



OWASP

Open Web Application
Security Project

Zed Attack Proxy (ZAP)

Daniel W – OWASP Chapter Lead



ZAP

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?

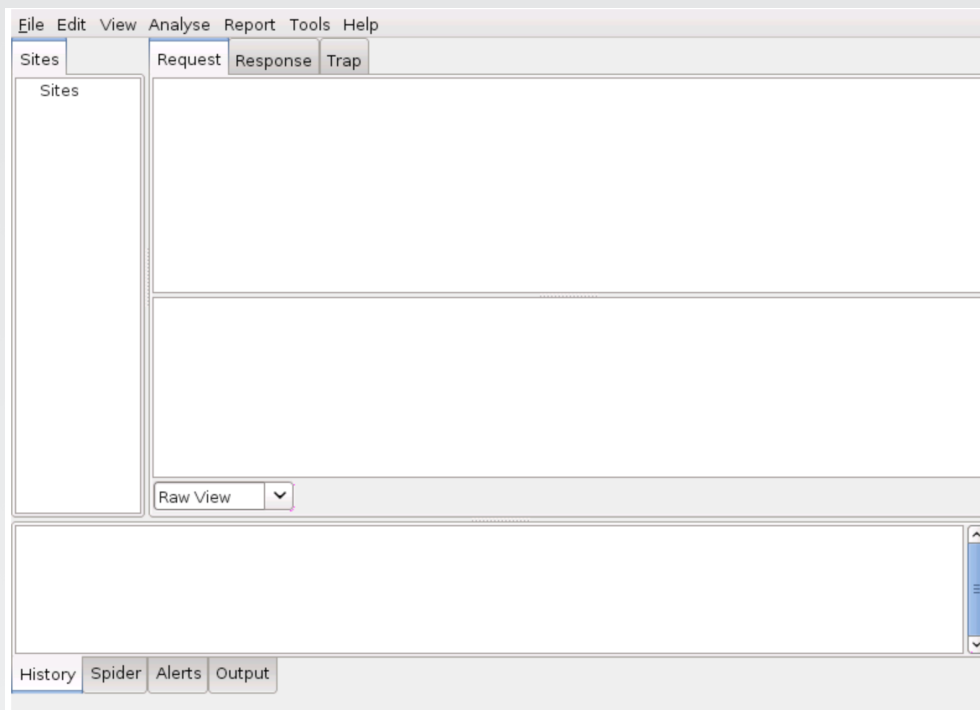


The world's most popular free web security tool, actively maintained by a dedicated international team of volunteers.

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.

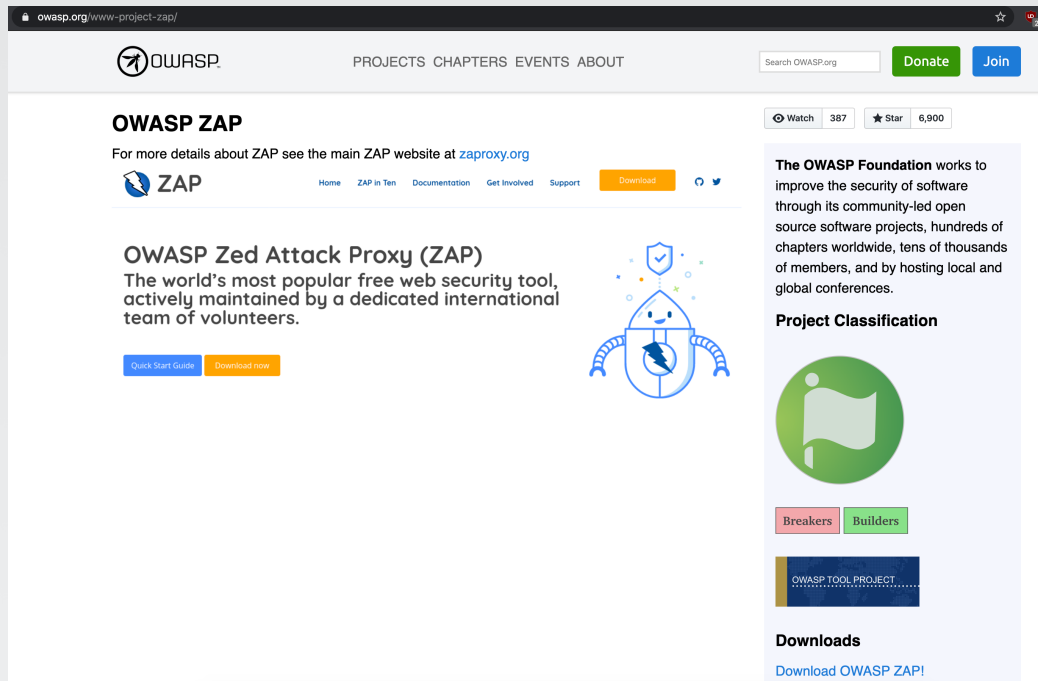
How does it work?

