OWASP
Open Web Application
Security Project

Zed Attack Proxy (ZAP)

Daniel W – OWASP Chapter Lead

About me

- OWASP Dorset Chapter Lead
- Over a decade in Information Security
  - Likes to solve root cause through Security Architecture
- Any further questions over pizza and beer

The talk

- ZAP
  - What is it?
  - History
  - Meet the ancestor
  - How does it work
  - Where to get ZAP
  - How you can use it
  - Who uses it
  - Where to go next

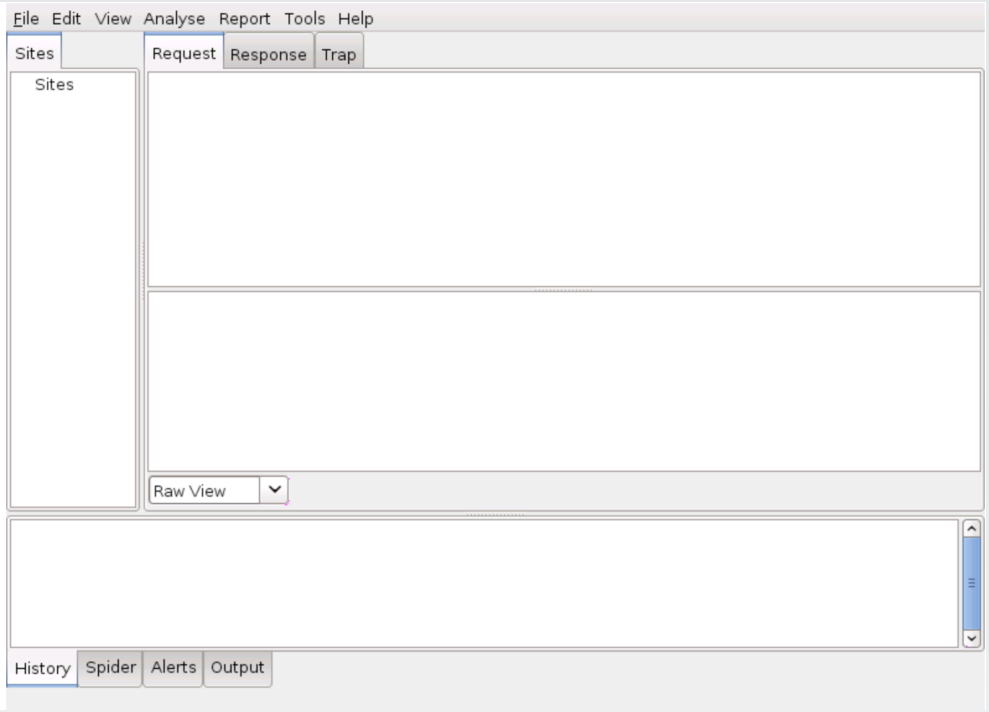
What is it?

The world's most popular free web security tool, actively maintained by a dedicated international team of volunteers.

History

- Simon Bennetts
- Find obvious vulnerabilities automatically
- Get other developers using security tools
- OWASP Flagship Project
- Supported internationally

Meet the ancestor



- Paros Proxy

Latest release Aug. 8, 2006
(13 years, 5 months ago)

