

# Complete OWASP ZAP Guide



Vasileiadis A. (CyberKid) · [Follow](#)

12 min read · Sep 4, 2024



Having trouble finding an OWASP ZAP tutorial that shows you how to use it effectively?

ZAP is an extremely powerful tool for end-to-end testing. It is often used by people who want to take an in-depth look at a web application.

In this tutorial, we'll walk you through its setup and show you an overview of its main interface and some of its features. We will shortly discuss the comparison between ZAP and Burp Suite and show you how to run tests with ZAP.

We'll show you how to use spidering, passive and active scanning, and give you a good start on using ZAP. As you gain confidence, you will be able to discover its other tools.

If you're ready to learn how to use ZAP, let's get started.

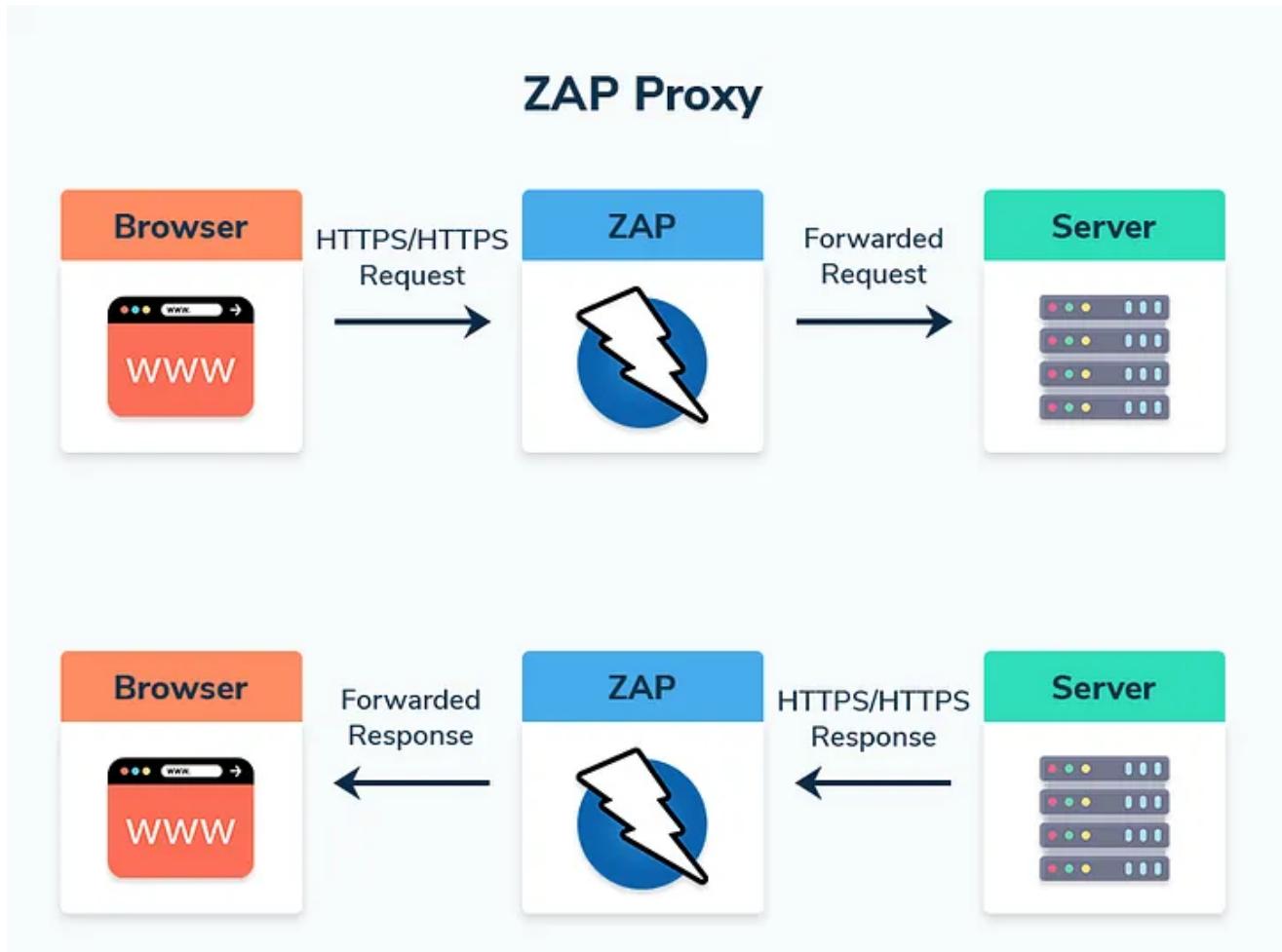
## What is ZAP?

Zed Attack Proxy (ZAP) is an open source penetration testing tool, formerly known as OWASP ZAP. It is a multi-dimensional tool often used by penetration testers, bug bounty hunters and developers to scan web applications for security risks during the application testing process.

ZAP offers many features including active and passive scanning and API testing capabilities.

In essence, it is a proxy that acts as a “manipulator-in-the-middle”. It allows you to see all the requests you make to a web application and all the responses you receive from it, enabling you to identify vulnerabilities and potential attack vectors in real time.

By intercepting and modifying the traffic between your browser and the web application, ZAP helps you understand how the application behaves under different scenarios and conditions.



## ZAP proxy

ZAP can be installed on Windows, Linux and macOS. Docker images are also available. We will show you how to install it on Kali Linux.

## The ZAP Open Source Program

ZAP recently joined the Software Security Project (SSP) as one of its founding projects. Despite being free and open source, ZAP has grown into the most popular web scanning tool worldwide and competes directly with commercial projects.

We spoke to Simon Bennetts, the project's founder, who admitted: "We're competing against commercial companies with hundreds of employees... So it's tough."

ZAP is a not-for-profit company run entirely by Bennetts and supported by a small team of dedicated volunteers.

Acknowledging this challenge, Bennetts said, “We’re always looking for people to contribute — ZAP is a shared project.” This call for community involvement speaks volumes for ZAP’s collaborative approach. See ZAP’s contribution guide for ways to get involved.

The project depends on sponsors to raise money, and the Crash Override Open Source Fellowship supports its development. However, ZAP will remain independent.

ZAP encourages users to contribute to the Software Security Project (SSP) to help fund ZAP and other important open source projects.

## ZAP with Numbers

### Title Statistics for February 2024:

- Number of ZAP starts: 4.708.566
- Number of active scans: 922.722
- Number of notifications: 1.123.926.095
- Number of active scan messages sent: 3.274.968.334

## ZAP vs. Burp Suite

ZAP and Burp Suite are similar tools for web application security. However, ZAP is faster and lighter than Burp Suite, and it’s open source and free.

The free version of Burp Suite may be limited in its functionality. There is a paid version with more advanced features, but many of these tools are already included in ZAP.

For example, Burp Suite’s auto-scan feature is only available in its professional version, while ZAP has the same functionality called “ATTACK Mode.”

Burp Suite has an intruder tool, although it is limited to single-core operation. ZAP has an equivalent tool called “Fuzzer.”

ZAP also has features not found in the Burp Suite, such as an automation framework that allows you to control ZAP via a YAML file and a HUD (heads-up display). With the HUD, you can use your favorite ZAP features inside the browser.

## Burp Suite to ZAP Feature Map

Burp Suite ZAP Collaborator (Community) OAST Support Add-on Compare Diff Decoder Encoder DOM Invader Eval Villian Add-on Extender Marketplace, Scripts Intercept breakpoints Intruder (Throttled) Fuzzer Live scan (Community) ATTACK Mode Project Files (Community) Session Files proxy proxy Repeater Manual Request Editor, Requestor Add-on Scanner (Community) Active Scanner Sequencer Token Generation and Analysis Target contexts

## Setting up Zed Attack Proxy on Kali Linux

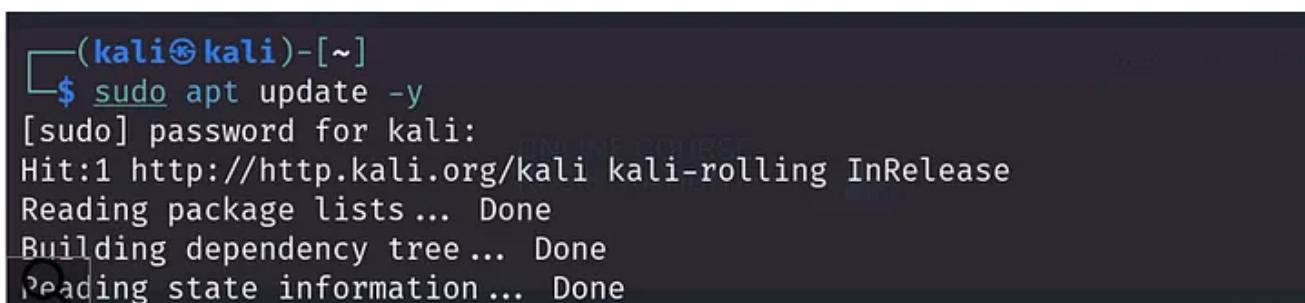
Let's go through the ZAP installation process from start to finish.

### Installing ZAP on Kali Linux

ZAP is not installed in the current version of Kali, which is 2024.1 at the time of this writing. However, it can be easily installed.

Before installing, always update the repositories to ensure the latest version with the command:

```
sudo apt update -y
```



```
(kali㉿kali)-[~]
$ sudo apt update -y
[sudo] password for kali:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Once done, you can install ZAP with the command:

