

Overview

This document is intended to serve as a basic introduction for using OWASP's Zed Attack Proxy (ZAP) tool to perform security testing, even if you don't have a background in security testing. To that end, some security testing concepts and terminology is included but this document is not intended to be a comprehensive guide to either ZAP or security testing.

If you are already familiar with security or penetration testing, you may want to start with [Introducing ZAP](#).

If you are already familiar with ZAP 2.7 then you may want to start with the [ZAP Desktop UI](#) as it covers the new Quick Start screens.

See [Useful Links](#) for additional resources and information on ZAP.

Security Testing Basics

Software security testing is the process of assessing and testing a system to discover security risks and vulnerabilities of the system and its data. There is no universal terminology but for our purposes, we define assessments as the analysis and discovery of vulnerabilities without attempting to actually exploit those vulnerabilities. We define testing as the discovery and attempted exploitation of vulnerabilities.

Security testing is often broken out, somewhat arbitrarily, according to either the type of vulnerability being tested or the type of testing being done. A common breakout is:

- **Vulnerability Assessment** - The system is scanned and analyzed for security issues.
- **Penetration Testing** - The system undergoes analysis and attack from simulated malicious attackers.
- **Runtime Testing** - The system undergoes analysis and security testing from an end-user.
- **Code Review** - The system code undergoes a detailed review and analysis looking specifically for security vulnerabilities.

Note that risk assessment, which is commonly listed as part of security testing, is not included in this list. That is because a risk assessment is not actually a test but rather the analysis of the perceived severity of different risks (software security, personnel security, hardware security, etc.) and any mitigation steps for those risks.

More About Penetration Testing

Penetration Testing (pentesting) is carried out as if the tester was a malicious external attacker with a goal of breaking into the system and either stealing data or carrying out some sort of denial-of-service attack.

Pentesting has the advantage of being more accurate because it has fewer false positives (results that report a vulnerability that isn't actually present), but can be time-consuming to run.

Pentesting is also used to test defence mechanisms, verify response plans, and confirm security policy adherence.

Automated pentesting is an important part of continuous integration validation. It helps to uncover new vulnerabilities as well as regressions for previous vulnerabilities in an environment which quickly changes, and for which the development may be highly collaborative and distributed.

The Pentesting Process

Both manual and automated pentesting are used, often in conjunction, to test everything from servers, to networks, to devices, to endpoints. This document focuses on web application or web site pentesting.

Pentesting usually follows these stages:

- **Explore** – The tester attempts to learn about the system being tested. This includes trying to determine what software is in use, what endpoints exist, what patches are installed, etc. It also includes searching the site for hidden content, known vulnerabilities, and other indications of weakness.
- **Attack** – The tester attempts to exploit the known or suspected vulnerabilities to prove they exist.
- **Report** – The tester reports back the results of their testing, including the vulnerabilities, how they exploited them and how difficult the exploits were, and the severity of the exploitation.

Pentesting Goals

The ultimate goal of pentesting is to search for vulnerabilities so that these vulnerabilities can be addressed. It can also verify that a system is not vulnerable to a known class or specific defect; or, in the case of vulnerabilities that have been reported as fixed, verify that the system is no longer vulnerable to that defect.

Introducing ZAP

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible.

At its core, ZAP is what is known as a “man-in-the-middle proxy.” It stands between the tester’s browser and the web application so that it can intercept and inspect messages sent between browser and web application, modify the contents if needed, and then forward those packets on to the destination. It can be used as a stand-alone application, and as a daemon process.



If there is another network proxy already in use, as in many corporate environments, ZAP can be configured to connect to that proxy.



ZAP provides functionality for a range of skill levels – from developers, to testers new to security testing, to security testing specialists. ZAP has versions for each major OS and Docker, so you are not tied to a single OS. Additional functionality is freely available from a variety of add-ons in the ZAP Marketplace, accessible from within the ZAP client.

Because ZAP is open-source, the source code can be examined to see exactly how the functionality is implemented. Anyone can volunteer to work on ZAP, fix bugs, add features, create pull requests to pull fixes into the project, and author add-ons to support specialized situations.

For more information, see the [Zed Attack Proxy Project Page](#).

