



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?

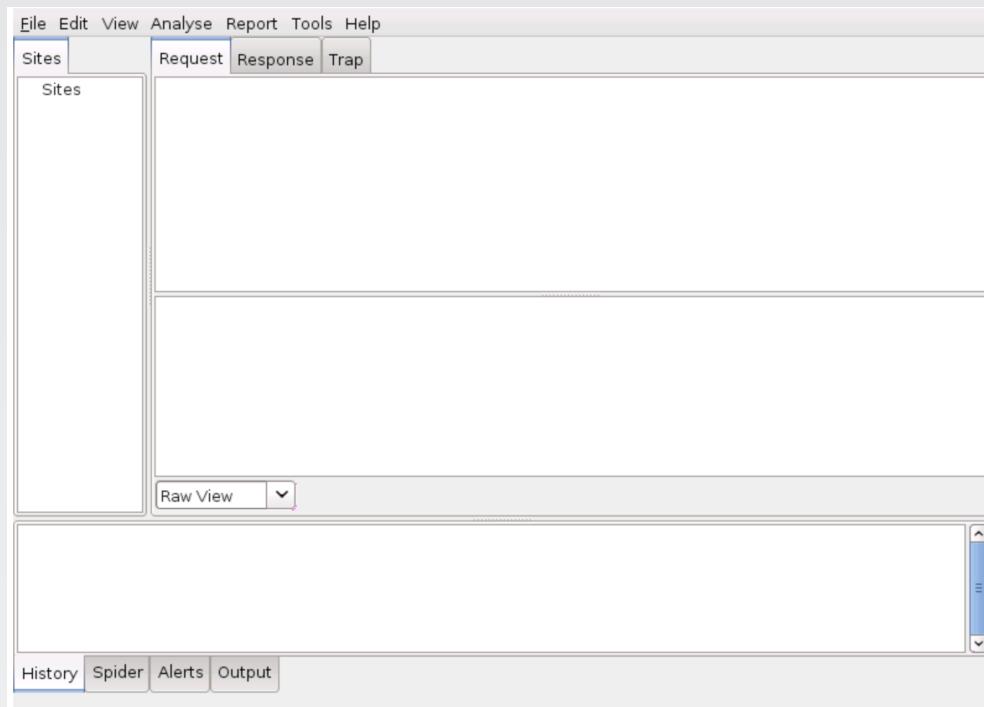


The world's most popular free web security tool, actively maintained by a dedicated international team of volunteers.

History

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

Meet the ancestor



- Paros Proxy

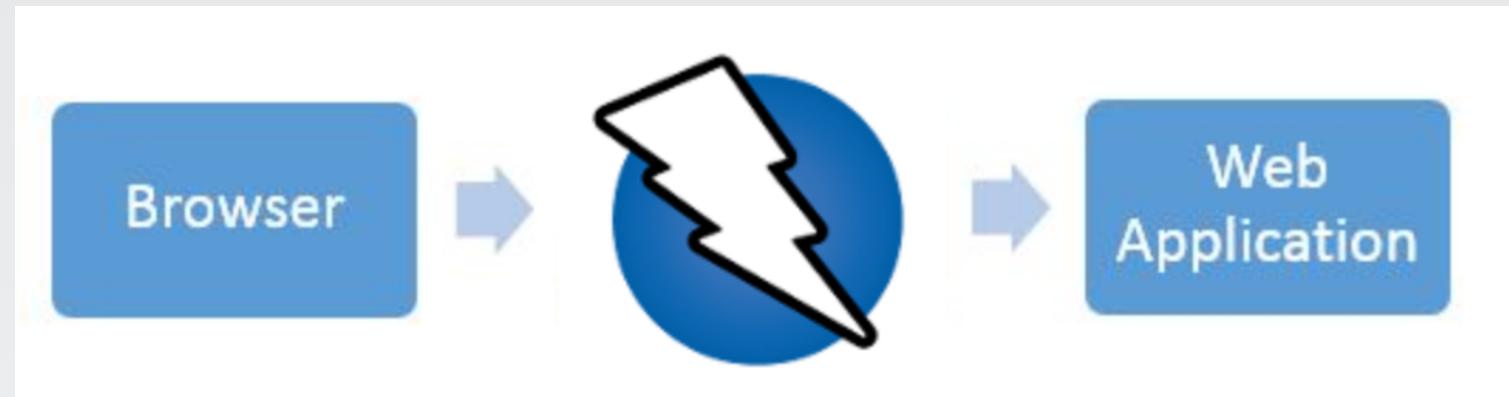
Latest release Aug. 8, 2006
(13 years, 5 months ago)

