Recommended Settings for using ZAP

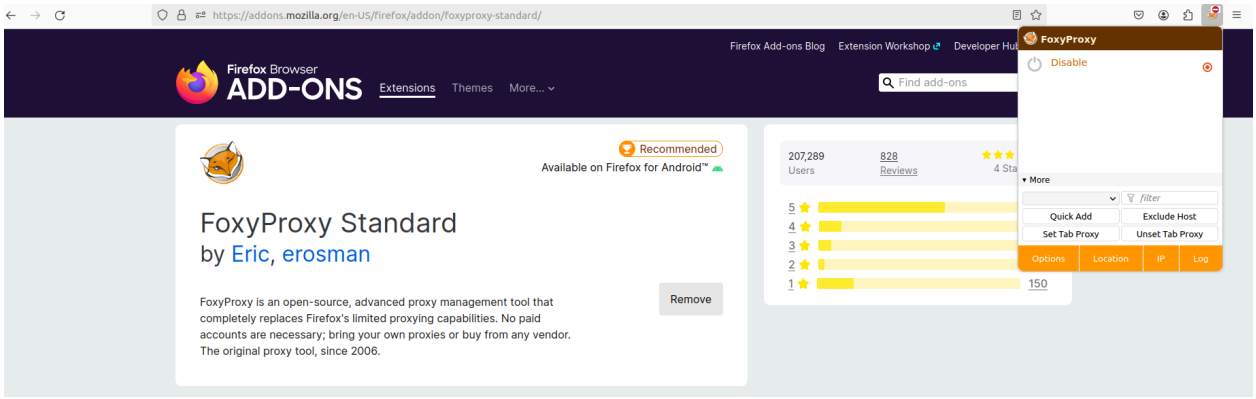
Introduction

When using ZAP we recommend some settings to be done beforehand to have a smooth lab experience. To that extent below sections will guide you step-by-step through those settings.

Step-1: FoxyProxy extension setup

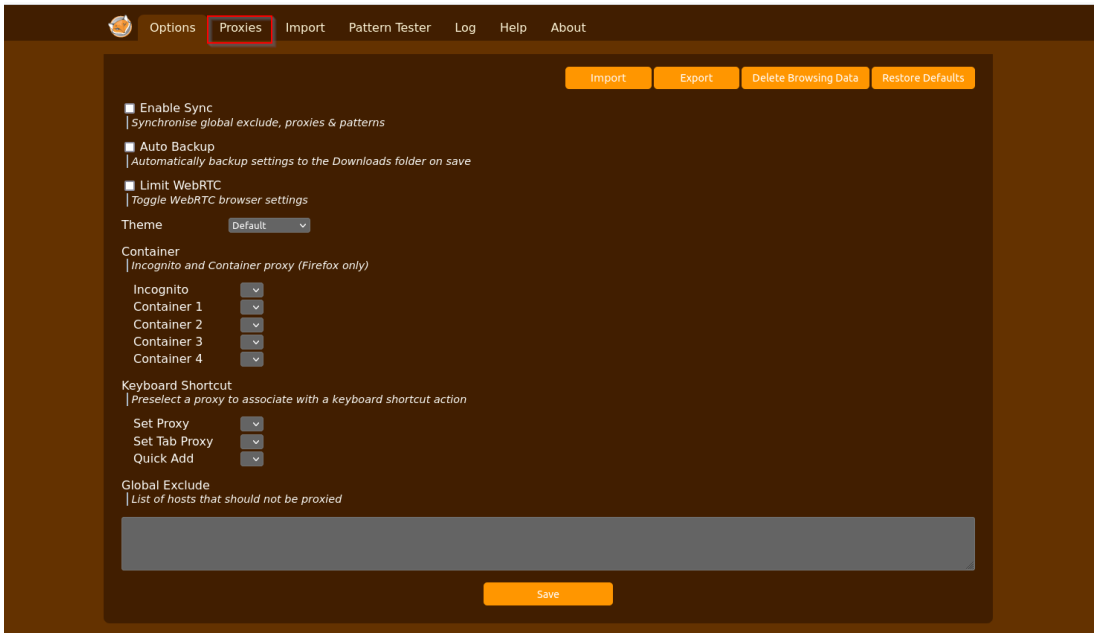
To analyze traffic and also to change GET/POST requests before they hit the server, one needs to capture the traffic being sent by the browser. FoxyProxy will help with that. It is an extension pack for browsers, easily available on the browser extension marketplace. It just directs all the http and https traffic of browser to some service/process configured on a specific IP:Port