In essence - a fancy proxy with some lovely extras.

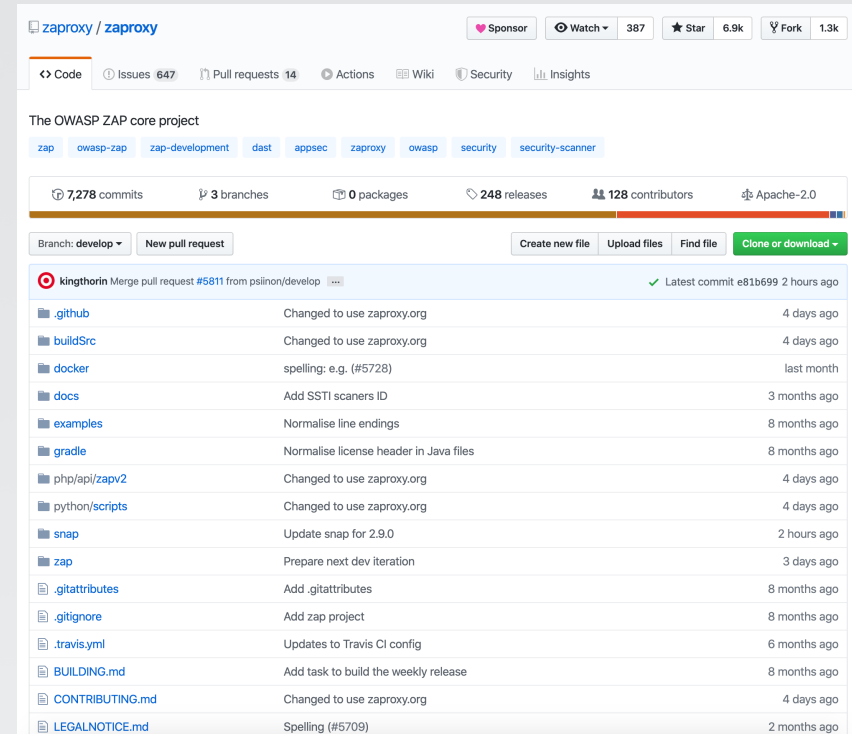
- Intercepting Proxy
- Active and Passive Scanners
- Traditional and Ajax Spiders
- Brute Force Scanner
- Port Scanner
- Web Sockets



Where to get ZAP



The screenshot shows the OWASP ZAP website. At the top, there's a navigation bar with 'PROJECTS CHAPTERS EVENTS ABOUT' and a search bar. The main heading is 'OWASP ZAP'. Below it, a subheading says 'For more details about ZAP see the main ZAP website at zaproxy.org'. There's a 'Download' button and a 'Quick Start Guide' button. A large illustration of the ZAP robot is on the right. Below the robot, there's a section titled 'The OWASP Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.' This is followed by 'Project Classification' with a green flag icon and buttons for 'Breakers' and 'Builders'. At the bottom, there's a 'Downloads' section with a link to 'Download OWASP ZAP!'.



The screenshot shows the Zaproxy GitHub repository page. At the top, there's a navigation bar with 'Sponsor', 'Watch', 'Star', 'Fork', and '1.3k'. Below this, there's a section for 'The OWASP ZAP core project' with tabs for 'zap', 'owasp-zap', 'zap-development', 'dast', 'appsec', 'zaproxy', 'owasp', 'security', and 'security-scanner'. The repository statistics show 7,278 commits, 3 branches, 0 packages, 248 releases, 128 contributors, and Apache-2.0 license. A table of recent commits is shown below, with columns for the commit message and the time since the commit. The commits include changes to .github, buildSrc, docker, docs, examples, gradle, php/api/zapv2, python/scripts, snap, zap, .gitattributes, .gitignore, .travis.yml, BUILDING.md, CONTRIBUTING.md, and LEGALNOTICE.md.

