OWASP ZAP Documentation

DeepakVakkala (DevOps Intern)

ABOUT

ZAP(Zed Attack Proxy), Previously an OWASP Project, is now powered by checkmarx.

- The Windows and Linux versions require Java 17 or higher
- The installers are built using a multi-platform installer builder which provides an unattended mode.
- MacOS has pre-installed Java17Version in it.
- Current version Release **2.16.1**
- Introduced in 2 December 2001
- For Documentation follow https://www.zaproxy.org/docs/
- To check the Running version of ZAP https://raw.githubusercontent.com/zaproxy/zap-admin/master/ZapVersions.xml
- We can add more functionality using ZAP Marketplace (https://www.zaproxy.org/addons/)

PURPOSE

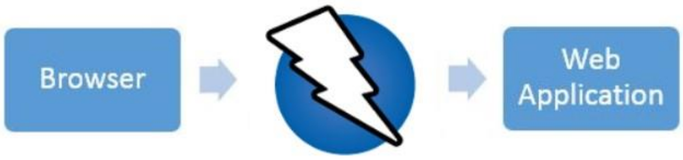
- Identify vulnerabilities: Helps security professionals, developers, and testers detect vulnerabilities in web applications.
- Automated and manual testing: Provides tools for both automated and manual security testing.
- Simulate attacks: Simulates various types of attacks to uncover weaknesses in web applications.
- Security insights: Offers valuable insights into the security posture of web applications.
- Continuous integration: Supports integration into CI/CD workflows to test vulnerabilities during development.
- Customizable: Features are customizable to suit both beginners and experienced security professionals.
- Enhance web security: Ensures web applications are secure and resilient against potential threats.

FEATURES OF OWASP ZAP

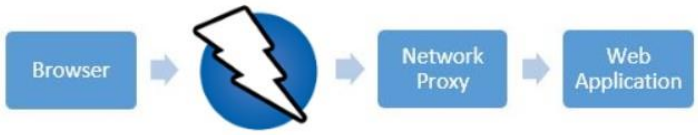
- Quick Start Tab
- Spider
- Passive and Active Scanning
- Alerts

INTRODUCTION

- ZAP by Checkmarx is a free, open-source tool for testing the security of web applications. It works as a middleman between browser and server to inspect and modify traffic.
- We can use ZAP either as a normal app with a user interface or run it quietly in the background as a service.
- It's available on all major OSes and Docker
- Being open-source, anyone can view the code, contribute fixes, add new features, or create custom add-ons

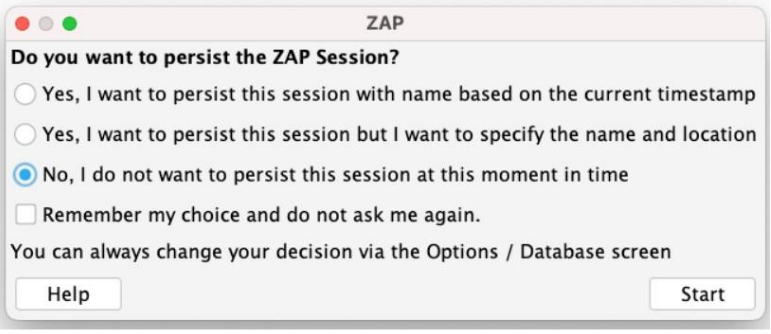


If there is another network proxy already in use, ZAP can be configured to connect to that proxy.



HOW IT WORKS

- When you open ZAP, it asks if you want to save your session. By default, it saves everything to a temporary file(HSQLDB database), which gets deleted when you close ZAP.
- If you choose to save the session, the data will be stored on your computer, and you can give it a custom name and location to access it later.



ZAP

Do you want to persist the ZAP Session?

○ Yes, I want to persist this session with name based on the current timestamp

○ Yes, I want to persist this session but I want to specify the name and location

● No, I do not want to persist this session at this moment in time

□ Remember my choice and do not ask me again.

