PRACTICAL - 4

AIM: Perform a comprehensive scan of a web application, detecting and documenting security vulnerabilities using OWASP ZAP.

Solution:

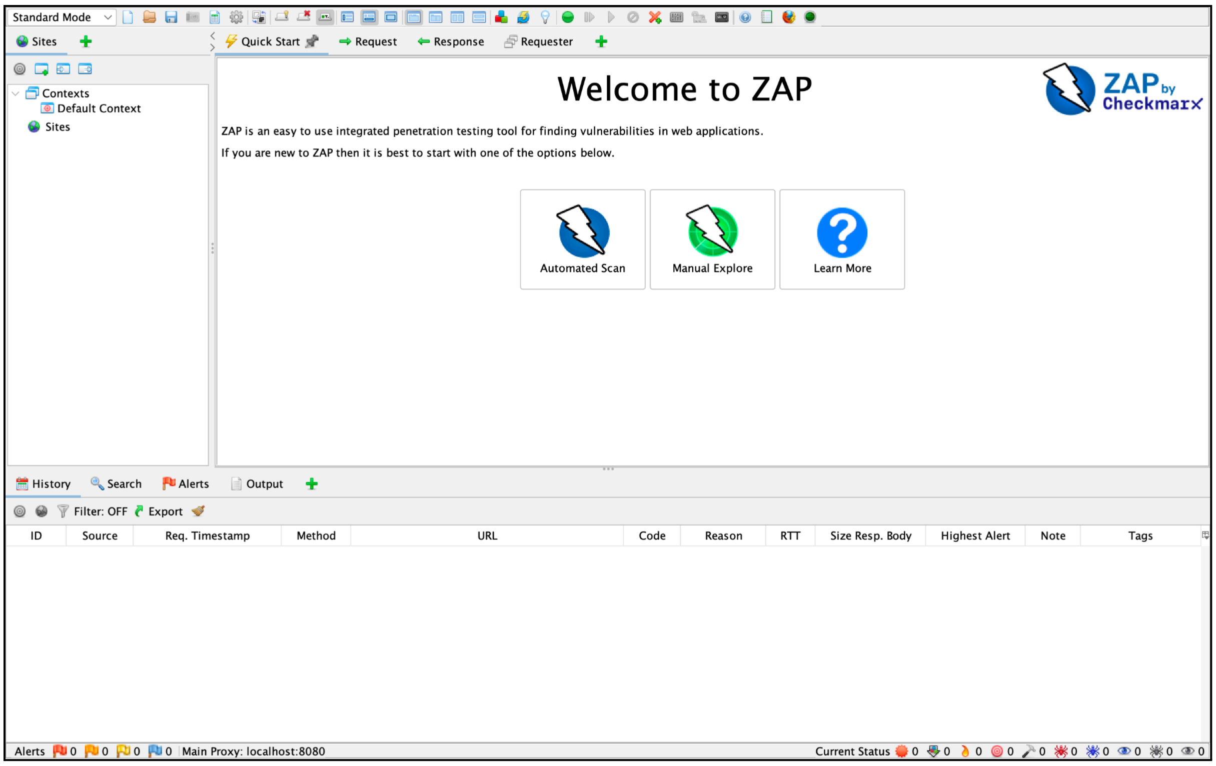
Introduction

OWASP ZAP (Zed Attack Proxy) is a widely used, open-source security tool developed by the **Open Worldwide Application Security Project (OWASP)**. It is specifically designed to help developers and security professionals identify vulnerabilities in web applications through both **automated scanning** and **manual testing**. As one of the most active open-source security projects, ZAP plays a crucial role in detecting a wide range of issues, including those listed in the **OWASP Top 10** such as **Cross-Site Scripting (XSS)**, **SQL Injection** and **Broken Authentication**.

Procedure

Step 1: Install and Launch ZAP

OWASP ZAP was downloaded and installed from the official website. The application was launched in **Standard Mode** for full functionality.

