1.0 Lab Setup & Access

This document contains the list of resources to set up a local environment to access the labs taught in the course.

The instructor makes use of a Kali Linux VM installed using VMWare. In the Kali Linux VM, the following four tools are used throughout the course.

- Burp Suite Community Edition (Pre-installed in Kali)
- Burp Suite Professional Edition (Requires installation and purchase)
- Visual Studio (requires free installation)
- FoxyProxy Firefox extension (requires free installation)

Once the setup of the local environment is completed, the labs are accessible from a free online platform called the Web Security Academy. This platform is created and maintained by PortSwigger.

Students are free to use any local environment they wish to use. It is not required to follow the steps outlined in this document to set up a local environment.

1.1 Local Environment Setup

This section provides you with the setup instructions for the local environment used by the instructor.

1.1.1 VMware / VirtualBox Setup

The instructor makes use of VMware Fusion Player to install the Kali Linux virtual machine. Depending on the operating system used by the student, either one of the following two recommended options can be used to install and host virtual machines.

- VirtualBox: https://www.virtualbox.org/wiki/Downloads
- VMware Fusion: https://www.vmware.com/ca/products/fusion/fusion-evaluation.html

Follow the instructions on the above listed links to download and install VirtualBox / VMware.

1.1.2 Kali Linux Installation

The instructor makes use of a Kali Linux virtual machine to access and attack the intentionally vulnerable labs. Kali Linux is an open-source operating system that was designed for penetration testing. It comes pre-installed with many offensive security tools, including the Burp Suite tool which will be used in the course.

To download the latest version of the Kali Linux VM, select one of the options provided in the following link depending on whether you have VirtualBox, or VMware installed.

- https://www.kali.org/get-kali/#kali-virtual-machines

Refer to online resources (blogs, videos, etc.) for step-by-step instructions on how to install Kali Linux on the operating system and hypervisor software you're using.

