

Lab – Configuring BurpSuite as a Proxy

Overview

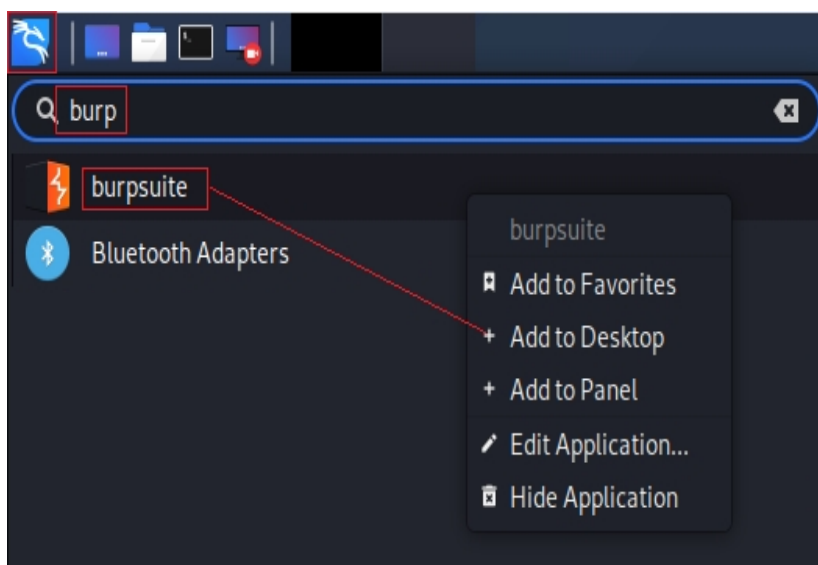
In this short lab, you will learn how to set up BurpSuite using a virtual install of Kali Linux. Burp or BurpSuite is a set of tools used for penetration testing of web applications. Developed by the company named Portswigger, BurpSuite aims to be an all in one set of tools, and its capabilities can be enhanced by installing add-ons that are called BApps.

Lab Requirements

- Install of VirtualBox with the extension pack
- One updated virtual install of Kali Linux
- Internet connection

Introduction and first time run of BurpSuite

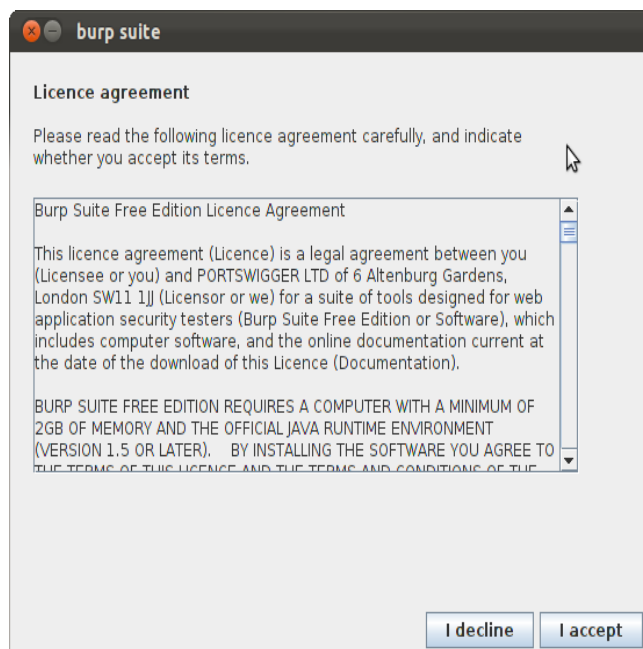
The free BurpSuite community edition comes preinstalled inside of Kali Linux. To access BurpSuite, click on the application launch icon in the upper left corner of your Kali desktop. In the search bar, type **burp**, and from the results, right-click on **burpsuite** and from the context menu, click on **Add to Desktop**.



