ZAP DAST Tool

AUBURN UNIVERSITY

CPSC 4970 Applied Cyber Security

ZAP Overview

AUBURN

- An easy to use Web Application DAST testing tool.
- Completely free and open source
- Supported by OWASP organization
- Ideal for beginners, but also used by professionals
- Developers can use desktop version for local testing
- Update with new capabilities for advanced testing and new vulnerabilities
- Cross platform
- Internationalized - 20+ languages
- Fully documented
- Work well with other tools and automation frameworks
- Embeds other well regarded security tools
  - JBroFuzz, fuzzdb, DirBuster, CrawlJax

Main Features

AUBURN

- Intercepting Proxy
  - Embedded server that intercepts the connection between an browser and server without modifying requests and responses.
- Active and Passive Scanners
- Spider - automatically discover new resources (URLs) on a particular Site
- Ajax Spiders - Allows you to spider sites that make heavy use of JavaScript false
- WebSockets support - intercepts and shows websocket messages
- Forced Browsing - try to discover files and directories on a web server
- Fuzzing (using fuzzdb & OWASP JBroFuzz)
- Online Add-ons Marketplace

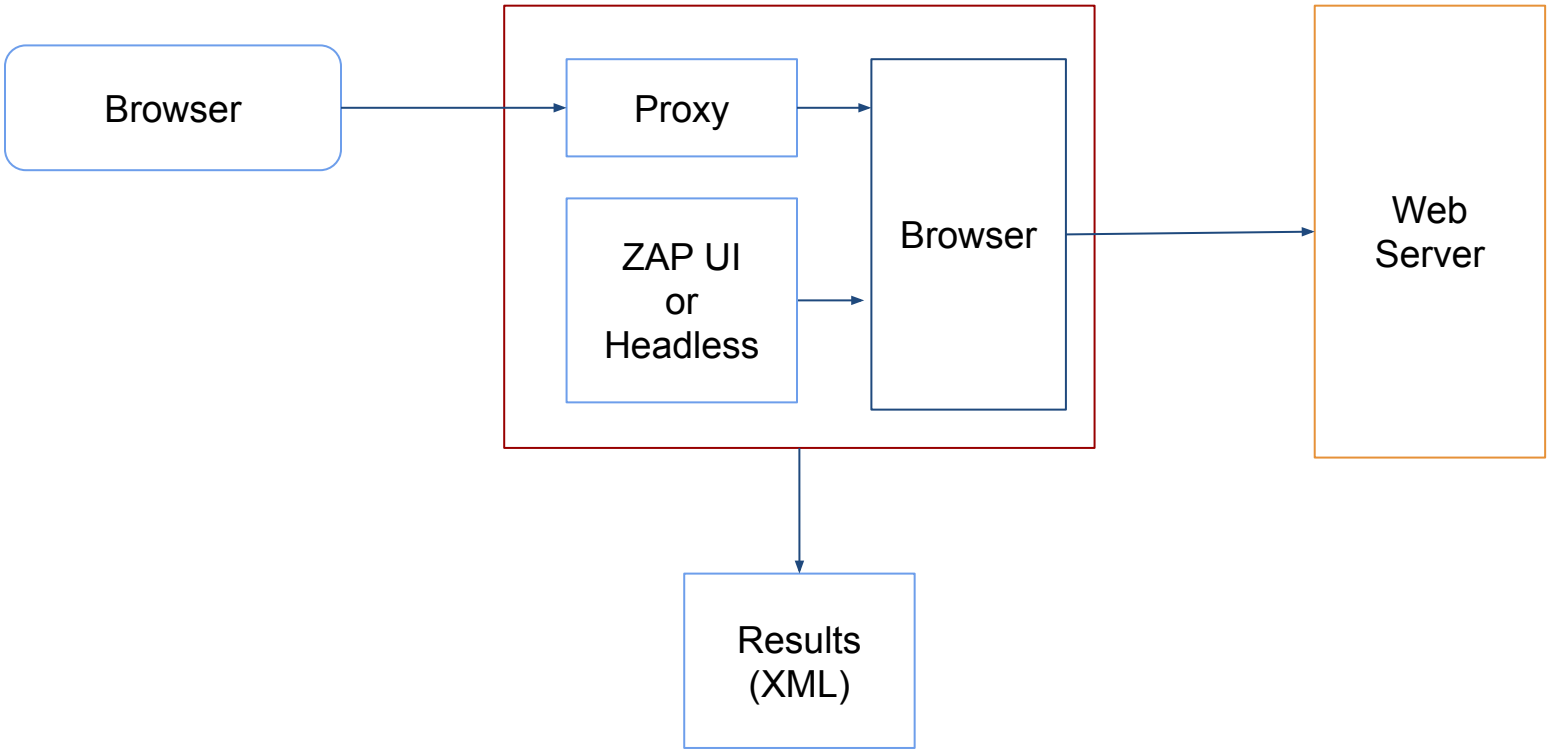
Main Features

AUBURN

- Auto tagging - tag requests based on regular expressions
- Port scanner - discovers open ports on web site servers
- Session management - handles several methods of sessions ids
- Invoke external apps to integrate with other tools.
- API + Headless mode to integrate into automation tools
- Dynamic SSL Certificates to encrypt/decrypt requests and responses (man in the middle)
- Anti CSRF token handling support

