Proxy Setup

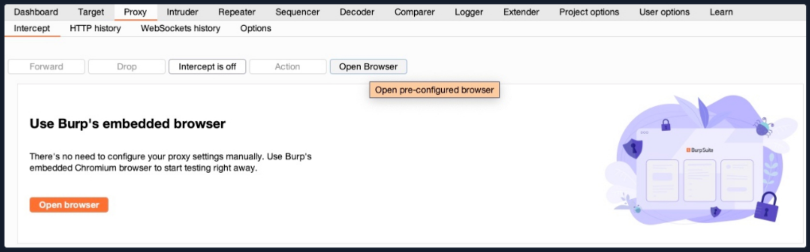
Now that we have installed and started both tools, we'll learn how to use the most commonly used feature; `Web Proxy`.

We can set up these tools as a proxy for any application, such that all web requests would be routed through them so that we can manually examine what web requests an application is sending and receiving. This will enable us to understand better what the application is doing in the background and allows us to intercept and change these requests or reuse them with various changes to see how the application responds.

Pre-Configured Browser

To use the tools as web proxies, we must configure our browser proxy settings to use them as the proxy or use the pre-configured browser. Both tools have a pre-configured browser that comes with pre-configured proxy settings and the CA certificates pre-installed, making starting a web penetration test very quick and easy.

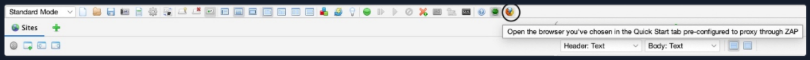
In Burp's (`Proxy>Intercept`), we can click on `Open Browser`, which will open Burp's pre-configured browser, and automatically route all web traffic through Burp:



Use Burp's embedded browser

There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

In ZAP, we can click on the Firefox browser icon at the end of the top bar, and it will open the pre-configured browser:



Open the browser you've chosen in the Quick Start tab pre-configured to proxy through ZAP

For our uses in this module, using the pre-configured browser should be enough.

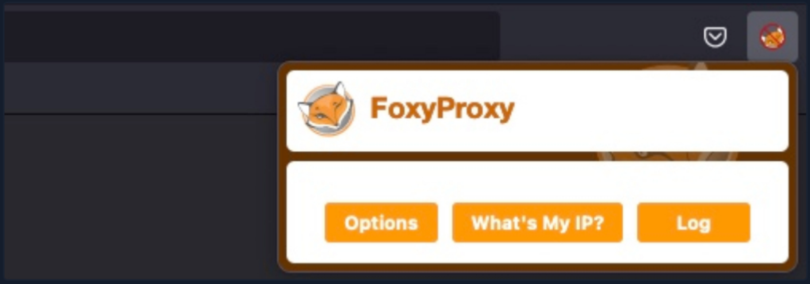
Proxy Setup

In many cases, we may want to use a real browser for pentesting, like Firefox. To use Firefox with our web proxy tools, we must first configure it to use them as the proxy. We can manually go to Firefox preferences and set up the proxy to use the web proxy listening port. Both Burp and ZAP use port `8080` by default, but we can use any available port. If we choose a port that is in use, the proxy will fail to start, and we will receive an error message.

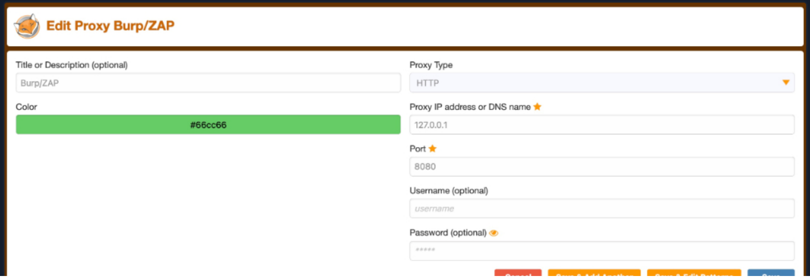
> **Note:** In case we wanted to serve the web proxy on a different port, we can do that in Burp under (`Proxy>Options`), or in ZAP under (`Tools>Options>Local Proxies`). In both cases, we must ensure that the proxy configured in Firefox uses the same port.

Instead of manually switching the proxy, we can utilize the Firefox extension Foxy Proxy to easily and quickly change the Firefox proxy. This extension is pre-installed in your PwnBox instance and can be installed to your own Firefox browser by visiting the Firefox Extensions Page and clicking `Add to Firefox` to install it.