You can always change your decision via the Options / Database screen

INSTALL AND CONFIGURE ZAP

- ZAP has installers for Windows, Linux, and macOS & for Docker Image - Standard (docker pull zaproxy/zap-stable:latest)

  For Linux Installer Package
  For Windows 32 64
  For MacOS ClickHere

  Linux Repo ClickHere
  Windows : winget install –id=ZAP.ZAP –e
  MacOS: brew install –cask zap

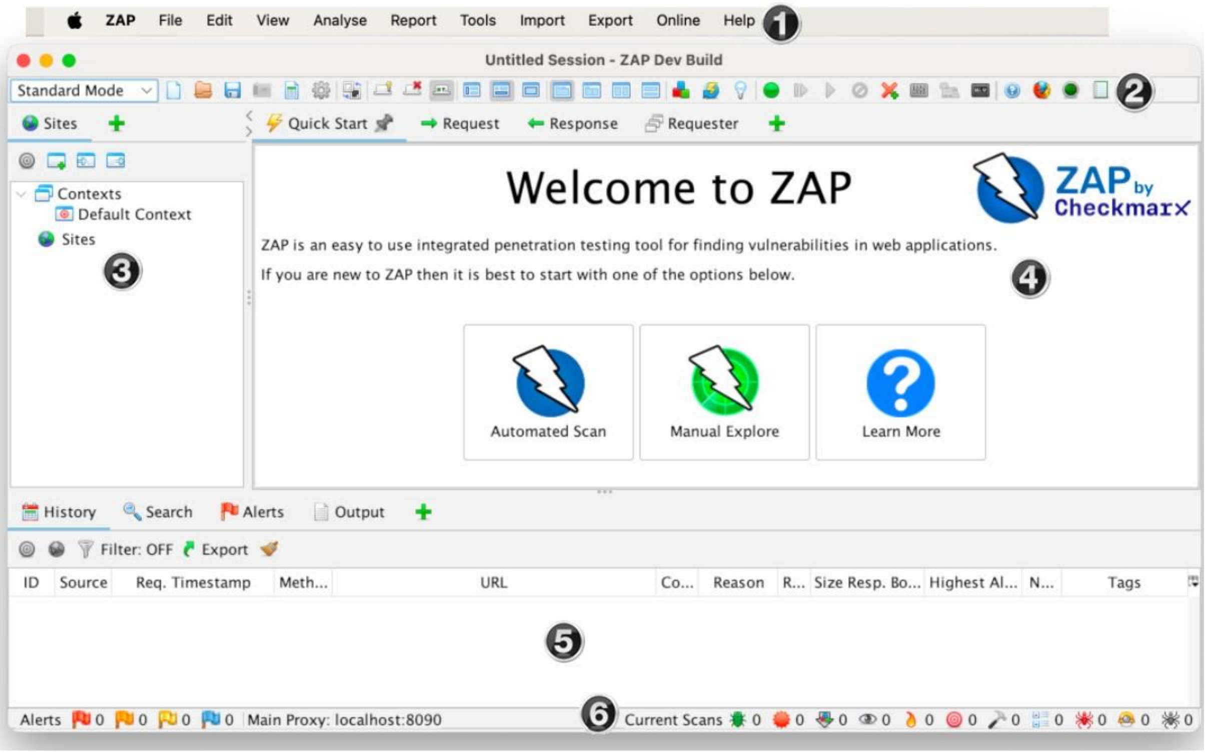
- On Windows, you might see a warning saying the ZAP file isn't commonly downloaded.
  Error **ZAP_<version>_windows.exe isn't commonly downloaded**
  To Avoid click continue,
  → Keep → Show more → Keep anyway

- In case of MacOS you might see a warning saying ZAP can't be opened because the developer isn't verified.
  To Avoid go to System Preferences > Security & Privacy, find the message about ZAP being blocked, and click Open anyway if you trust it.

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



ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

Note: Only use ZAP to test websites that you are allowed to test, especially when using the active attack option. This option acts like a real attack and can break things or change data on the site.