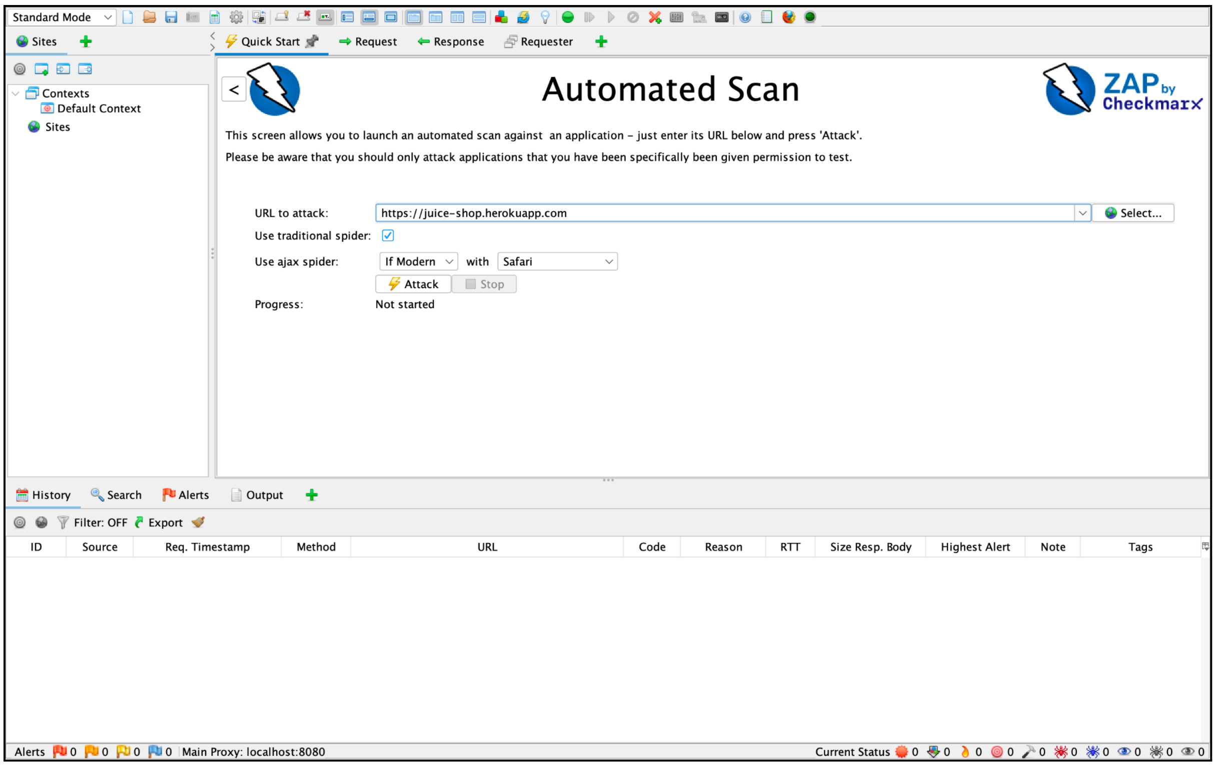


ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

Step 2: Select Target Web Application

The chosen target for testing was **OWASP Juice Shop**, a deliberately insecure application hosted at: " https://juice-shop.herokuapp.com "



Automated Scan

This screen allows you to launch an automated scan against an application – just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.