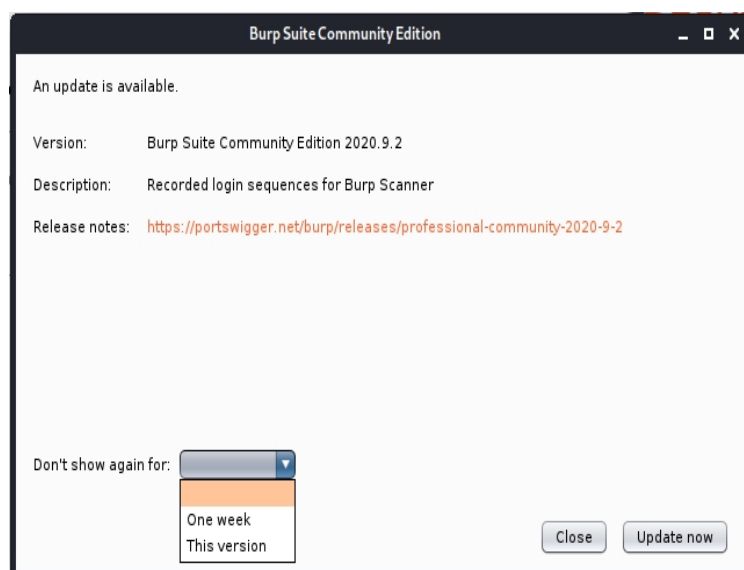
You should now see a shortcut for burpsuite sitting on your desktop. Click on the icon to launch burpsuite for the first time.



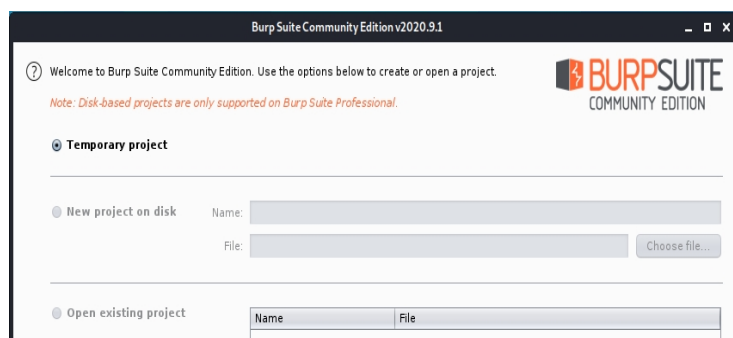
Accept the license agreement.



You may be prompted to update burpsuite. You may choose to update now or be prompted later using the **Don't show again for:** option:



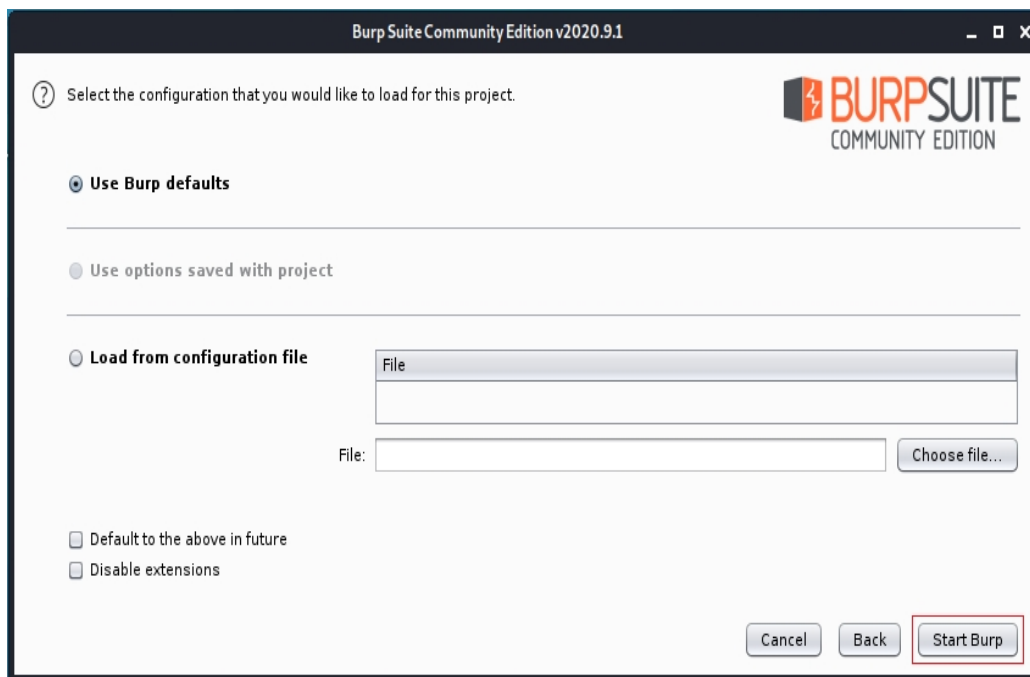
On the next screen, you are introduced to the first limitation of using the free edition as apposed to Burp Suite Professional; you cannot create a disk-based project, only a temporary project. Click Next.