As with most open source projects, donations are welcome to help with costs for the projects. You can find a donate button on the owasp.org page for ZAP at <https://www.owasp.org/index.php/ZAP>.

Install and Configure ZAP

ZAP has installers for Windows, Linux, and Mac OS/X. There are also Docker images available on the download site listed below.

Install ZAP

The first thing to do is install ZAP on the system you intend to perform pentesting on. Download the appropriate installer from ZAP's download location at <https://github.com/zaproxy/zaproxy/wiki/Downloads> and execute the installer.

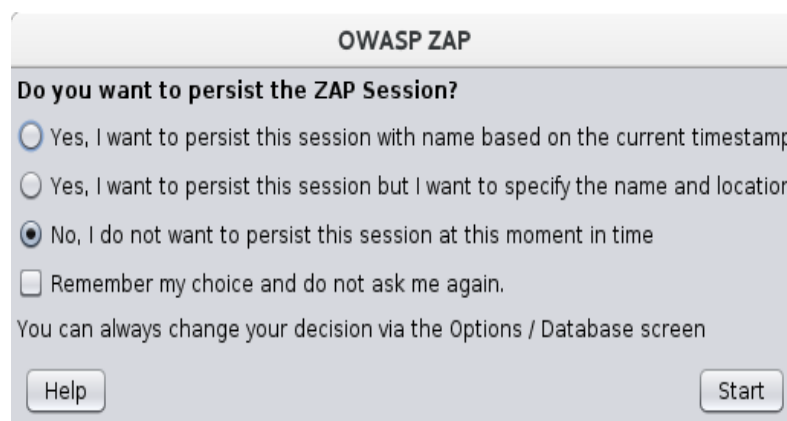
Note that ZAP requires Java 8+ in order to run. The Mac OS/X installer includes an appropriate version of Java but you must install Java 8+ separately for Windows, Linux, and Cross-Platform versions. The Docker versions do not require you to install Java.

Once the installation is complete, launch ZAP and read the license terms. Click **Agree** if you accept the terms, and ZAP will finish installing, then ZAP will automatically start.

Persisting a Session

When you first start ZAP, you will be asked if you want to persist the ZAP session. By default, ZAP sessions are always recorded to disk in a HSQLDB database with a default name and location. If you do not persist the session, those files are deleted when you exit ZAP.

If you choose to persist a session, the session information will be saved in the local database so you can access it later, and you will be able to provide custom names and locations for saving the files.