If you don’t want to take any risk, you can turn on safe mode in ZAP. It makes ZAP safer to use, but some features won’t work.

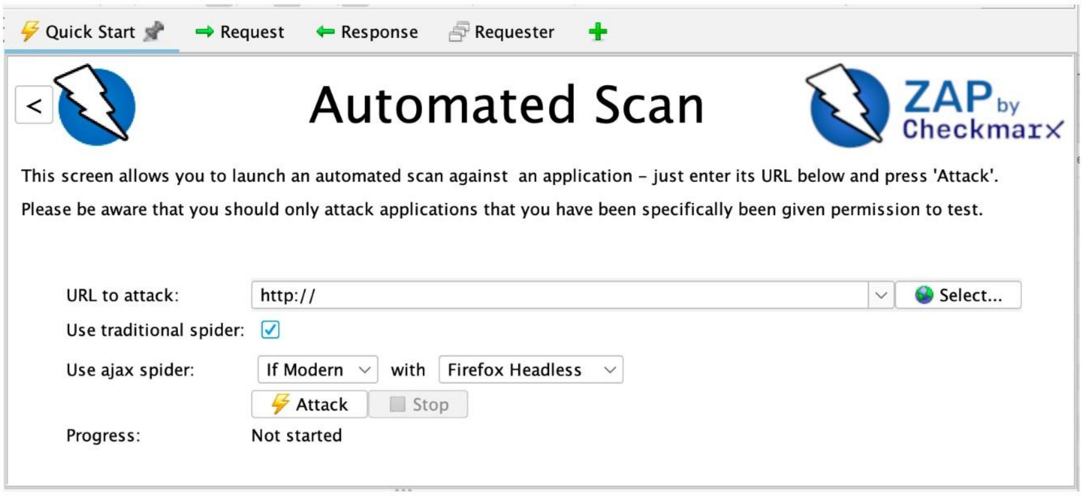
- For safe mode - Click the mode dropdown on the toolbar and select safe.

MECHANISM

The easiest way to use ZAP is through the **Quick Start** tab, which comes pre-installed with ZAP.

To run a Quick Start Automated Scan :

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



Automated Scan

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 been given permission to test.

URL to attack: http://

Use traditional spider: ☑

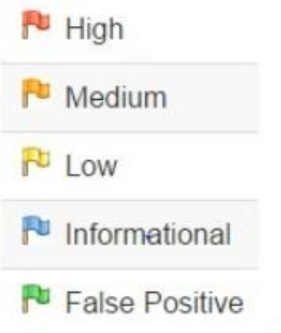
Use ajax spider: If Modern with Firefox Headless

Progress: Not started

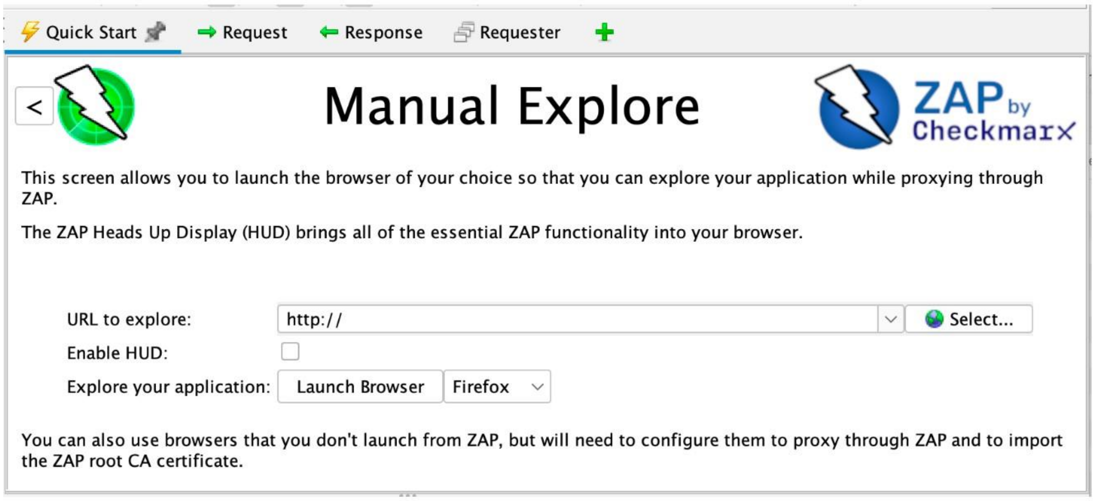
- ZAP will proceed to crawl the web application with its spider and passively scan each page it finds
- ZAP provides 2 spiders for crawling web applications
- ZAP provides 2 spiders for crawling web applications
- AJAX spider is better for modern (JavaScript-heavy) sites, as it uses a browser to follow those links, but it’s slower and needs extra setup in some cases.
- Active scanning goes a step further. It sends real attack patterns to find vulnerabilities. It can affect the system, so use it only if you have permission
- Passive scanning helps find basic vulnerabilities and gives an idea of the web app’s overall security
- As ZAP scans your web app, it builds a map of its pages, records all requests and responses, and shows alerts if it finds any issues.
- The left side of the footer shows the number of alerts found, grouped by risk levels: High, Medium, Low, and Informational.