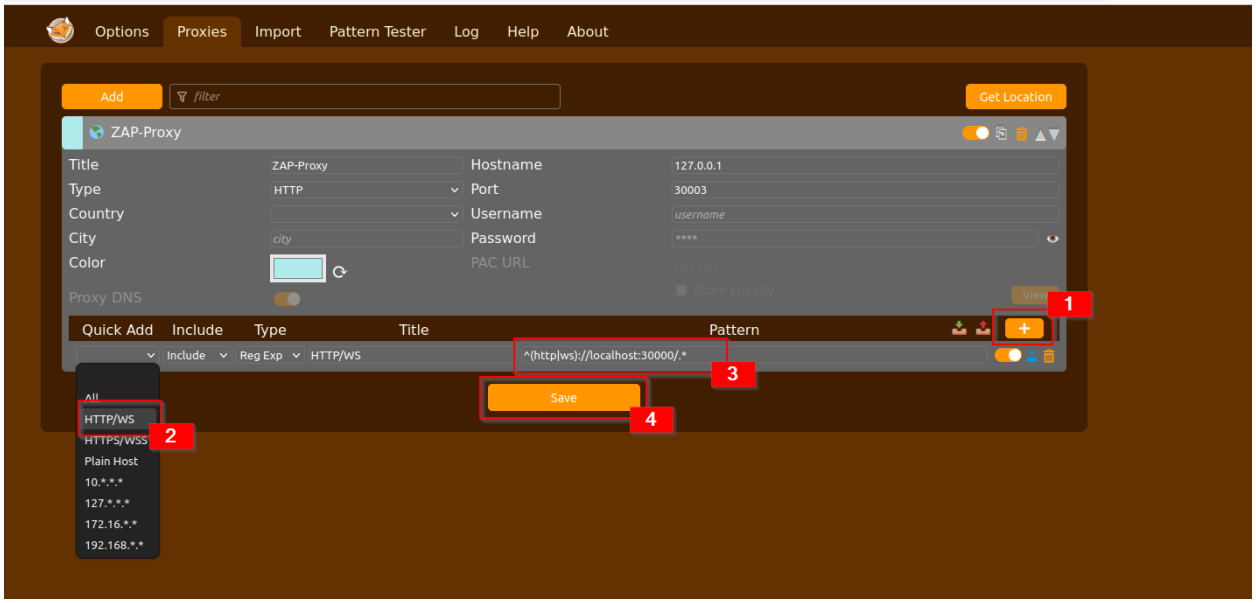
- To install FoxyProxy extension pack go to:
    - **Google Chrome: Chrome-web-store**
    - **Mozilla Firefox: Mozilla-addons**
- From here onwards we are taking Mozilla Firefox as reference, the settings for Google Chrome remain the same.
- Once you install the extension pack, you can verify installation by clicking on the puzzle piece icon in the top bar of the browser.



- We need to tell foxyproxy where to send the browser traffic to (this would be to our ZAP service). Further we do not want to send all browser traffic, it will make it difficult to analyze. We only want to send traffic of the website of interest. Assuming ZAP is running locally and say listening on port 30003. Further assuming the website of interest is also running locally and is on port 30000. We can specify all this in foxyproxy as below. See figure. Click on extensions, then foxyproxy, then options, then proxies tab. Click on “Add” and fill the form as shown. Further click on “+” and follow steps 1,2,3 and 4 as indicated in