- 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

owasp.org/www-project-zap/

OWASP PROJECTS CHAPTERS EVENTS ABOUT

Search OWASP.org

Donate Join

OWASP ZAP

For more details about ZAP see the main ZAP website at zaproxy.org

ZAP

Home ZAP in Ten Documentation Get Involved Support Download

Quick Start Guide Download now

OWASP Zed Attack Proxy (ZAP)
The world's most popular free web security tool, actively maintained by a dedicated international team of volunteers.

Project Classification

Breakers Builders

OWASP TOOL PROJECT

Downloads

Download OWASP ZAP!

zaproxy / zaproxy

Sponsor Watch 387 Star 6.9k Fork 1.3k

Code Issues 647 Pull requests 14 Actions Wiki Security Insights

The OWASP ZAP core project

zap owasp-zap zap-development dast appsec zaproxy owasp security security-scanner

7,278 commits 3 branches 0 packages 248 releases 128 contributors Apache-2.0

Branch: develop New pull request Create new file Upload files Find file Clone or download

kingthorin Merge pull request #5811 from psilinon/develop ... Latest commit e81b699 2 hours ago

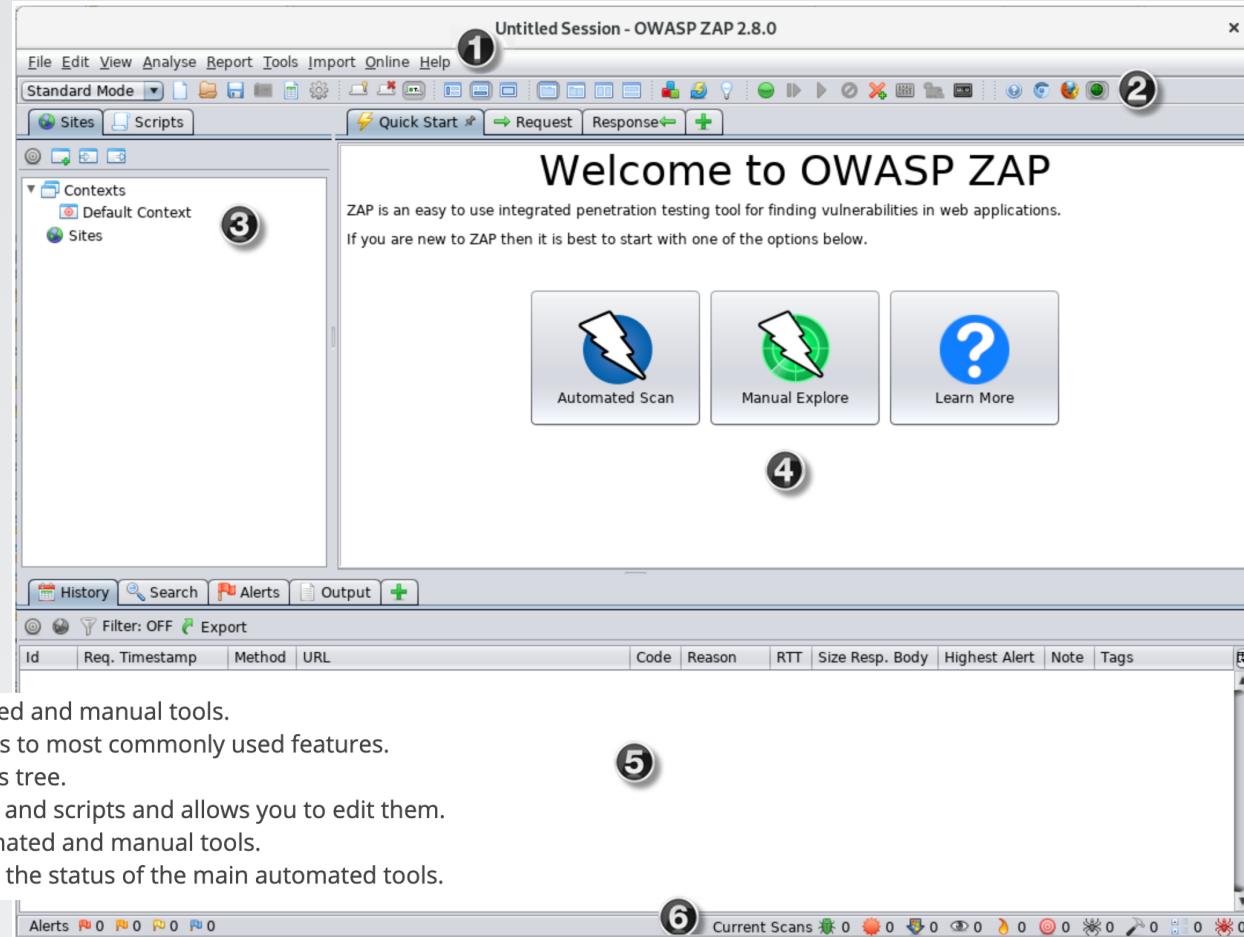
File	Description	Time Ago
.github	Changed to use zaproxy.org	4 days ago
buildSrc	Changed to use zaproxy.org	4 days ago
docker	spelling: e.g. (#5728)	last month
docs	Add SSTI scanners ID	3 months ago
examples	Normalise line endings	8 months ago
gradle	Normalise license header in Java files	8 months ago
php/api/zapv2	Changed to use zaproxy.org	4 days ago
python/scripts	Changed to use zaproxy.org	4 days ago
snap	Update snap for 2.9.0	2 hours ago
zap	Prepare next dev iteration	3 days ago
.gitattributes	Add .gitattributes	8 months ago
.gitignore	Add zap project	8 months ago
.travis.yml	Updates to Travis CI config	6 months ago
BUILDING.md	Add task to build the weekly release	8 months ago
CONTRIBUTING.md	Changed to use zaproxy.org	4 days ago
LEGALNOTICE.md	Spelling (#5709)	2 months ago

<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)