```
sudo apt install zaproxy
```

```
(kali㉿kali)-[~]
$ sudo apt install zaproxy
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libboost-dev libboost1.83-dev libopenblas-dev libopenblas-pthread-dev libopenblas0 libpython3-all-dev libpython3.12
  libpython3.12-dev libxsimd-dev python3-all-dev python3-beniget python3-gast python3-pythran python3.12-dev xtl-dev
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  zaproxy
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 197 MB of archives.
After this operation, 248 MB of additional disk space will be used.
Get:1 http://mirror.accuris.ca/kali kali-rolling/main amd64 zaproxy all 2.14.0-0kali1 [197 MB]
Fetched 197 MB in 5s (40.4 MB/s)
Selecting previously unselected package zaproxy.
(Reading database ... 413600 files and directories currently installed.)
Preparing to unpack .../aproxy_2.14.0-0kali1_all.deb ...
Unpacking zaproxy (2.14.0-0kali1) ...
Setting up zaproxy (2.14.0-0kali1) ...
Processing triggers for kali-menu (2023.4.7) ...
```

## Proxy Setup

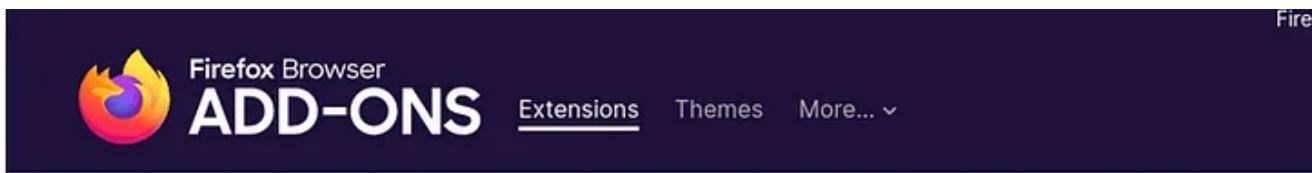
You don't need to set up a proxy like FoxyProxy for your browser like in Burp Suite, as ZAP handles it all. Bennetts tells us that "it's best to let ZAP launch them."

The "Browser Launch" function is automatically configured to work through ZAP and ignore certificate warnings, making it much easier to launch without changing settings. This allows you to quickly start web application testing without additional setup or configuration. Just launch ZAP and you're good to go.

However, if you want to use any of your browsers with an existing profile, like other browser plugins, you must manually configure your browser to use ZAP and import and trust ZAP's CA Certificate.

We'll show you how to set it up in Firefox on Kali.

The first thing you need to do is download it [add FoxyProxy](#).



The screenshot shows the Firefox Add-ons page for the "FoxyProxy Standard" extension. At the top, there's a logo of a fox, the extension name "ADD-ONS", and navigation links for "Extensions", "Themes", and "More...". A "Recommended" badge with a trophy icon is visible. Below the extension details, there's a description: "FoxyProxy is an open-source, advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. No paid accounts are necessary; bring your own proxies or buy from any vendor. The original proxy tool, since 2006." To the right, a large blue button with the text "Add to Firefox" is highlighted with a red border and a red arrow points towards it.

## FoxyProxy Standard by Eric, erosman

FoxyProxy is an open-source, advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. No paid accounts are necessary; bring your own proxies or buy from any vendor. The original proxy tool, since 2006.

Add to Firefox

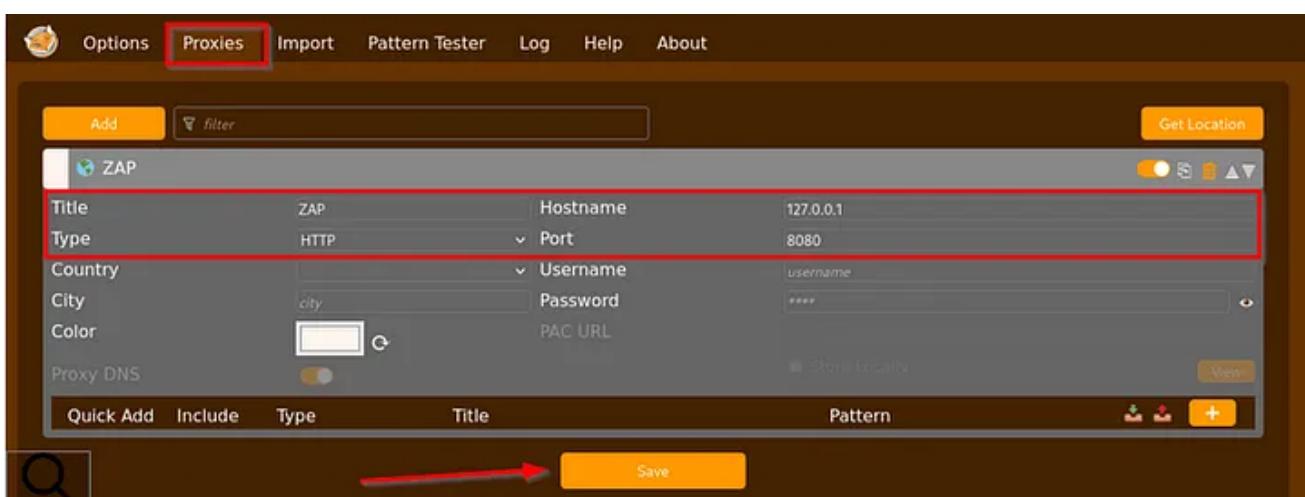


Then open FoxyProxy to set it up.

From here, go to the proxies tab and enter the following information:

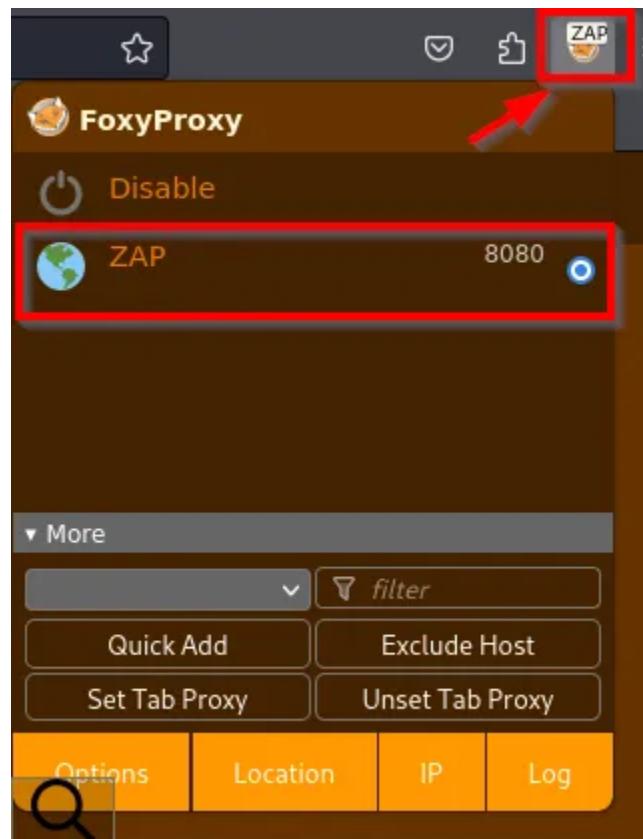
- Title: ZAP
- Type: HTTP
- Hostname: 127.0.0.1
- Port: 8080

Once you're done, click "Save."



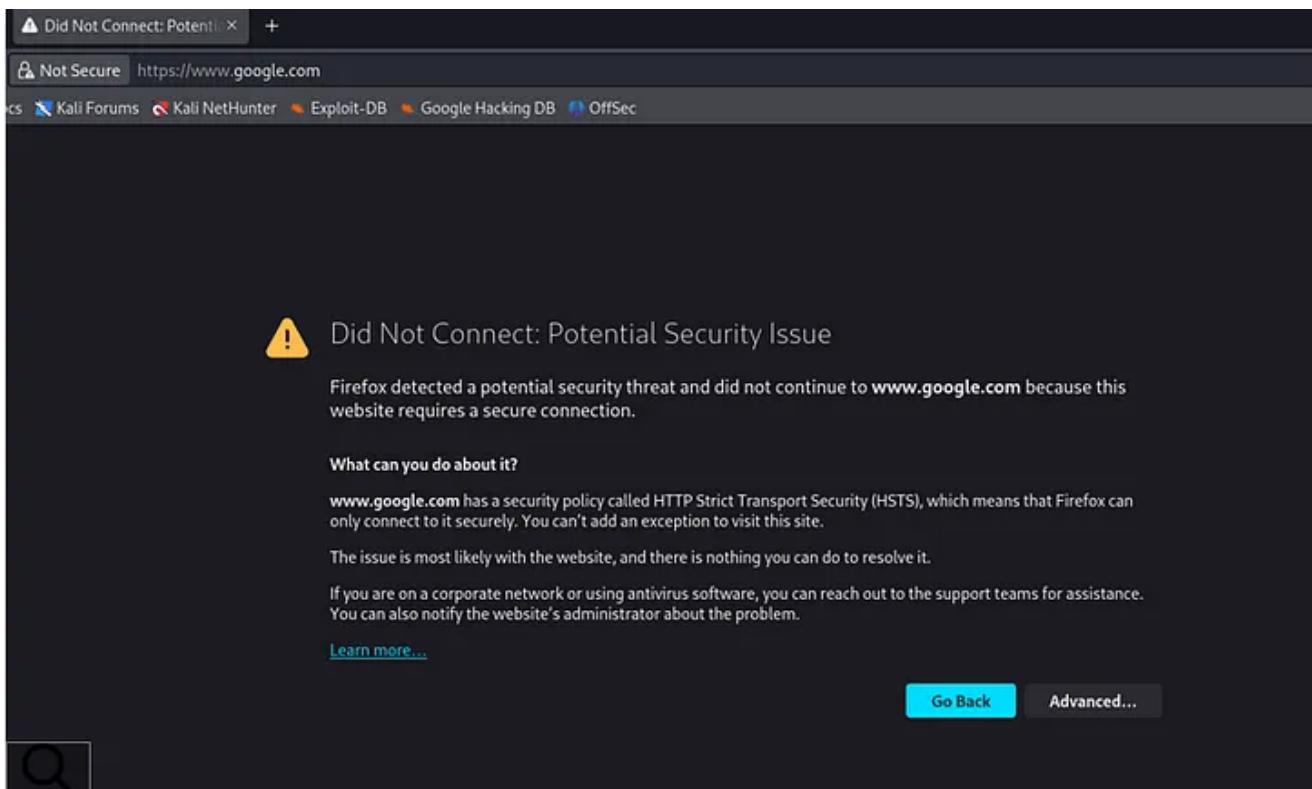
The screenshot shows the FoxyProxy configuration interface. The "Proxies" tab is selected. A table lists a single proxy entry: "Title" is "ZAP", "Type" is "HTTP", "Hostname" is "127.0.0.1", and "Port" is "8080". The "Save" button at the bottom right is highlighted with a red arrow.

Whenever you want to promote traffic through ZAP, go to the plugin and select “ZAP.”



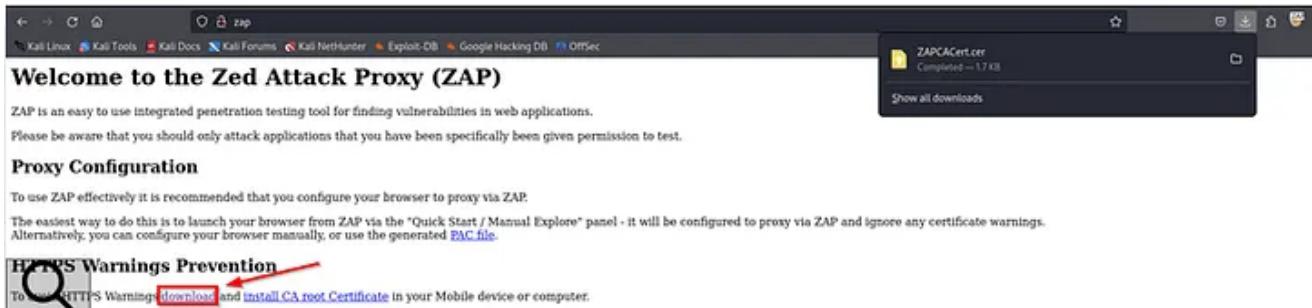
## ZAP Certificate Installation

If you are not using ZAP’s built-in browser feature, you will need to manually set up the certificate in your browser. If you try to access any website that uses SSL/TLS while using your browser outside of ZAP, you must set it to use ZAP’s CA certificate to avoid any certificate warnings.



