
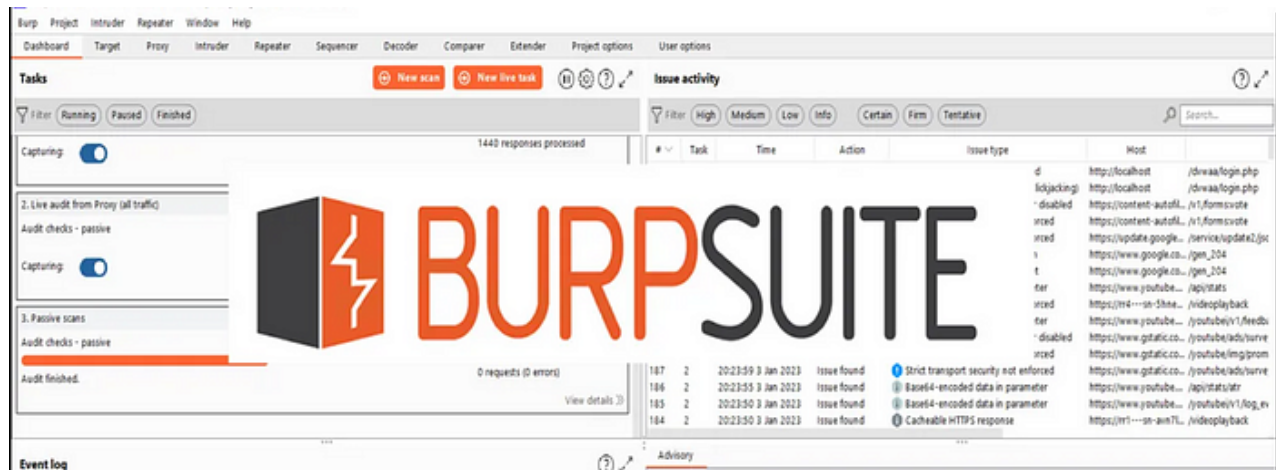


A Step-by-Step Guide to Using BurpSuite for Web Application Security Testing

 medium.com/@uhabiba503/a-step-by-step-guide-to-using-burpsuite-for-web-application-security-testing-da9fae620270

Umme Habiba

May 4, 2023



Burp Suite is one of the most popular security testing tool. Burp Suite can be used to identify different types of vulnerabilities, such as SQL injection or cross-site scripting, by testing the web application beyond its graphical user interface (GUI). It is a type of proxy server, which means it sits between the user's web browser and the web server to observe and manipulate all the data that is being sent back and forth.

Burp Suite has different features such as **proxy, Repeater, intruder, scanner, decoder**, and more.

- Burp Suite's proxy function allows users to intercept and modify HTTP requests between a user's web browser and the web server. This allows for the observation and manipulation of web traffic, which can help identify potential security issues.
- Burp Suite Repeater lets us grab a request, change it however we want, and send it again and again. This can be super useful, especially when we have to guess a payload by trying different things (like in SQLi) or when we want to see if an endpoint has any bugs.
- Burp Suite's intruder feature contains several different attacks that can be performed on a remote website. These attacks include dictionary attacks and brute force attacks, which can help identify vulnerabilities in the web application's authentication mechanisms.
- Burp Suite's scanner function allows users to scan a particular website for potential vulnerabilities. This feature automates the testing process and provides detailed reports on any vulnerabilities that are found.
- Burp Suite's decoder function allows users to decode different types of data, such as URL encoding. This can help identify potential security issues in the web application's handling of data.

When to use Burp suite?

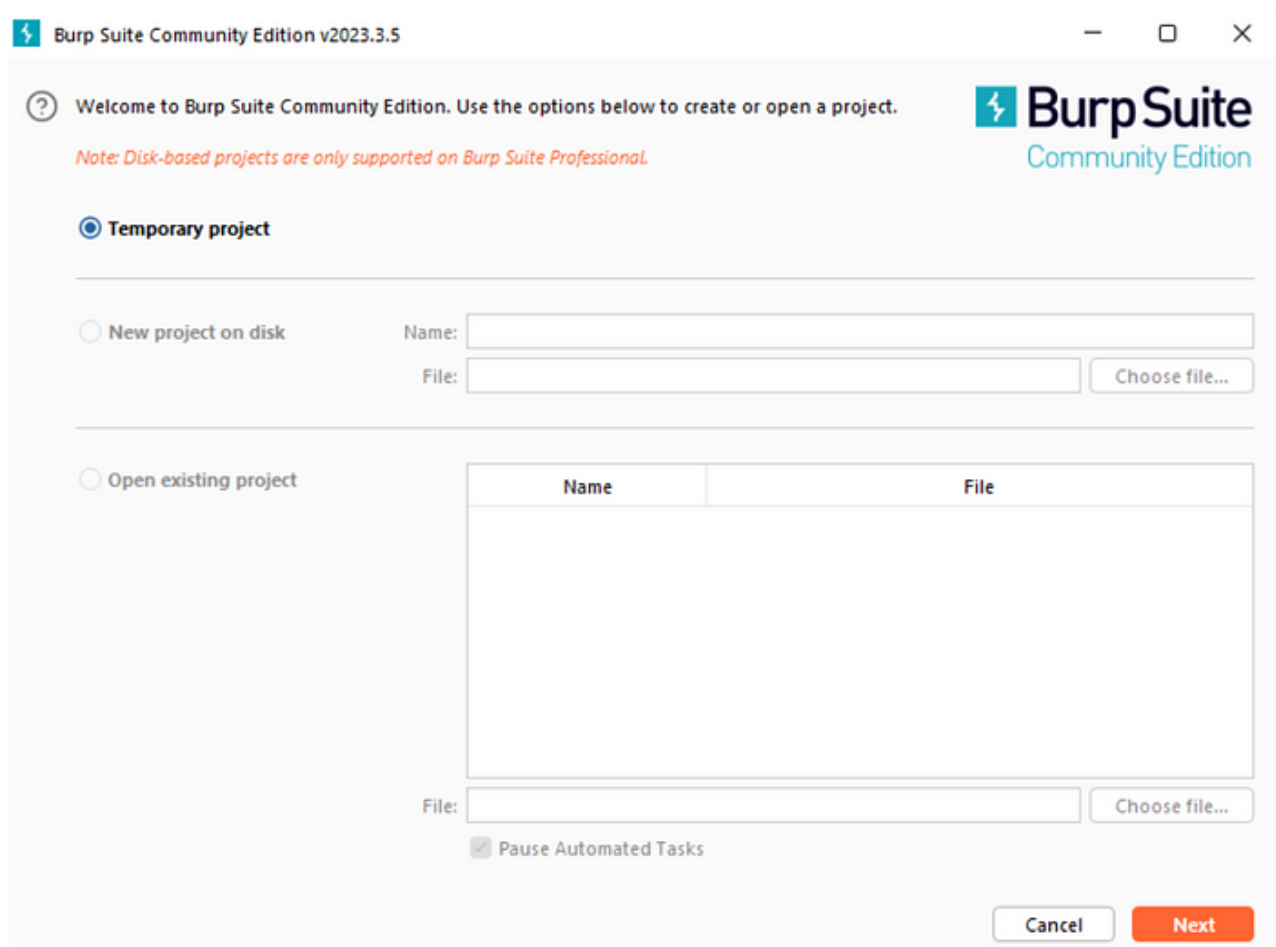
Hackers are always looking for ways to intercept calls so make sure hackers won't be able to intercept the calls.