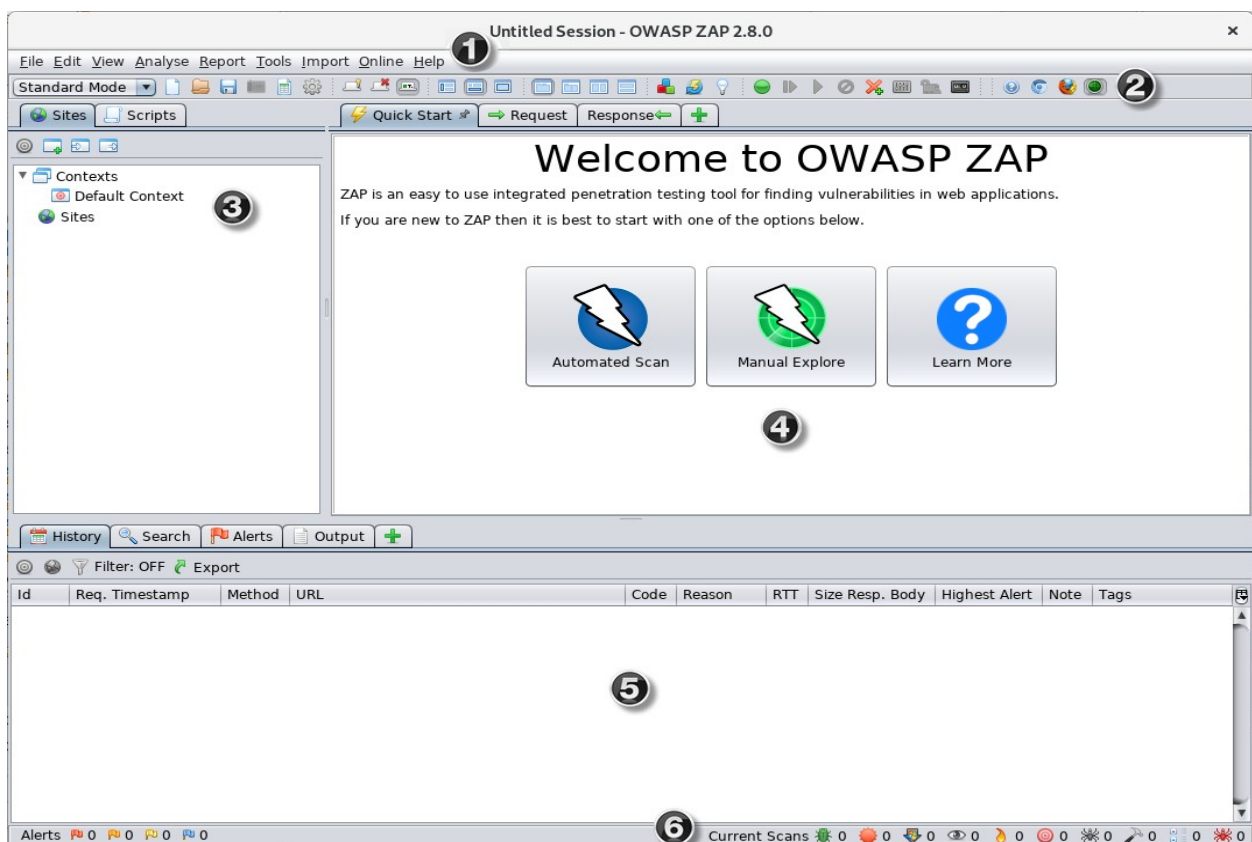


For now, select **No, I do not want to persist this session at this moment in time**, then click **Start**. The ZAP sessions will not be persisted for now.

ZAP Desktop UI

The ZAP Desktop UI is composed of the following elements:

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.



While using ZAP, you can click **Help** on the Menu Bar or press F1 to access context-sensitive help from the ZAP Desktop User Guide. It is also available [online](#).

For more information about the UI, see [ZAP UI Overview](#) in the ZAP online documentation.

ZAP also supports a powerful API and command line functionality, both of which are beyond the scope of this guide.

IMPORTANT: You should only use ZAP to attack an application you have permission to test with an active attack. Because this is a simulation that acts like a real attack, actual damage can be done to a site's functionality, data, etc. If you are worried about using ZAP, you can prevent it from causing harm (though ZAP's functionality will be significantly reduced) by switching to safe mode.

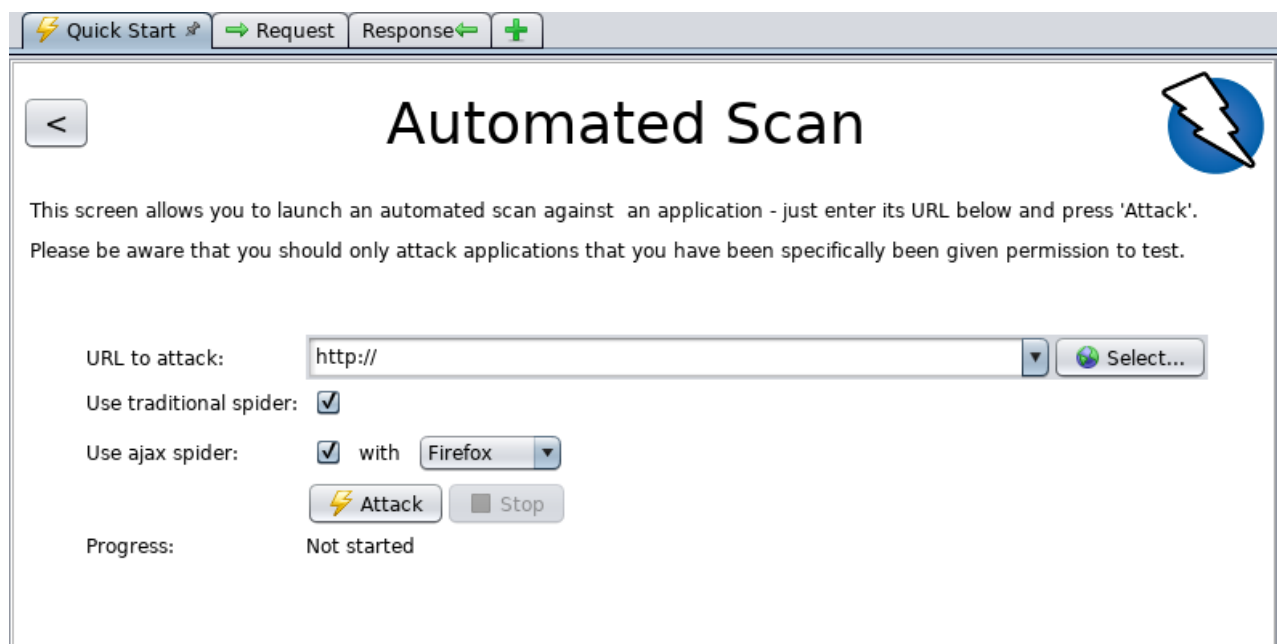
To switch ZAP to safe mode, click the arrow on the mode dropdown on the main toolbar to expand the dropdown list and select **Safe Mode**.