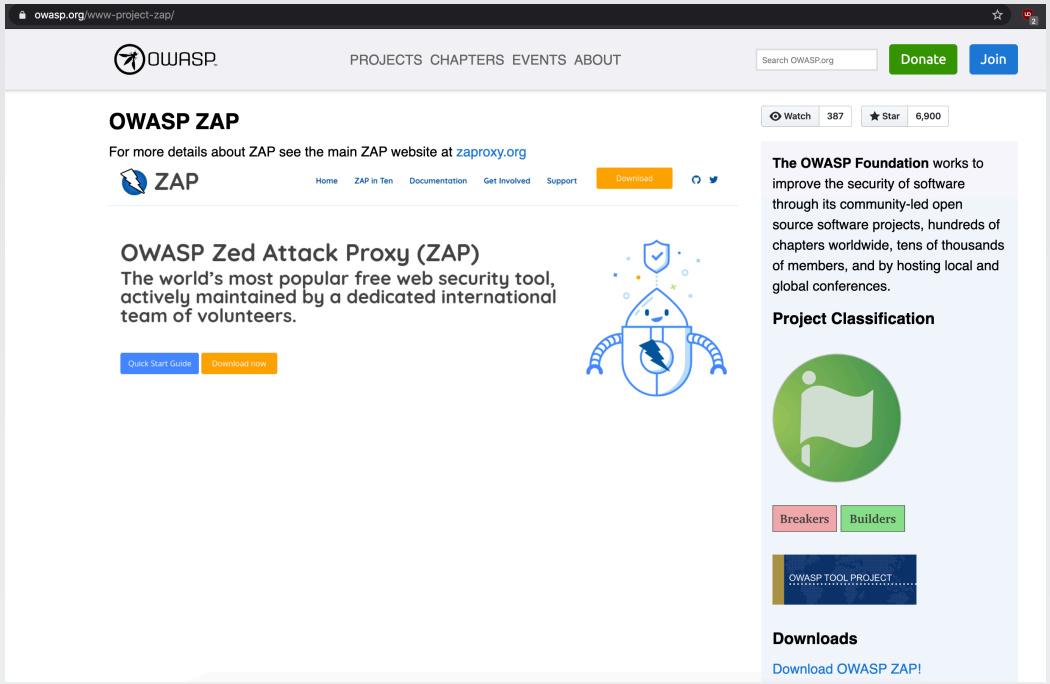
- Zap started life as a fork of the paros proxy.

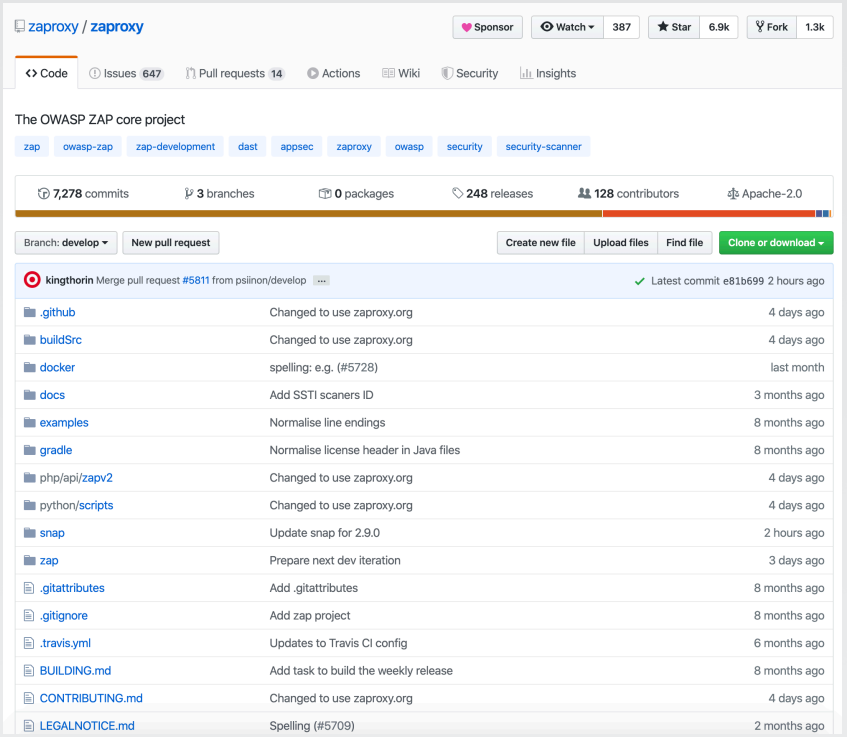
How does it work?

In essence - a fancy proxy with some lovely extras.