File:

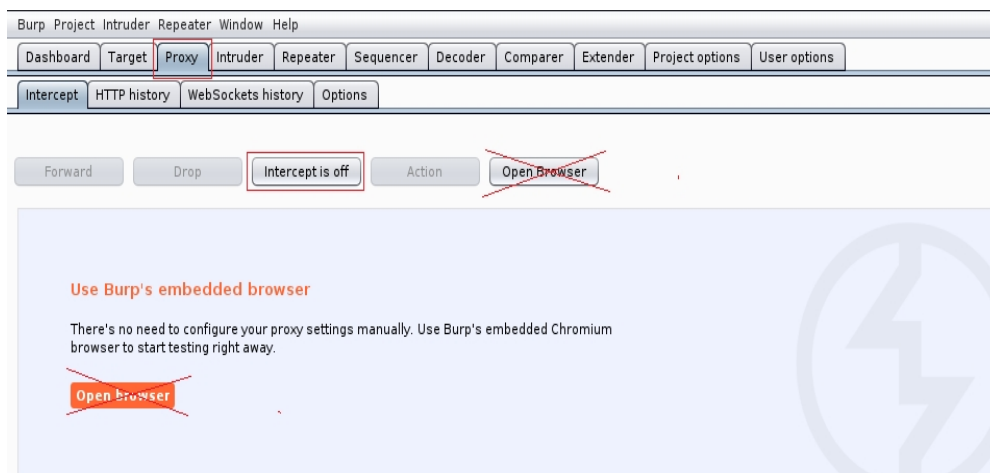
☒ Pause Automated Tasks

On the next screen, accept the default settings and click the Start Burp button.

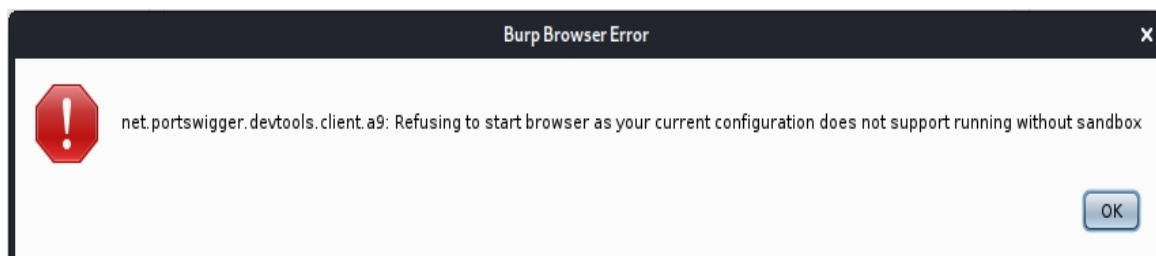


Using the BurpSuite embedded browser (not!)

In the burpsuite project window, click on the Proxy tab.



