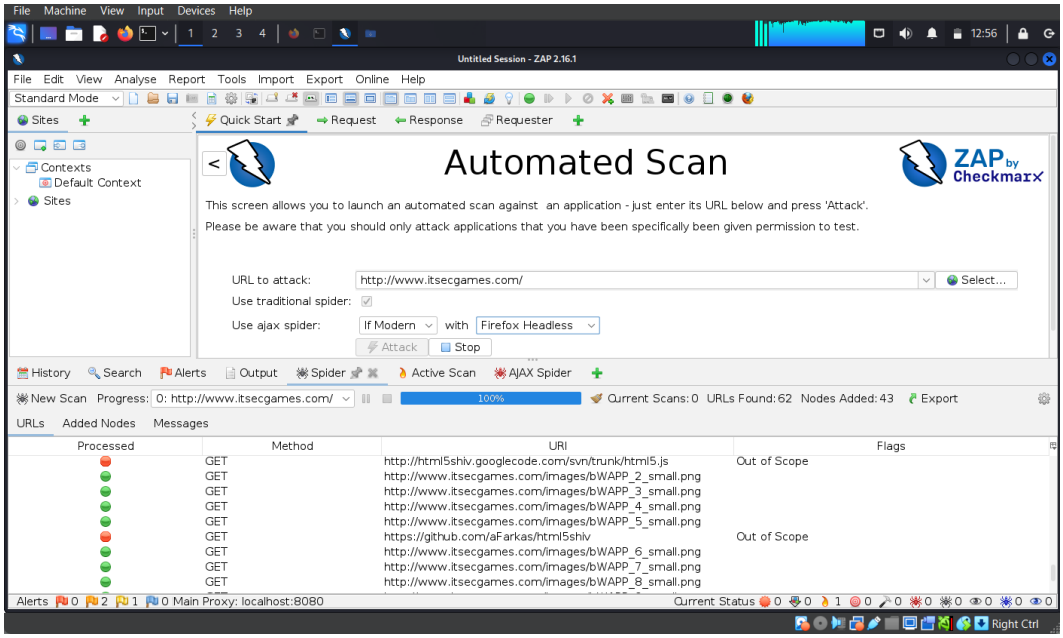
• New Alerts Found: 0

Alerts Summary:

• 1 alert (Risk: Medium, Confidence: High)

• 1 alert (Risk: Medium, Confidence: Medium)

• 1 alert (Risk: Low, Confidence: Medium)



5. Observations & Recommendations

• No critical vulnerabilities were found.
• Manual testing is advised to uncover logic flaws and deeper authentication issues.
• Consider enabling authenticated scans for more comprehensive testing.