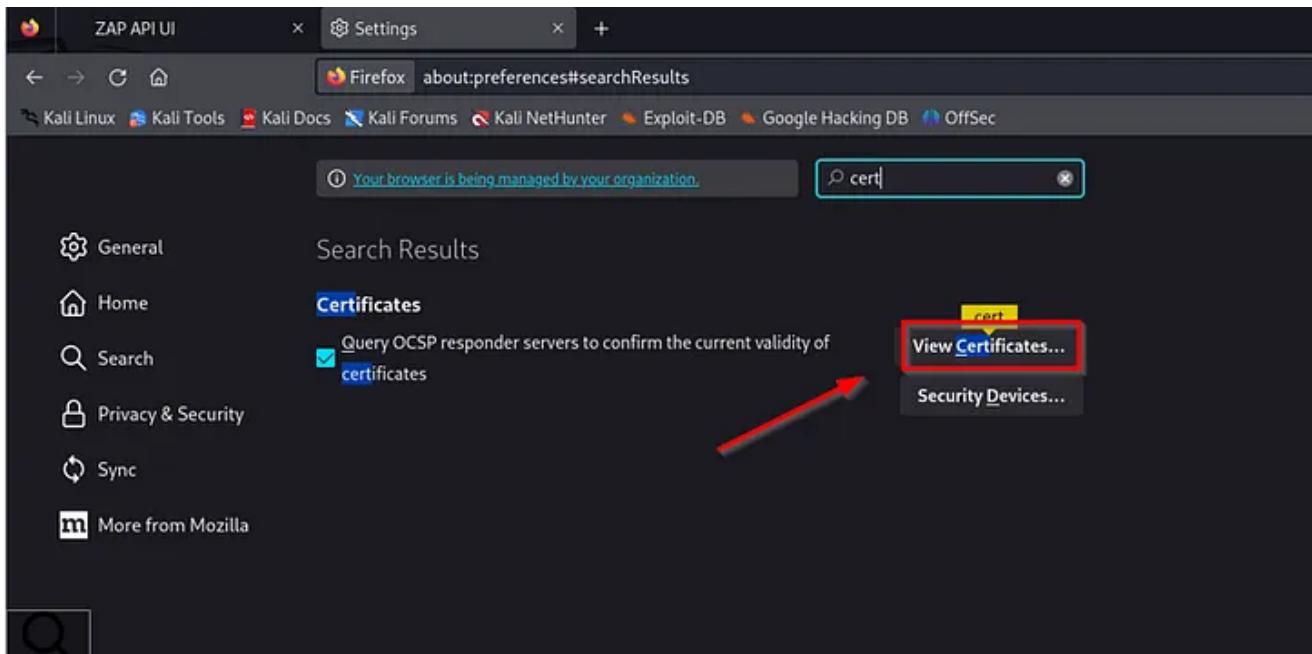
ZAP recommends launching your browser through the “Quick Start” area, but if you prefer to set up your browser manually, here’s how to install the certificate. We install it in Firefox.

First, with ZAP enabled and FoxyProxy enabled to use ZAP, go to <http://zap>. Once there, select “Download” to download the certificate to your system.

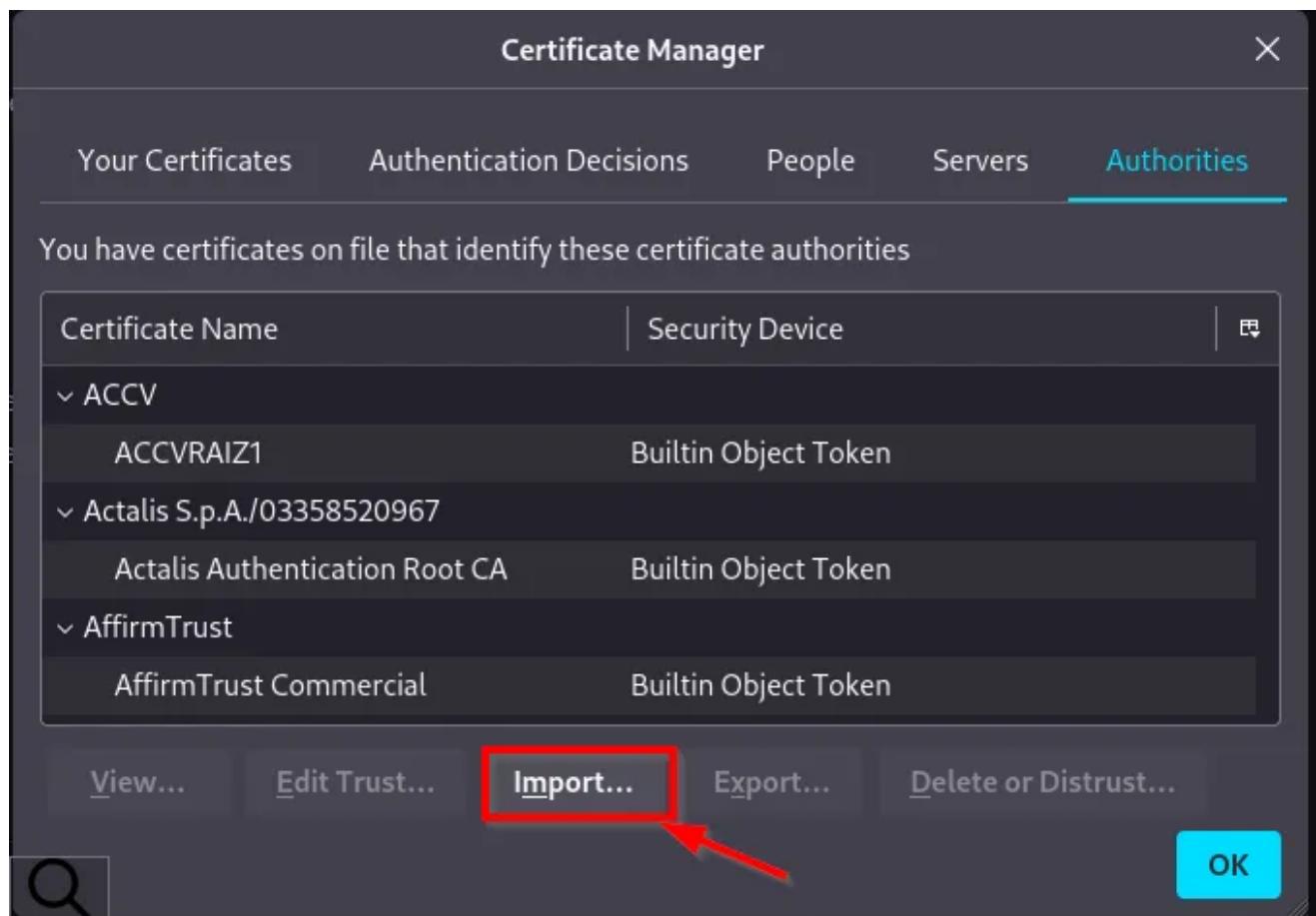


Then go to the Firefox search bar, type about

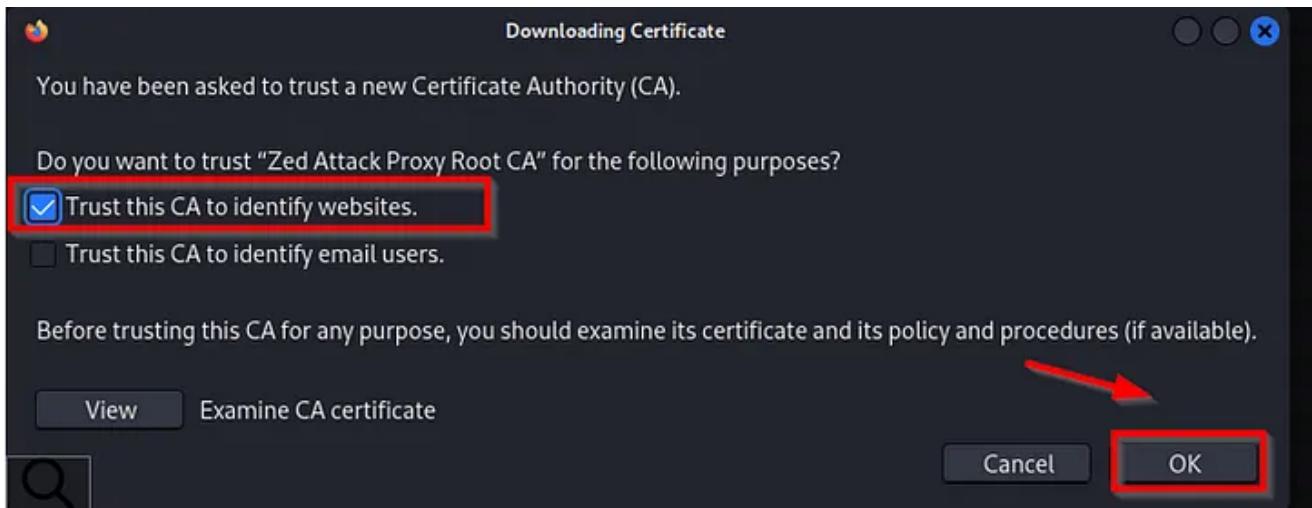
and press Enter. This will take you to the settings page. Search for “certificates” and find the option “View Certificates.”



The “View Certificates” button allows you to view all your trusted CA certificates. You can import a new certificate for ZAP by clicking “Import” and selecting the file you downloaded.



In the pop-up window, select “Trust this CA to identify websites” and click OK.

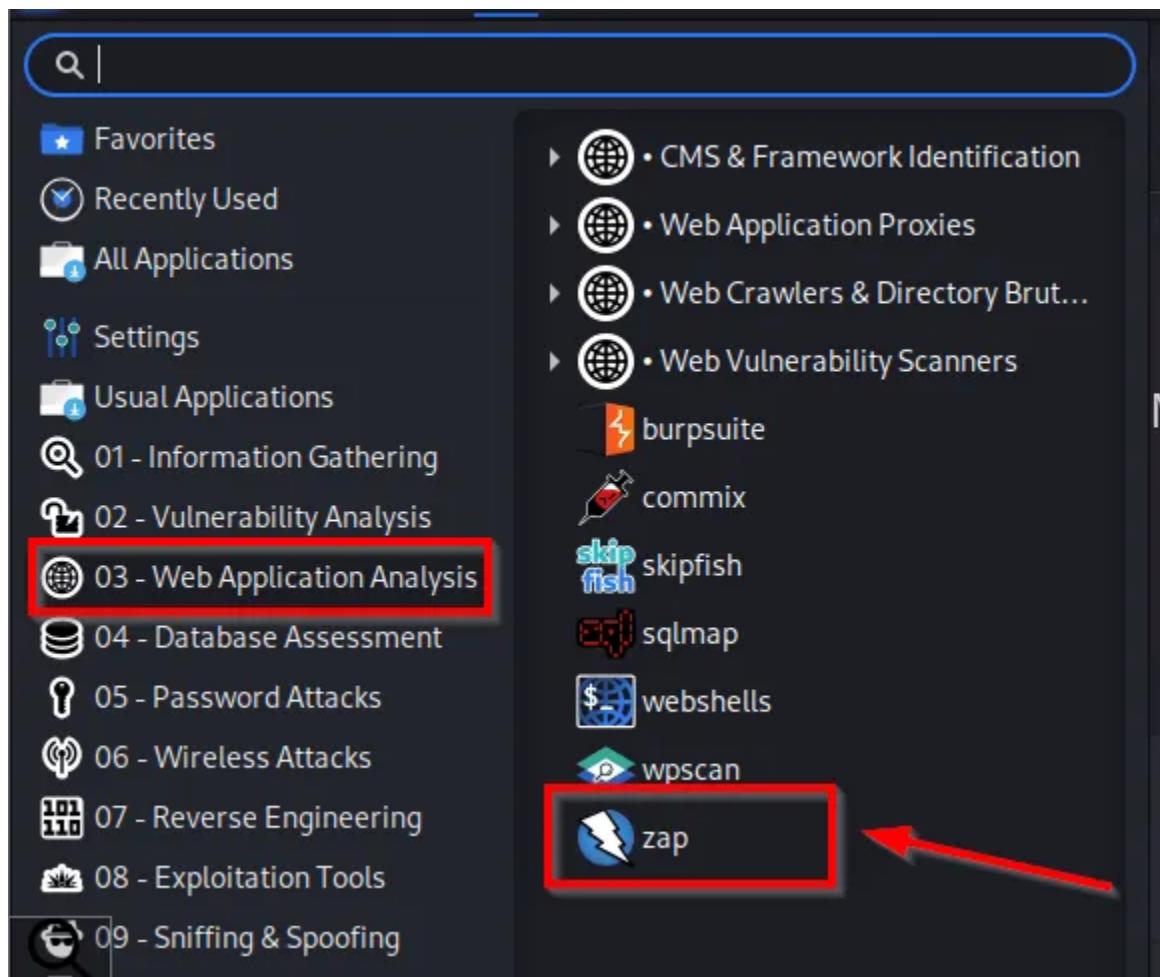


Any encrypted traffic will work when the ZAP proxy is active, allowing us to intercept requests.

Now that everything is set up, in the next section we'll walk you through using some of ZAP's features. ZAP has a lot of tools, but we won't be able to cover them all here. We'll show you a few to get you started.

## Starting ZAP

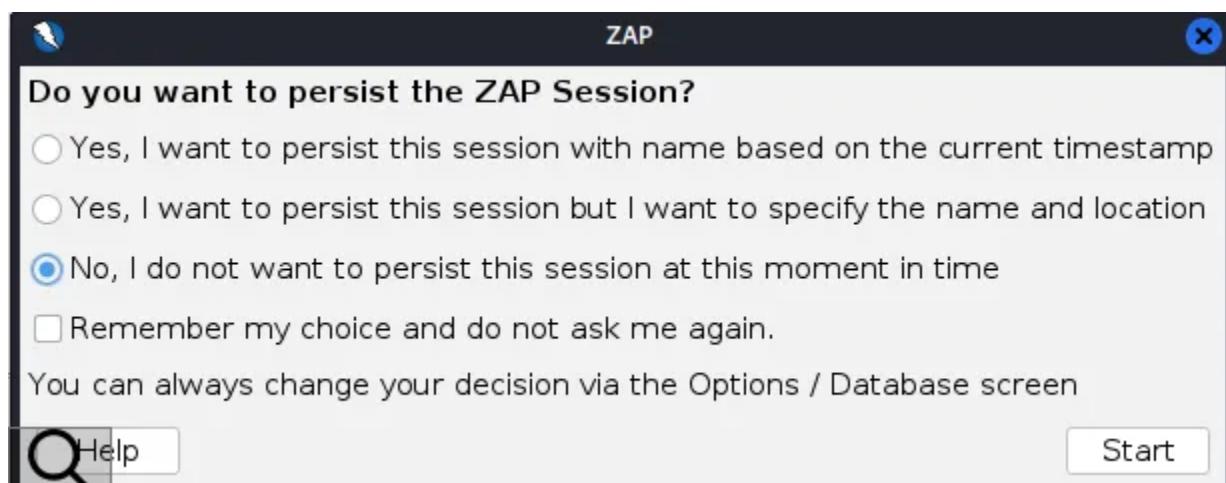
You can start ZAP in Kali in one of two ways: by entering zaproxy in the terminal or by opening it from the application menu under “Web Application Analysis.”



When you start ZAP, you will see a screen asking, “Do you want to keep this ZAP session?”

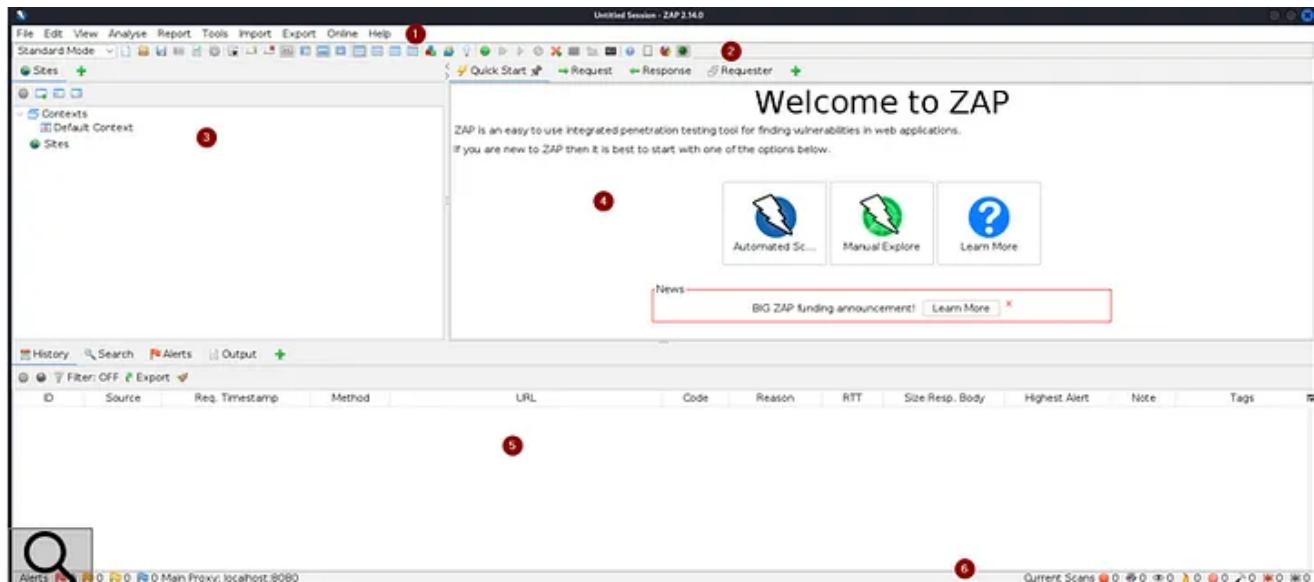
Retention will store everything in an HSQL database that you can access to view its contents or reload into ZAP to view all request history, site information, etc.

We'll select “No, I don't want to keep this session right now.”



## Overview of ZAP

Before we start using ZAP, let's take a look at the main interface and show where some of the main features are located. The interface has a lot of information, but remember, ZAP does a lot of things.



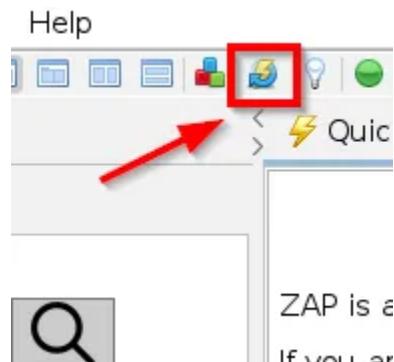
- **Menu:** Here you can create and manage sessions, generate reports, find tools, get help and more.
  - **Toolbar:** It includes buttons that provide shortcuts to the most frequently used features.
  - **Tree Window:** Displays the hierarchical view of the site you are testing and the script tree.
  - **Quick Start/Task Window:** This is a quick and easy way to use ZAP, especially if you are new to it. It also displays requests, responses, and scripts that you can edit.
  - **History tab:** Displays a log of all HTTP requests and responses sent and received through ZAP.
  - **Search Tab:** Allows you to search through requests and responses.
  - **Notifications Tab:** Displays security alerts found during scans.
  - **Exit Tab:** Provides detailed output from various scans and processes.

- **Footer:** Displays ZAP status information.
- **Notification Counter:** Displays a summary of the notifications found. It is colored (such as red, yellow, etc.) to represent the severity of alerts found during the scanning process.
- **Main Proxy:** This is the primary proxy setting that ZAP uses, which is set to “localhost:8080.”
- **Current Scans:** This section displays any current scans, with icons indicating their status or progress.

## Updating Extensions

Before you start using ZAP, you should always check and update any extensions that need updating. This ensures you have the latest experience.

Press CTRL + U or use the toolbar shortcut to check for updates.



This will open the installed extensions. Next to each extension, you can see the version number and a brief description of what it does. If a newer version of an extension is available, you'll see “Update” to the right of the description.