The idea of using the default browser that comes with burpsuite is to forgo the need to configure the proxy settings of your Kali browser. The burpsuite browser cannot be used as root; when you attempt to launch it, you will receive the following error message:

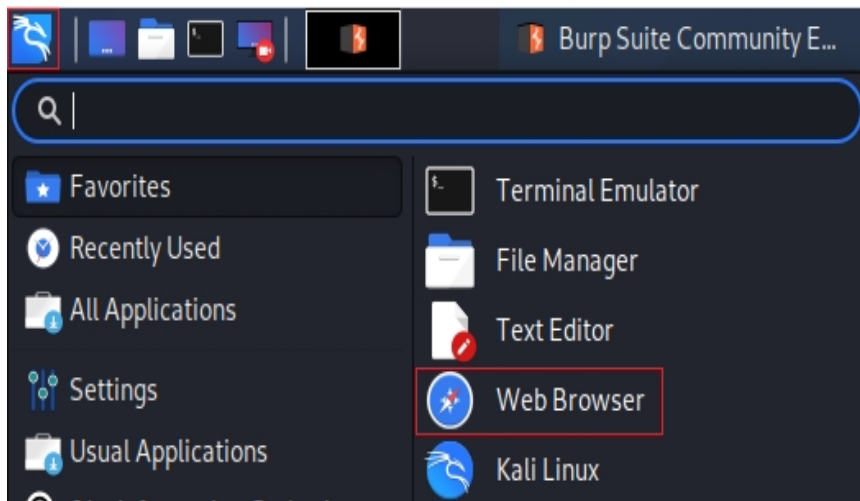


Even as a non-root user, the browser will not launch. Best to configure the proxy settings for

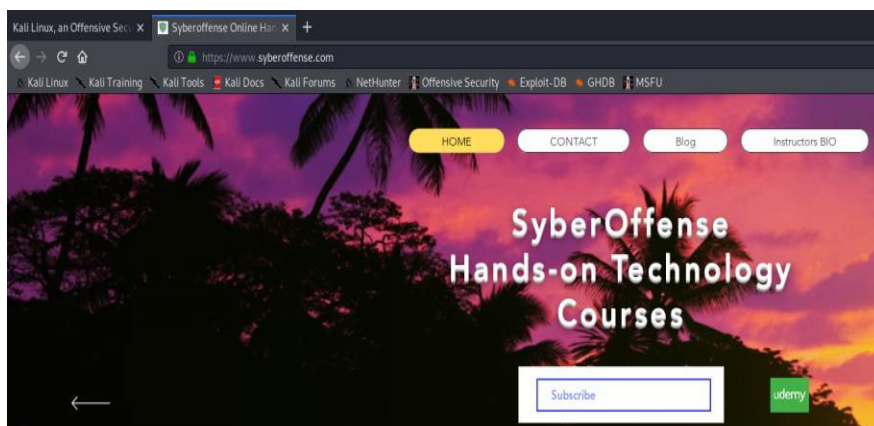
your Kali browser to use burpsuite.

You can turn the intercept off for now.

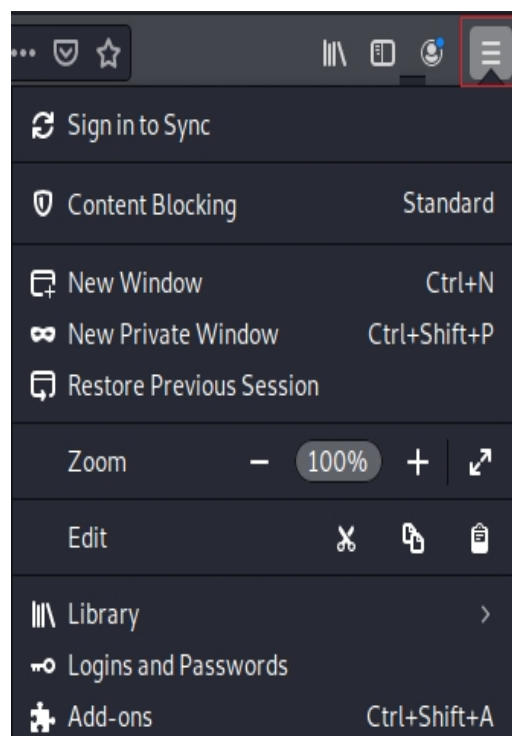
From the Kali application launch, open your Kali browser.