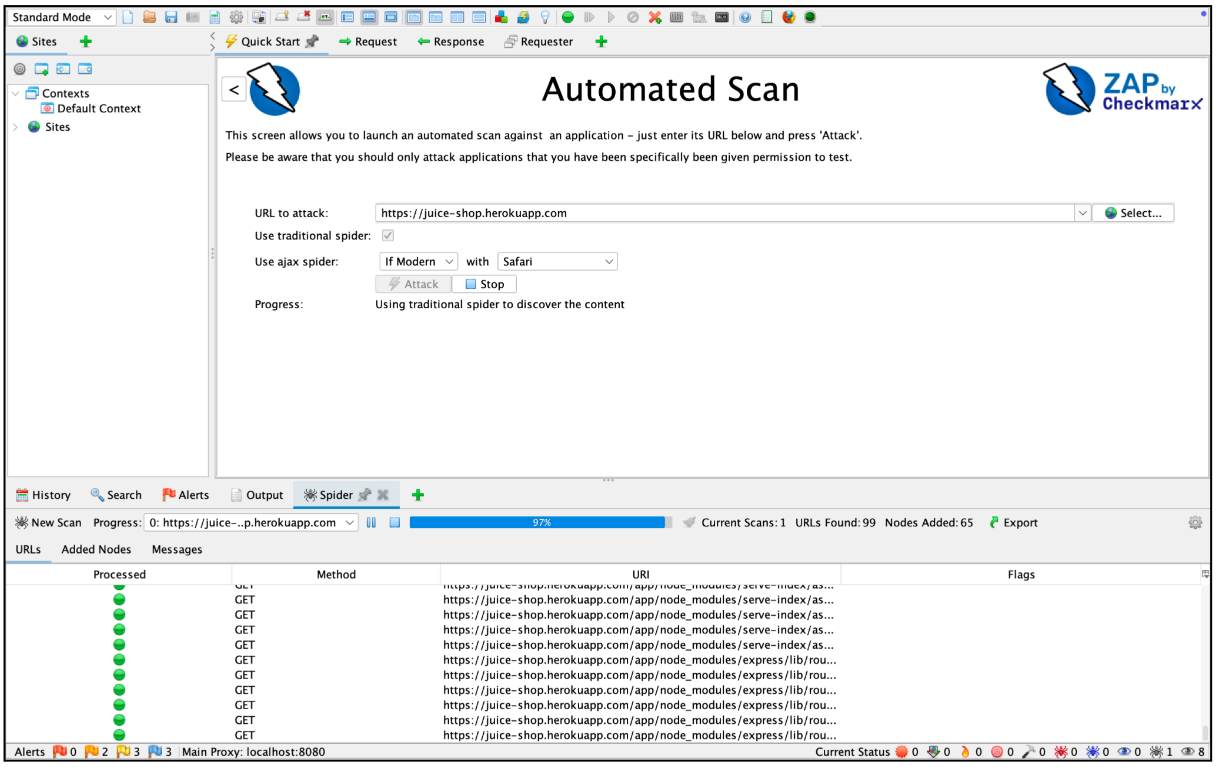
URL to attack: https://juice-shop.herokuapp.com
Use traditional spider: ✓
Use ajax spider: If Modern with Safari
Progress: Not started

ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags

Alerts 0 0 0 0 Main Proxy: localhost:8080 Current Status 0 0 0 0 0 0 0 0 0 0

Step 3: Configure Automated Scan

The **Automated Scan** option was selected from the **Quick Start** menu. The target URL (https://juice-shop.herokuapp.com) was entered and both **Traditional Spider** and **AJAX Spider** options were enabled. The scan was initiated by clicking the **Attack** button and its progress was monitored through the ZAP interface.



Automated Scan

This screen allows you to launch an automated scan against an application – just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: https://juice-shop.herokuapp.com
Use traditional spider: ✓
Use ajax spider: If Modern with Safari
Progress: Using traditional spider to discover the content

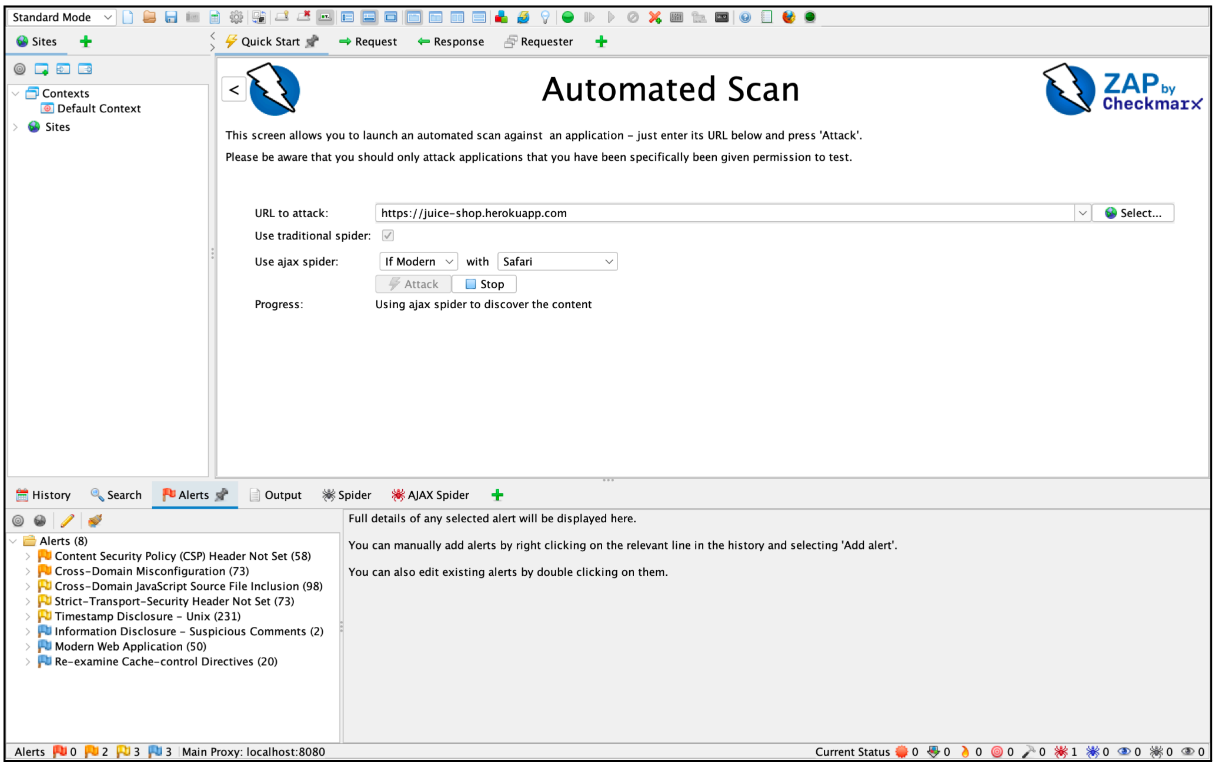
New Scan Progress: 0: https://juice-..p.herokuapp.com 97% Current Scans: 1 URLs Found: 99 Nodes Added: 65 Export