- Intercepting Proxy
- Active and Passive Scanners
- Traditional and Ajax Spiders
- Brute Force Scanner
- Port Scanner
- Web Sockets

Where to get ZAP



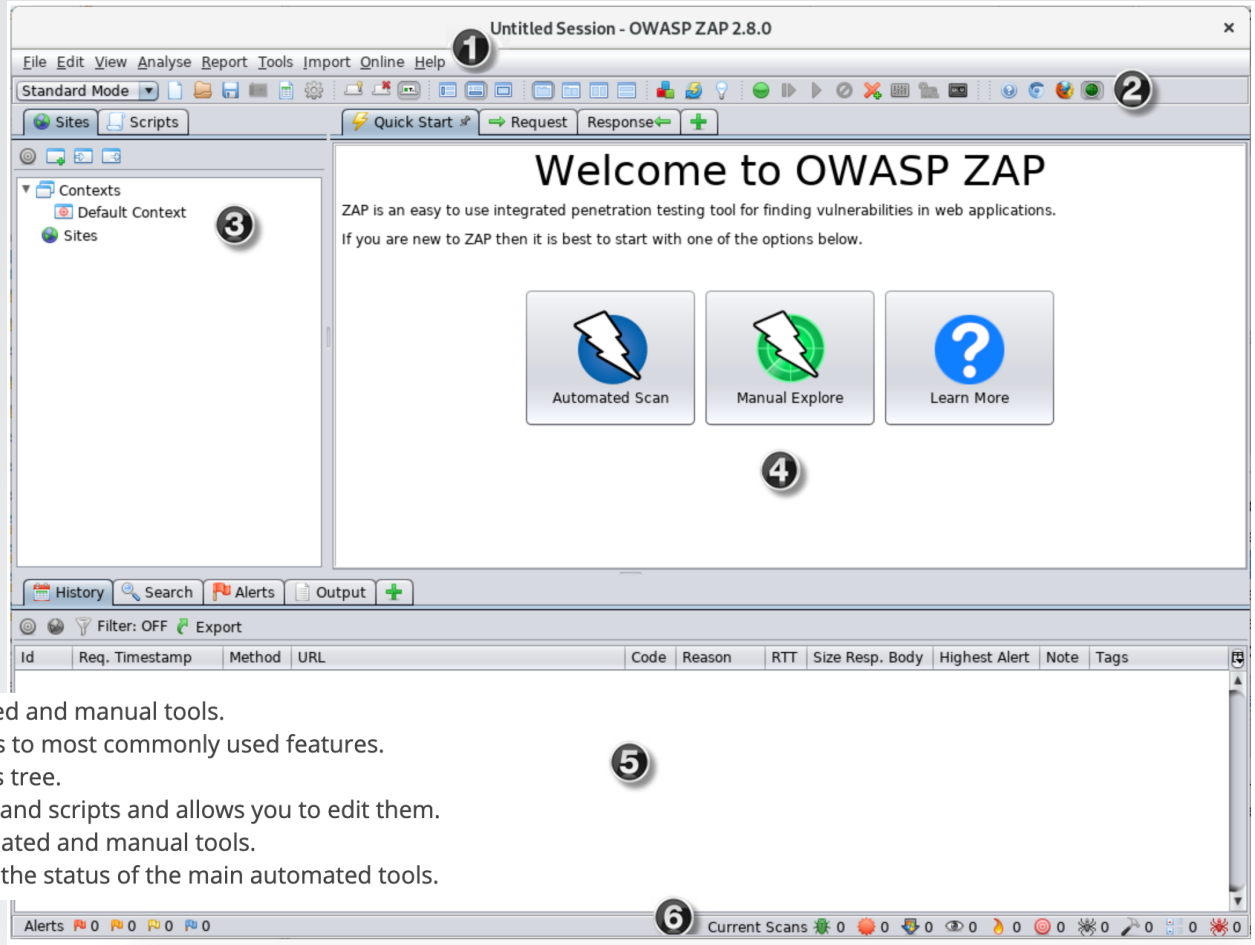


https://www.zaproxy.org/
https://owasp.org/www-project-zap/
https://github.com/zaproxy/zaproxy

How you can use it

- Three interfaces
  - Desktop
  - API
  - Heads Up Display (HUD - new)
- Automation ready (API or docker)