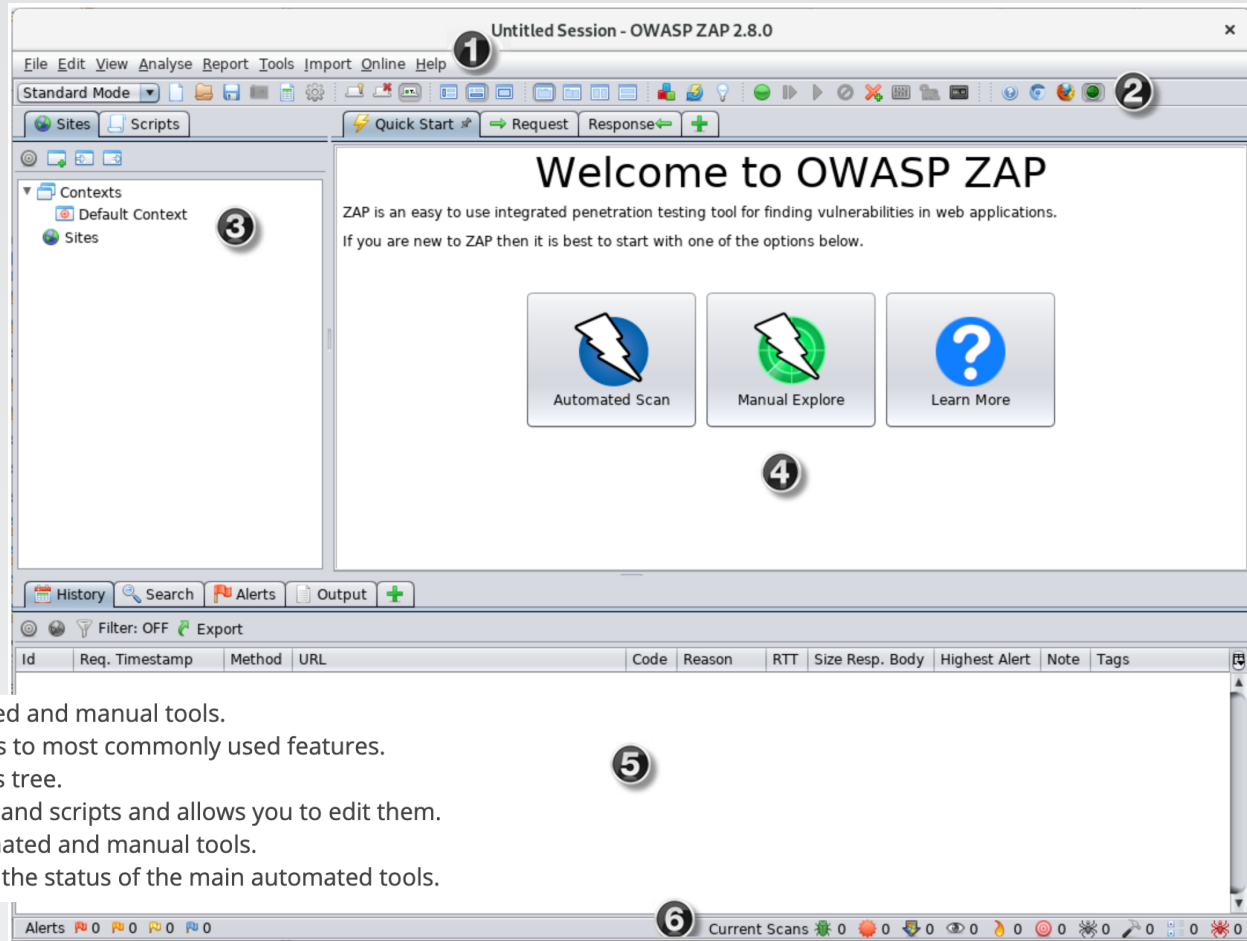
Commit Message	Time Since Commit
kingthorin Merge pull request #5811 from psinon/develop	Latest commit e81b699 2 hours ago
Changed to use zaproxy.org	4 days ago
Changed to use zaproxy.org	4 days ago
spelling: e.g. (#5728)	last month
Add SSTI scanners ID	3 months ago
Normalise line endings	8 months ago
Normalise license header in Java files	8 months ago
Changed to use zaproxy.org	4 days ago
Changed to use zaproxy.org	4 days ago
Update snap for 2.9.0	2 hours ago
Prepare next dev iteration	3 days ago
Add .gitattributes	8 months ago
Add zap project	8 months ago
Updates to Travis CI config	6 months ago
Add task to build the weekly release	8 months ago
Changed to use zaproxy.org	4 days ago
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)