Processed	Method	URI	Flags
●	GET	https://juice-shop.herokuapp.com/app/node_modules/serve-index/as...	
●	GET	https://juice-shop.herokuapp.com/app/node_modules/serve-index/as...	
●	GET	https://juice-shop.herokuapp.com/app/node_modules/serve-index/as...	
●	GET	https://juice-shop.herokuapp.com/app/node_modules/serve-index/as...	
●	GET	https://juice-shop.herokuapp.com/app/node_modules/serve-index/as...	
●	GET	https://juice-shop.herokuapp.com/app/node_modules/express/lib/rou...	
●	GET	https://juice-shop.herokuapp.com/app/node_modules/express/lib/rou...	
●	GET	https://juice-shop.herokuapp.com/app/node_modules/express/lib/rou...	
●	GET	https://juice-shop.herokuapp.com/app/node_modules/express/lib/rou...	
●	GET	https://juice-shop.herokuapp.com/app/node_modules/express/lib/rou...	
●	GET	https://juice-shop.herokuapp.com/app/node_modules/express/lib/rou...	

Alerts 0 2 3 3 Main Proxy: localhost:8080 Current Status 0 0 0 0 0 0 0 0 1 8

Step 4: Analyze Alerts

After scanning, OWASP ZAP provided a **list of vulnerabilities**. Each alert included the name, risk level, affected element, evidence and suggested mitigation.



This screen allows you to launch an automated scan against an application – just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: https://juice-shop.herokuapp.com
Use traditional spider: ✓
Use ajax spider: If Modern with Safari
Attack Stop
Progress: Using ajax spider to discover the content

Alerts (8)
- Content Security Policy (CSP) Header Not Set (58)
- Cross-Domain Misconfiguration (73)
- Cross-Domain JavaScript Source File Inclusion (98)
- Strict-Transport-Security Header Not Set (73)
- Timestamp Disclosure - Unix (231)
- Information Disclosure - Suspicious Comments (2)
- Modern Web Application (50)
- Re-examine Cache-control Directives (20)