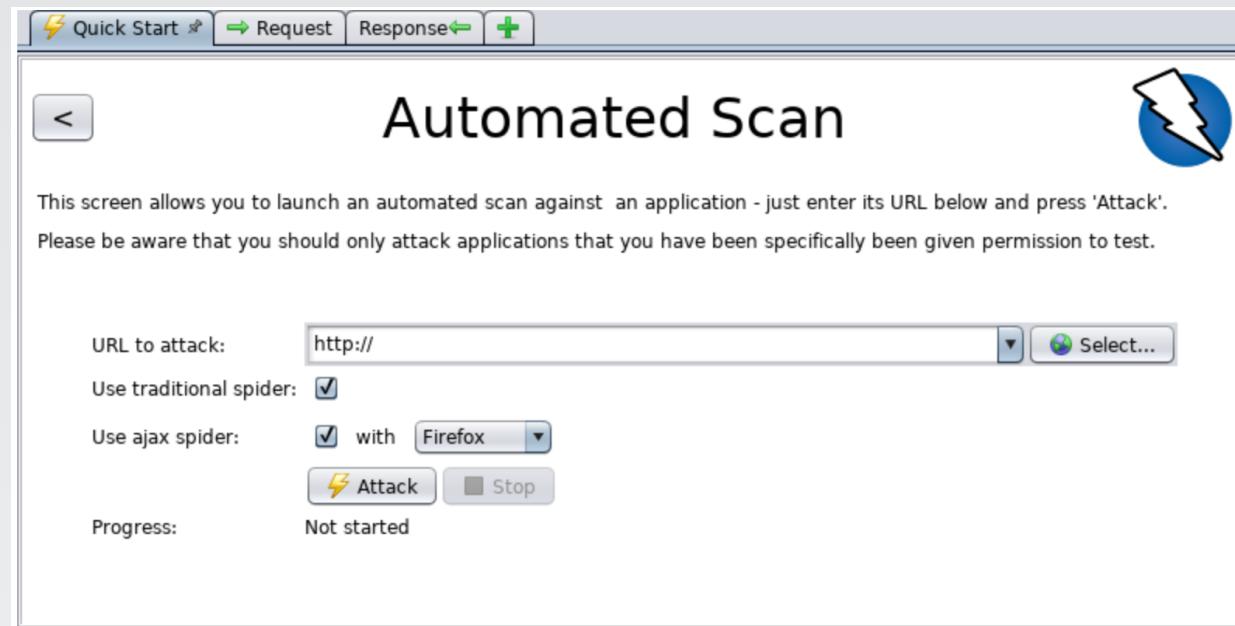
Desktop



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.

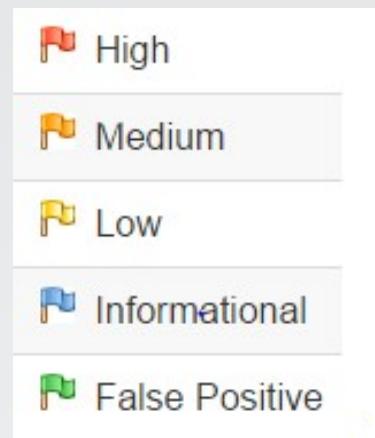
Automated scans

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



The screenshot shows the OWASP ZAP 2.5.0 interface. The left sidebar displays a tree view of contexts, sites, and their associated URLs and requests. The main panel shows a network request for a login page with detailed headers and a body. Below this, a table lists processed requests with columns for Method, URI, and Flags. A specific row for a GET request to 'Content/Site.css' is highlighted with a red border and labeled 'OUT_OF_CONTEXT'.