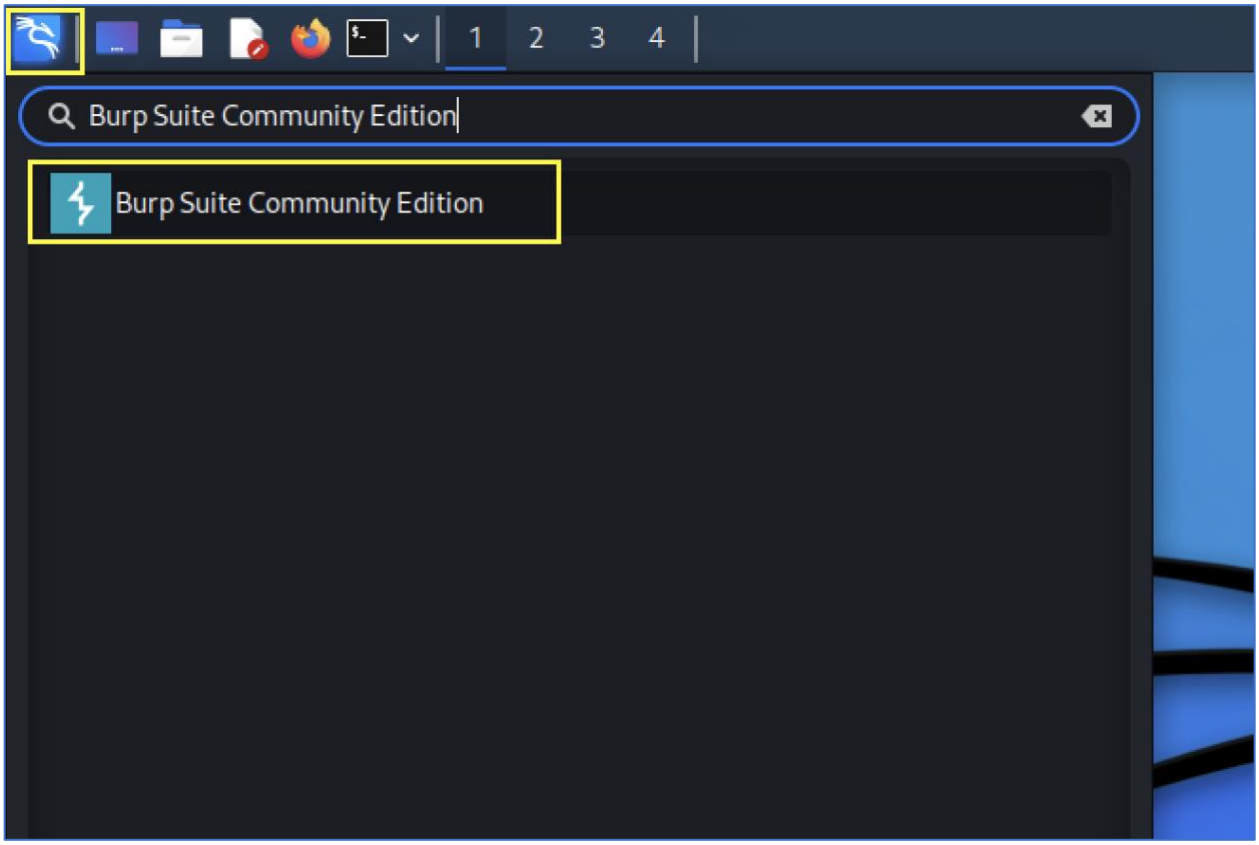
1.1.3 Kali Linux Setup

Once the Kali Linux virtual machine is up and running, the following tools will be used in the lab videos of the course.

- Burp Suite Community Edition (Pre-installed in Kali)
- Burp Suite Professional Edition (Requires installation and purchase)
- Visual Studio (requires free installation)
- FoxyProxy Firefox extension (requires free installation)

Access to Burp Suite Community Edition

Burp Suite Community Edition comes pre-installed in Kali Linux and can be accessed by selecting the search icon at the top left of the VM and searching for “Burp Suite Community Edition”.



Click on **Burp Suite Community Edition** to start up Burp, then select **Next** > **Start Burp**.

Installation and Access to Burp Suite Professional

Burp Suite Professional does not come pre-installed in Kali Linux and requires purchase. Most of the lab videos in the course do not make use of the Professional version. The Professional version is only used when access to the Intruder and Collaborator functionality is required.

Students are not required to purchase Burp Suite Professional. Students that don't have the Professional version and do not wish to buy it, can simply watch the related videos to understand how to use the functionality included in the professional version.

If you wish to buy and install Burp Suite Professional, use the following link:

- https://portswigger.net/burp/pro

Installation and Access to Visual Studio

Visual Studio is a code editor that is used by the instructor to develop and run Python scripts. It does not come pre-installed in Kali Linux; however, it can be downloaded for free for personal use.

To download and install Visual Studio on the Kali Linux VM, apply the steps outlined in the following link:

- https://www.ceos3c.com/security/install-vscode-on-kali-linux-easiest-way/?expand_article=1

FoxyProxy Extension (NOT REQUIRED)

FoxyProxy is a Firefox extension that simplifies configuring the browser to access proxy servers. At the time of recording, Burp Suite did not have a built-in browser, therefore, the instructor used the FoxyProxy extension to easily configure the browser to send requests to Burp.

Since the new version of Burp contains a built-in browser (refer to section 1.3 "Intercept Requests Using Burp Proxy"), it is highly recommended that students use the built-in browser.

However, if you wish to install the extension, it can be downloaded and installed using the following link:

- https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/

1.2 Web Security Academy Access

The Web Security Academy is a free online web security training platform that is created and maintained by PortSwigger. The academy is an excellent resource to learn about web application security. Each topic covered in the Academy contains interactive labs that allow you to gain hands-on experience exploiting real world vulnerabilities in a safe and legal manner.

This course uses several modules in the Web Security Academy platform; therefore, attendees are required to create an account on the platform.