Why to use Burp suite?

- Ensure that app/web applications are secure and reliable.
- By using the burp suite we can check the vulnerability of websites and applications.

Downloading and Setting Up Burp Suite on Windows

1. Go to the Burp Suite website and download the installer from [here](#).
2. Run the installer and follow the prompts to complete the installation process, select "new temporary project", followed by "use burp defaults"
3. Click on



Create temporary project on Burp Suite Community edition

? Select the configuration that you would like to load for this project.



☒ Use Burp defaults

☐ Use settings saved with project

☐ Load from configuration file

File

File:

Choose file...

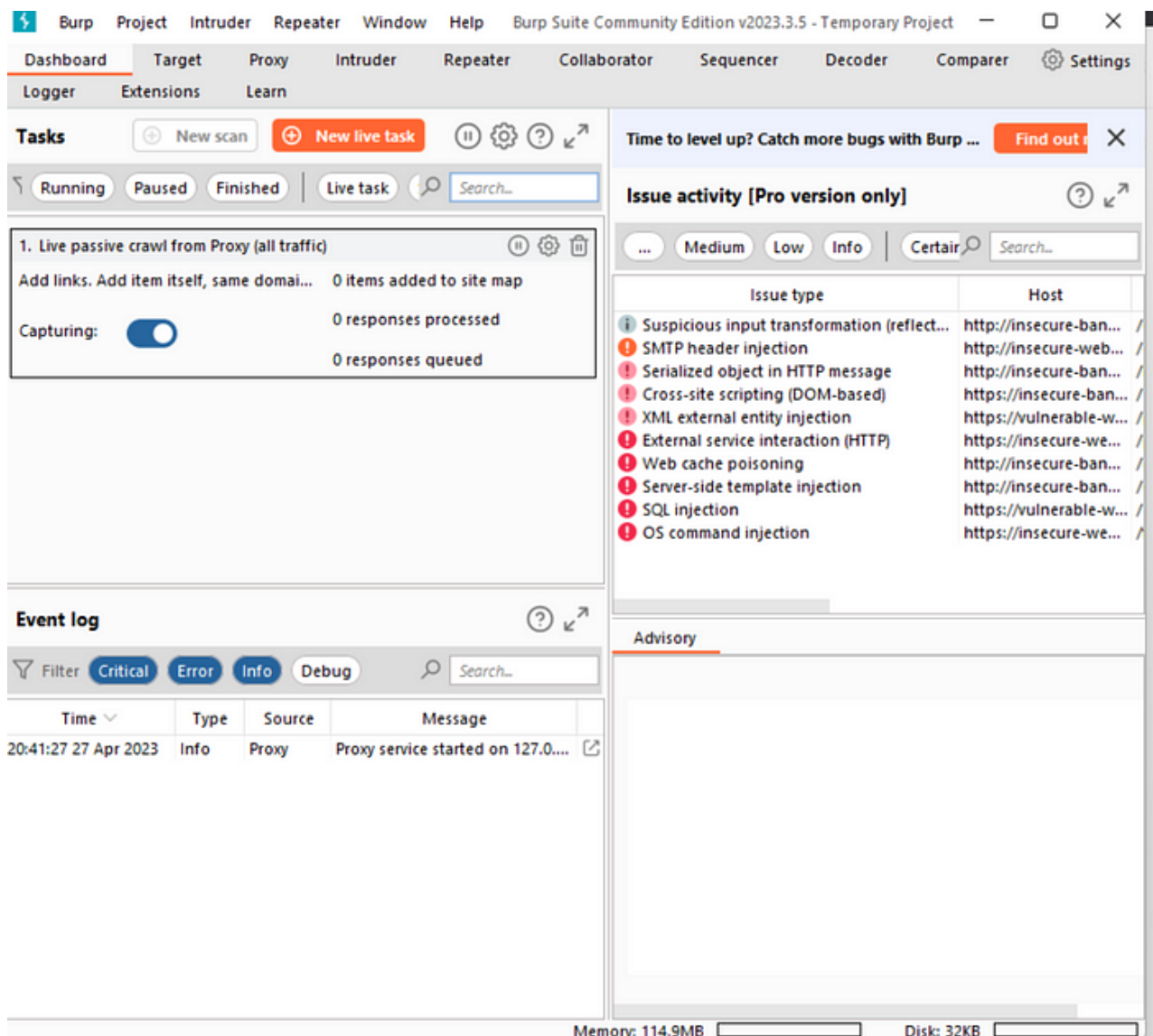
☐ Default to the above in future

☐ Disable extensions

Cancel

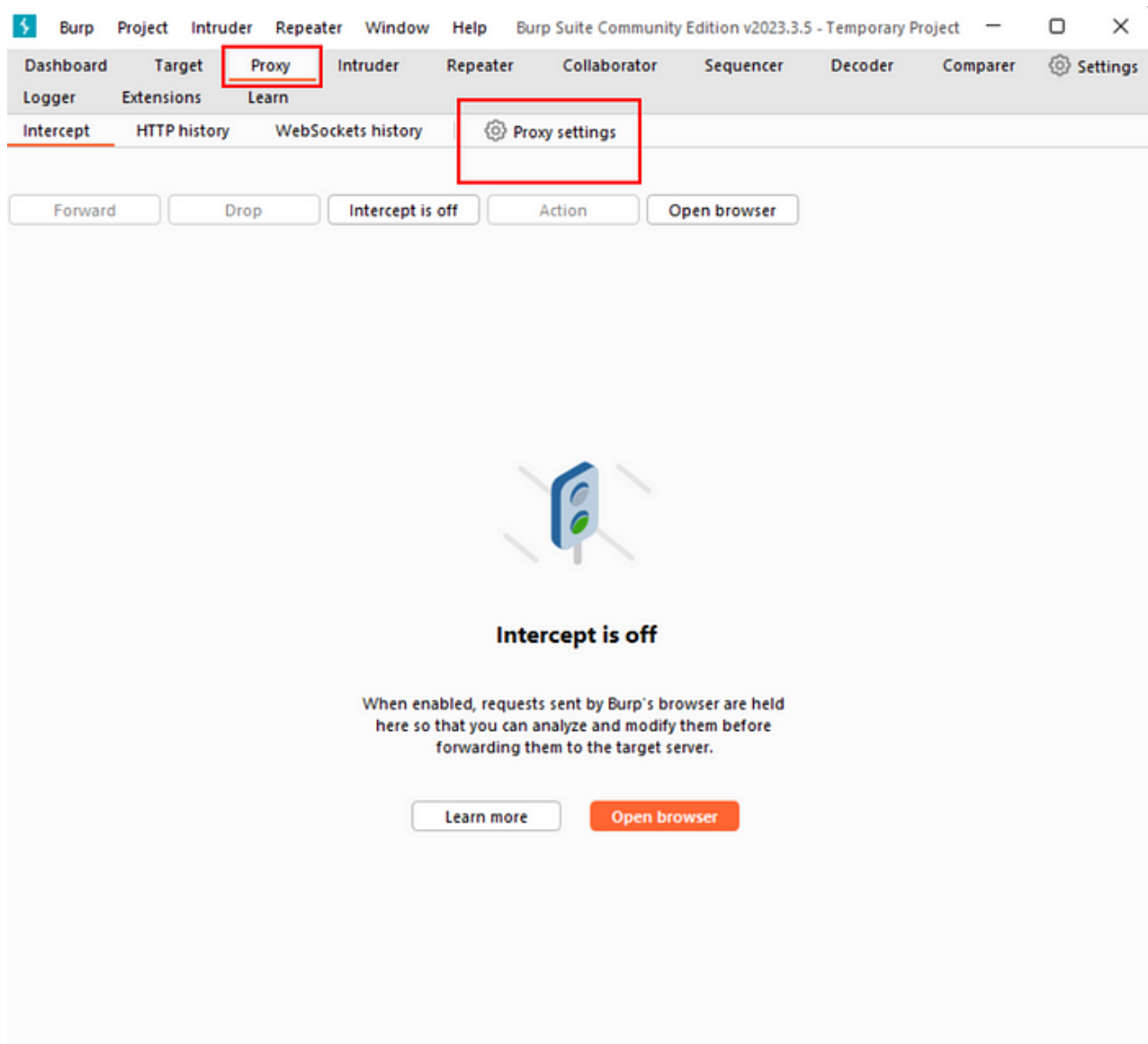
Back

Start Burp



Configuring Burp Suite

1. : In order to intercept traffic, you need to configure the proxy settings in Burp Suite. Go to the "Proxy" tab, then click on the sub-tab "Options/Proxy Setting"



2. You should see an entry in the table with a ticked Checkbox in the Running column, and “127.0.0.1:8080” showing in the Interface column.

The screenshot shows the Burp Suite Settings window with the 'Tools > Proxy' section selected. The left sidebar contains a search bar and a tree view with categories: Tools (expanded), Project, Network, User interface, Suite, and Configuration library. Under 'Tools', 'Proxy' is highlighted. The main content area has a title bar 'Tools > Proxy' and a 'Manage global settings' link. The 'Proxy listeners' section includes a description, buttons for 'Add', 'Edit', and 'Remove', and a table with columns: Running, Interface, Invisible, Redirect, and an unlabeled column. A single listener is listed with 'Running' checked and 'Interface' set to '127.0.0.1:8080'. Below the table is a note about CA certificates and buttons for 'Import / export CA certificate' and 'Regenerate CA certificate'. The 'Request interception rules' section includes a description, a checked checkbox for 'Intercept requests based on the following rules', and a table with columns: Enabled, Operator, Match type, Relationship, and an unlabeled column. A single rule is listed with 'Enabled' checked, 'Match type' set to 'File extension', and 'Relationship' set to 'Does not match'.

Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You can add, edit, or remove listeners.

Running	Interface	Invisible	Redirect	
<input checked="" type="checkbox"/>	127.0.0.1:8080			P

Each installation of Burp generates its own CA certificate that Proxy listeners can use. You can import or export the certificate for use in other tools or another installation of Burp.

[Import / export CA certificate](#) [Regenerate CA certificate](#)

Request interception rules

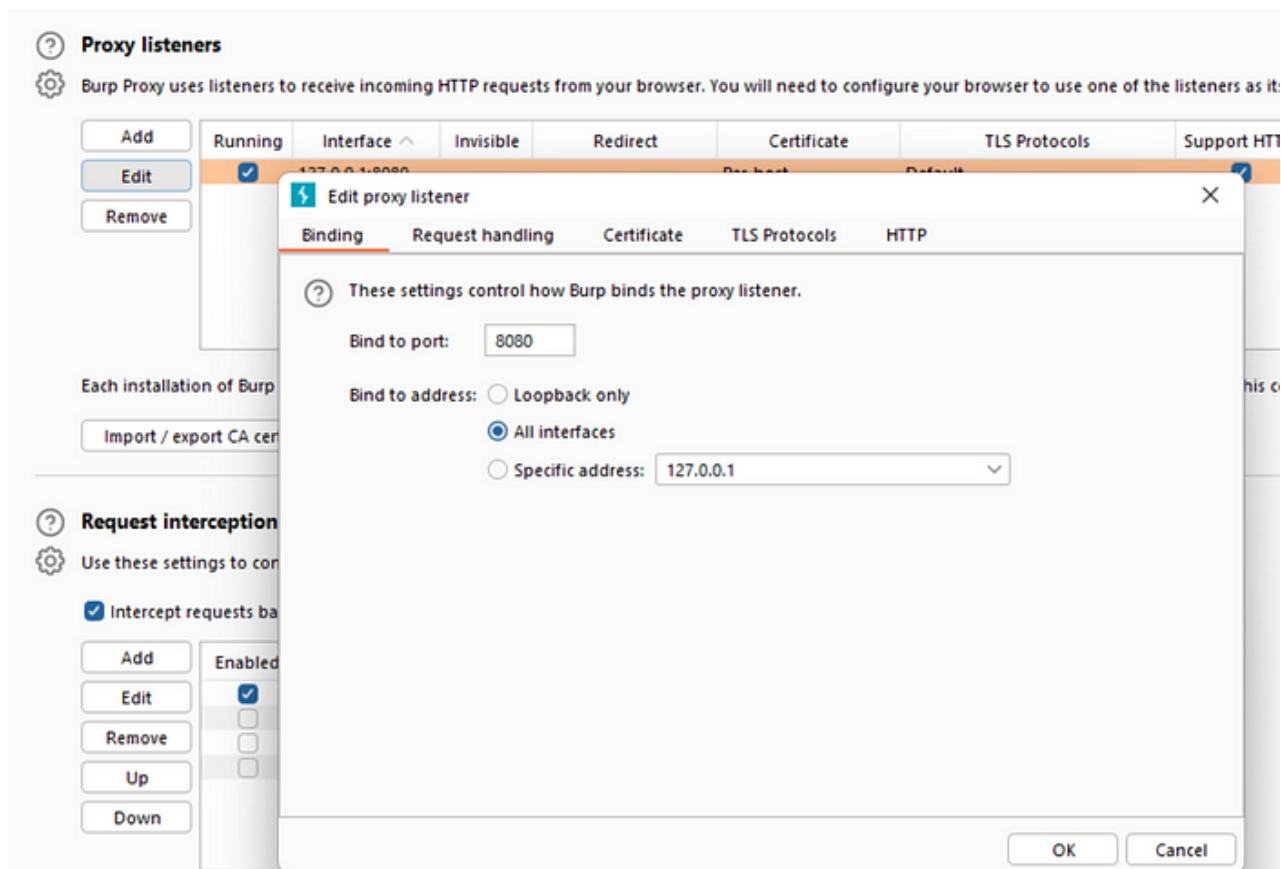
Use these settings to control which requests are stalled for viewing and editing in the Proxy.

☒ Intercept requests based on the following rules: *Master interception is turned off*

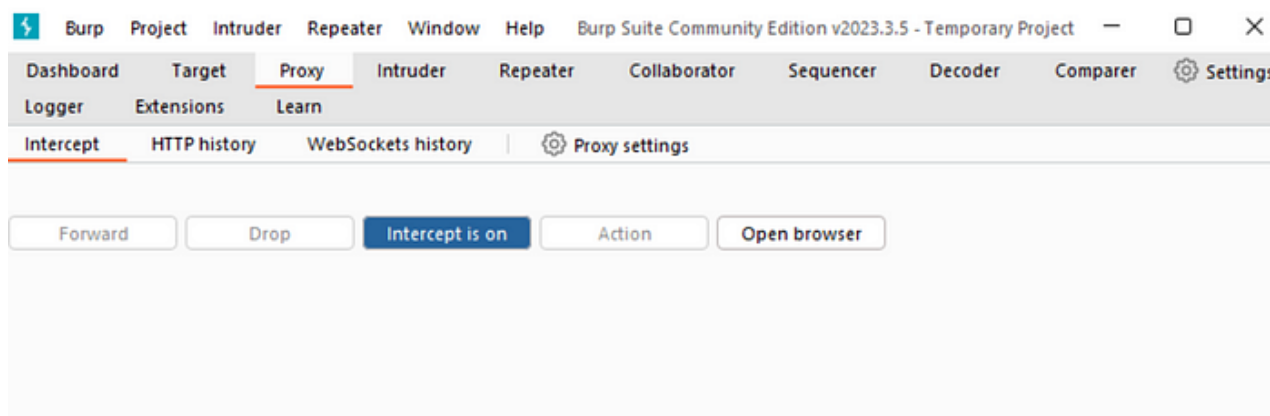
Enabled	Operator	Match type	Relationship	
<input checked="" type="checkbox"/>		File extension	Does not match	(/

By default Burp Suite runs on port 8080

3. You can modify this setting for it to listen to other ports by just clicking on the “Edit”, button and changing the port number of the listener to a different number.