Header: Text

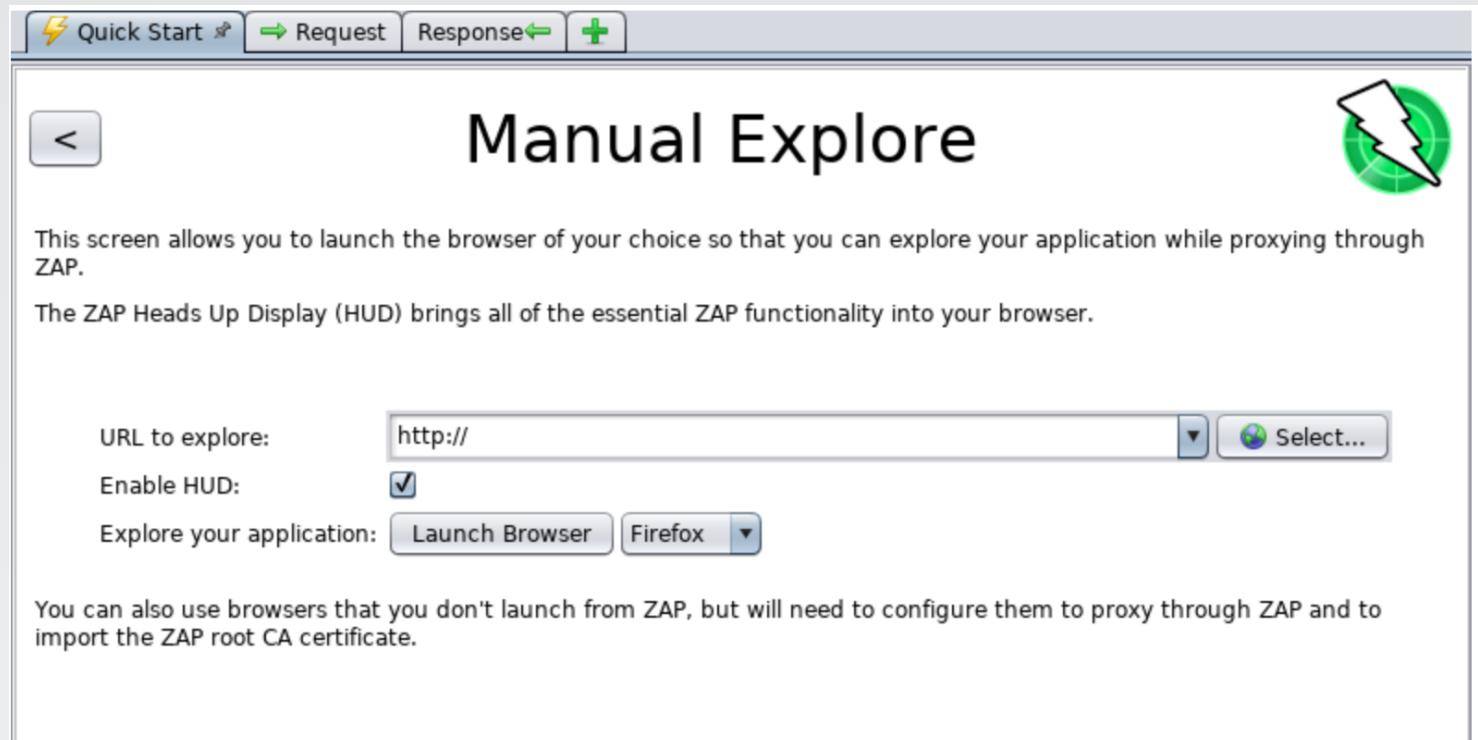
Body: Text

```
GET https://kdartstage.kdealer.com/Home/Login HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: br
Cookie: s_fid=2DB5F53E89AA5399-2BA38143FF6BD6A9; ASP.NET_SessionId=i5eet0qyuc54rzs2xbhqjrw8NjbwizStYKOLod9sX5NdVcF0Os=; s_cc=true; s_sq=%5B%5BB%5D%5D; __RequestVerificationToken=QXIDTSBngiURcXAZRiGaGFuhC1k90yTed3S_7aocS2wTQ459LdH1XMiGtKu76KwQmTqOJCHRARw3JqZa9_UJr-z5Zc1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: kdartstage.kdealer.com
```

Processed	Method	URI	Flags
	GET	https://kdartstage.kdealer.com/Home/Login	SFED
	GET	https://kdartstage.kdealer.com/Content/Site.css	OUT_OF_CONTEXT
	POST	https://kdartstage.kdealer.com/Home/Login	
	POST	https://kdartstage.kdealer.com/Home/Login	
	POST	https://kdartstage.kdealer.com/Home/Login	

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

The image shows two software windows for web spider configuration:

Spider Window:

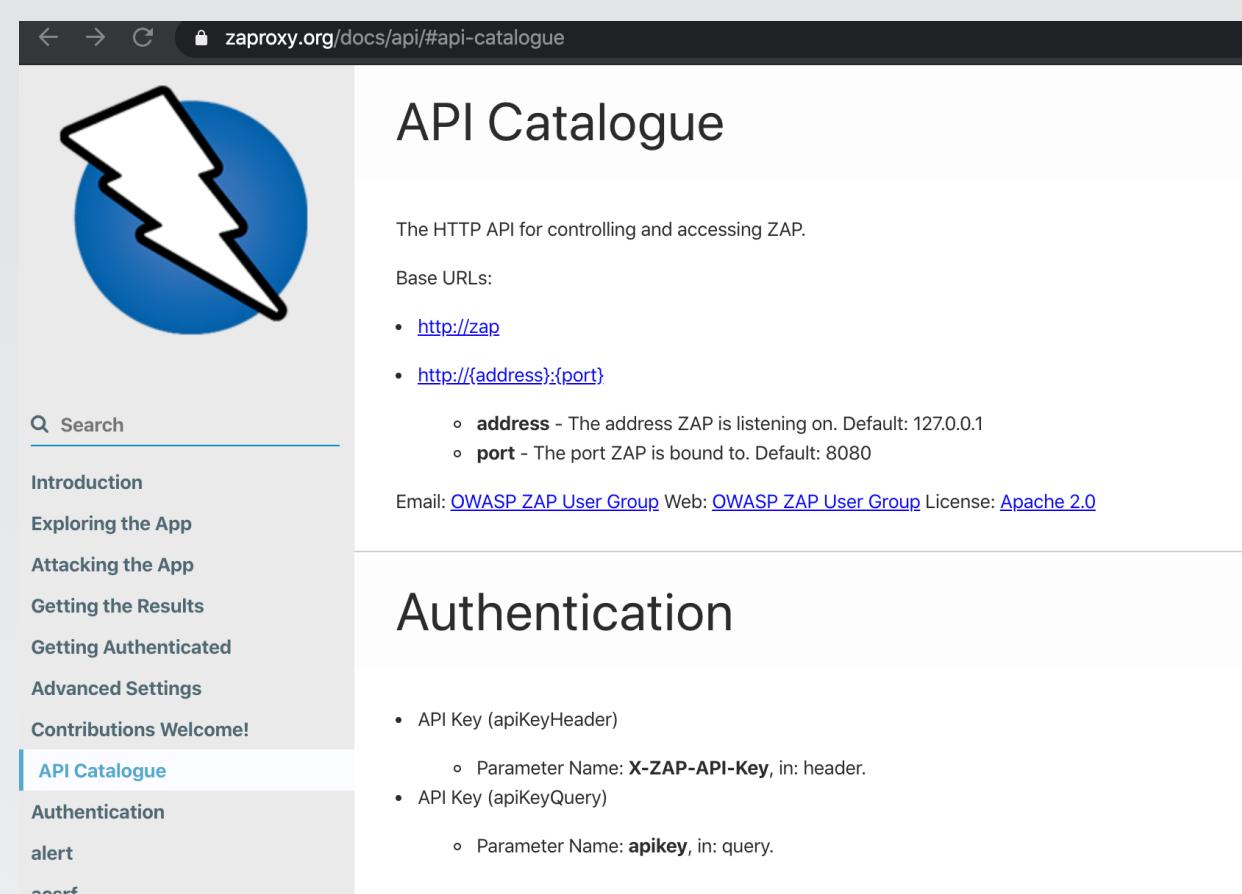
- Scope tab selected.
- Maximum Depth to Crawl (0 Is Unlimited): 5
- Maximum Children to Crawl (0 Is Unlimited): 0
- Maximum Duration (Min, 0 Is Unlimited): 0
- Maximum Parse Size (Bytes): 2621440
- Send 'Referer' Header:
- Accept Cookies:
- Process Forms:
- POST Forms:
- Parse HTML Comments:
- Parse 'robots.txt':
- Parse 'sitemap.xml':
- Parse SVN Metadata:
- Parse Git Metadata:
- Handle OData Parameters:

AJAX Spider Window:

- Scope tab selected.
- Number of Browser Windows to Open: 10
- Maximum Crawl Depth (0 is Unlimited): 10
- Maximum Crawl States (0 is Unlimited): 0
- Maximum Duration (Min, 0 is Unlimited): 60
- Event Wait time (ms): 1000
- Reload Wait time (ms): 1000

Buttons at the bottom: Cancel, Reset, Start Scan.