Running an Automated Scan

The easiest way to start using ZAP is via the Quick Start tab. Quick Start is a ZAP add-on that is included automatically when you installed ZAP.

To run a Quick Start Automated Scan :

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** button.



The screenshot shows the 'Automated Scan' window in ZAP. At the top, there's a toolbar with 'Quick Start', 'Request', 'Response', and a '+' button. The window title is 'Automated Scan'. Below the title, there's 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 main form has a 'URL to attack:' label, a text box containing 'http://', a dropdown arrow, and a 'Select...' button. Below this, there are two checkboxes: 'Use traditional spider:' (checked) and 'Use ajax spider:' (checked). The 'Use ajax spider:' checkbox is followed by the word 'with' 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 the buttons, there's a 'Progress:' label and 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.

ZAP provides 2 spiders for crawling web applications, you can use either or both of them from this screen.

The traditional ZAP spider which discovers links by examining the HTML in responses from the web application. This spider is fast, but it is not always effective when exploring an AJAX web application that generates links using JavaScript.

For AJAX applications, ZAP's AJAX spider is likely to be more effective. This spider explores the web application by invoking browsers which then follow the links that have been generated. The AJAX spider is slower than the traditional spider and requires additional configuration for use in a "headless" environment.

ZAP will passively scan all of the requests and responses proxied through it. So far ZAP has only carried out passive scans of your web application. Passive scanning does not change responses in any way and is considered safe. Scanning is also performed in a background

thread to not slow down exploration. Passive scanning is good at finding some vulnerabilities and as a way to get a feel for the basic security state of a web application and locate where more investigation may be warranted.

Active scanning, however, attempts to find other vulnerabilities by using known attacks against the selected targets. Active scanning is a real attack on those targets and can put the targets at risk, so do not use active scanning against targets you do not have permission to test.

Interpret Your Test Results

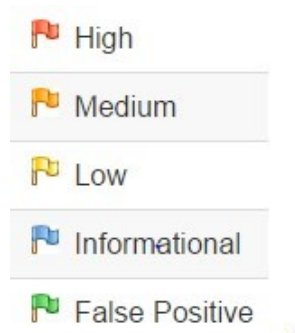
As ZAP spiders your web application, it constructs a map of your web applications' pages and the resources used to render those pages. Then it records the requests and responses sent to each page and creates alerts if there is something potentially wrong with a request or response.

See Explored Pages

To examine a tree view of the explored pages, click the **Sites** tab in the Tree Window. You can expand the nodes to see the individual URLs accessed.

View Alerts and Alert Details

The left-hand side of the Footer contains a count of the Alerts found during your test, broken out into risk categories. These risk categories are:



To view the alerts created during your test:

1. Click the **Alerts** tab in the Information Window.
2. Click each alert displayed in that window to display the URL and the vulnerability detected in the right side of the Information Window.
3. In the Workspace Windows, click the **Response** tab to see the contents of the header and body of the response. The part of the response that generated the alert will be highlighted.