4. Go to the **Proxy > Intercept** tab and Click the **Intercept is off** button, so it toggles to **Intercept is on**. This toggle allows you to intercept any request or response, and modify it before forwarding it.

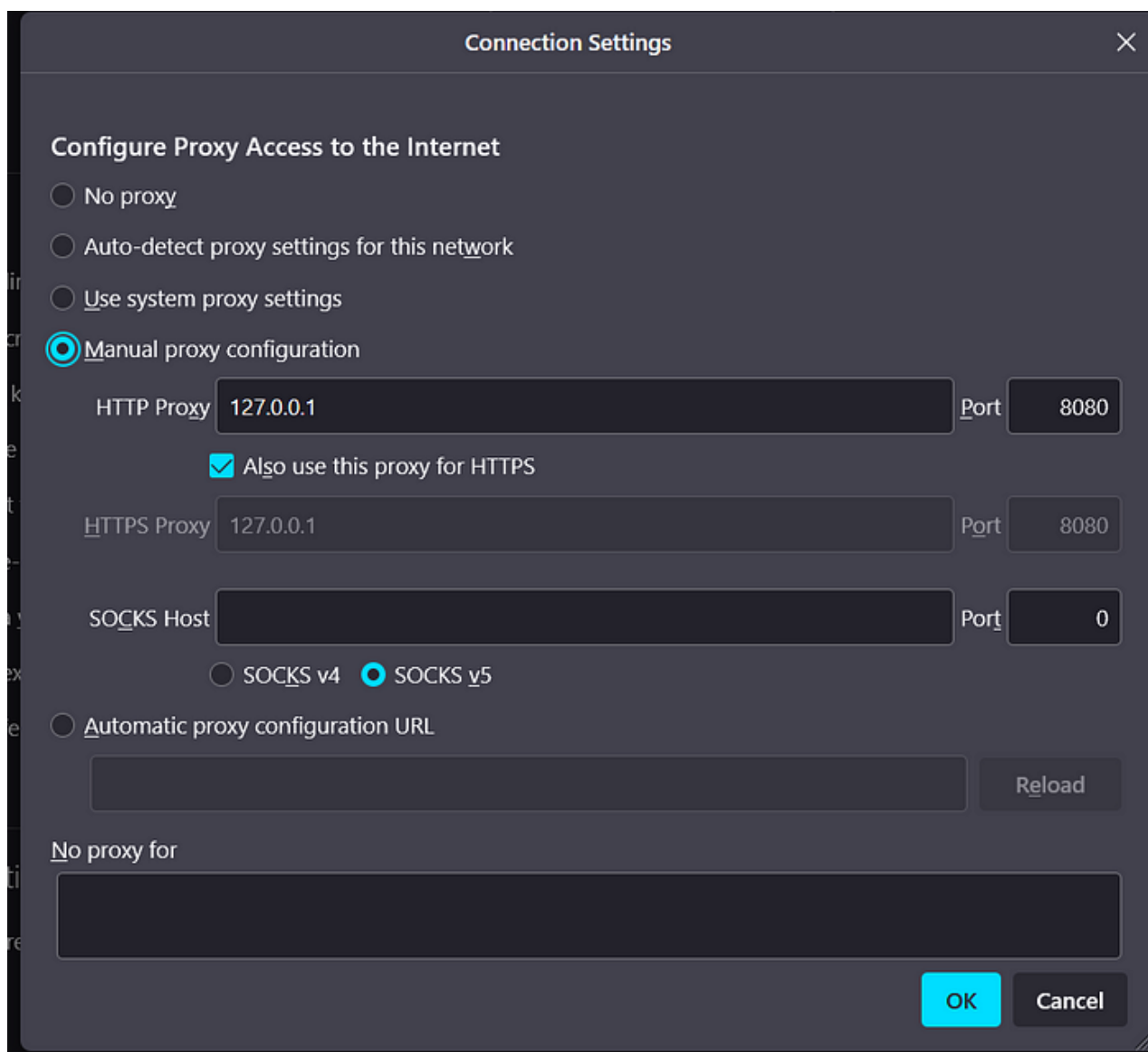
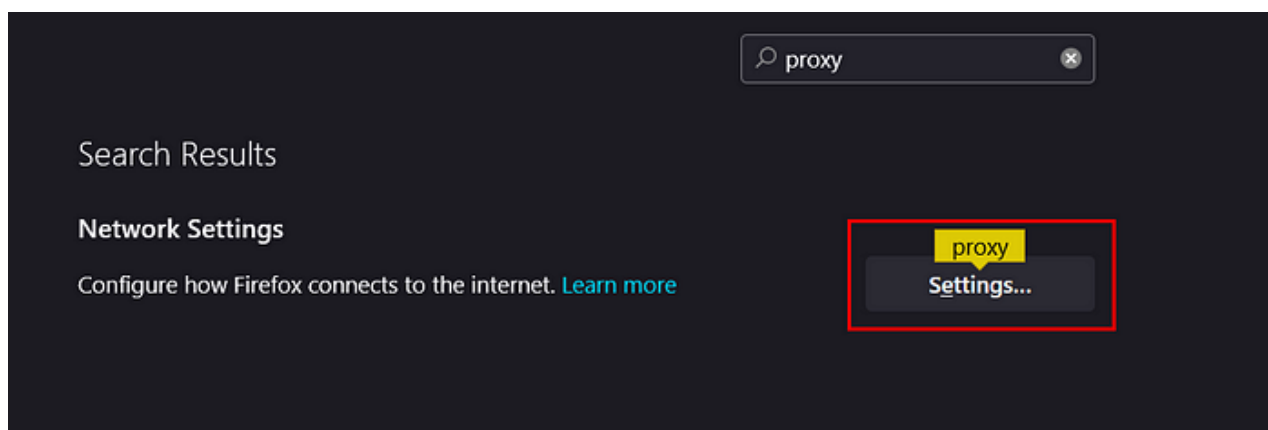