API



The screenshot shows a web browser window displaying the ZAP API Catalogue. The URL in the address bar is `zaproxy.org/docs/api/#api-catalogue`. The page features a large blue lightning bolt icon at the top left. To its right, the title "API Catalogue" is displayed in a large, dark font. Below the title, a brief description states: "The HTTP API for controlling and accessing ZAP." A section titled "Base URLs:" lists two items: "<http://zap>" and "<http://{{address}}:{{port}}>". Underneath these, there are two bullet points: "address - The address ZAP is listening on. Default: 127.0.0.1" and "port - The port ZAP is bound to. Default: 8080". At the bottom of the page, contact information is provided: Email: [OWASP ZAP User Group](#), Web: [OWASP ZAP User Group](#), License: [Apache 2.0](#). On the left side of the page, there is a sidebar with a search bar and a list of navigation links. The "API Catalogue" link is highlighted with a blue border, indicating it is the current page. Other links in the sidebar include "Introduction", "Exploring the App", "Attacking the App", "Getting the Results", "Getting Authenticated", "Advanced Settings", "Contributions Welcome!", "Authentication", "alert", and "acsrf".

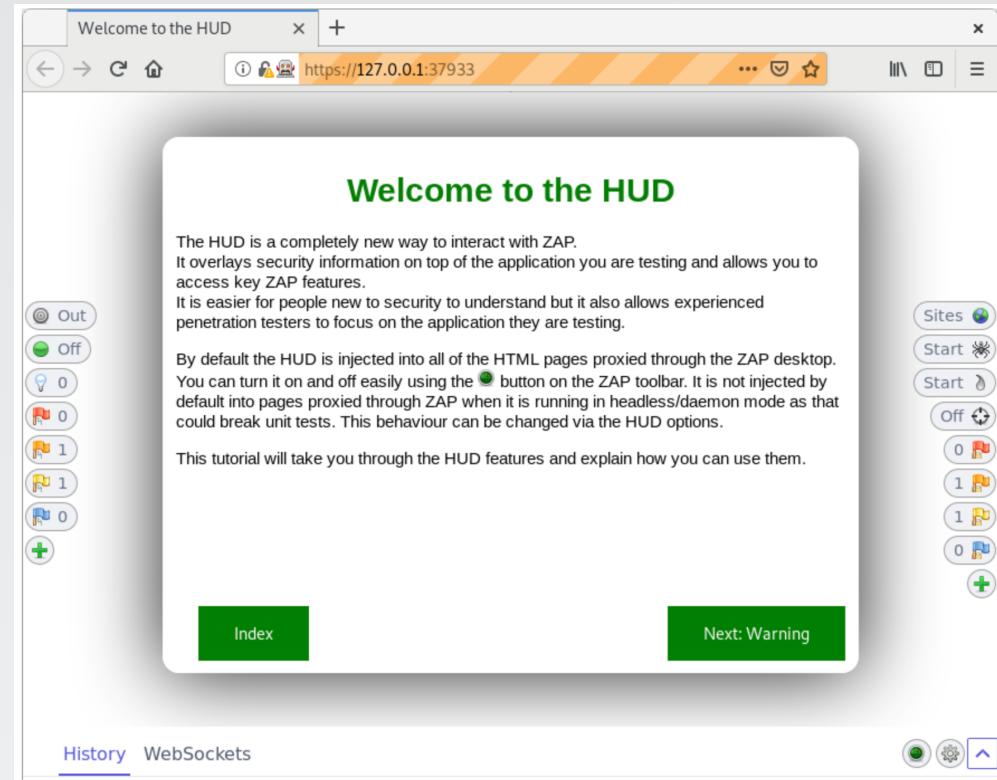
<https://www.zaproxy.org/docs/api/#api-catalogue>

Heads Up Display (cool)

The Heads Up Display (HUD) is a new and 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)