1.2.1 Register an Account

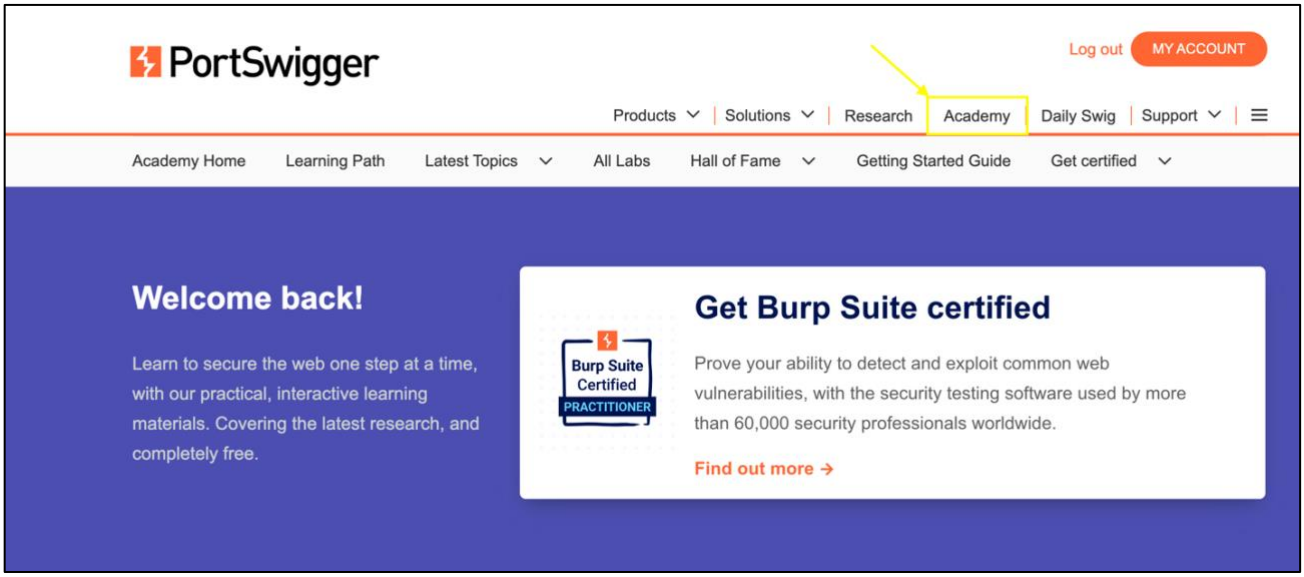
To register an account on the Web Security Academy, enter your email address on the following link: https://portswigger.net/users/register.

Once the email address is submitted, an email will be sent with instructions on how to complete your registration.

1.2.2 Log Into the Academy

To log into the Web Security Academy, enter your email address and associated password on the Login page: https://portswigger.net/users.

Next, click on the Academy tab to access the Web Security Academy.