You can choose the ones you want to update individually, but the best way is to update everything at once.

Select any extension and “Update All” to start the update.

Description	Update	
The release status Active Scanner rules	100%	<input type="checkbox"/>
Allows you to spider sites that make heavy use of JavaScript using Crawljax	53%	<input type="checkbox"/>
Allows you to automate the changing of alert risk levels.	100%	<input type="checkbox"/>
Helps identify and set up authentication handling	100%	<input type="checkbox"/>
Automation Framework.	100%	<input type="checkbox"/>
Handles all of the calls to ZAP services.	100%	<input type="checkbox"/>
A common library, for use by other add-ons.	43%	<input type="checkbox"/>
Provides database engines and related infrastructure.		<input type="checkbox"/>
Displays a dialog showing the differences between 2 requests or responses. It us...		<input type="checkbox"/>
List of directory names to be used with Forced Browse or Fuzzer add-on.		<input type="checkbox"/>
DOM XSS Active scanner rule		<input type="checkbox"/>
Adds encode/decode/hash dialog and support for scripted processors as well		<input type="checkbox"/>
Forced browsing of files and directories using code from the OWASP DirBuster tool		<input type="checkbox"/>
Advanced fuzzer for manual testing		<input type="checkbox"/>
A short Getting Started with ZAP Guide		<input type="checkbox"/>
Provides the GraalVM JavaScript engine for ZAP scripting		<input type="checkbox"/>

dialogue with the selected Context.

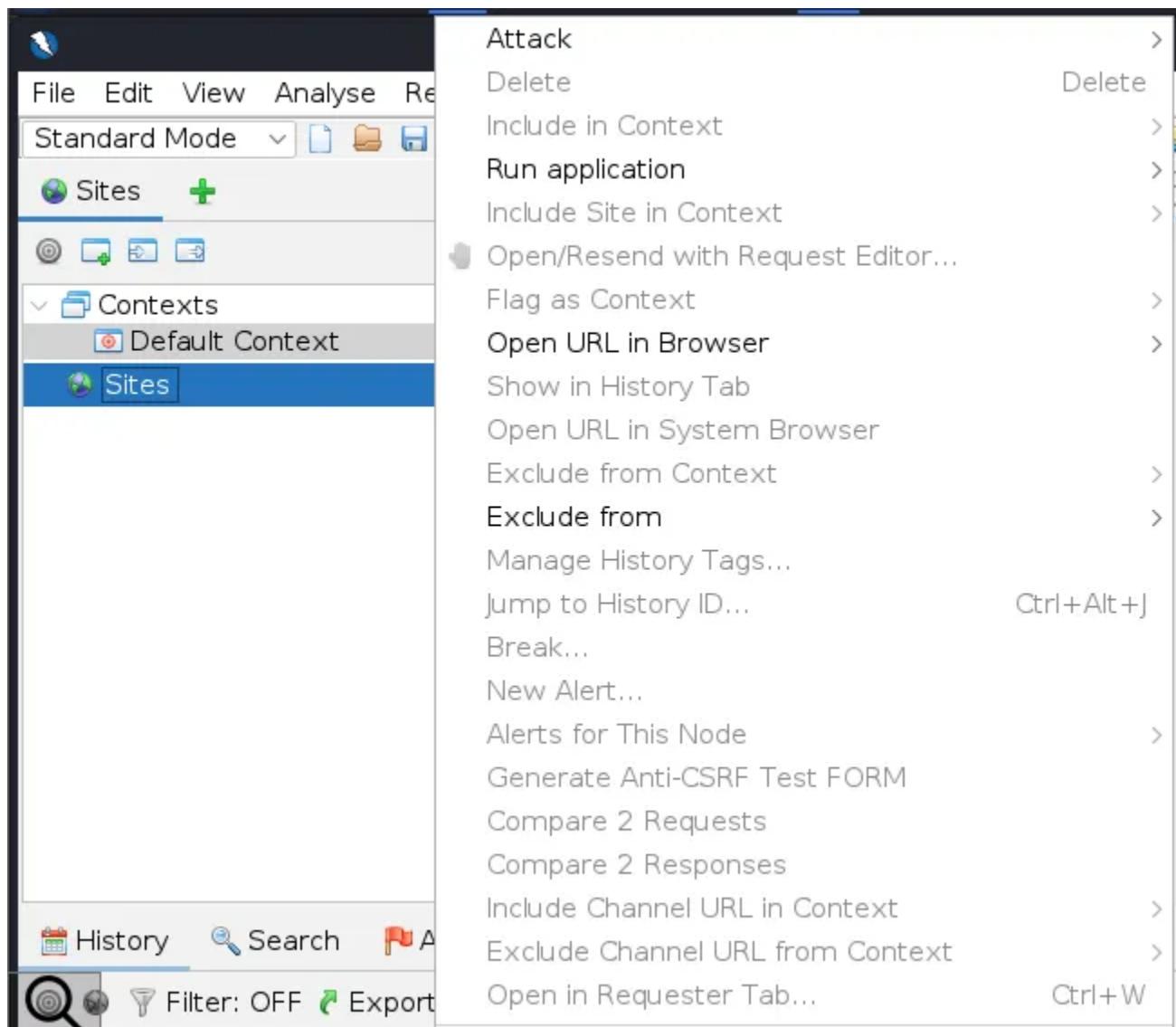


Uninstall Selected
Update Selected
Update All
Close

## Tips for ZAP

Before we get started, here are some tips to keep in mind when using ZAP.

- Right-click everywhere and anywhere to see what options are available to you.



- If you need help, you can use the detailed ZAP user guide found by pressing F1.

The screenshot shows the 'The ZAP Desktop User Guide' window. The left sidebar contains a search bar and links to 'Search', 'Favorites', 'Contents', and 'Index'. A 'Find:' input field is also present. The main content area is titled 'ZAP Desktop User Guide' and contains the following text:

Welcome to the Zed Attack Proxy (ZAP) Desktop User Guide.

This is available both as context sensitive help within ZAP and online at <https://www.zaproxy.org/docs/desktop/>.

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

It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing.

ZAP provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually.

ZAP can also be run in a completely automated way - see the [ZAP website](#) for more details.

If you are new to ZAP then its recommended that you look at the [Getting Started](#) section.

ZAP is a fork of the open source variant of the [Paros Proxy](#).

**See also**

[Getting Started](#) for details of how to start using ZAP  
[Features](#) for details of various features provided by ZAP  
[UI Overview](#) for an overview of the User Interface

## Spidering with ZAP

The first tool we'll show you is the standard ZAP spider. This spider requests web pages and analyzes them for links to other pages within the same web application. This recursive process continues as new links are discovered.

The spider builds the website tree, showing you all the pages found.

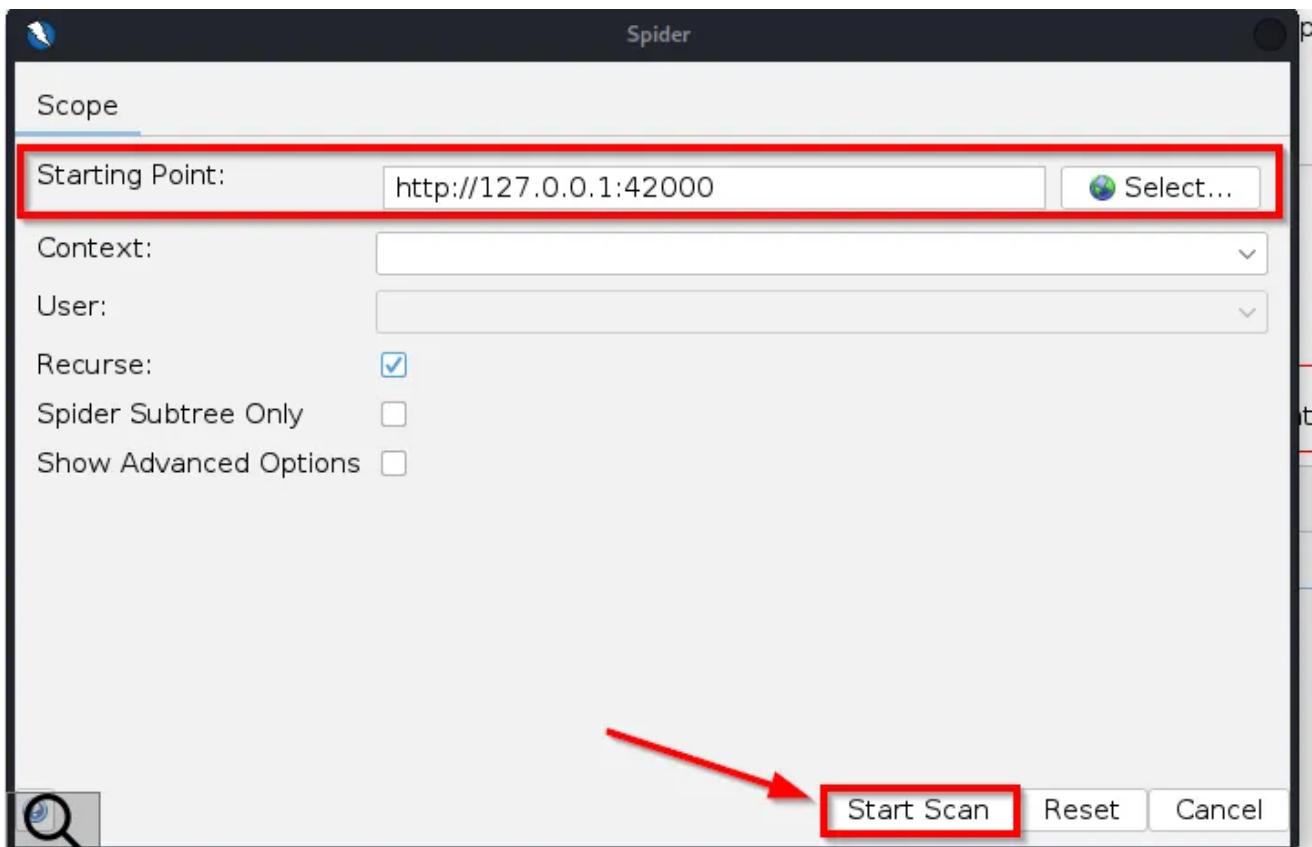
This spider is quite fast and can be used for typical applications. However, you should consider using this spider in conjunction with the AJAX spider for more modern applications.

You can select “Spider” from the “Tools” menu or use the shortcut CTRL + ALT + S to launch it.

Browse API	
Toggle Break on All Requests	Ctrl+B
Toggle Break on All Responses	Ctrl+Alt+B
Submit and Step to Next Request or Response	Ctrl+S
Submit and Continue to Next Breakpoint	Ctrl+C