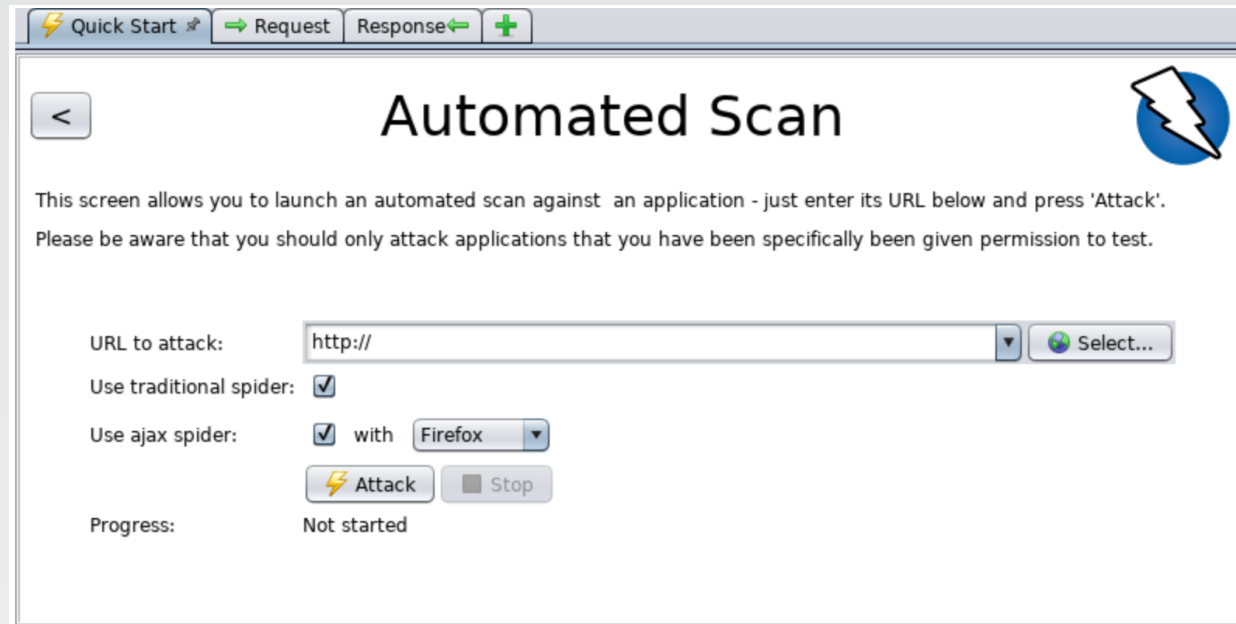
Desktop



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

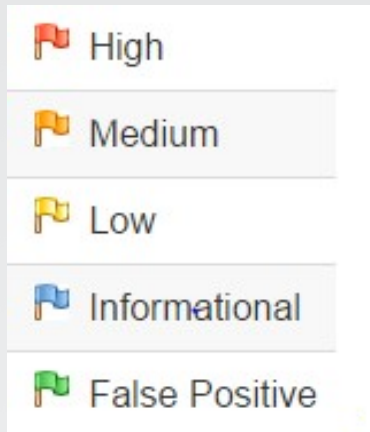
1. Start ZAP and click the **Quick Start** tab of the Workspace Window.
2. Click the large Automated Scan button.
3. In the **URL to attack** text box, enter the full URL of the web application you want to attack.
4. Click the **Attack**



The screenshot shows the 'Automated Scan' dialog box in ZAP. At the top, there are tabs for 'Quick Start', 'Request', 'Response', and a plus sign. The 'Quick Start' tab is active. The dialog has a title bar with a back button and a lightning bolt icon. The main title is 'Automated Scan'. Below the title, there is a warning message: '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 given permission to test.' The 'URL to attack:' field contains 'http://'. To the right of the field is a 'Select...' button. Below the URL field, there are two checkboxes: 'Use traditional spider:' (checked) and 'Use ajax spider:' (checked). Next to 'Use ajax spider:' is a 'with' label and a dropdown menu showing 'Firefox'. At the bottom, there are two buttons: 'Attack' (with a lightning bolt icon) and 'Stop' (with a square icon). Below these buttons, the 'Progress:' label is followed by the text 'Not started'.