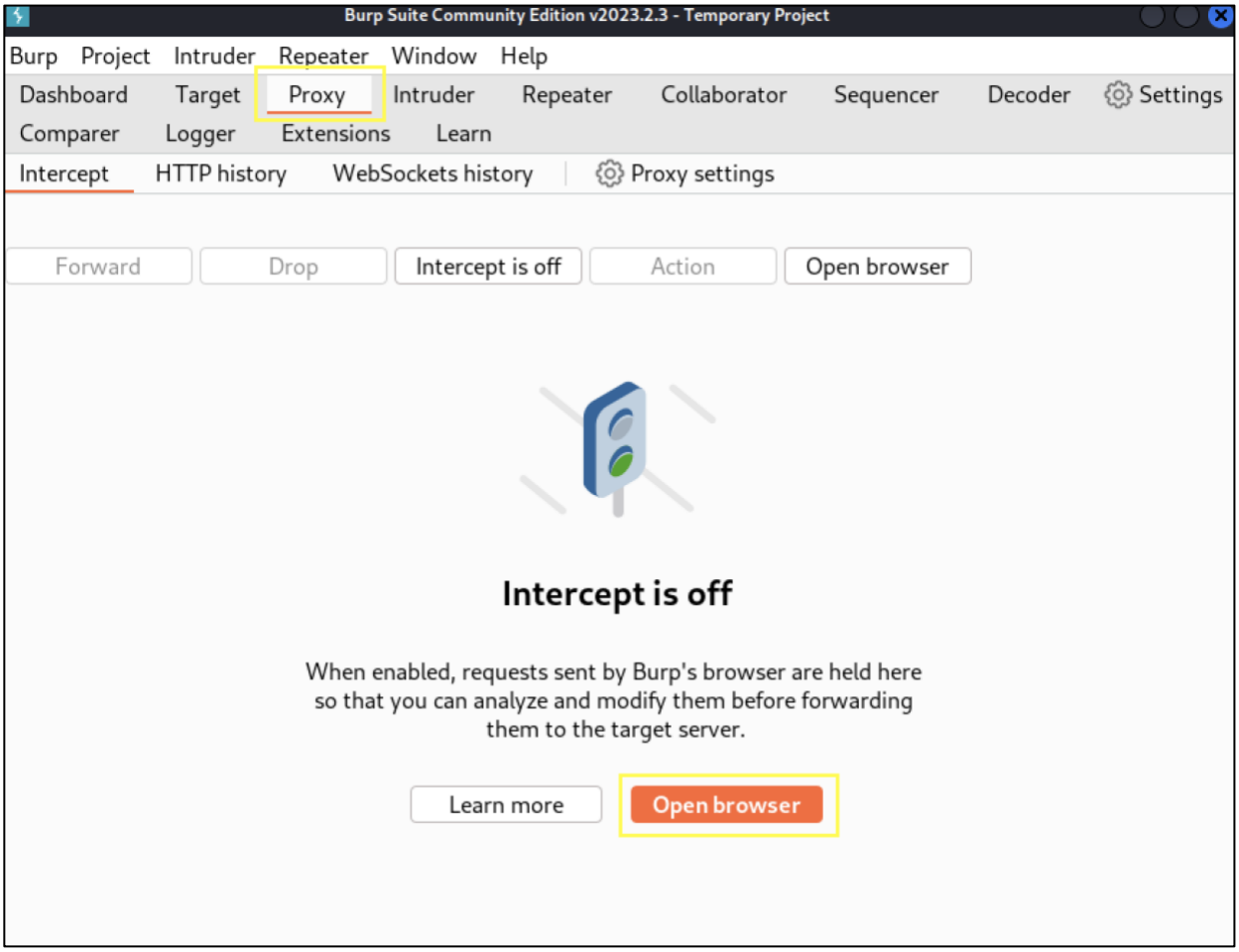
1.3 Intercept Requests Using Burp Proxy

Burp Proxy is a component of Burp Suite that is used for intercepting, viewing, and modifying requests and responses passing between the browser and the application that requires testing.

The latest version of Burp Suite contains a built-in browser that does not require configuration. In this section, we'll discuss how to access the built-in browser in the latest version and how to configure previous versions of Burp.

1.3.1 Latest Version of Burp (Preferred)

Students are strongly recommended to use the latest version of Burp Suite that contains a built-in browser. To access the built-in browser, open Burp and visit the **Proxy** tab. Then click on **Open browser**.

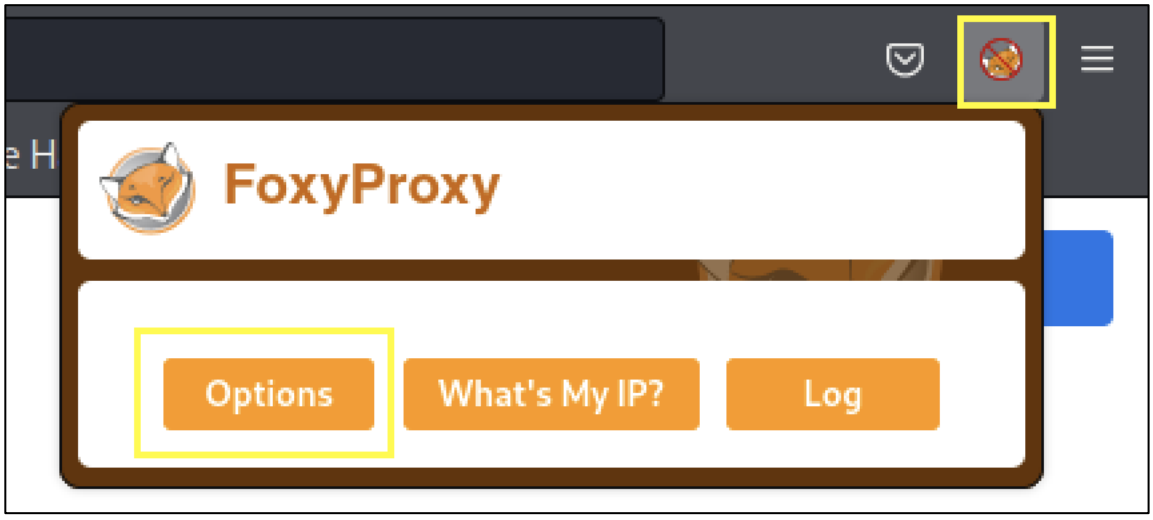


The built-in browser will automatically send requests to Burp and does not require any further configuration.