Bin Request or Response	Ctrl+X
Add a Custom HTTP Breakpoint...	Ctrl+A
Active Scan...	Ctrl+Alt+A
Run the Garbage Collector	
Encode/Decode/Hash...	Ctrl+E
🕒 Manual Request Editor...	Ctrl+M
Open Message in Requester Tab...	Ctrl+W
✳️ AJAX Spider...	Ctrl+Alt+X
Retest...	
Fuzz...	Ctrl+Alt+F
WebSocket Message Editor	
Spider...	Ctrl+Alt+S
Replacer Options	Ctrl+R
👤 Authentication Tester...	Ctrl+T
🔍 Options...	Ctrl+Alt+O

In the window that appears, enter the URL of the web application you are scanning and select “Recurse.” This tells ZAP to scan all URLs or directories from the original URL.

Once you are ready, select “Start Scan.”



Once the scan is complete, you will see all the items found for the web app. The lower right corner indicates “Nodes Added: 69,” which tells us the number of new items Spider has found and added to the Site Tree during the scan.

The screenshot shows the ZAP interface after a scan. On the left, the Site Tree shows a large number of URLs under the root node 'http://127.0.0.1:42000', which is highlighted with a red box. The main panel displays the 'Welcome to ZAP' page with various buttons like 'Automated Scan', 'Manual Explore', 'Support', and 'Learn More'. The status bar at the bottom right shows 'Nodes Added: 69', also highlighted with a red box. The bottom navigation bar includes tabs for 'History', 'Search', 'Alerts', 'Output', 'Spider', and 'Requester'.

## AJAX Spidering

Most modern applications use JavaScript, and the traditional ZAP spider doesn't really understand how to crawl those properly.

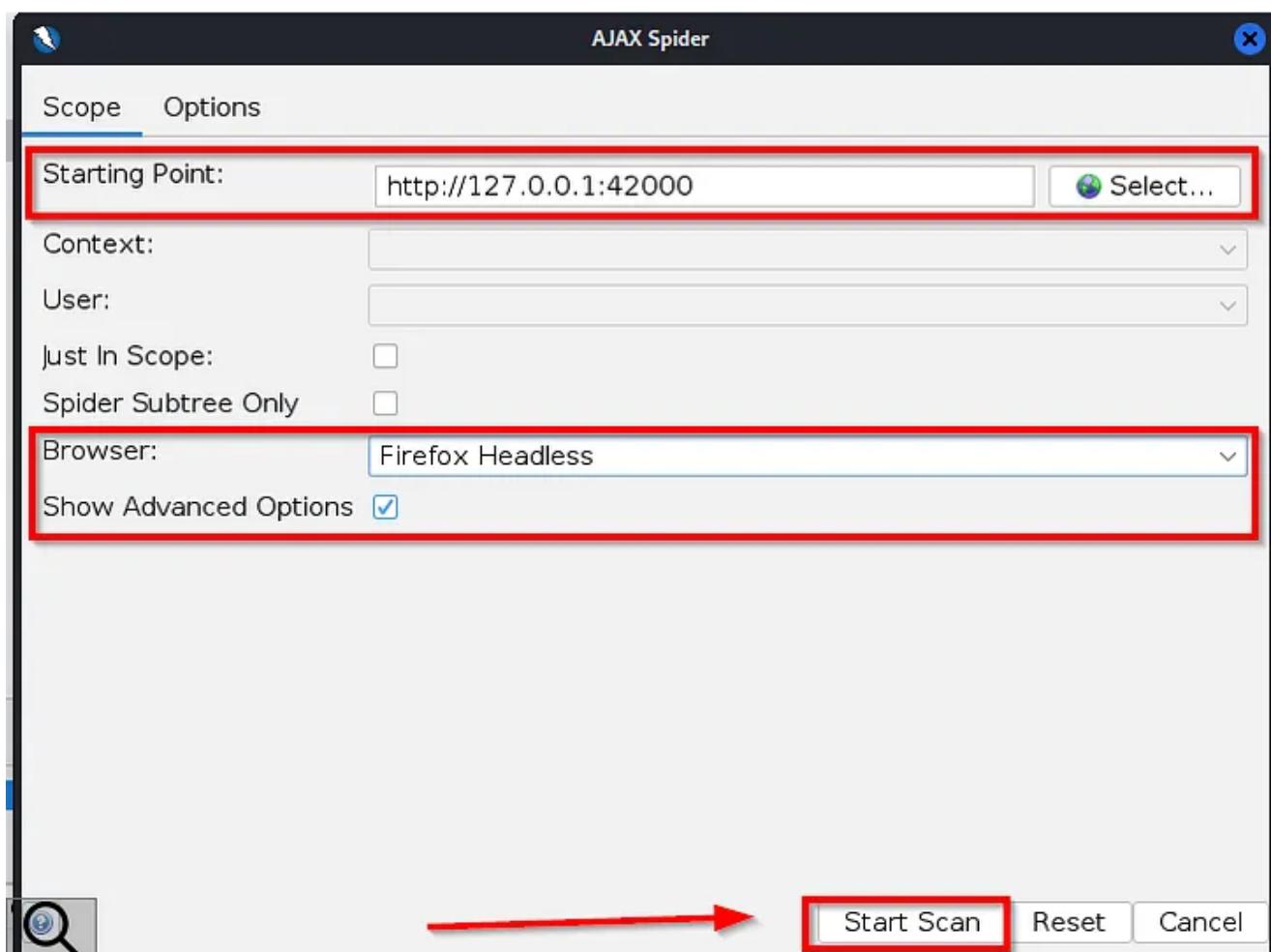
This is where the AJAX spider comes in. This spider launches a browser, clicks things, and even fills out forms, giving you a more complete overview of your web application. It tries to mimic the behavior of a user while interacting with the application.

This spider is much slower than the standard one, but works much better with today's modern applications.

To open the AJAX spider, use the “Tools” menu or the shortcut CTRL + ALT + X.

Here, you'll set the URL of the application you want to test and the browser the spider will use. Options include Firefox, Chrome and Safari.

You can also set advanced options. When you are ready, select “Start Scan.”



Once the scan is complete, all items found will appear in the site tree area with a red spider next to them. The AJAX spider crawled 1103 URLs compared to 116 for the standard spider.

The screenshot shows the ZAP interface with a red box highlighting the 'Crawled URLs:1103' tab in the bottom navigation bar. The main pane displays a table of requests with columns: Processed, ID, Req. Timestamp, Method, URL, Code, and Reason. The table lists 1103 entries, mostly 'Out of Scope' (green), with one entry '168' having a 'GET' method and a '200 OK' response. The browser preview pane shows a page with a blue header and a red box around the 'News' and 'BIG' sections.

Processed	ID	Req. Timestamp	Method	URL	Code	Reason
	168	3/18/24, 1:00:33 PM	GET	http://127.0.0.1:42000/	200	OK
Out of Scope	169	3/18/24, 1:00:33 PM	POST	https://shavar.services.mozilla.com/downloads?...	403	Forbidden
	170	3/18/24, 1:00:34 PM	GET	http://127.0.0.1:42000/polyfills.js	200	OK
	171	3/18/24, 1:00:34 PM	GET	http://127.0.0.1:42000/runtime.js	200	OK
	172	3/18/24, 1:00:34 PM	GET	http://127.0.0.1:42000/main.js	200	OK
	173	3/18/24, 1:00:33 PM	GET	http://cdnjs.cloudflare.com/ajax/libs/cookieconse...	200	OK
	179	3/18/24, 1:00:34 PM	GET	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4...	200	OK
	182	3/18/24, 1:00:34 PM	GET	http://127.0.0.1:42000/vendor.js	200	OK
	183	3/18/24, 1:00:34 PM	GET	http://cdnjs.cloudflare.com/ajax/libs/cookieconse...	200	OK

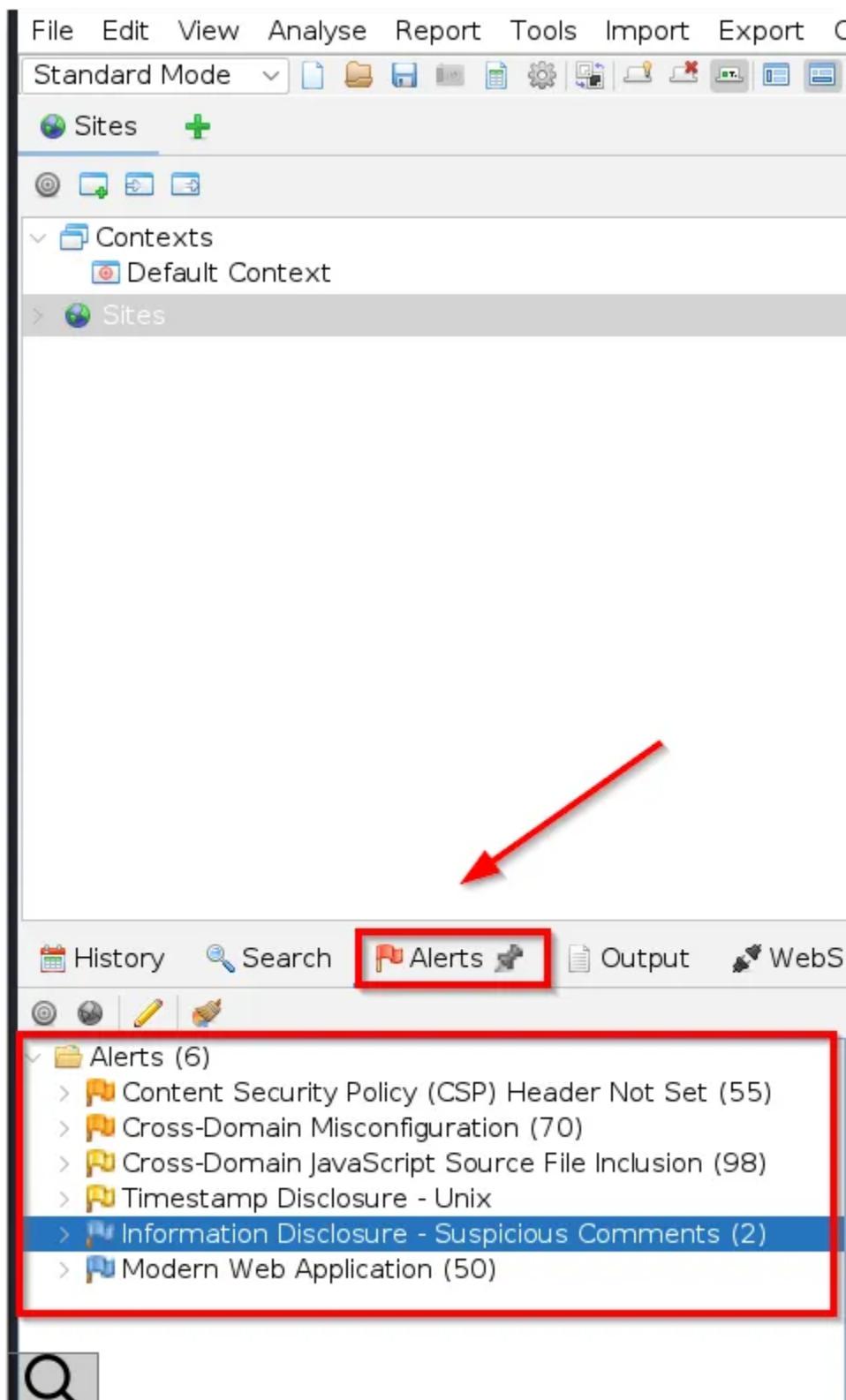
## Scan with ZAP

Before we show you ZAP's scanning features, remember that you should always use active method scanning only to attack an application that you have explicit permission to test.