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



Untitled Session - OWASP ZAP 2.5.0

File Edit View Analyse Report Tools Online Help

Protected Mode

Quick Start Request Response

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=2DB5F53E89AA5399-2BA38143FF68D6A9; ASP.NET_SessionId=i5eet0qyuc54rzs2xfbhqjrw8NjbwizStYKOLod9sX5NdVcF0Os=; s_cc=true; s_sq=%5B%5B%5D%5D; __RequestVerificationToken=QXIDTS8ngiWURcXAZRiGaGFuhClK90yTed3S_7aocS2w7Q459LdHiXMiGtKu76KwQmTq0JCHARw3JqZa9_UJr-z5Zc1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: kdartstage.kdealer.com

Contexts

- Default Context
- Sites
 - https://hisnakiamotors.122.2o7.net
 - https://kdartstage.kdealer.com
 - Dashboard
 - GET:viewDashboard
 - GET:GetWidgetTree
 - GET:GetWidgetTree(id)
 - POST:GetKpiDataByWidgetID_Read(ChartType)
 - POST:readGraph(MonthID,YearID,chart,dlr,dst)
 - FixedOperationReport
 - GET:ViewFixedOperationReportRevise
 - Home
 - POST:ActivityDetailHome_Read(filter.group,pag
 - GET:Logout
 - GET:Login
 - POST:GridAssignmentsNew_Read(filter.group
 - POST:HomeGrid_Read(aggregate,filter.group,
 - POST:Login>Password,UserName,Requ

History Search Alerts Output Spider

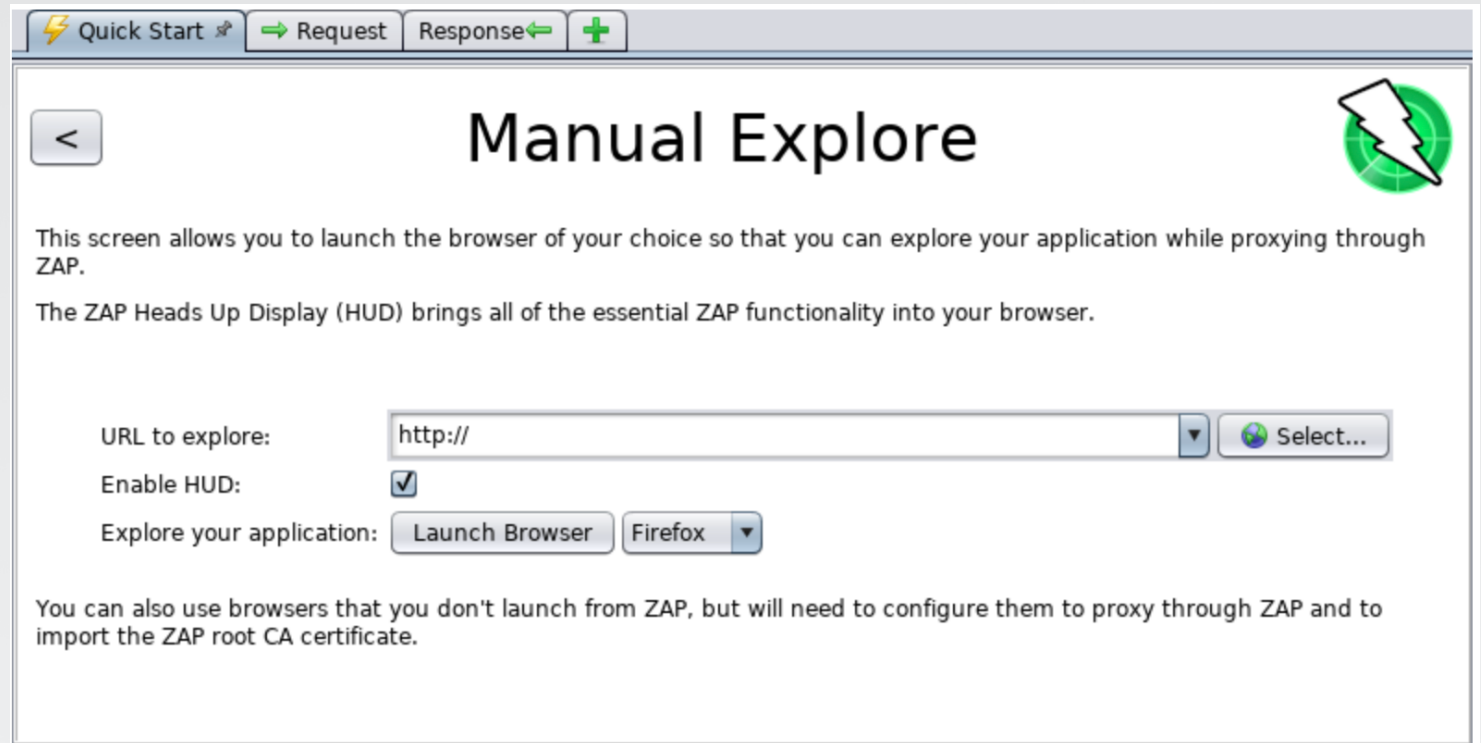
New Scan Progress: 2: Context: Default Context 100% Current Scans: 0 URIs Found: 6 Show Messages