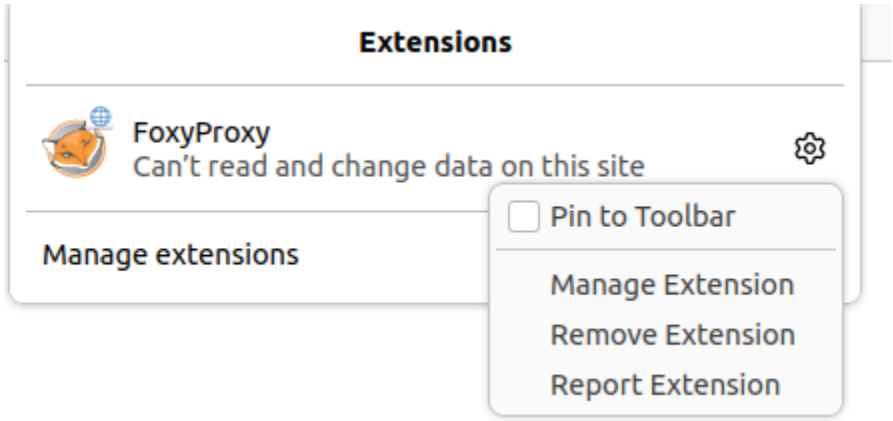
figure.

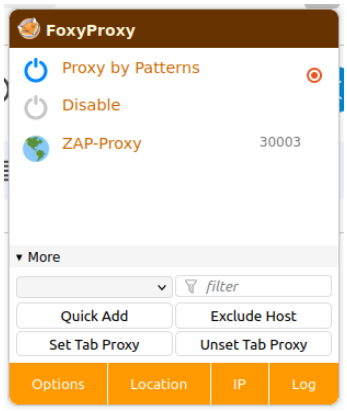




- You should see FoxyProxy under extensions and for convenience, you can also pin the foxyproxy icon to the top bar, by clicking on settings and then check the box Pin to toolbar.

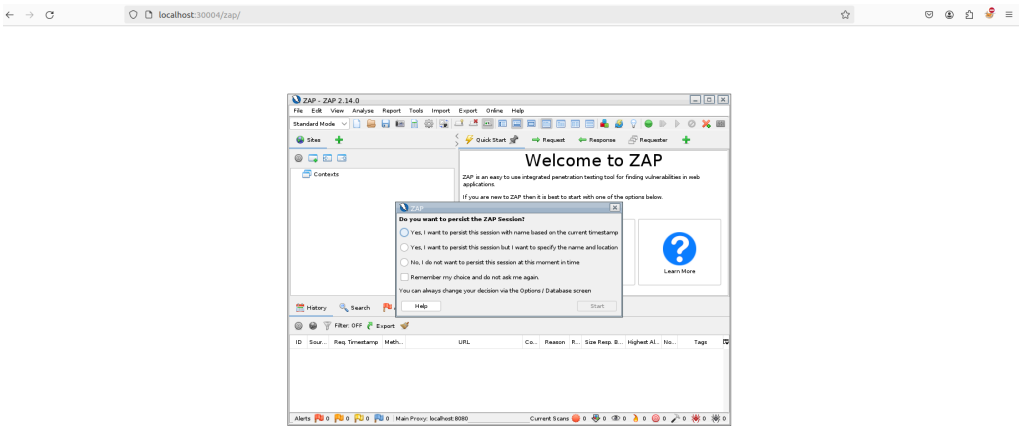
Clicking on Foxyproxy icon should show you “Proxy by Patterns”, enable it i.e. red dot against it.