- Passive Scanning:** Passive scanning simply involves looking at the raw requests and responses. ZAP doesn't do anything, it just monitors the traffic that goes through it. It analyzes this traffic to detect potential risks without sending new requests.

Passive scanning is safe to use in any web application.

When you scan a website, ZAP performs a passive scan and reports any alerts in the "Alerts." tab.



- **Active Scanning:** Active scanning tries to find other vulnerabilities using known attacks against the selected targets. It can find specific vulnerabilities such as XSS, SQL injection, buffer overflows, Log4Shell and remote file inclusion.

Active scanner cannot find logical vulnerabilities such as broken access control.

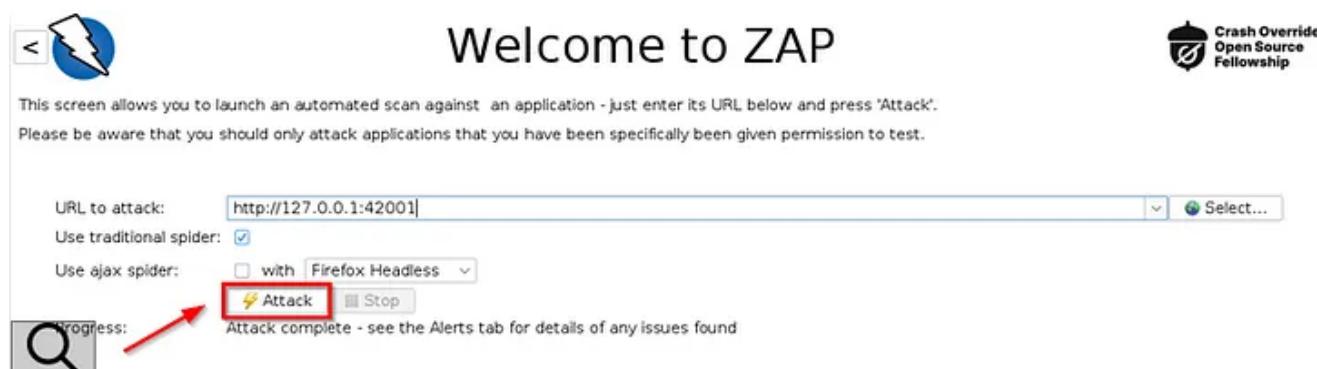
You can set policies for your scans, although we won't discuss that here. These policies allow you to set the threshold for the number of issues reported, and the strength options determine the number of attacks performed per parameter.

As with most tools in ZAP, you can set options for active scans. These include the number of guests being scanned simultaneously, the maximum scan duration, and whether to manage CSRF tokens.

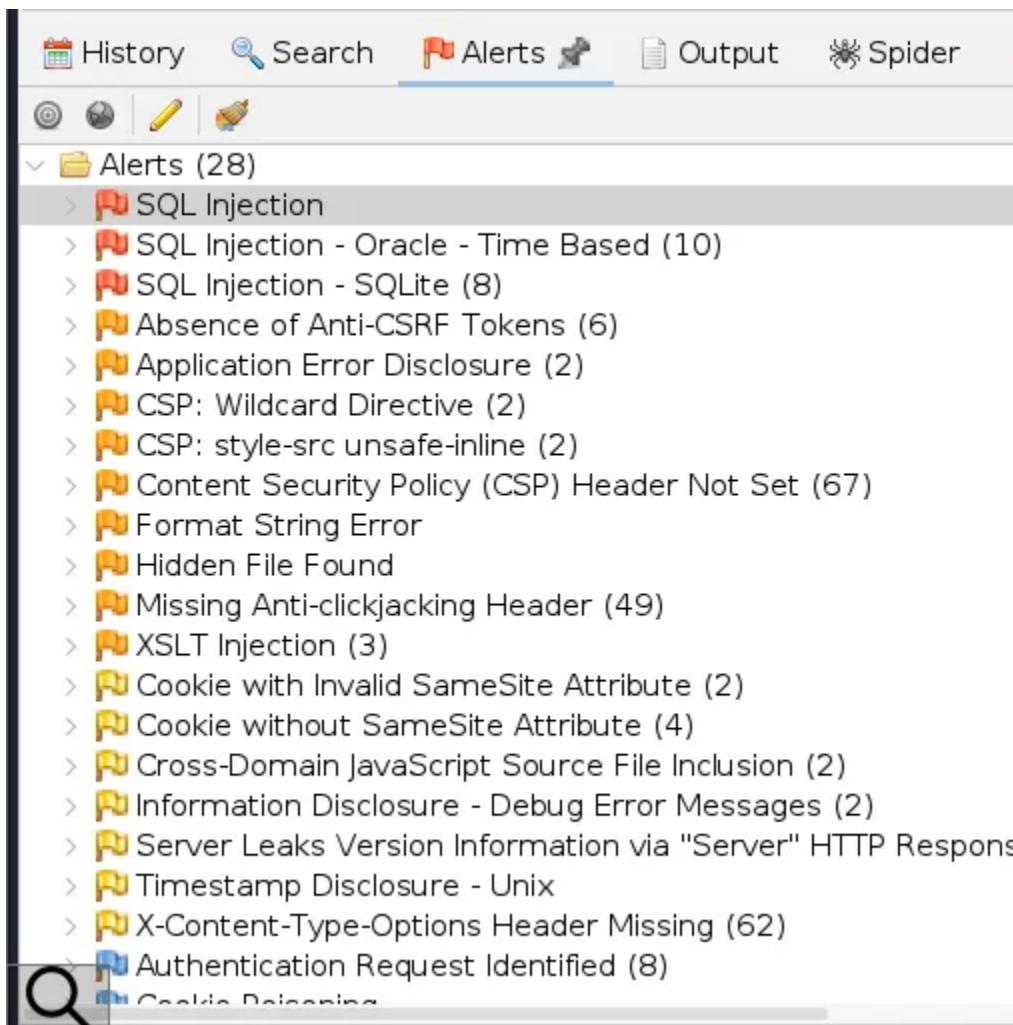
Select "Automated Scan" from the quick launch menu to begin.



This will open the auto scan startup screen. Here, you'll set up the URL and spider and browser you want to use. When you're ready, select "Attack" to begin.



Once the scan is complete, you can find all the alerts reported by ZAP under the "Alerts." tab.



As you can see from the image above, ZAP found 28 vulnerabilities organized by severity: high (red), medium (orange), low (yellow), and informational (blue).

ZAP shows you the number of vulnerabilities it has found. Let's take a closer look at SQL injection. Select the arrow next to it to see where the problem was found in the application. Then select the URL to view detailed information about the notification.

The screenshot shows a detailed view of a selected SQL injection alert. The alert details are as follows:

- URL:** http://127.0.0.1:42001/vulnerabilities/weak\_id/
- Risk:** High
- Confidence:** Medium
- Parameter:** weak\_id
- Attack:** AND 1=1 --
- Evidence:** POST: http://127.0.0.1:42001/vulnerabilities/weak\_id/
- CWE ID:** 89
- WASC ID:** 19
- Source:** Active (40018 - SQL Injection)
- Input Vector:** Form Query
- Description:** SQL injection may be possible.

**Other Info:**

The page results were successfully manipulated using the boolean conditions [ AND 1=1 -- ] and [ AND 1=2 -- ]. The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison. Data was returned for the original parameter.

**Solution:**

Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'.

ZAP provides quite a bit of information. In the right panel, you'll see the URL where the alert was found and its risk and confidence level. You will also see a CWE and WASC ID from common software vulnerability lists. Each vulnerability has its own ID number.

You will then see a description of the alert and how ZAP acknowledged this alert. Notes the attack method used ("AND 1=1 -"). You should confirm this to see if the vulnerability actually exists.

It also suggests a possible workaround: don't trust the client-supplied data and use server-side validation, such as prepared statements, to mitigate the risk.

## Conclusions

In this ZAP tutorial, we've shown you how to get started with this powerful tool. We've given you an overview of some of its most popular features and shown you how to get started testing web apps.

You must be well prepared to explore more features of ZAP. Remember to update ZAP regularly to get the latest features and extensions. Keep practicing and experimenting with different settings to get the most out of the tool.