Test your browser to ensure you have Internet access and can access a website.

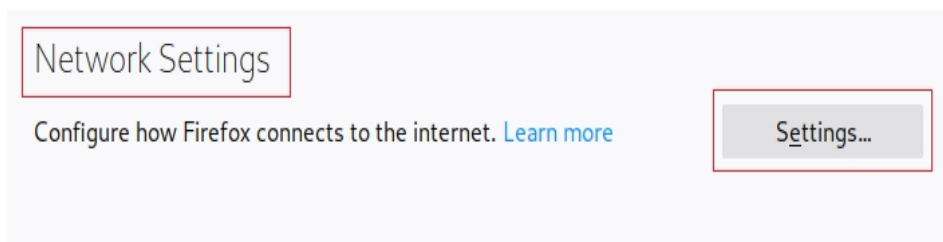


Over to the right of your browsers address bar, expand your browser settings and from the context menu, select **Preferences**:

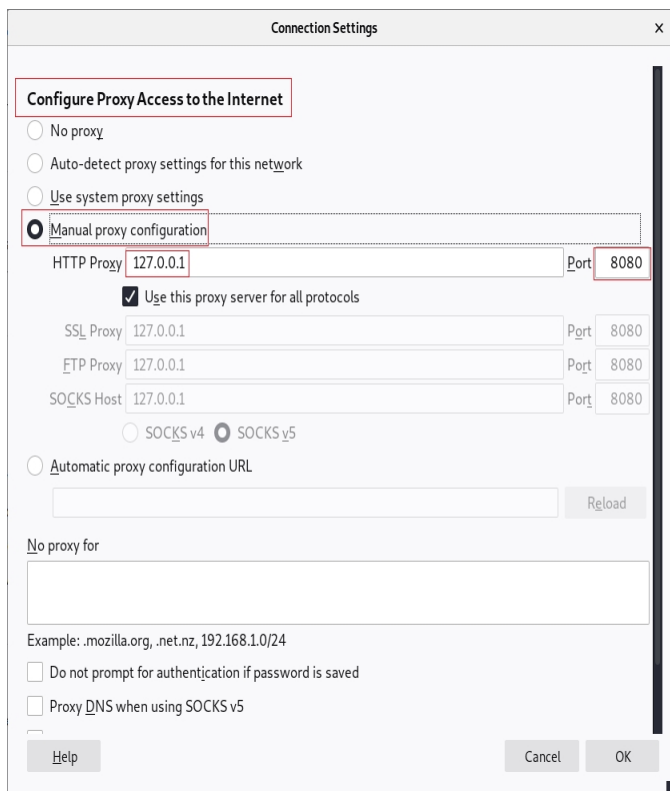


 Preferences Customize...

From the **General** page, scroll down until you come to **Network Settings**. Click on the **Settings** tab.