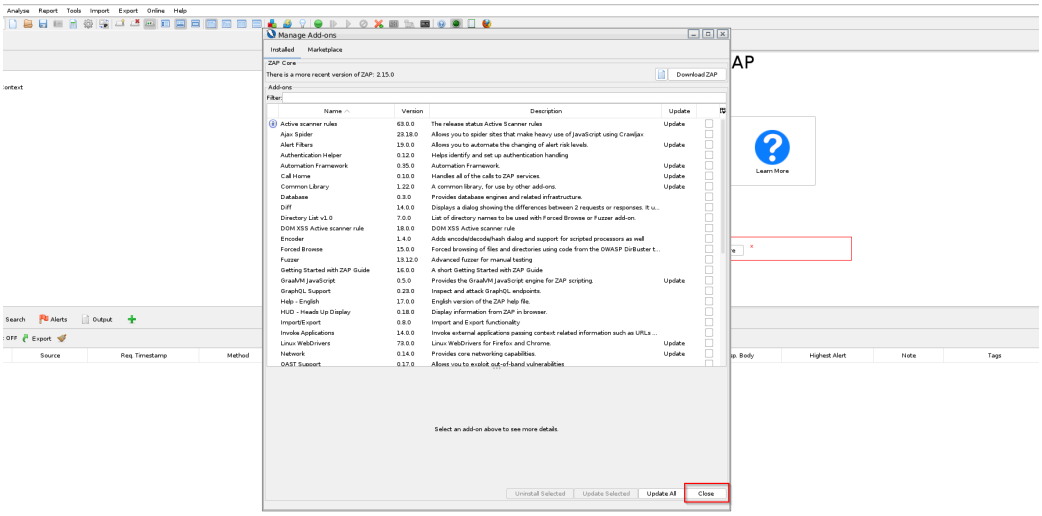


Step-2: ZAP Setup

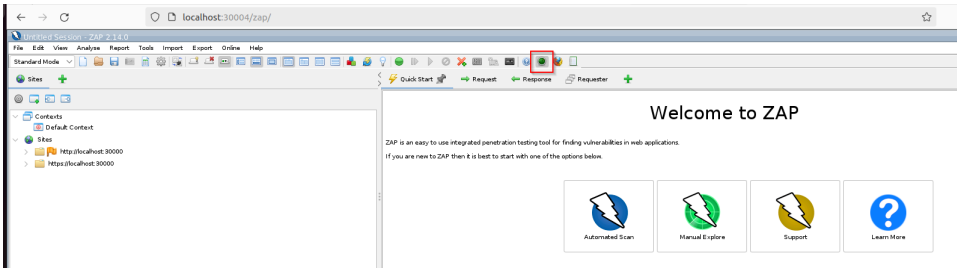
Instead of you having to install ZAP, as part of our cLab app, we have provided you with a container with ZAP installed. Note: ZAP is not running directly on your local host, it is running in a container launched by our clab app. You can however access it via a local browser i.e. browser running on your local host. To access the web interface of ZAP, visit “http://localhost:30004/zap/”. Note the ZAP application may take up to 2 minutes to start. In the meantime it may see “unable to connect” or blank screen or no connection etc, but just wait a while. Once the application is loaded, you should see a window like below



- Select “No, I do not want to persist …” option and then press on “start”. You will be given a new popup window asking you to update as shown in the image below. Press on “Cancel”, **DO NOT UPDATE** , since it may cause autograders to fail.