Ensure intercept is turned on

Configuring browser

To use Burp Suite as a proxy, you need to configure your browser. The process varies depending on the browser you're using; in this example, I'll use **Firefox**. However, you can refer to the Burp Suite documentation [here](#) on how to configure other browsers.

1. Open in the top right corner and go to Settings and then search for the word proxy. Click on the icon to open proxy settings.



Setting up a proxy server for Firefox

To configure your host computer, open the relevant configuration options and select 'Manual proxy configuration.' Enter the same HTTP Proxy and Port number as entered on Burp Suite, and then click 'OK' to save the settings.

Join Medium for free to get updates from this writer.

Now the browser is already setup to use Burp Suite as a proxy which is listening at port 8080. Now you need to install Burp's CA cert.

- Go to burp in Firefox.
- Click on 'CA Certificate' in the top menu bar to download it.

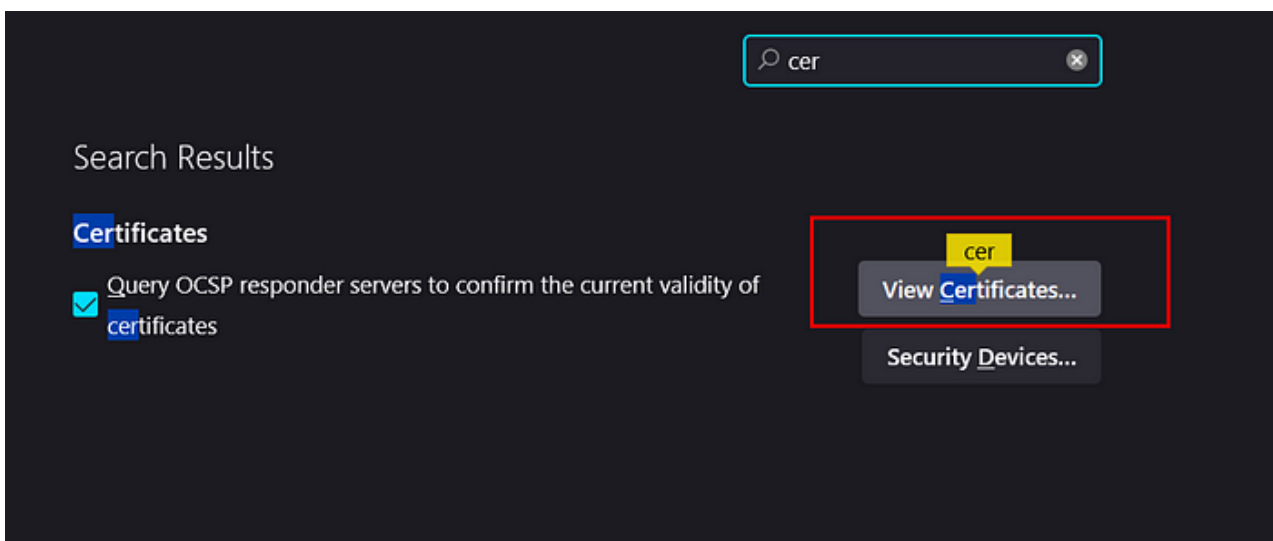


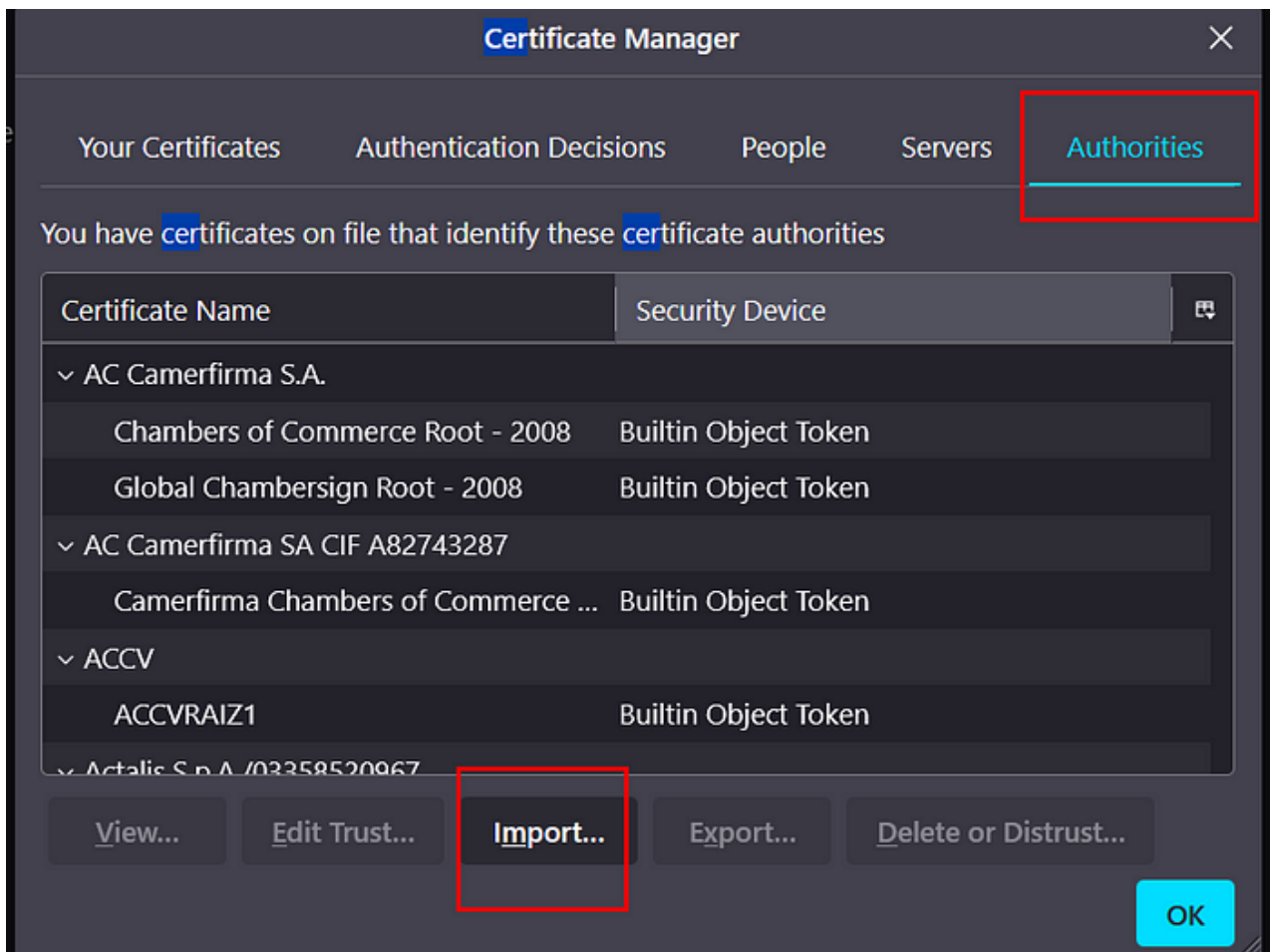
Download Burp's CA cert



Downloaded Burp Certificate

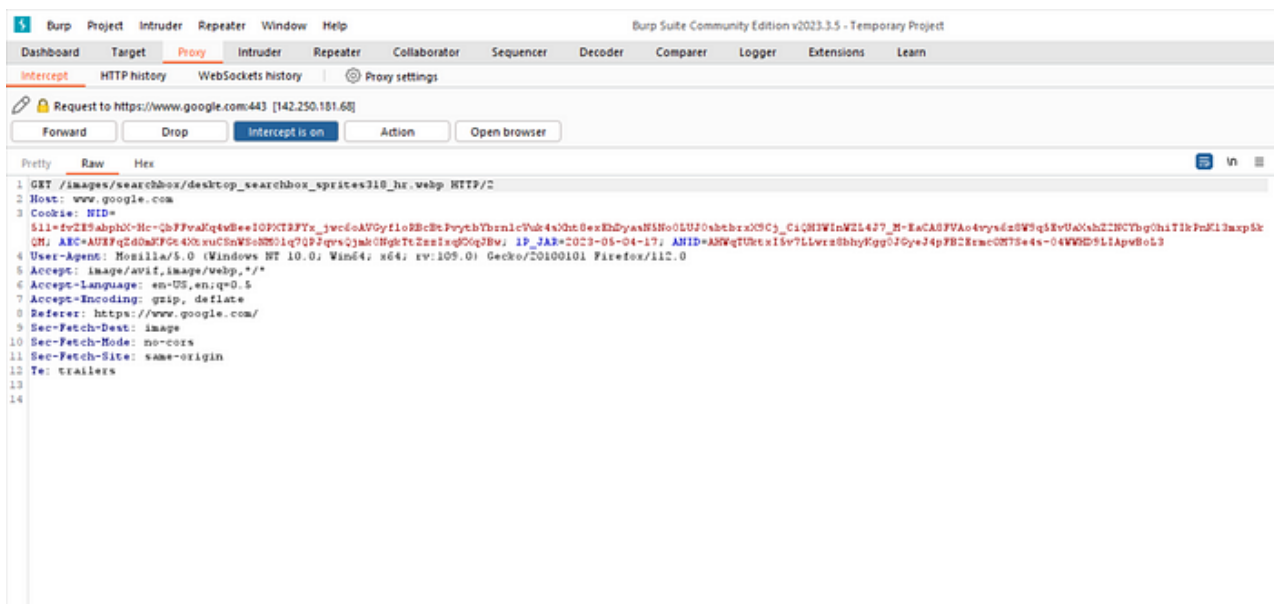
The CA cert must be installed in your browser as a trusted root so that the browser will trust the SSL connections made to Burp Suite. Go to > Click on Options from the side menu > Write Certificates in the search field and then Click on "" > > I