Exploring an Application Manually

The passive scanning and automated attack functionality is a great way to begin a vulnerability assessment of your web application but it has some limitations. Among these are:

- Any pages protected by a login page are not discoverable during a passive scan because, unless you've configured ZAP's authentication functionality, ZAP will not handle the required authentication.
- You don't have a lot of control over the sequence of exploration in a passive scan or the types of attacks carried out in an automated attack. ZAP does provide many additional options for exploration and attacks outside of passive scanning.

Spiders are a great way to explore your basic site, but they should be combined with manual exploration to be more effective. Spiders, for example, will only enter basic default data into forms in your web application but a user can enter more relevant information which can, in turn, expose more of the web application to ZAP. This is especially true with things like registration forms where a valid email address is required. The spider may enter a random string, which will cause an error. A user will be able to react to that error and supply a correctly formatted string, which may cause more of the application to be exposed when the form is submitted and accepted.

You should explore all of your web application with a browser proxying through ZAP. As you do this, ZAP passively scans all the requests and responses made during your exploration for vulnerabilities, continues to build the site tree, and records alerts for potential vulnerabilities found during the exploration.

It is important to have ZAP explore each page of your web application, whether linked to another page or not, for vulnerabilities. Obscurity is not security, and hidden pages sometimes go live without warning or notice. So be as thorough as you can when exploring your site.


You can quickly and easily launch browsers that are pre-configured to proxy through ZAP via the Quick Start tab. Browsers launched in this way will also ignore any certificate validation warnings that would otherwise be reported.

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: Firefox

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.

To Manually Explore your application:

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** button.

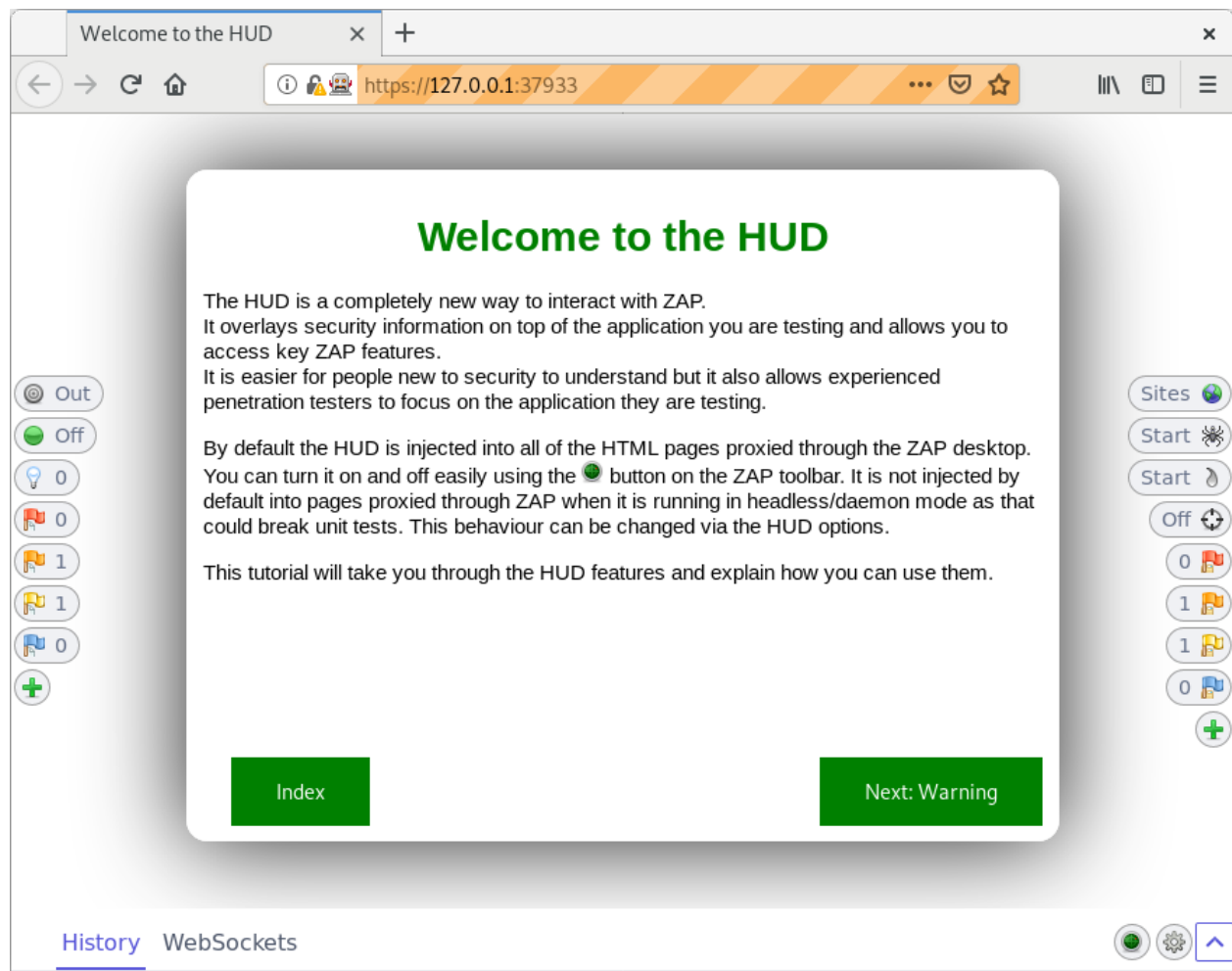
This option will launch any of the most common browsers that you have installed with new profiles.