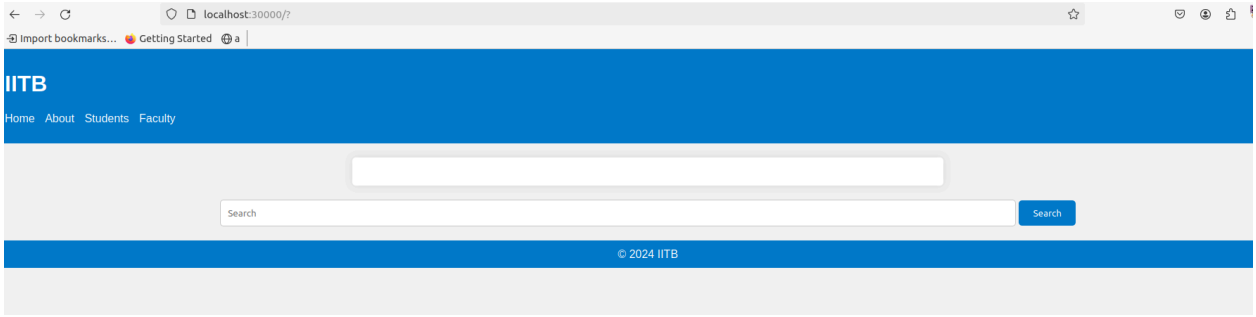


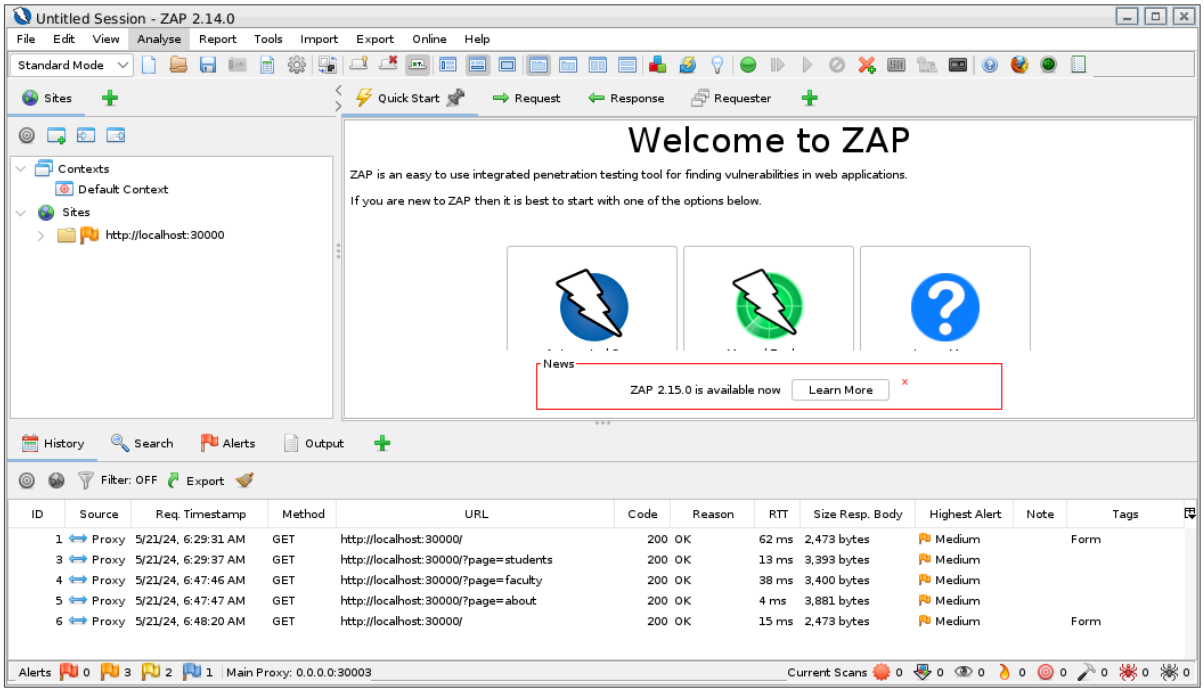
- By default ZAP converts any and all HTTP requests to HTTPS requests but our labs deal with http i.e. websites built on http for ease of setup and analysis. To avoid auto-conversion of protocols, we have to disable “HUD”. To do that go to our ZAP application, and click on the “Disable HUD” option as shown below. You may have to make ZAP window full screen to see the option. Hover over the icons, it will tell you if your selection is right.



Step-3: Check Overall Setup

If everything works, when you visit the local website i.e. “http://localhost:30000/” as configured, you should see the traffic in ZAP window. Be sure HUD is disabled. You can use the broom icon to clear the screen