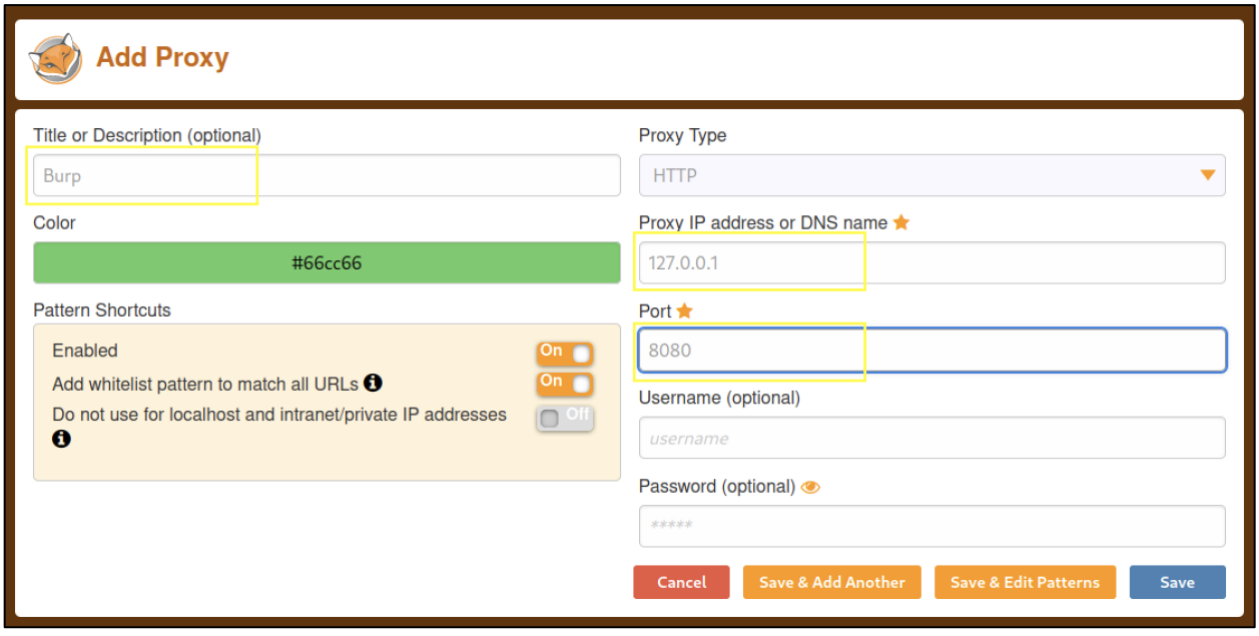
1.3.2 Previous Versions of Burp (Not Preferred)

Students are strongly recommended to use the latest version of Burp Suite that contains a built-in browser. However, if you're using a previous version of Burp that does not contain a built-in browser, then apply the following steps to configure the browser using the FoxyProxy extension.

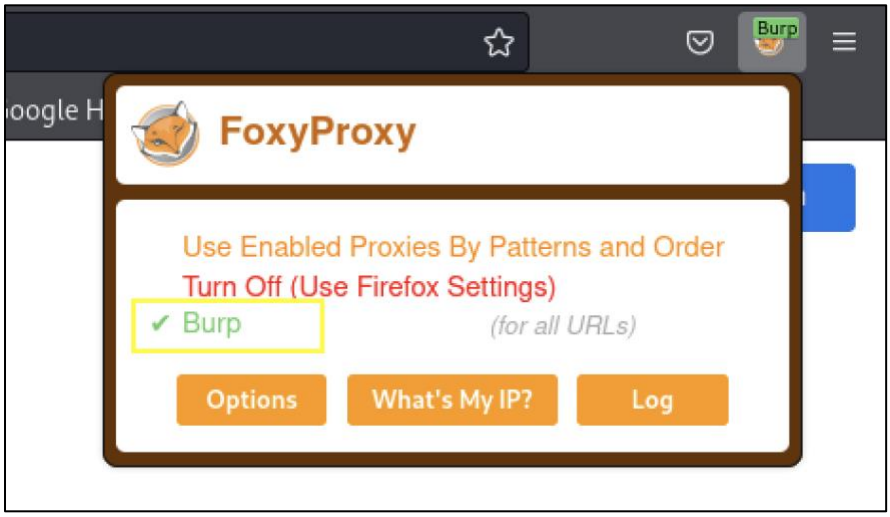
After the FoxyProxy extension is installed (refer to section 1.1.3 "Kali Linux Setup"), click on the FoxyProxy icon on the top right of the browser and select **Options**.