To view alerts:

1. Click the Alerts tab in the Information Window.
2. Select an alert to see the URL and vulnerability.
3. In the Workspace Window, click the Response tab to view the response details, with the highlighted part causing the alert.



- Pages behind login screens aren't discovered unless authentication is set up in ZAP.
- Limited control over the scan sequence and attack types, though ZAP offers more options for detailed exploration and attacks.
- Passive scanning and automated attacks are useful for initial vulnerability assessments but have limitations.
- Pages protected by login are not discovered unless authentication is configured in ZAP.
- Limited control over the scan sequence and attack types in passive scanning and automated attacks.
- Spiders should be combined with manual exploration for better results, as they only enter basic data in forms.
- Always explore every page of the web application, including hidden pages, for vulnerabilities because hidden pages sometimes go live without warning or notice.
- ZAP allows launching pre-configured browsers to proxy through it for easy scanning.
- You can easily open browsers that are set up to work with ZAP by using the Quick Start tab. These browsers will also ignore any certificate errors that might normally appear.



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: http://

Enable HUD: □

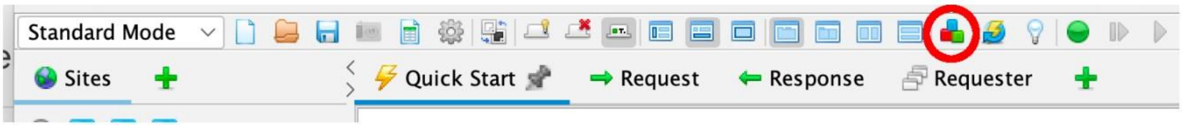
Explore your application: Launch Browser Firefox

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

MARKET PLACE



SECURITY

Software security testing is the process of finding and fixing weaknesses in a system or its data.

Here’s a simplified breakdown:

- **Assessment**: Finds security issues without trying to exploit them.
- **Testing**: Finds and tries to exploit security issues.

Common types of security testing:

- **Vulnerability Assessment**: Scans the system for security problems.
- **Penetration Testing**: Simulates hacker attacks to find weaknesses.
- **Runtime Testing**: Tests security while the system is running, like an end-user would.
- **Code Review**: Checks the code for security flaws

Penetration Testing:

- Penetration Testing (Pentesting) simulates a malicious attack to identify vulnerabilities.
- The goal is to steal data or cause harm (e.g., denial-of-service attacks).
- Pentesting is accurate with fewer false positives but can be time-consuming.
- It tests defense mechanisms, verifies response plans, and checks security policy adherence.
- Automated Pentesting helps detect new and old vulnerabilities in fast-evolving, collaborative environments.
- It is an essential part of continuous integration validation.