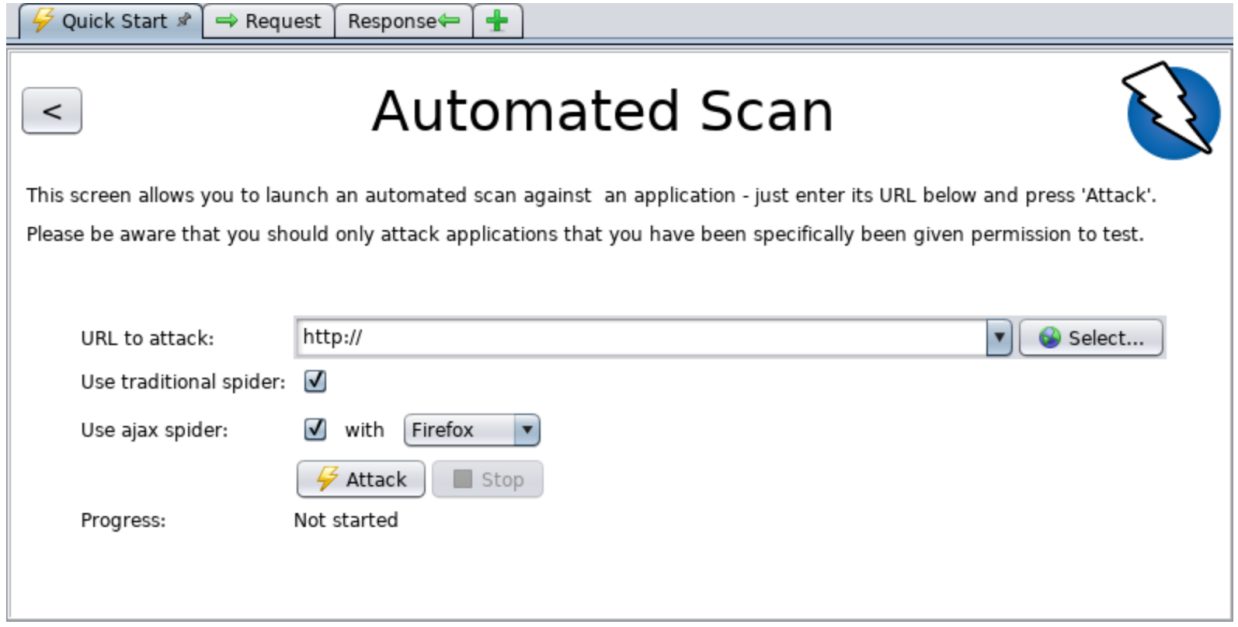
Desktop



1. **Menu Bar** – Provides access to many of the automated and manual tools.
2. **Toolbar** – Includes buttons which provide easy access to most commonly used features.
3. **Tree Window** – Displays the Sites tree and the Scripts tree.
4. **Workspace Window** – Displays requests, responses, and scripts and allows you to edit them.
5. **Information Window** – Displays details of the automated and manual tools.
6. **Footer** – Displays a summary of the alerts found and the status of the main automated tools.