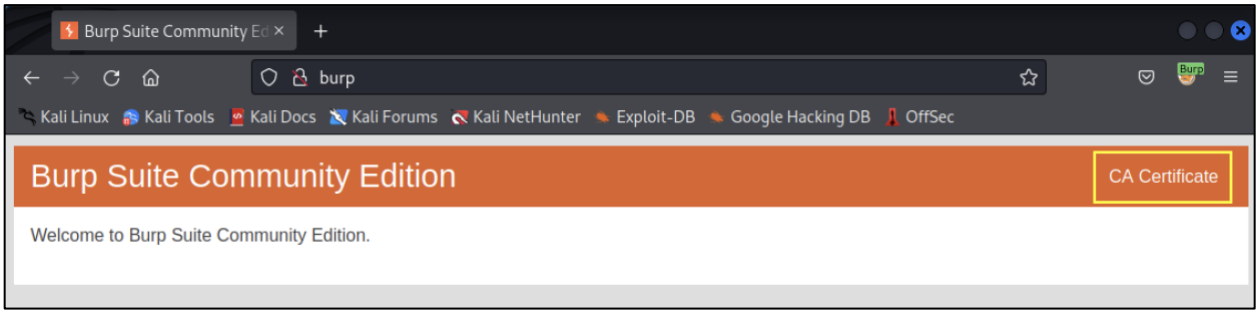
Then add the following Burp proxy configuration and save it.



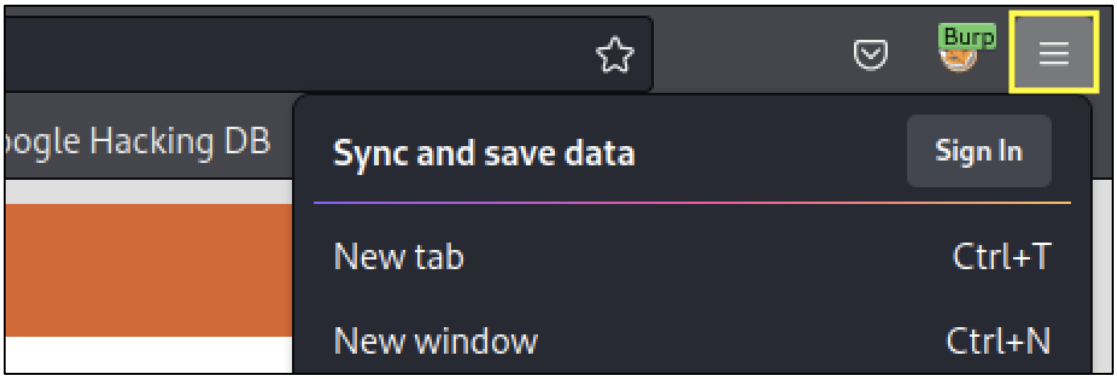
To send requests to Burp, click on the FoxyProxy icon in the browser and select the newly added option “Burp”.



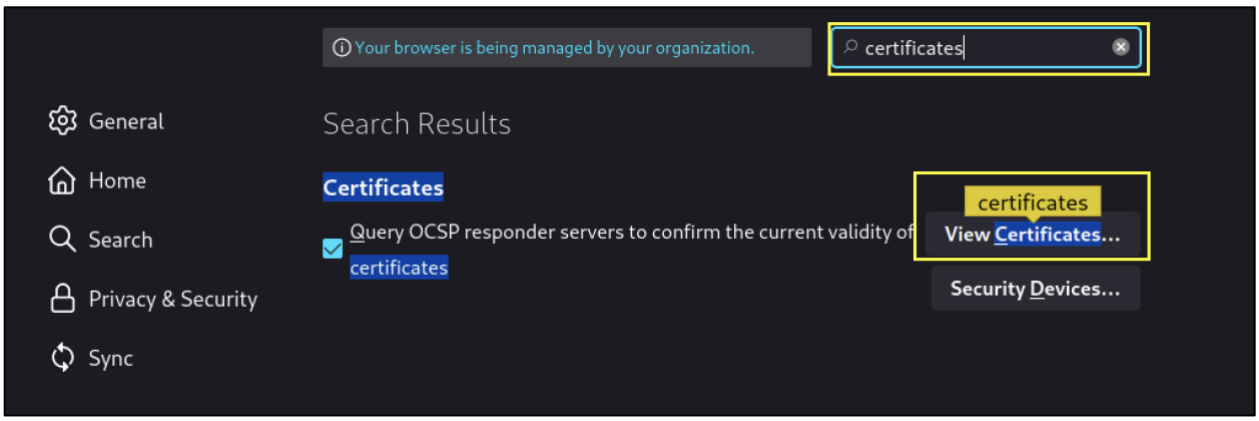
Next, the Burp Suite certificate needs to be added to the browser. First, visit the URL http://burp and click on **CA Certificate**.