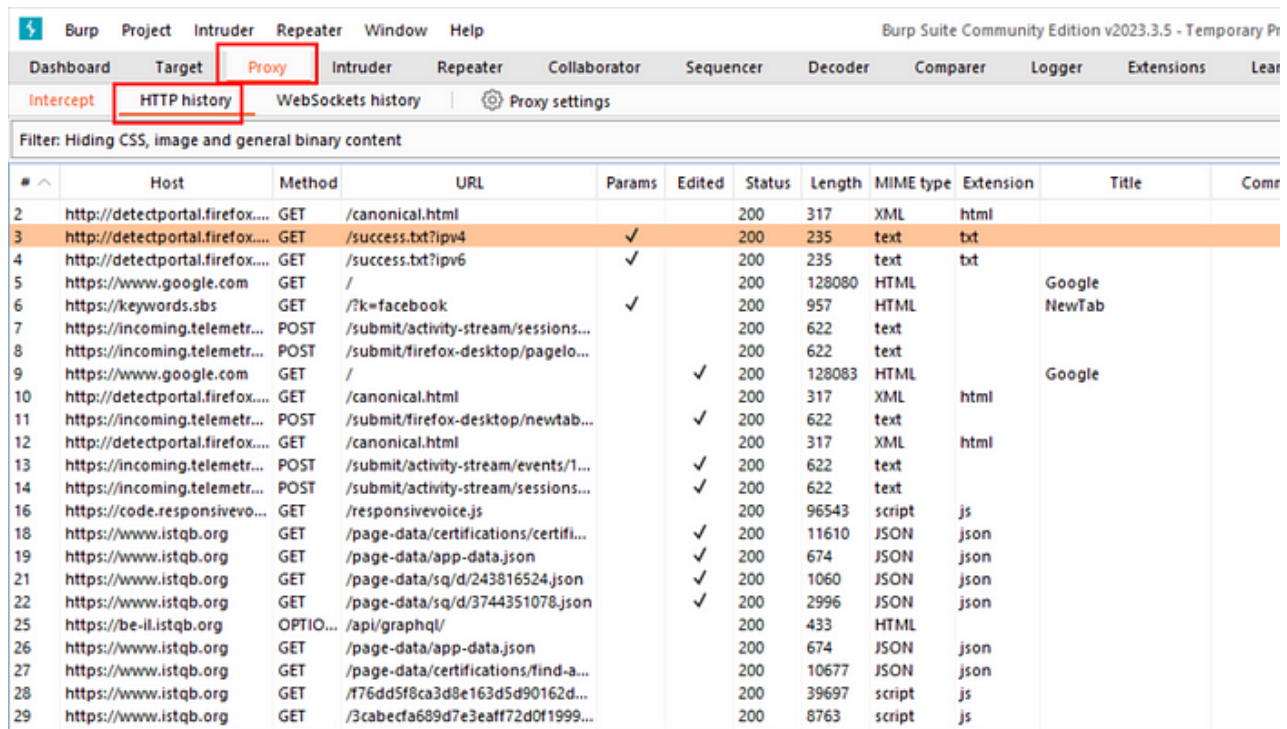
Once the Burp's CA cert is installed you should have no problem using Burp Suite as an interceptor. At Firefox, try to browse to <https://google.com> and you will not see any security warning.

At Burp Suite, when the interceptor is turned on, you will see all the requests made by the browser. You can analyze the requests and make any modifications. When you're satisfied, click on the Forward button to send the message.



Intercepting a request

You can also click on the HTTP History tab to view the list of request history.



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comments
2	http://detectportal.firefox.com	GET	/canonical.html			200	317	XML	html		
3	http://detectportal.firefox.com	GET	/success.txt?ipv4		✓	200	235	text	txt		
4	http://detectportal.firefox.com	GET	/success.txt?ipv6		✓	200	235	text	txt		
5	https://www.google.com	GET	/			200	128080	HTML		Google	
6	https://keywords.sbs	GET	?k=facebook		✓	200	957	HTML		NewTab	
7	https://incoming.telemetry.mozilla.org	POST	/submit/activity-stream/sessions...			200	622	text			
8	https://incoming.telemetry.mozilla.org	POST	/submit/firefox-desktop/pagelo...			200	622	text			
9	https://www.google.com	GET	/		✓	200	128083	HTML		Google	
10	http://detectportal.firefox.com	GET	/canonical.html			200	317	XML	html		
11	https://incoming.telemetry.mozilla.org	POST	/submit/firefox-desktop/newtab...		✓	200	622	text			
12	http://detectportal.firefox.com	GET	/canonical.html			200	317	XML	html		
13	https://incoming.telemetry.mozilla.org	POST	/submit/activity-stream/events/1...		✓	200	622	text			
14	https://incoming.telemetry.mozilla.org	POST	/submit/activity-stream/sessions...		✓	200	622	text			
16	https://code.responsivevoice.com	GET	/responsivevoice.js			200	96543	script	js		
18	https://www.istqb.org	GET	/page-data/certifications/certifi...		✓	200	11610	JSON	json		
19	https://www.istqb.org	GET	/page-data/app-data.json		✓	200	674	JSON	json		
21	https://www.istqb.org	GET	/page-data/sq/d/243816524.json		✓	200	1060	JSON	json		
22	https://www.istqb.org	GET	/page-data/sq/d/3744351078.json		✓	200	2996	JSON	json		
25	https://be-il.istqb.org	OPTIO...	/api/graphql/			200	433	HTML			
26	https://www.istqb.org	GET	/page-data/app-data.json			200	674	JSON	json		
27	https://www.istqb.org	GET	/page-data/certifications/find-a...			200	10677	JSON	json		
28	https://www.istqb.org	GET	/f76dd5f8ca3d8e163d5d90162d...			200	39697	script	js		
29	https://www.istqb.org	GET	/3cabecfa689d7e3eaff72d0f1999...			200	8763	script	js		

HTTP request history

Conclusion:

In this blog, you learned how to configure Burp Suite as a proxy and use Firefox to make it easier to configure a proxy in the browser.

Let me know if this was helpful. If you ever need my help, you can write in the comments section. Also, you can contact me through my [LinkedIn](#) Profile. Thank you!

For more information, I leave the reference links below:

[How to use Burp Suite for penetration testing — PortSwigger](#)