Automated scans

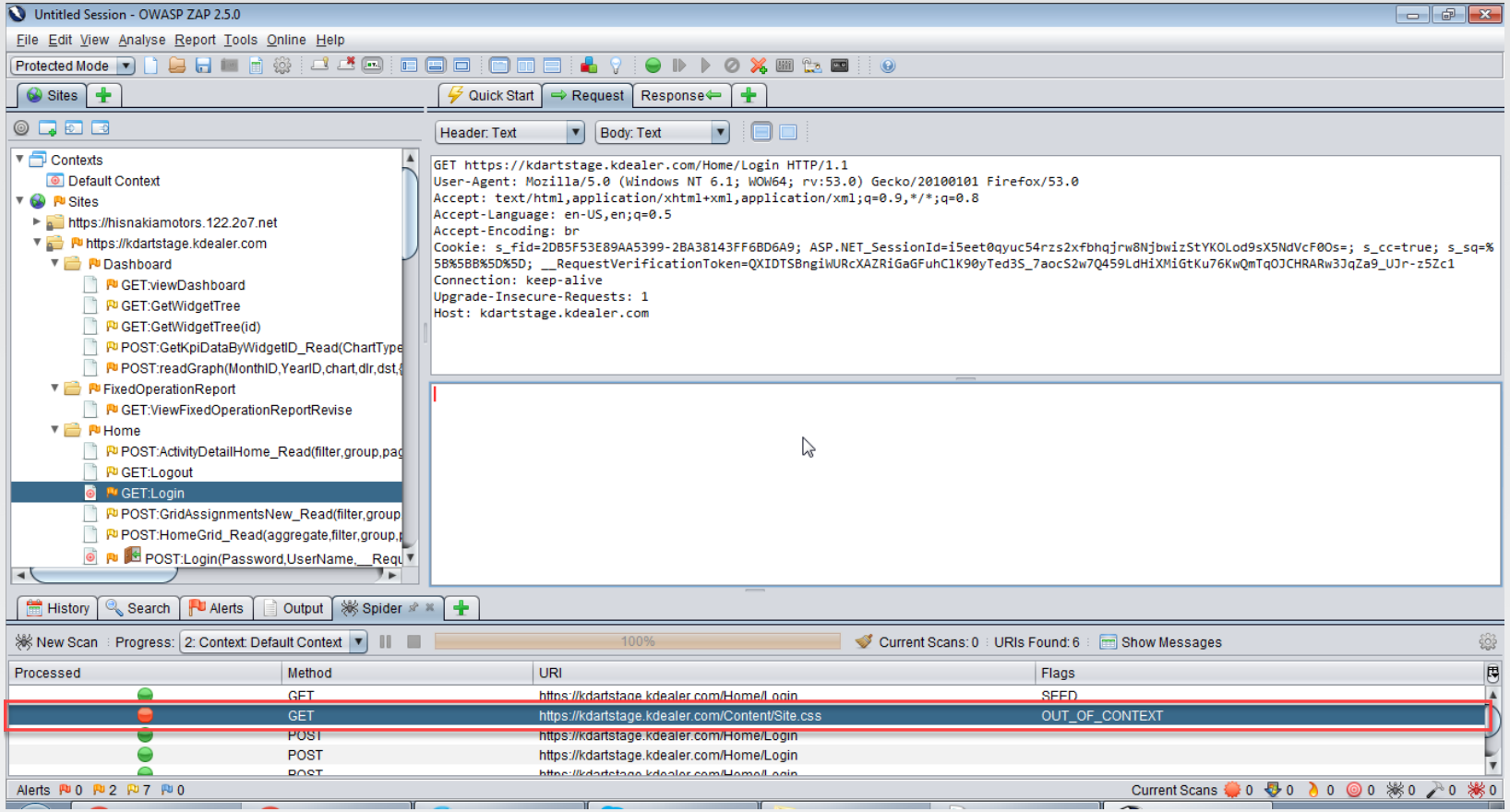
1. Start ZAP and click the **Quick Start** tab of the Workspace Window.
2. Click the large Automated Scan button.
3. In the **URL to attack** text box, enter the full URL of the web application you want to attack.
4. Click the **Attack**



ZAP will proceed to crawl the web application with its spider and passively scan each page it finds. Then ZAP will use the active scanner to attack all of the discovered pages, functionality, and parameters.