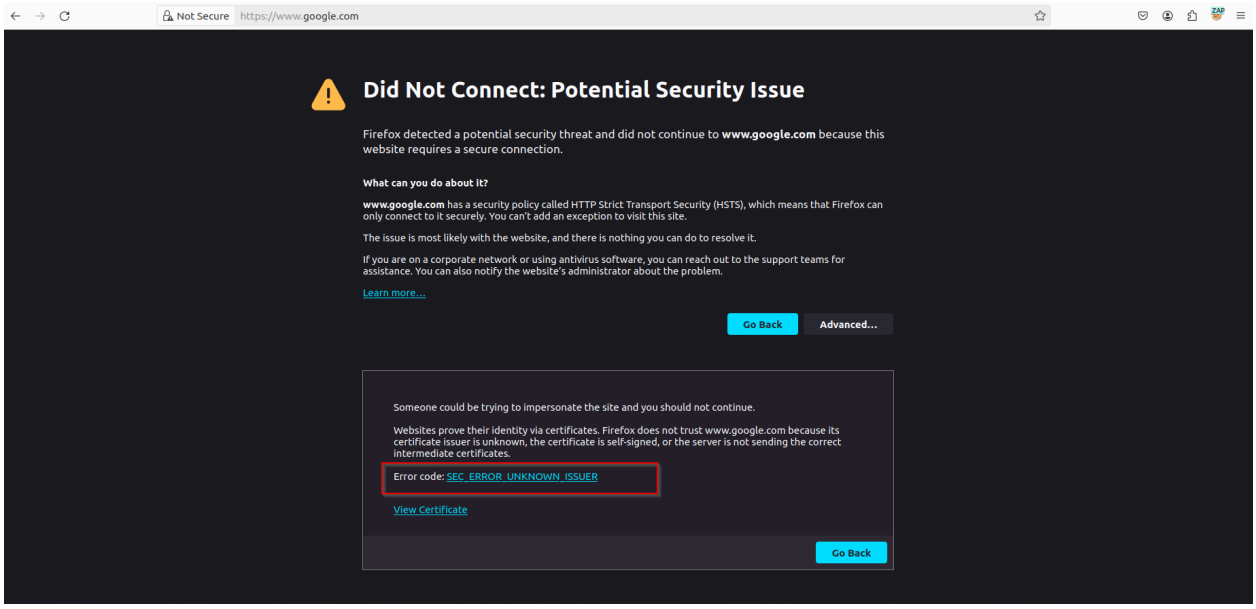




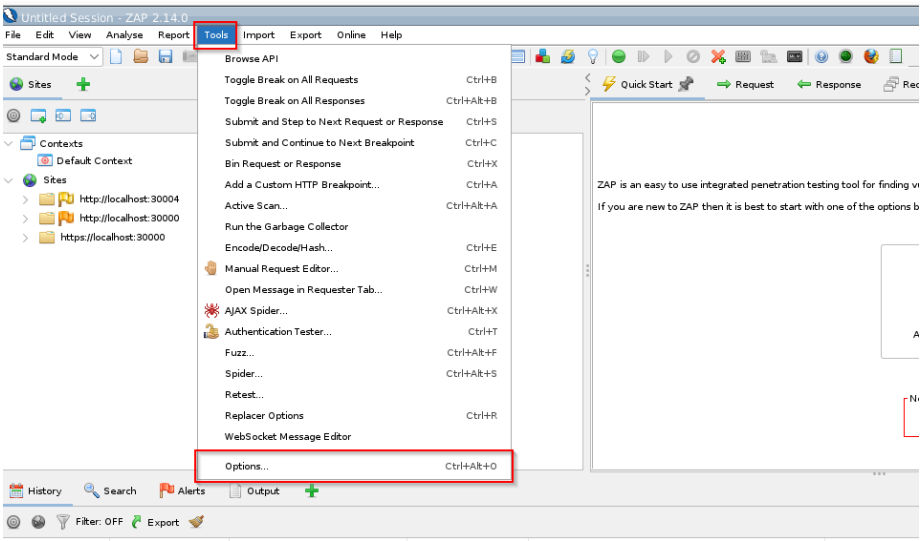
Step-4: [OPTIONAL] Enable ZAP proxy for HTTPS traffic

NOTE that this is an OPTIONAL setting, and will not be required for any lab activity. This is for information purposes.