Processed	Method	URI	Flags
	GET	https://kdartstage.kdealer.com/Home/Login	SEED
	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	

Alerts 0 2 7 0 Current Scans 0 0 0 0 0 0 0 0

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**



The screenshot shows the ZAP Manual Explore interface. At the top, there's a toolbar with 'Quick Start' (lightning bolt icon), 'Request' (green arrow), 'Response' (green arrow), and a '+' button. Below this is a header with a back button, the title 'Manual Explore', and a green lightning bolt icon. The main content area contains explanatory text and configuration options. The 'URL to explore' field has 'http://' entered. The 'Enable HUD' checkbox is checked. The 'Explore your application' section has a 'Launch Browser' button and a browser selection dropdown currently showing 'Firefox'. A 'Select...' button with a globe icon is next to the URL field. At the bottom, there's a note about using external browsers and proxying.

Quick Start Request Response +

Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.

The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

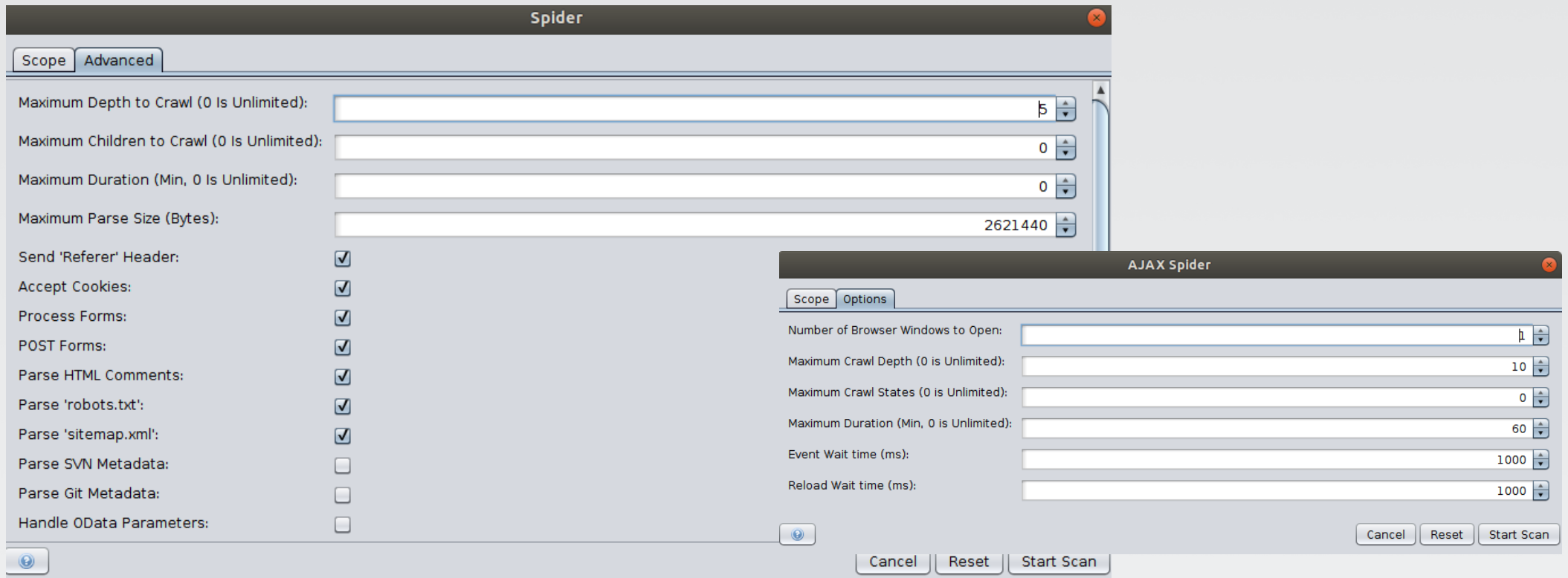
URL to explore:  Select...

Enable HUD: ☒

Explore your application: 

You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.