Infosec

Cybersecurity

Pentesting

Hacking

Security



## Written by Vasileiadis A. (CyberKid)

2.8K Followers

Cybersecurity Evangelist | Offensive Security Consultant (Red Team Operator) | Information Security Analyst

More from Vasileiadis A. (CyberKid)

Services	
SSH	910,453
HTTP	762,776
HTTPS	542,273
SIP	324,724
SNMP	288,254

**92.27.82.**  
TalkTalk  
Added on 02.05.2014  
  
[Details](#)  
.net

SSH-1.99-Cisco-1.25

Top Countries	
United States	972,795
Russian Federation	158,737
China	141,487
Italy	125,144
Mexico	111,372

**200.94.27.**  
Alestra, S. de R.L. de C.V.  
Added on 02.05.2014  
  
[Details](#)  
.mx

HTTP/1.0 401 Unauthorized  
Date: Fri, 02 May 2014 17:17:26 GMT  
Server: cisco-IOS  
Connection: close  
Accept-Ranges: none  
WWW-Authenticate: Basic realm="level\_15 or v

Top Organizations	
Cox Communications	258,050
Uninet S.A. de C.V.	72,149
Turk Telekom	71,133
Telestra Internet	64,709

**60.199.236.**  
Taiwan Fixed Network, Telco and Network Service Pr  
Added on 02.05.2014  
  
[Details](#)  
.tw

HTTP/1.0 401 Unauthorized  
Date: Fri, 02 May 2014 17:23:27 GMT  
Server: cisco-IOS  
Connection: close

scan your website with **netsparker**

**Hurricane LABS**

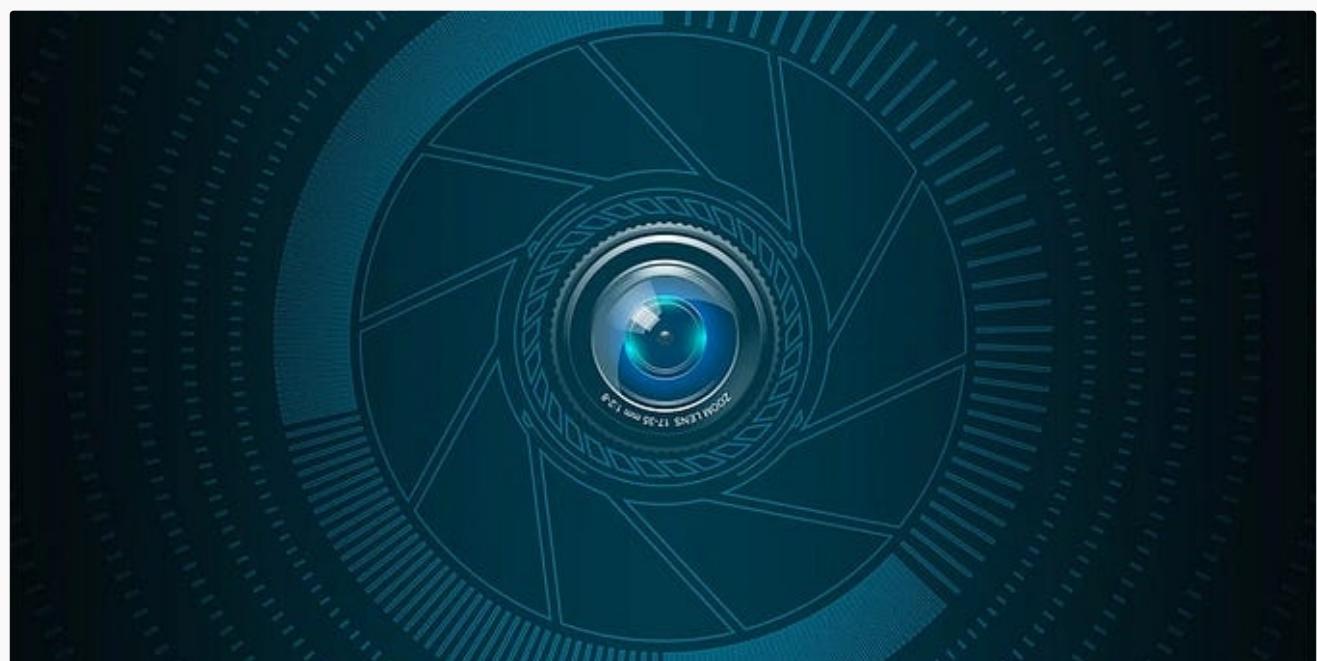
**HackerTarget.com**  
BUILT ON OPEN

 Vasileiadis A. (CyberKid)

## Protect your WiFi from Hackers

Wi-Fi Hacking is much easier than most people think and the way to achieve it is some common techniques that most hackers use. With a few...

Aug 29  1.2K  11



 Vasileiadis A. (CyberKid)

## Detect hidden surveillance cameras with your phone

A family recently it had a big surprise on their Airbnb: a hidden camera disguised as a smoke detector in the living room, monitoring their...

Aug 5 5K 34



# The ZMap Project

The ZMap Project is a collection of open source tools designed to help researchers to perform large-scale studies of the systems that compose the public Internet.

Vasileiadis A. (CyberKid)

## Scan the entire web in 45 minutes with Zmap!

Most of you know the power of nmap and nmap scripts to identify a target and networks in general. These tools can be used for numerous...

Jul 29 316 5





Vasileiadis A. (CyberKid)

## Shodan: The most dangerous search engine in the world!

Almost all of us have used a search engine like Google or Bing to find material online. These search engines scan the entire internet and...

Jul 26 1K 9



See all from Vasileiadis A. (CyberKid)

## Recommended from Medium



 Harshad Shah  in Offensive Black Hat Hacking & Security

## Kali New Release 2024.3 | Explore 11 New Tools for Hacking

Advanced Penetration Testing using Kali Linux | Hacker Associate

Sep 15  147  1

A graphic showing a table of Common Vulnerabilities and Exposures (CVEs). The table has columns for CVE ID, CVSS Score, and CVSS Version. The data is as follows:

CVE ID	CVSS Score	CVSS Version
2.9BS	2.9	(CVSS 3.1)
2.86T	2.8	(CVSS 3.1)
LMSS	0.85	(CVSS 3.1)
CUST	1.05	(CVSS 3.1)
IV/HY	1.05	(CVSS 3.1)
LIBS	1.05	(CVSS 3.1)
INDCI	1.05	(CVSS 3.1)
DISSE	1.05	(CVSS 3.1)
NIBS	1.05	(CVSS 3.1)

A large illustration of a hooded hacker is on the right side of the table.

 Jonathan Mondaut

## How ChatGPT Turned Me into a Hacker

Discover how ChatGPT helped me become a hacker, from gathering resources to tackling CTF challenges, all with the power of AI.

## Lists



### Tech & Tools

20 stories · 319 saves



### Medium's Huge List of Publications Accepting Submissions

334 stories · 3684 saves



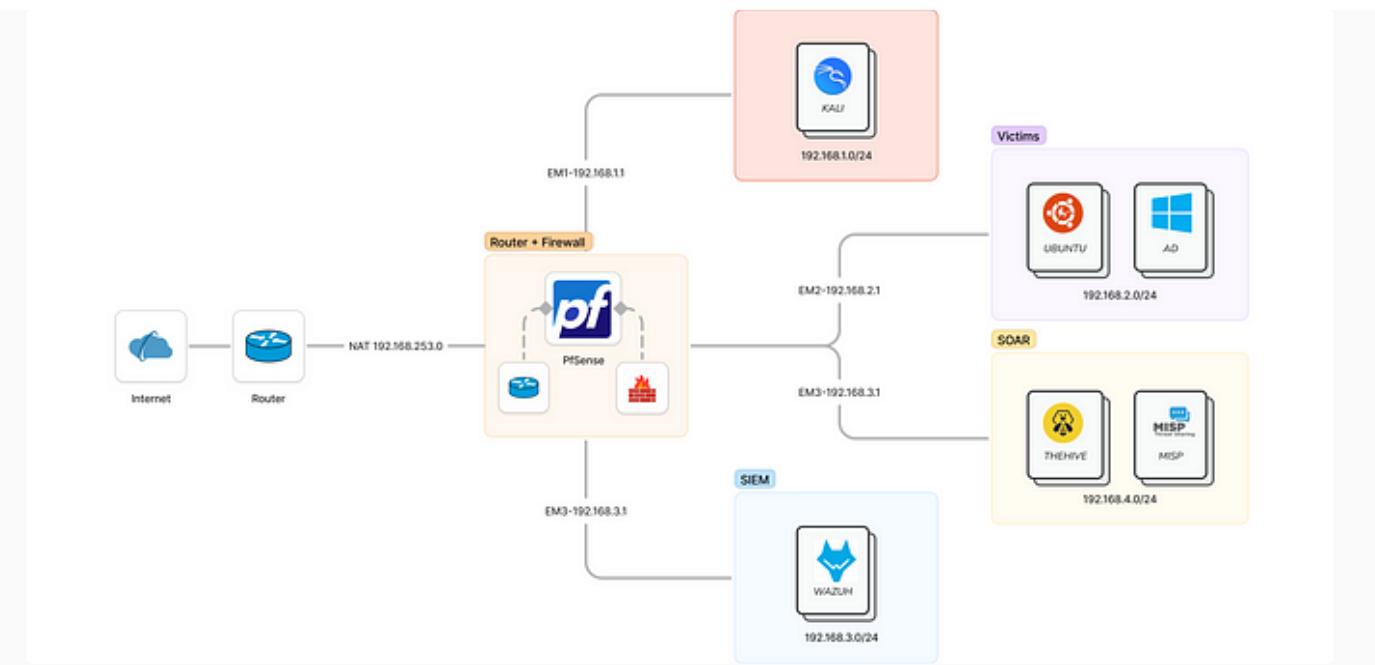
### Staff Picks

748 stories · 1367 saves



### Natural Language Processing

1751 stories · 1347 saves



SchesmuTwo

## Build Your Own Lab SOC: A Step-by-Step Guide to Creating a SOC from Scratch—Part 1

Introduction

Aug 22 61