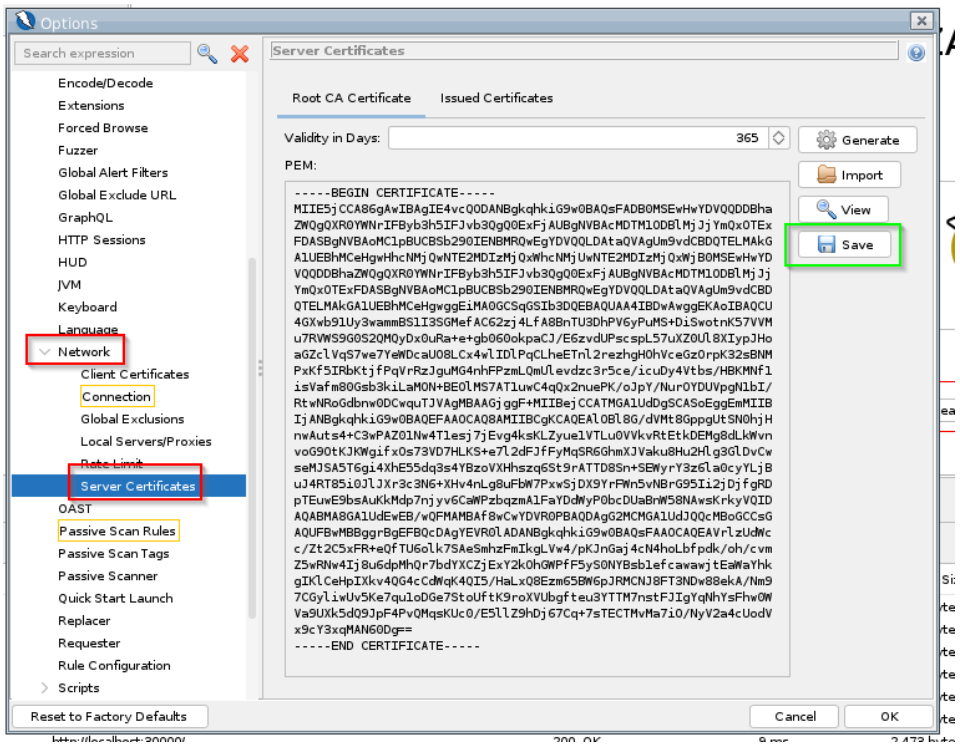
- In the previous steps, we enabled ZAP proxy HTTP traffic. To enable ZAP proxy for HTTPS traffic we have to authorize the SSL certificate in our browser, generated by the ZAP application.
- Let's assume we want to proxy HTTPS traffic of "https://www.google.com" through the ZAP application. Before we achieve this, let's see what our current proxy setting does. Enable the proxy setting using FoxyProxy, and go to "https://www.google.com" . You will see below the error generated by our browsers.
    - The reason behind generating this error, is because when the HTTPS traffic is proxied through ZAP application, the SSL certificate used locally by ZAP application is not recognized by our browser and thus our browser thinks of it as some kind of MITM attack and blocks the request. Hence the error "SEC_ERROR_UNKNOWN_ISSUER".



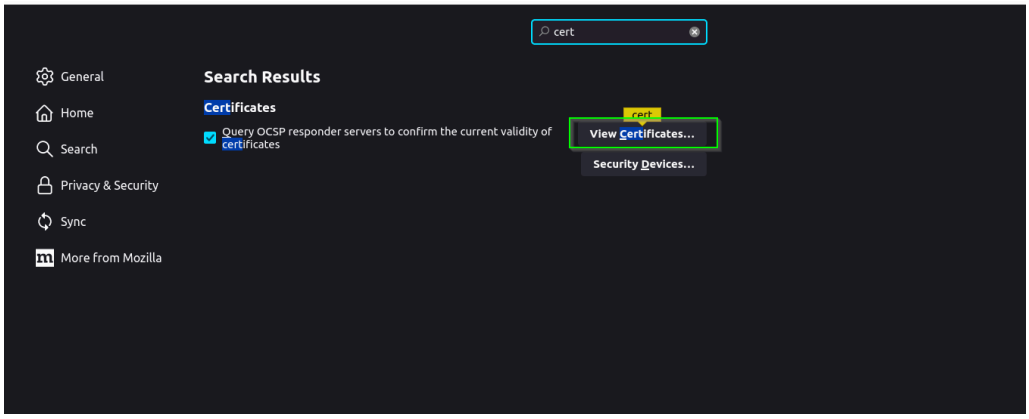
- To overcome this error, disable the proxy setting from FoxyProxy first, and then we can add our ZAP application's SSL certificate in the authorized certificate list of our browser. To do that, go to the ZAP application -> tools -> options menu. You will see the options menu pop-up for you as below.