Cost Details of OWASP ZAP

OWASP ZAP (Zed Attack Proxy) is a free, open-source security testing tool used for detecting vulnerabilities in web applications. Although ZAP itself is free to use, there are several factors that can contribute to the overall cost of implementing and using OWASP ZAP in a real-world setting. Below are the cost details:

1. License and Core Features:

- License: OWASP ZAP is an open-source tool and free to use under the Apache 2.0 license. No licensing fees are required.

- Core Features: All core features, such as active scanning, passive scanning, fuzzing, vulnerability detection, and automated scanning, are available for free.

2. Hosting and Infrastructure Costs:
   - Costs related to cloud services (AWS, Azure, Google Cloud) when hosting ZAP on virtual machines or containers.
   - Costs for compute resources, data transfer, storage, and network usage based on the hosting environment.
   - On-premise hosting will involve infrastructure maintenance, server costs, and network bandwidth costs.

3. Automation and Integration Costs:
   - Integrating ZAP with CI/CD tools like Jenkins, GitHub Actions, or GitLab can lead to additional costs for these platforms and associated resources.
   - Automating scans using tools like Docker or Kubernetes might incur additional infrastructure management costs.

4. Add-ons and Extensions:
   -Free Extensions: ZAP provides a wide range of free extensions for various features such as authentication handling and custom scripts.
   - Premium Features: Some third-party providers offer paid add-ons or extensions that might enhance ZAP's capabilities.

5. Professional Support:
   - ZAP offers community-based support, but organizations may need to pay for professional services or enterprise support contracts.
   - Commercial support might include service-level agreements (SLAs), bug fixes, consultations, or dedicated support teams.

6. Maintenance and Update:
   - Regular updates are necessary to keep ZAP in sync with the latest vulnerabilities and security techniques.
   - Maintenance costs involve staying up-to-date with new releases, security patches, and updates for integrations.

Factors Affecting the Cost of OWASP ZAP

While OWASP ZAP itself is free, the total cost can be affected by a number of factors, including the scale of implementation, usage, and the extent to which it is integrated with other tools. Below are the key factors that can affect the cost of using OWASP ZAP:

1. Infrastructure Requirements:
   - The need for compute resources, storage, and network capacity increases as the scale of testing grows, especially for large-scale scans.
   - Cloud hosting or on-premise servers will have direct implications for cost depending on the

resource usage.

2. Scalability and Performance:
    - High-frequency or high-volume scans require more processing power, leading to higher infrastructure costs.
    - The complexity of web applications or the number of domains being tested directly impacts the scalability needs and resource allocation.

3. Automation and Continuous Integration:
    - Automating ZAP scans through CI/CD tools increases both the flexibility and the operational complexity, requiring additional configuration and management resources.
    - Integrating with other DevOps tools like Jenkins, GitHub, or GitLab to trigger ZAP scans introduces operational overhead.

4. Customization and Extensions:
    - Although many ZAP features are free, organizations may require custom extensions or plugins that introduce development and maintenance costs.
    - Custom integrations with other security testing tools or SIEM systems may also increase costs.

5. Integration with Third-Party Tools:
    - ZAP is often integrated with various security tools such as vulnerability management platforms, authentication services, and reporting tools.
    - These integrations may require ongoing costs related to development, configuration, and testing.

6. Training and Skill Development:
    - Teams need to be trained to use ZAP effectively, interpret scan results, and integrate the tool into security workflows. This can require investments in training sessions or resources.
    - Specialized knowledge is needed for interpreting vulnerability reports and for developing custom configurations or integrations.

7. Support and Maintenance:
    - Support requirements might differ based on the level of expertise within the organization.
    - Businesses may need to allocate resources for troubleshooting, ongoing maintenance, and periodic updates.

REFERENCES

- OWASP ZAP Official Website
- ZAP User Guide

CONCLUSION

OWASP ZAP is a powerful tool for identifying security flaws in web applications. It is suitable for both new testers and seasoned security professionals. Through its automated and manual features, ZAP allows for effective vulnerability discovery and provides the necessary alerts to help strengthen web application security.