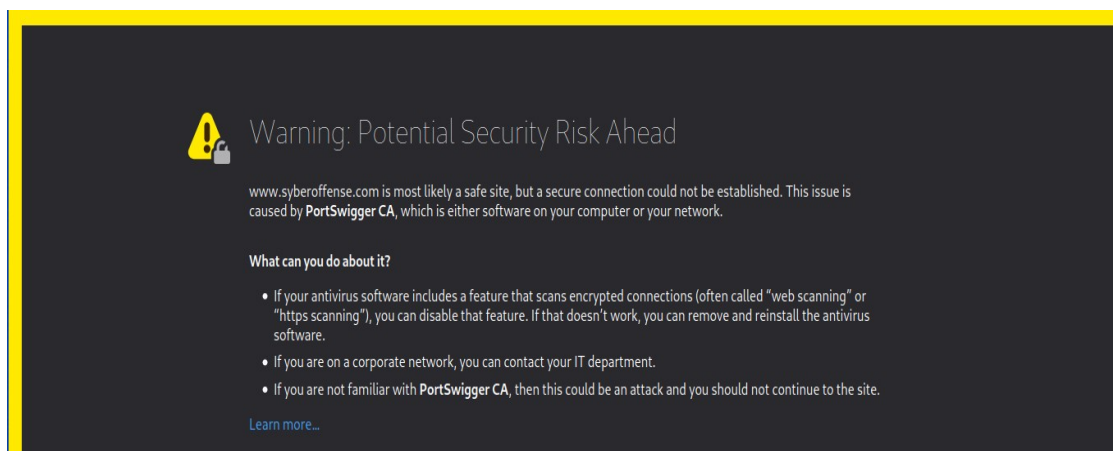


On the Configure Proxy Access to the Internet screen, select the radio button for Manual proxy configuration. For the HTTP proxy, type in 127.0.0.1, and for the port, type in 8080:

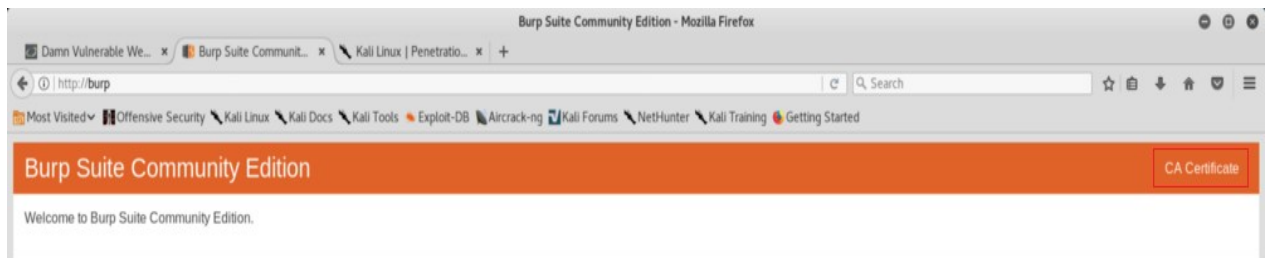


Installing the Portswigger CA

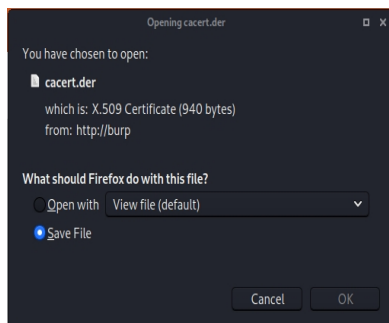
Firefox sees the Portswigger CA as not being trusted; therefore, Firefox will not use burpsuite as an authenticated proxy. To fix this issue, we will need to import the untrusted CA into the Firefox certificate store.



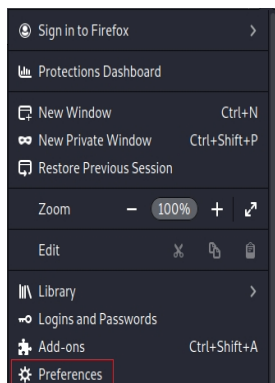
In the address bar of your browser, navigate to <http://burp> and download the certificate by clicking the **CA Certificate** link on the right.



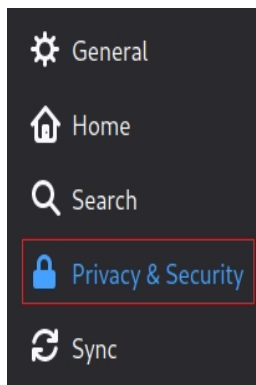
Save the CA to Kali's default location.



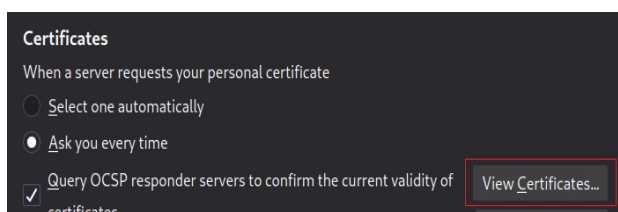
With the browser window still open, go to your browser settings and click on **Preferences**.