Spiders are powerful



The image shows two configuration windows for web spiders. The 'Spider' window is in the foreground, and the 'AJAX Spider' window is in the background.

Spider Configuration:

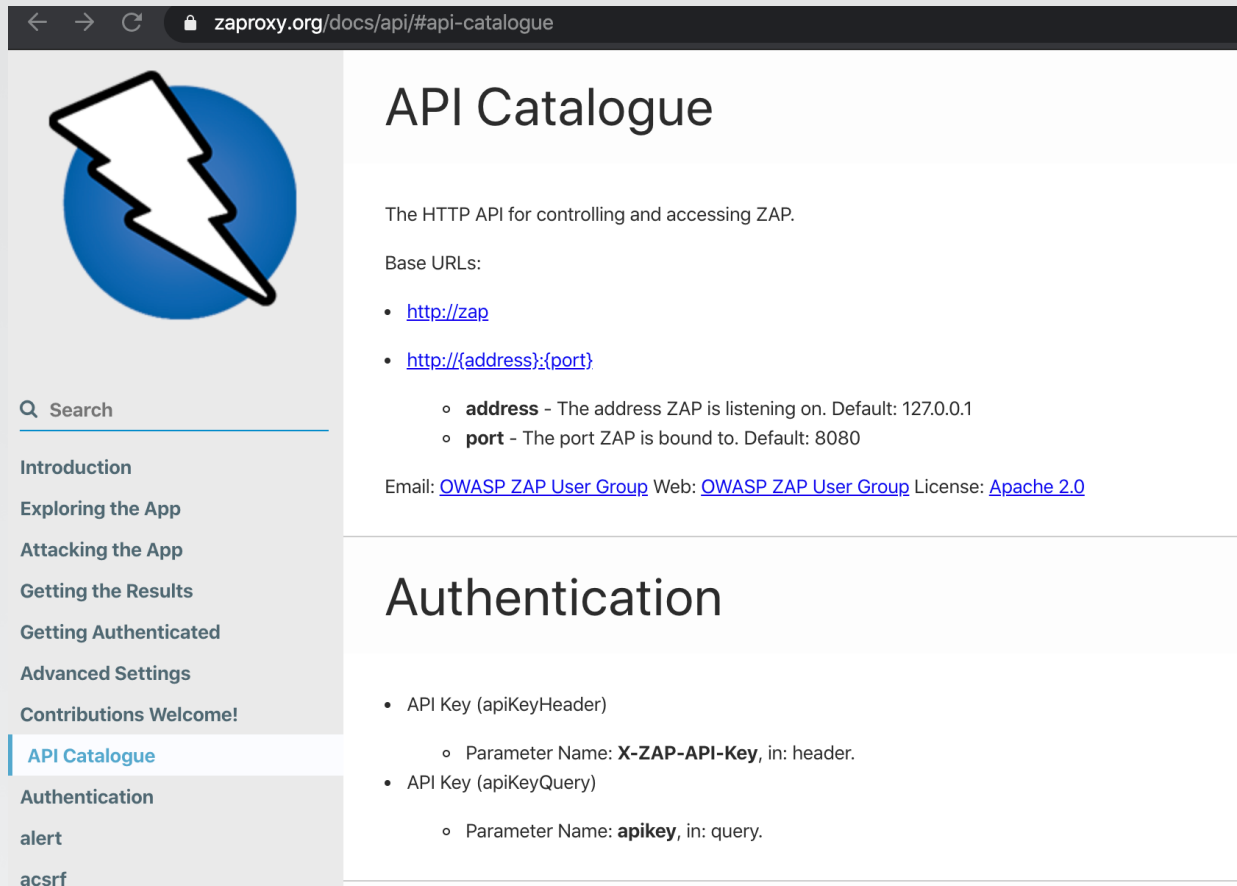
- Maximum Depth to Crawl (0 Is Unlimited): 5
- Maximum Children to Crawl (0 Is Unlimited): 0
- Maximum Duration (Min, 0 Is Unlimited): 0
- Maximum Parse Size (Bytes): 2621440
- Send 'Referer' Header: ☒
- Accept Cookies: ☒
- Process Forms: ☒
- POST Forms: ☒
- Parse HTML Comments: ☒
- Parse 'robots.txt':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

AJAX Spider Configuration:

- Number of Browser Windows to Open: 1
- 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: Cancel, Reset, Start Scan