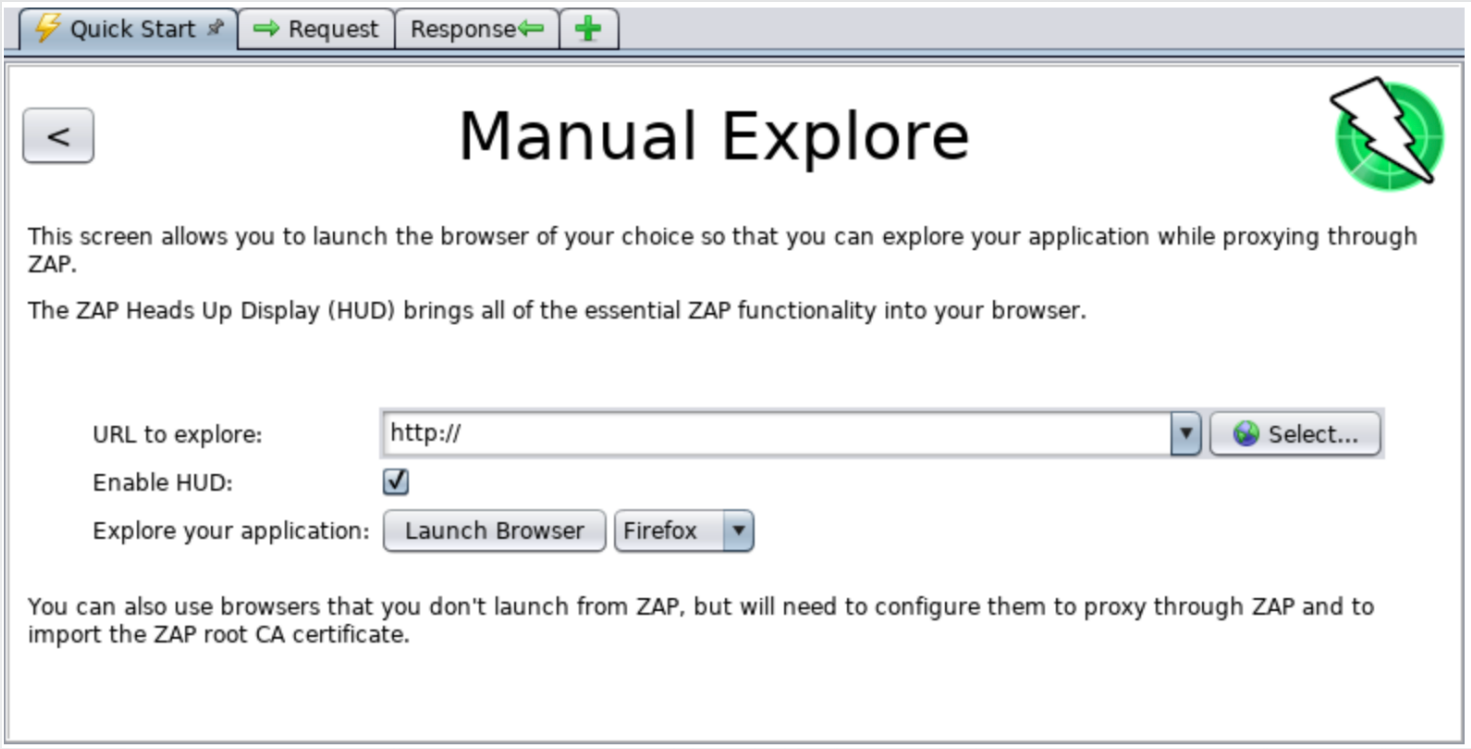
Alerts

- High
- Medium
- Low
- Informational
- False Positive

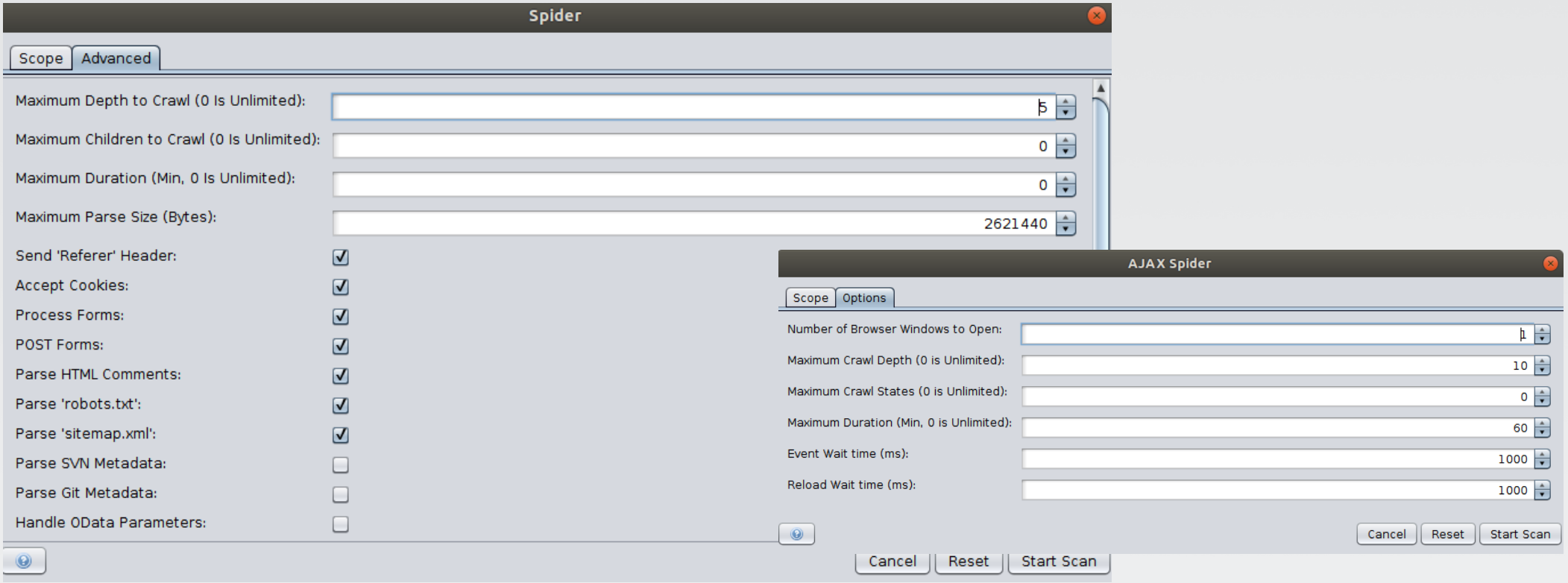


Manual Exploration

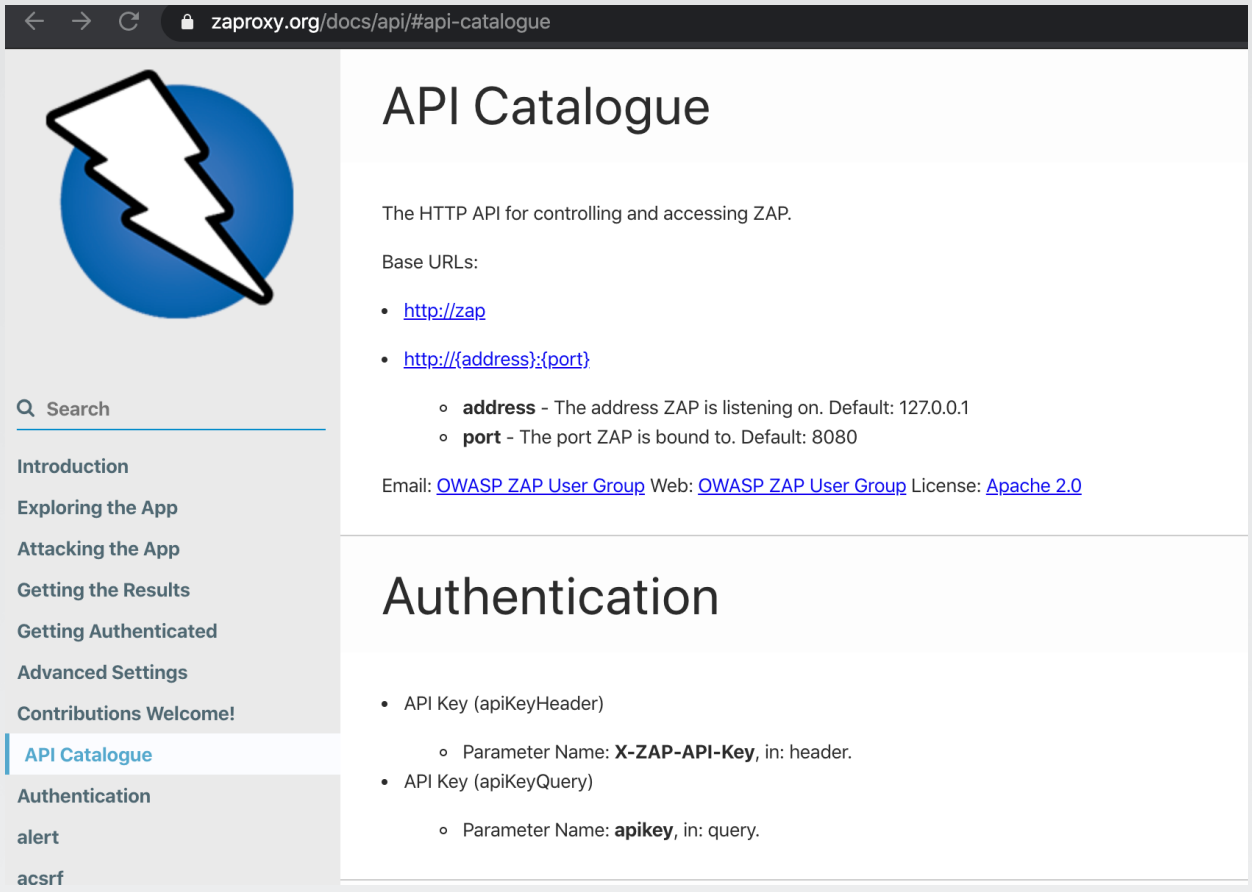
1. Start ZAP and click the **Quick Start** tab of the Workspace Window.
2. Click the large Manual Explore button.
3. In the **URL to explore** text box, enter the full URL of the web application you want to explore.
4. Select the browser you would like to use
5. Click the **Launch Browser**