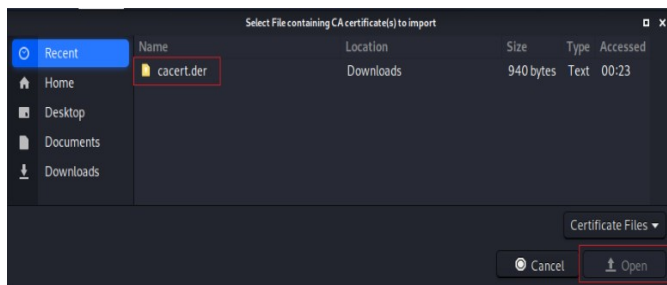
On the next screen, from the menu on the left, click on **Privacy and Security**.



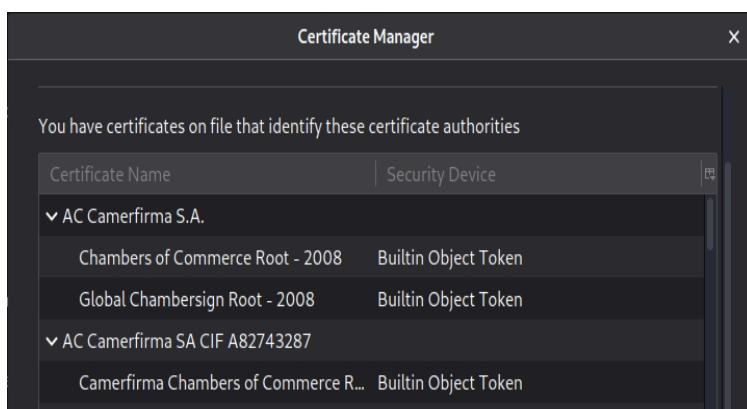
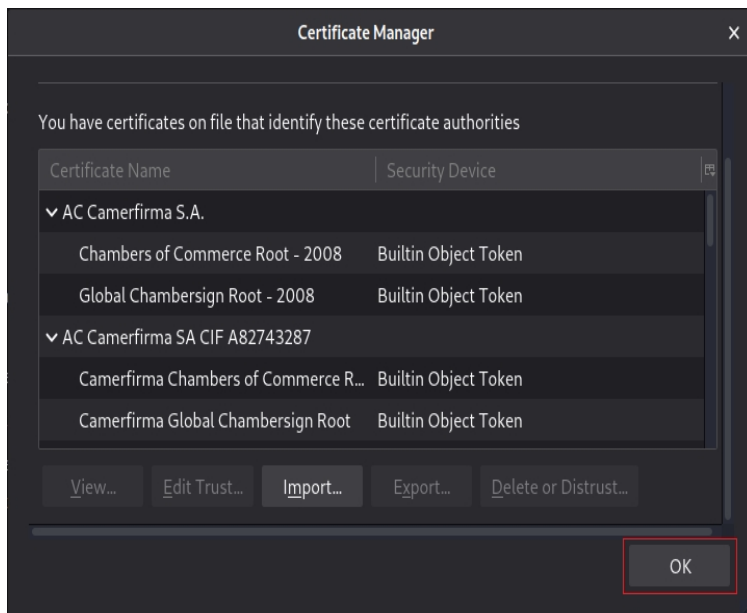
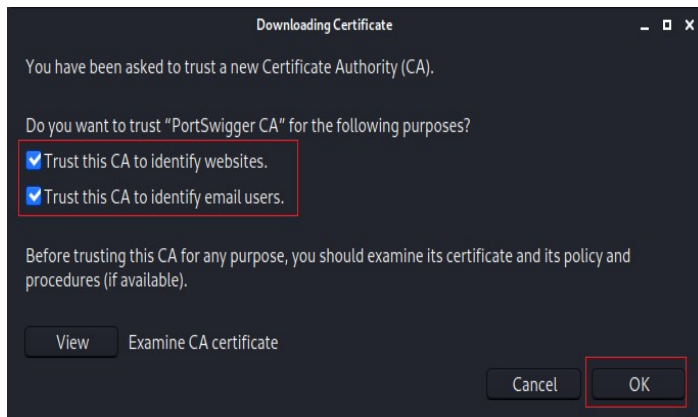
Scroll to the bottom until you come to the certificate and click on the **View Certificate** button.