If you would like to use any of your browsers with an existing profile, for example with other browser add-ons installed, then you will need to manually configure your browser to proxy via ZAP and import and trust the ZAP Root CA Certificate. See the ZAP Desktop User Guide for more details.

By default the ZAP Heads Up Display (HUD) will be enabled. Unchecking the relevant option on this screen before launching a browser will disable the HUD.

The Heads Up Display

The Heads Up Display (HUD) is a new and innovative interface that provides access to ZAP functionality directly in the browser. It is ideal for people new to web security and also allows experienced penetration testers to focus on an applications functionality while providing key security information and functionality.



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.

By default a splash screen is shown for the HUD which includes a link to a tutorial which will take you through the HUD features and explain how you can use them.

ZAP Advanced Features

Advanced Desktop Features

The desktop has a large number of features that are not immediately apparent so that new users are not overwhelmed.

There are many tabs that are not shown by default. They can be accessed via the right hand tabs with green '+' icons. You can pin any tabs you would like to always appear by right clicking on them. Many of the tabs hidden by default will appear when relevant. For example the Websockets tab will appear if an application you are proxying through ZAP starts to use Websockets.

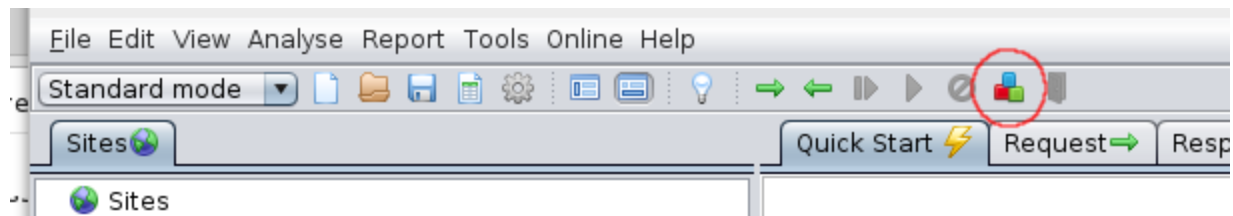
The desktop also makes heavy use of context sensitive right click options, so right click everywhere while you are getting used to the user interface.

The ZAP Marketplace

The ZAP desktop has a plugin architecture which means that new functionality can be added dynamically.

An online marketplace provides a wide range of ZAP add-ons which add many additional features to ZAP.

The marketplace can be accessed via the 'Manage Add-ons' button on the toolbar:



All of the add-ons on the marketplace are completely free.

Automation

ZAP is an ideal tool to use in automation.