Once we have the extension added, we can configure the web proxy on it by clicking on its icon on Firefox top bar and then choosing `options`:



Once we're on the `options` page, we can click on `add` on the left pane, and then use `127.0.0.1` as the IP, and `8080` as the port, and name it `Burp` or `ZAP`:



Edit Proxy Burp/ZAP

Title or Description (optional)	Burp/ZAP
Color	#66cc66
Proxy Type	HTTP
Proxy IP address or DNS name ★	127.0.0.1
Port ★	8080
Username (optional)	username
Password (optional)	*****

Cheat Sheet

Table of Contents

Getting Started

Web Proxy

Web Fuzzer

Web Scanner

Skills Assessment

My Workstation

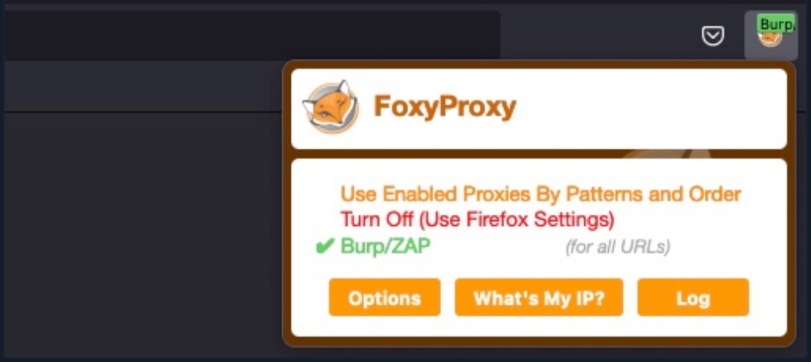
OFFLINE

Start Instance

∞ / 1 spawns left

Note: This configuration is already added to Foxy Proxy in PwnBox, so you don't have to do this step if you are using PwnBox.

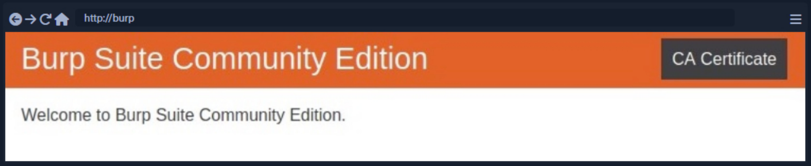
Finally, we can click on the `Foxy Proxy` icon and select `Burp/ZAP`.


Burp
FoxyProxy
Use Enabled Proxies By Patterns and Order
Turn Off (Use Firefox Settings)
✔ Burp/ZAP
(for all URLs)
Options
What's My IP?
Log

Installing CA Certificate

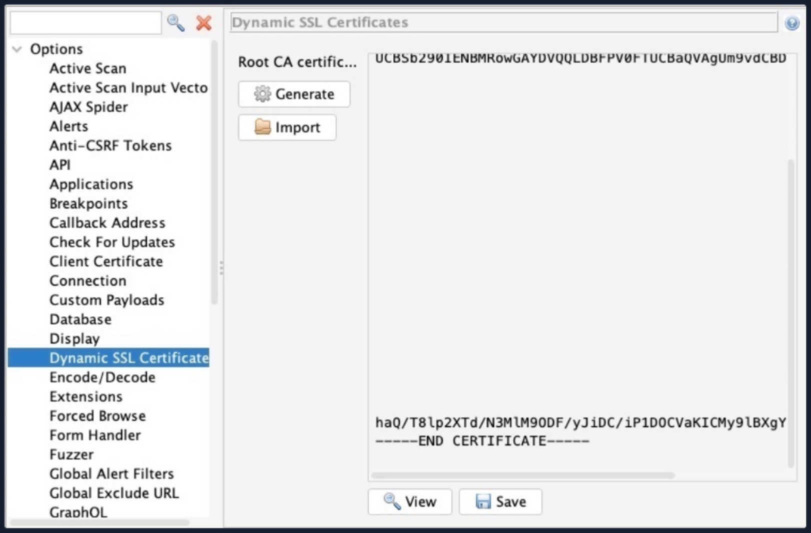
Another important step when using Burp Proxy/ZAP with our browser is to install the web proxy's CA Certificates. If we don't do this step, some HTTPS traffic may not get properly routed, or we may need to click `accept` every time Firefox needs to send an HTTPS request.

We can install Burp's certificate once we select Burp as our proxy in `Foxy Proxy`, by browsing to `http://burp`, and download the certificate from there by clicking on `CA Certificate`:



Welcome to Burp Suite Community Edition.