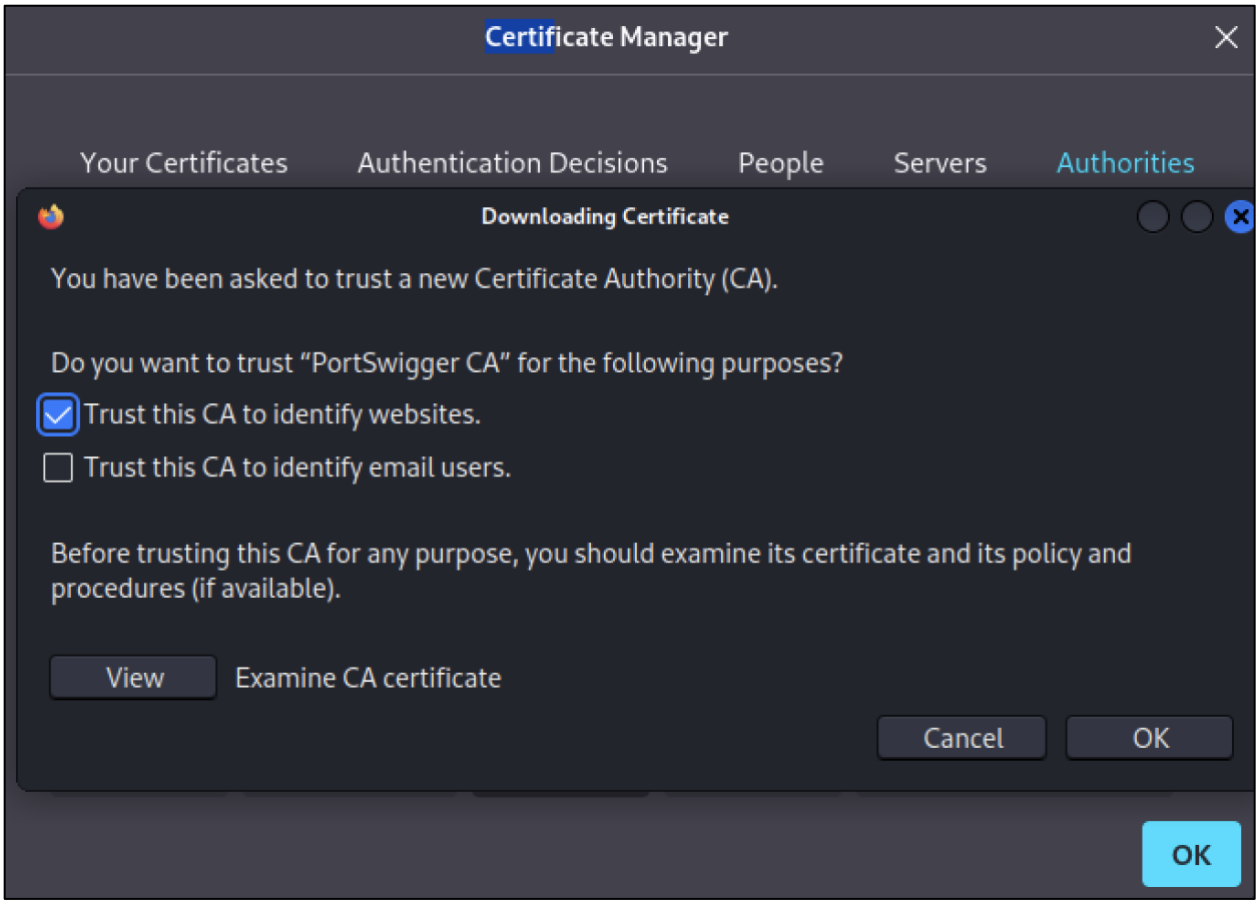
Select **Save File** and then select **OK**. Next, select the Open Menu icon in the browser.



Select **Settings**, then search for “certificates” in the **Find in Preferences** search bar. Next, click on **View Certificates**.



Click on **Import**, then select the options **Trust this CA to identify websites** and select **OK**.



Now the browser is configured to send all requests to Burp.