How ZAP Works

AUBURN



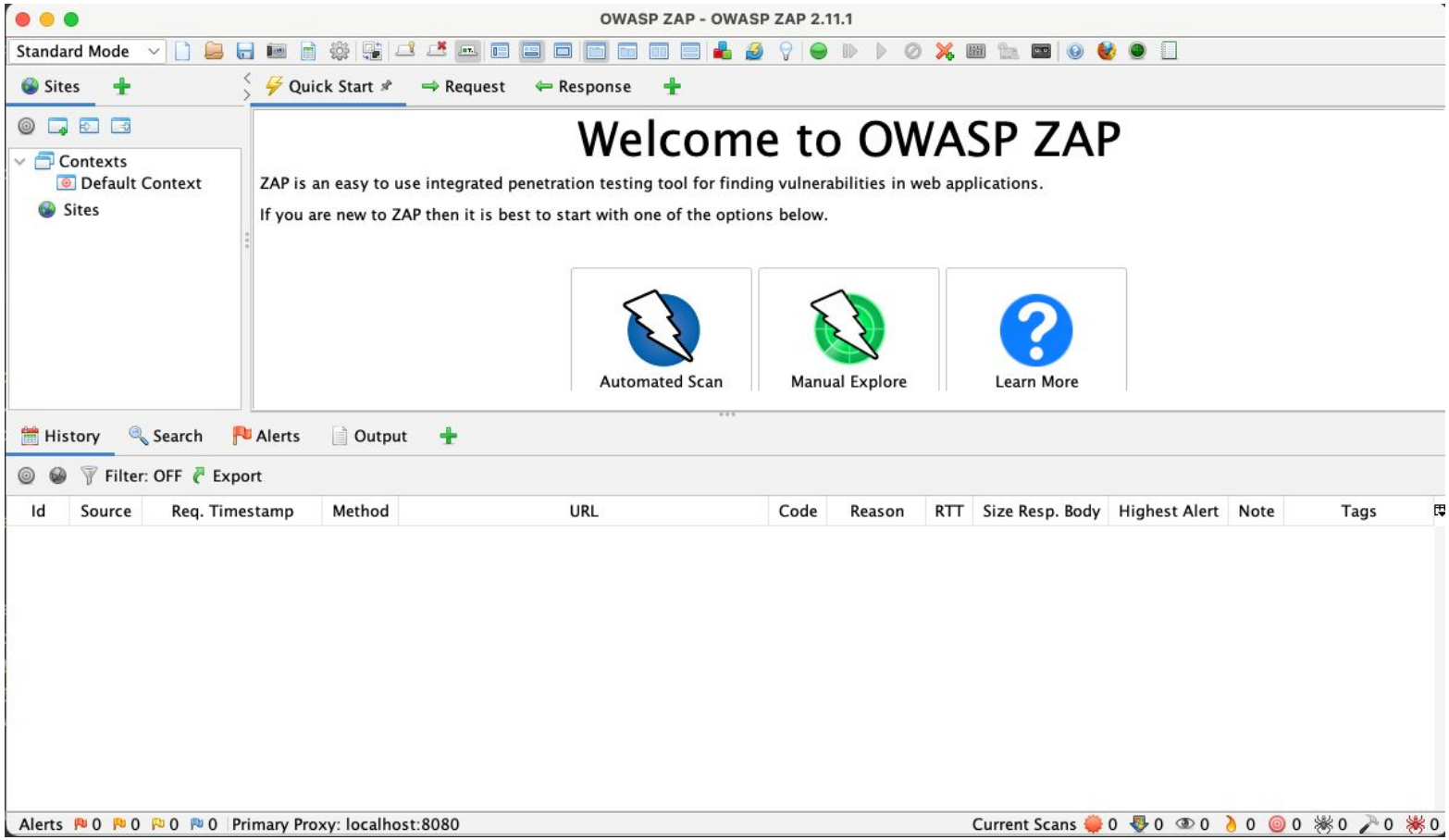
ZAP Terminology

AUBURN

- **Session** - Records configuration and activities performed in ZAP
  - Headless browser to use, context configuration
  - Enables saving a session so it used later.
- **Context** - Configuration of an attach
  - Specific technologies and components in use
  - Authentication to use when trying to login
  - Specific URLs to use or avoid.
- **Attacks** - several types can be configured
  - Passive
  - Active - attempts to find vulnerabilities
  - Quick - similar to Active, but less variability in attack.
- **Spider** - Automatically discover new resources/URLs on your website. It visits those URLs, identifies the hyperlinks and adds them to the list.'
- **Alerts** - Results of attacks performed by Spider/Active Scan (or any other attack). Alerts are the potential vulnerabilities which are flagged as High, Medium, or Low according to the risk level.

Demonstration

AUBURN



AUBURN UNIVERSITY