```
<!DOCTYPE html>
<html class="no-touch no-js mdl-js">
  <head>...</head>
  <body class="page-- itemscope itemtype="http://schema.org/Website"> ...</div>
  <link href="https://fonts.googleapis.com/css?family=Roboto+Mono:400,700|Roboto:400,300,500,700,400italic,700italic" rel="stylesheet" type="text/css">
  <script type="text/javascript" async src="https://www.google-analytics.com/analytics.js"></script>
  <script async src="https://www.googletagmanager.com/gtm.js?id=GTM-MB3LRF"></script>
  <script src="/static/is/material_design_light_bundle.js"></script>
  <script>...</script>
  <!-- Google Tag Manager -->
  <noscript>...</noscript>
  <script>...</script>
  <!-- End Google Tag Manager -->
</body>
</html>
```

Styles Computed Event Listeners DOM Breakpoints >

Filter :hover .cls +,

element.style {

}

body { tools.css:1

width: 100%;

min-height: 100%;

font-family: Helvetica,Arial,sans-serif;

margin: 0;

padding: 0;

word-wrap: break-word;

}

body { user agent stylesheet

display: block;

margin: 8px;

}

Inherited from html.no-touch.no-js.mdl-js

html { tools.css:1

color: #rgba(0,0,0,.87);

font-size: 1em;

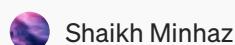
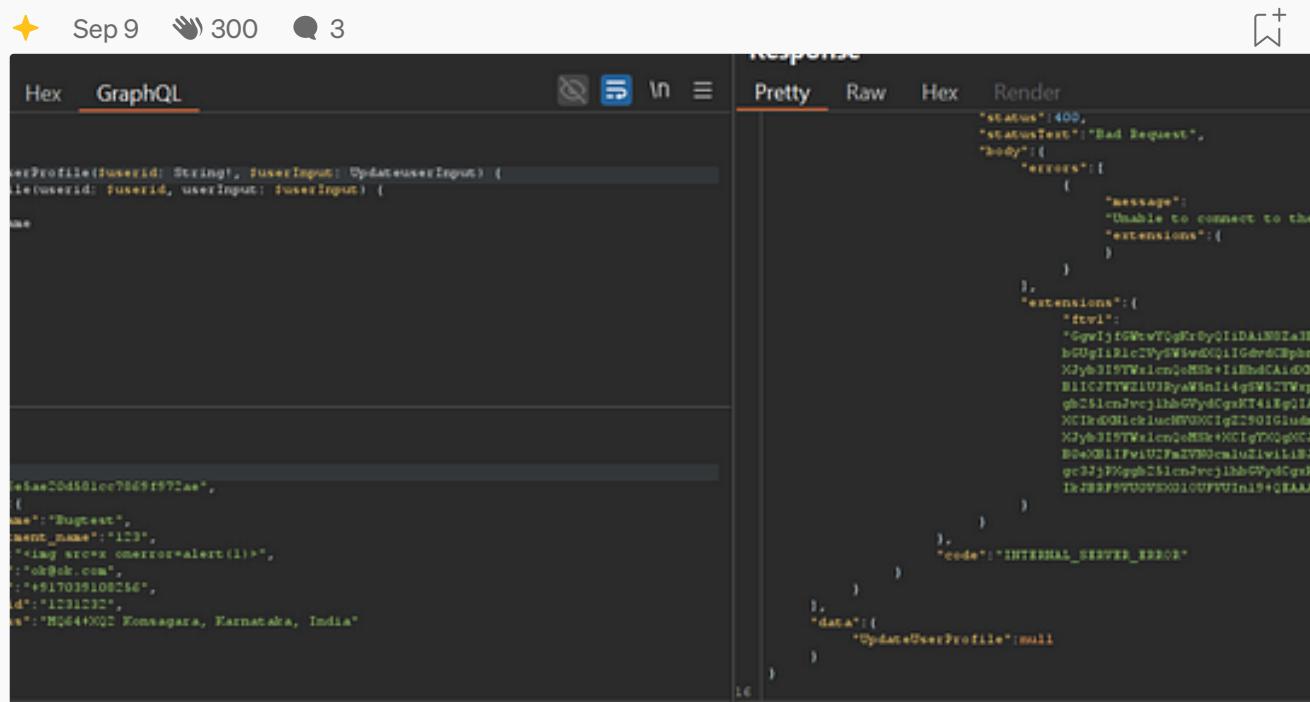
line-height: 1.4;

}

Satyam Pathania in InfoSec Write-ups

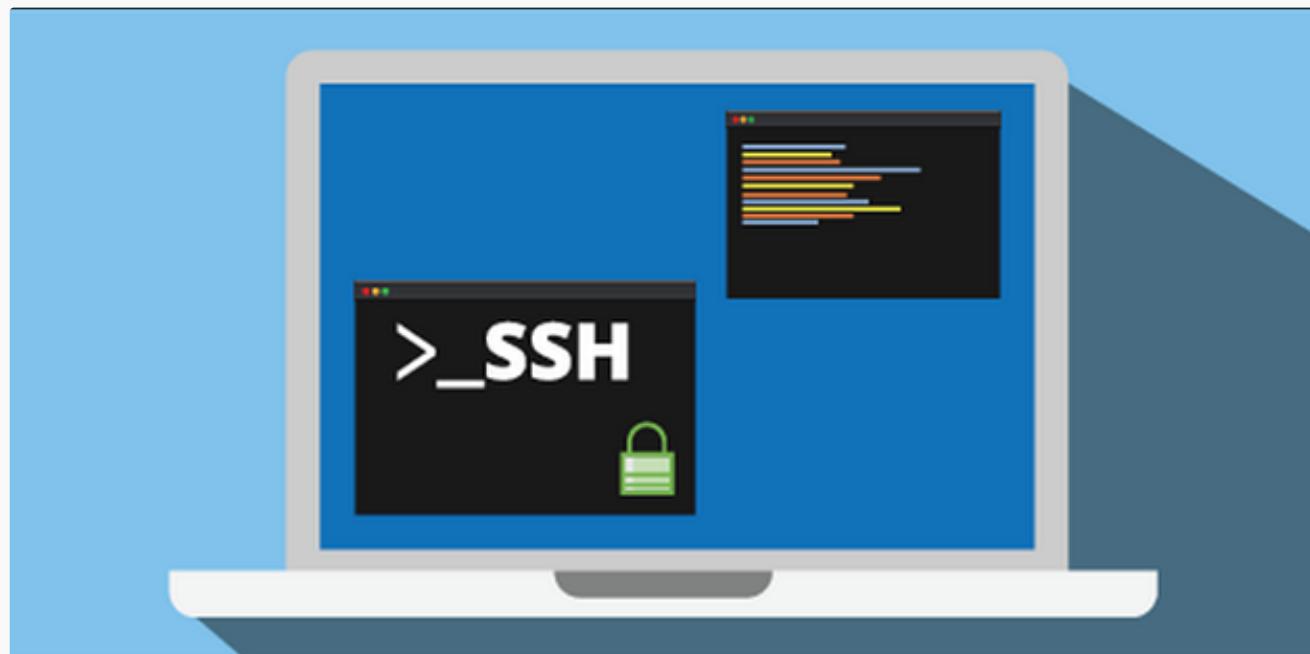
## How to Set Up Your Hacking Machine —Complete Beginner Edition

Well hello there , Hi i m Satyam , a cybersecurity passionate and content writer .. I love writing about Tech, Cybersecurity and framing....



## **Live Bug Bounty & Penetration Testing on Real Websites: Step-by-Step Guide (Part 1)**

Well, well, the article is here—ohh! Sorry, I mean the series of articles—where we will do penetration testing or bug bounty hunting...





Usama Malik in DevOps.dev

## 10 Essential SSH Server Security Tips & Best Practices

This article will outline 10 essential SSH server security tips and best practices that will protect your systems from potential threats.

⭐ Sep 3

🕒 251

💬 4



See more recommendations