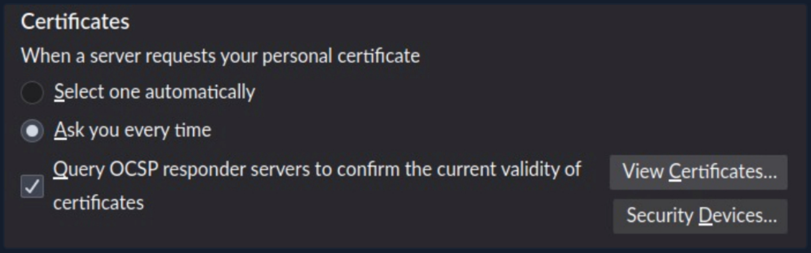
To get ZAP's certificate, we can go to (`Tools>Options>Dynamic SSL Certificate`), then click on `Save`:



```
UCBSb290IENBMRowGAYDVQQLDBFPV0FTUCBaQVAgUm9vdCBD
haQ/T8lp2XTd/N3MlM9ODF/yJiDC/iP1DOCVaKICMy9lBXgY
-----END CERTIFICATE-----
```

We can also change our certificate by generating a new one with the `Generate` button.

Once we have our certificates, we can install them within Firefox by browsing to about:preferences#privacy, scrolling to the bottom, and clicking `View Certificates`:



Certificates

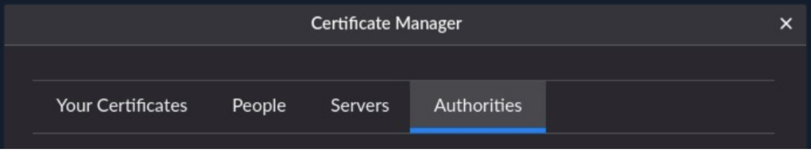
When a server requests your personal certificate

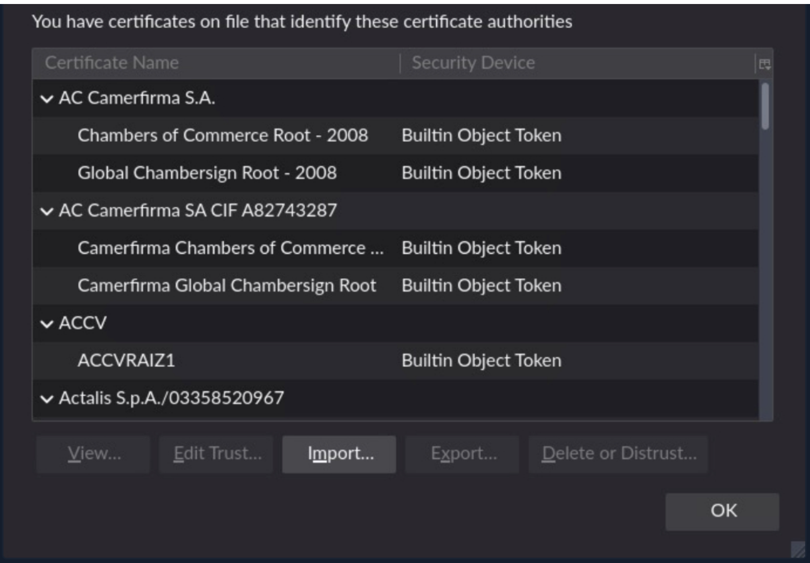
○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

After that, we can select the `Authorities` tab, and then click on `import`, and select the downloaded CA certificate:

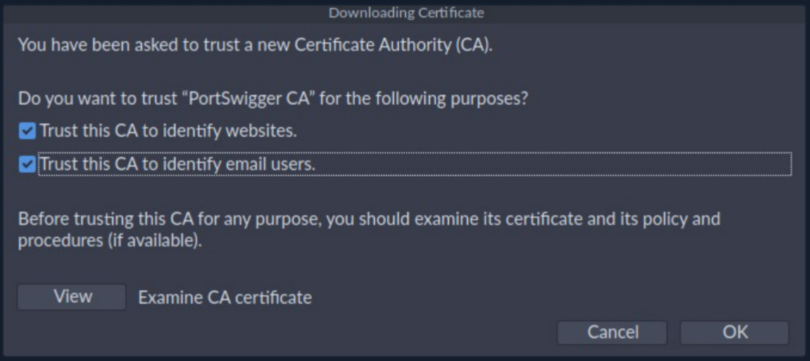




You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce ...	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
ACCV	
ACCVRAIZ1	Builtin Object Token
Actalis S.p.A./03358520967	

Finally, we must select `Trust this CA to identify websites` and `Trust this CA to identify email users`, and then click OK:



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "PortSwigger CA" for the following purposes?

☑ Trust this CA to identify websites.

☑ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Once we install the certificate and configure the Firefox proxy, all Firefox web traffic will start routing through our web proxy.

← Previous Next → Mark Complete & Next