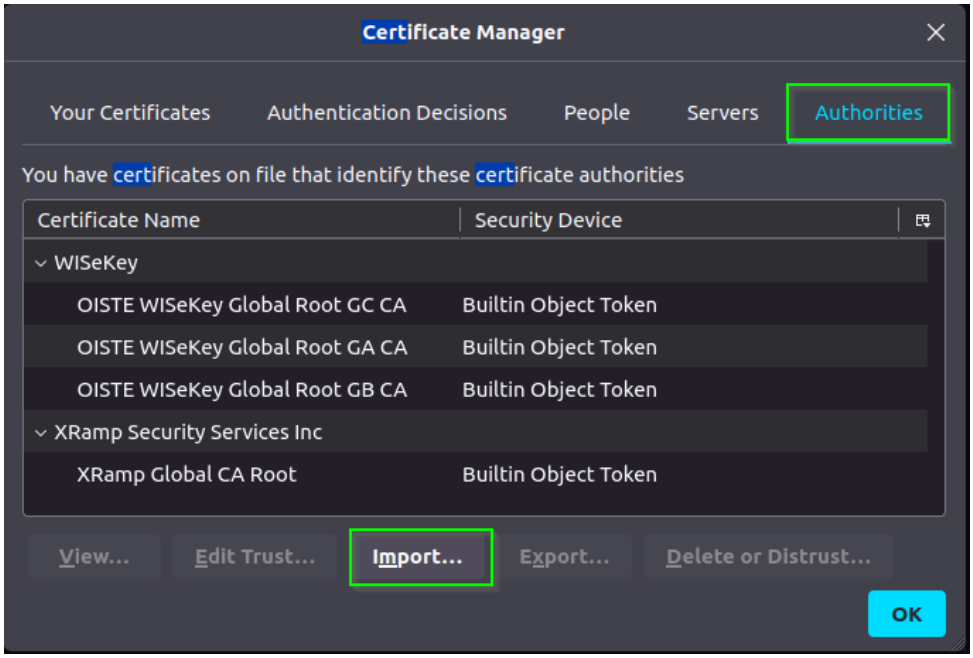
- Now go to Network -> Server Certificate, and press on the "Save" button as shown in the image below and save the certificate in a location you can access easily.



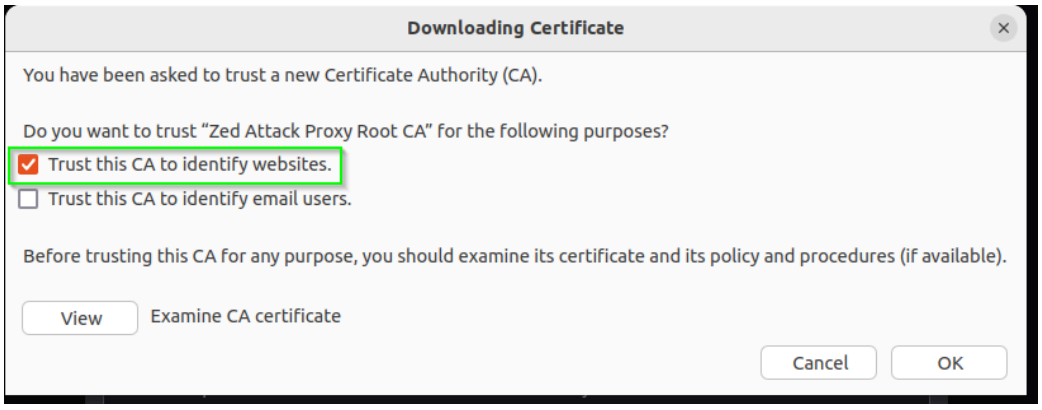
- Now in your browser, go to settings and search for “certificate”, you will see 2 options (for chrome options may differ) as shown in the image below. Click on the “View Certificates” option here.



- You will now see the “View Certificates” dialogue box, go to “Authorities” tab and click on “Import”. Now import the certificate from the location you saved your certificate, and press on “OK”.



- When you import the certificate, you will be prompted with a dialogue box like below. You **MUST** atleast select the option-1 “Trust this CA to identify websites” to be able to proxy through HTTPS protocols.



- Now enable the proxy setting from FoxyProxy first, and revisit the “https://www.google.com” , you will not see any errors and all the HTTP requests will also be proxied through our ZAP application.