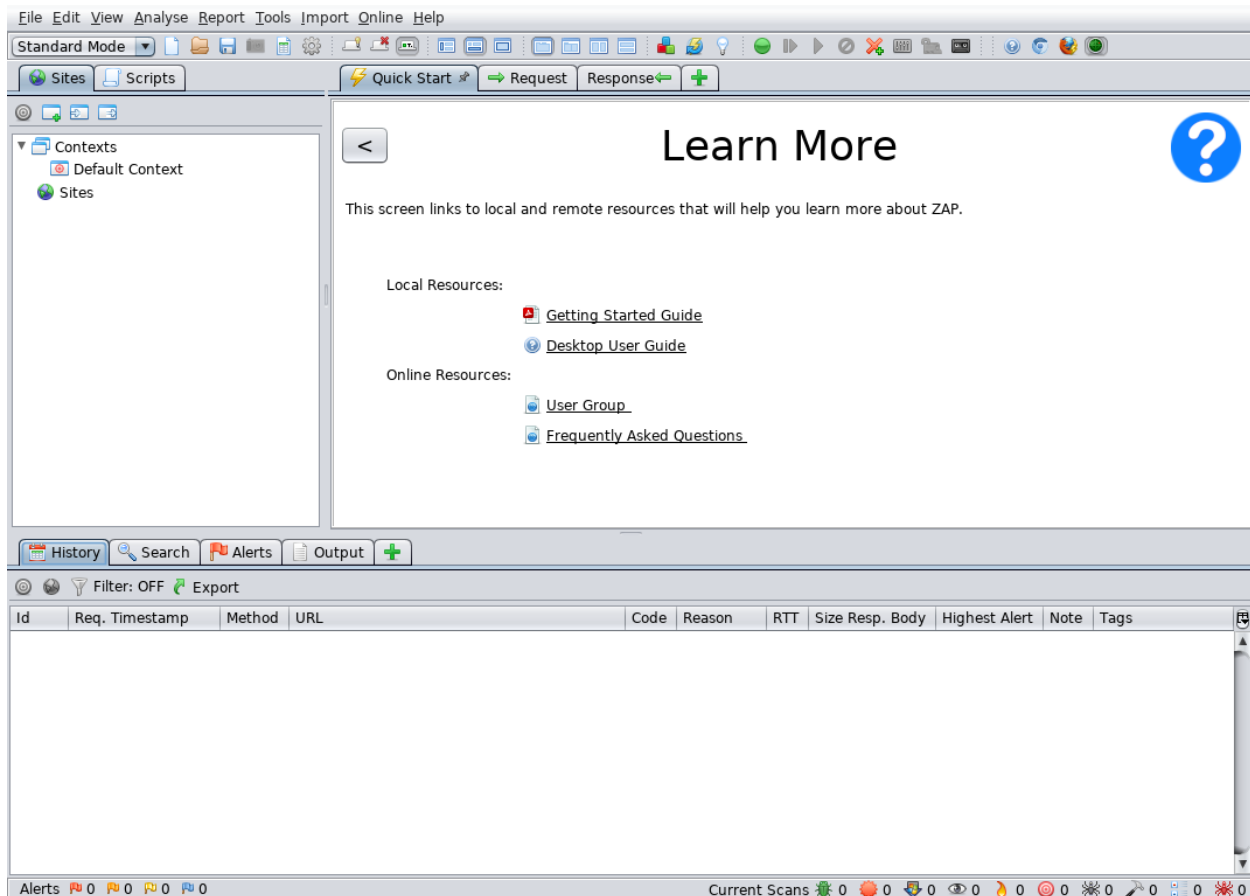
It can be run in headless mode and has a powerful API which allows you to control nearly all of the features available via the ZAP desktop.

For more details see the [ZAP wiki](#).

Learn More About ZAP

Now that you are familiar with a few basic capabilities of ZAP, you can learn more about ZAP's capabilities and how to use them from ZAP's [Desktop User Guide](#). The User Guide provides step-by-step instructions, references for the API and command-line programming, instructional videos, and tips and tricks for using ZAP.

Additional links are also available via the 'Learn More' button on the Quick Start top screen:



The page links to both local resources (if available) and online content. Additional links are included below.

Useful Links

[OWASP Zed Attack Proxy Project](#) – ZAP's main project page

[OWASP ZAP Wiki](#) – The ZAP Wiki

[OWASP ZAP Desktop User Guide](#) - The ZAP Desktop User Guide

[OWASP ZAP Hot Keys](#) - The list of ZAP hotkeys

[ZAP Users Group](#) – Google group for ZAP users

[ZAP Developers Group](#) – Google group for developers and contributors to ZAP