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

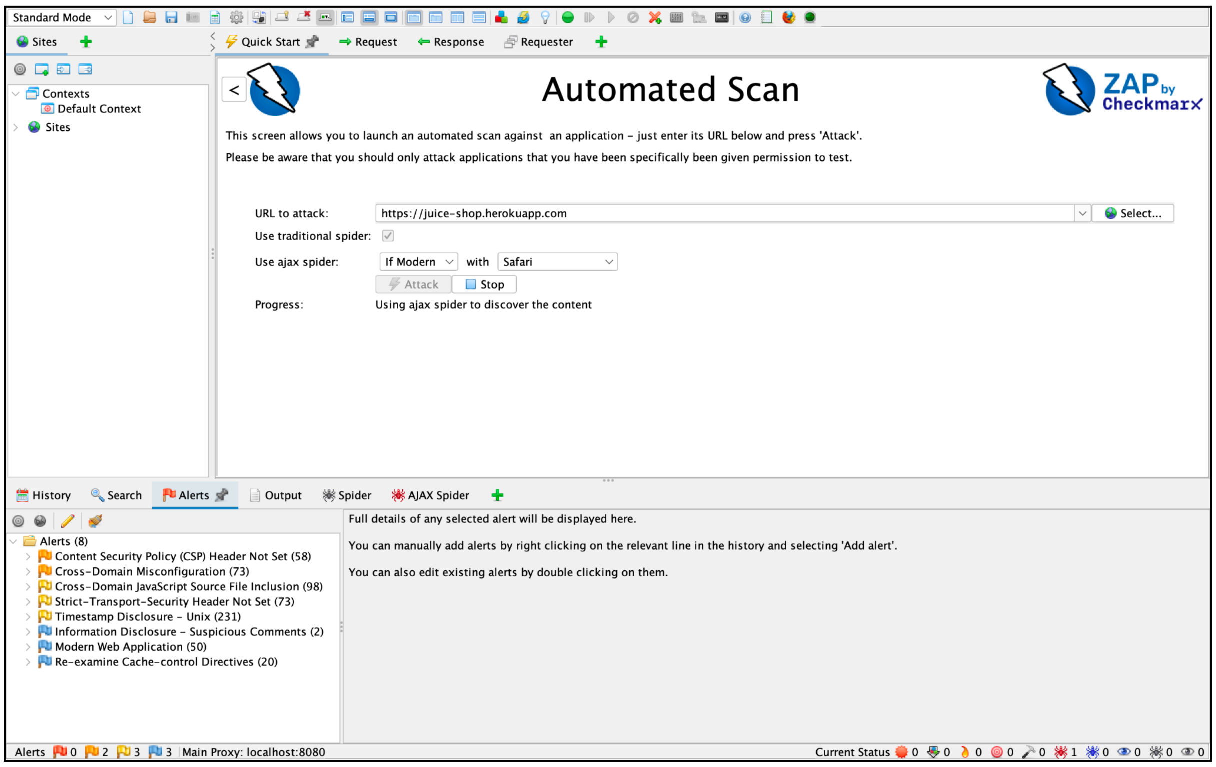
You can also edit existing alerts by double clicking on them.

Alerts 0 2 3 3 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 1 0 0 0 0

Vulnerabilities Identified

Vulnerability	Risk	Description	Affected Element	Suggested Mitigation
Cross-Domain JavaScript Source File Inclusion	Medium	Application loads JavaScript from third-party domains	External JS script	Load scripts from trusted, secure domains only
Strict-Transport-Security Header Not Set	Medium	Lack of HSTS header leaves the site open to downgrade and MITM attacks	HTTP response headers	Add Strict-Transport-Security header
Content Security Policy Header Not Set	Medium	CSP header missing, allowing untrusted script execution	HTTP response headers	Implement Content Security Policy to restrict resources

Cross-Domain Misconfiguration	Medium	Access-Control-Allow-Origin is set to wildcard	Response header	Restrict CORS access to trusted origins
Timestamp Disclosure – Unix	Low	Server reveals last-modified timestamps in response	Multiple endpoints	Avoid exposing detailed timestamps in responses



Automated Scan

This screen allows you to launch an automated scan against an application – just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: https://juice-shop.herokuapp.com
Use traditional spider: ✓
Use ajax spider: If Modern with Safari
Attack Stop
Progress: Using ajax spider to discover the content

Alerts (8)
Content Security Policy (CSP) Header Not Set (58)
Cross-Domain Misconfiguration (73)
Cross-Domain JavaScript Source File Inclusion (98)
Strict-Transport-Security Header Not Set (73)
Timestamp Disclosure - Unix (231)
Information Disclosure - Suspicious Comments (2)
Modern Web Application (50)
Re-examine Cache-control Directives (20)

Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.

Alerts 0 2 3 3 Main Proxy: localhost:8080 Current Status 0 0 0 0 0 1 0 0 0 0

Mitigation Recommendations

To improve security posture and fix the above vulnerabilities, the following general mitigations are recommended:

- Implement secure HTTP headers: HSTS, CSP, X-Content-Type-Options, etc.
- Avoid loading untrusted third-party scripts
- Configure CORS policy properly
- Use input validation and sanitization
- Regularly audit dependencies and JavaScript libraries
- Avoid exposing unnecessary server information or metadata