Spiders are powerful



API



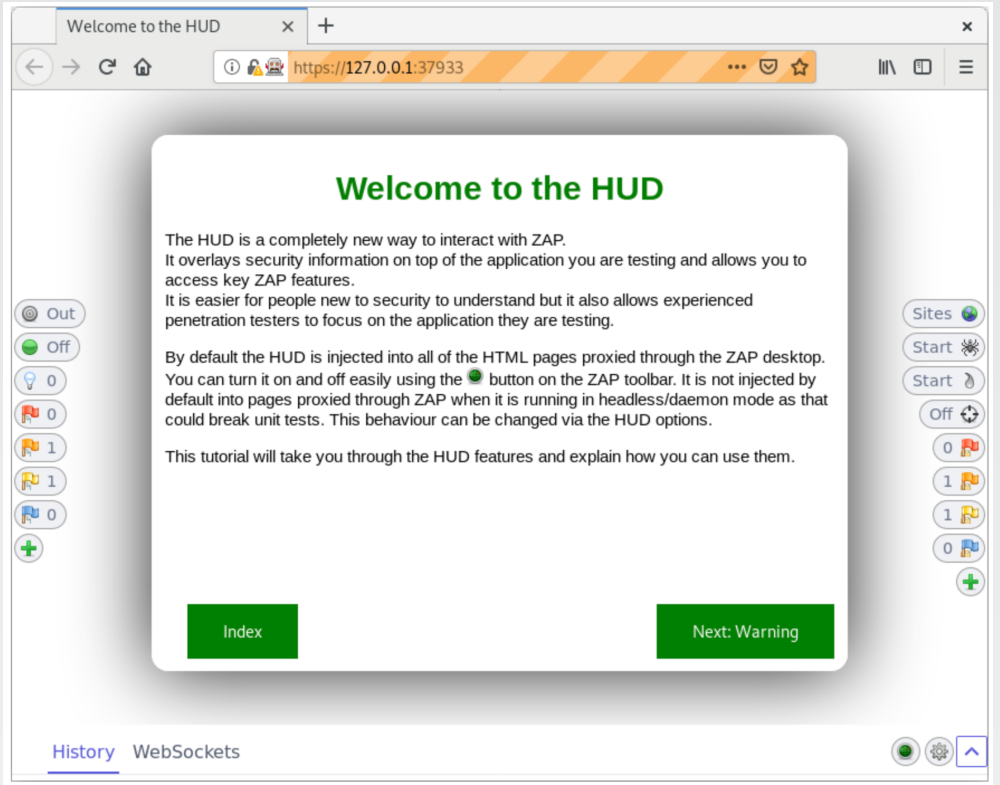
https://www.zaproxy.org/docs/api/#api-catalogue

Heads Up Display (cool)

The Heads Up Display (HUD) is a new an innovative interface that provides access to ZAP functionality directly in the browser.

The HUD is overlayed on top of the target application in your browser when enabled via the ‘Manual Explore’ screen or toolbar option.

Only modern browsers such as Firefox and Chrome are supported.



Reports (HTML, JSON or XML)

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	6
Informational	0

Alert Detail

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://public-firing-range.appspot.com/address/location/documentwrite
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/cors/alloworigin/dynamicAllowOrigin
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/angular/angular_body_alt_symbols_raw/1.6.0?q=test
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/address/baseURI/documentwrite
Method	GET
Parameter	X-Frame-Options

Where to go next

- Search for OWASP ZAP
- Download ZAP and Java
- Try some passive scans
- Try active scan (with permission only)
- Try automation
- Twitter @zaproxy
- https://www.zaproxy.org/
- https://owasp.org/www-project-zap/
- https://github.com/zaproxy/zaproxy

Questions (if time allows)