API



The screenshot shows a web browser window with the address bar displaying `zaproxy.org/docs/api/#api-catalogue`. The page content is divided into a left sidebar and a main area. The sidebar contains a search bar, a list of navigation links (Introduction, Exploring the App, Attacking the App, Getting the Results, Getting Authenticated, Advanced Settings, Contributions Welcome!, API Catalogue, Authentication, alert, acsrf), and a logo of a lightning bolt inside a blue circle. The main area has a heading 'API Catalogue' followed by a description: 'The HTTP API for controlling and accessing ZAP.' Below this, it lists 'Base URLs:' with two bullet points: `http://zap` and `http://{address}:{port}`. The second bullet point has sub-points for 'address' (default: 127.0.0.1) and 'port' (default: 8080). At the bottom of the main area, it provides contact information: Email: [OWASP ZAP User Group](#), Web: [OWASP ZAP User Group](#), License: [Apache 2.0](#). Below this, there is a section titled 'Authentication' with two bullet points: 'API Key (apiKeyHeader)' with a sub-point 'Parameter Name: X-ZAP-API-Key, in: header.' and 'API Key (apiKeyQuery)' with a sub-point 'Parameter Name: **apikey**, in: query.'

API Catalogue

The HTTP API for controlling and accessing ZAP.

Base URLs:

- <http://zap>
- <http://{address}:{port}>
 - **address** - The address ZAP is listening on. Default: 127.0.0.1
 - **port** - The port ZAP is bound to. Default: 8080

Email: [OWASP ZAP User Group](#) Web: [OWASP ZAP User Group](#) License: [Apache 2.0](#)

Authentication

- API Key (apiKeyHeader)
 - Parameter Name: **X-ZAP-API-Key**, in: header.
- API Key (apiKeyQuery)
 - Parameter Name: **apikey**, in: query.

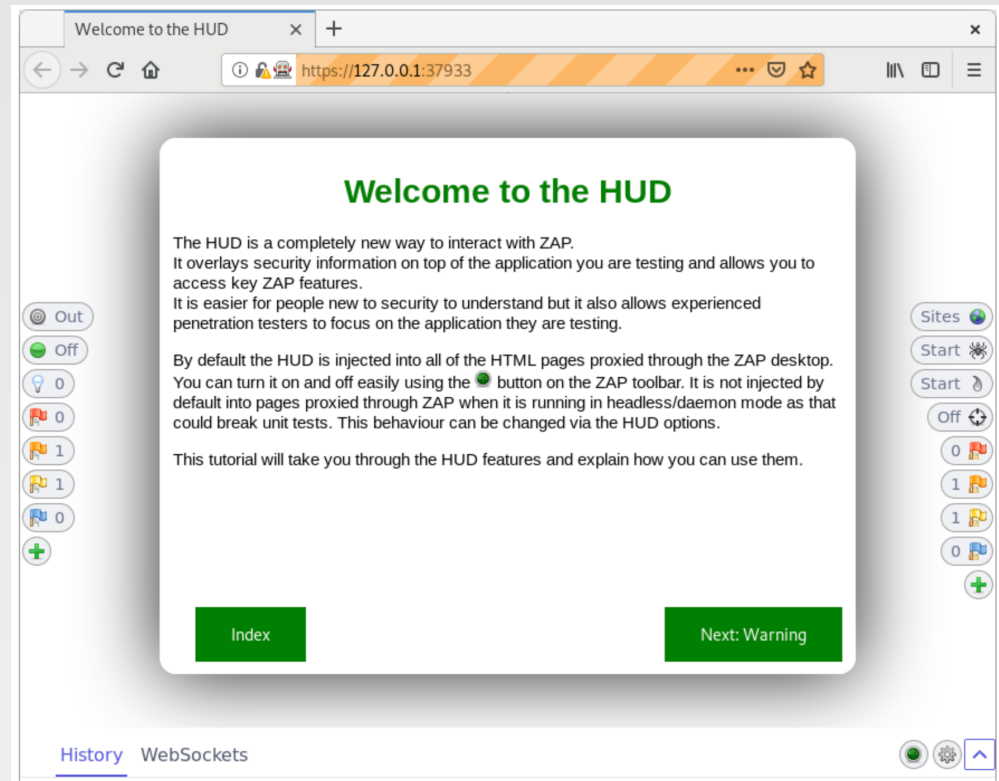
<https://www.zaproxy.org/docs/api/#api-catalogue>

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 overlaid 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/baseURL/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 @zapproxy
- <https://www.zaproxy.org/>
- <https://owasp.org/www-project-zap/>
- <https://github.com/zaproxy/zaproxy>

Questions (if time allows)