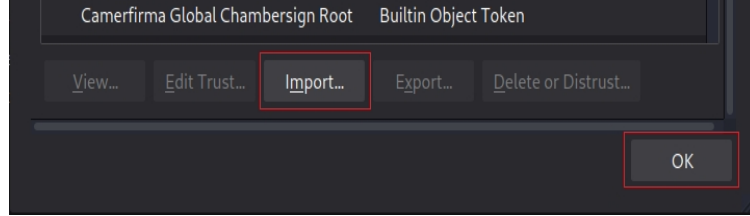


Browse to the certificate you downloaded and saved. 2X click the certificate.

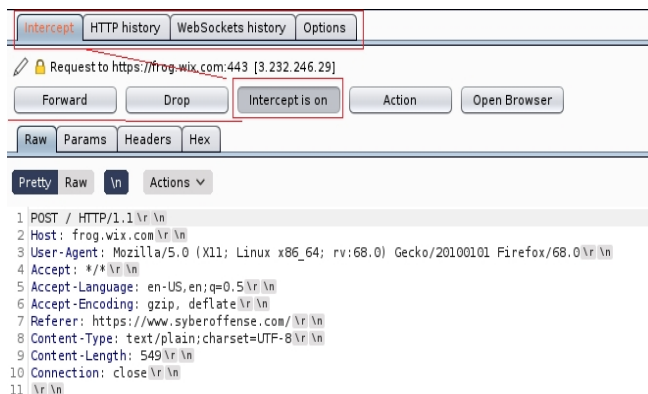


On the next screen, check all the boxes and then click OK.

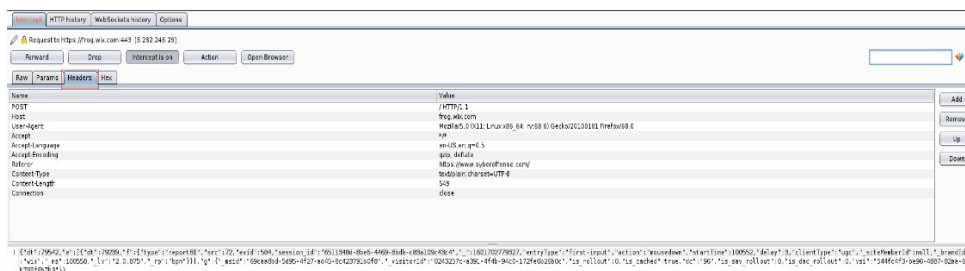




As soon as burpsuite begins to intercept traffic as a proxy, it opens an Intercept tab.



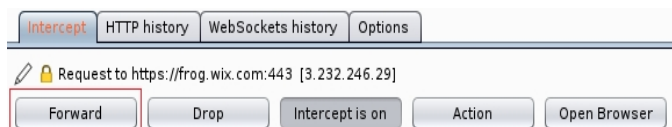
Under the Headers tab, we can see the captured header.



You can modify the header information over to the right before forwarding the request to its destination.

Back at your browser, if you open a new tab and attempt to access the same site, you see a message that says waiting for <name of site>. This is because burpsuite is waiting for you to allow the request to be forwarded.

To forward the request on, you must use the forward button inside the Intercept box.



If you turn the intercept off, burpsuite will act as a normal proxy without holding up the request. For this to remain the case, burpsuite must be up and running.

If you do not want to use burpsuite as a proxy, you can set configure your browser preferences for No proxy:

Connection Settings

Configure Proxy Access to the Internet

☒ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☐ Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☒ Use this proxy server for all protocols

SSL Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

SOCKS Host 127.0.0.1 Port 8080

☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

Summary

In this lab, you learned how to set up and configure BurpSuite as a proxy. BurpSuite Community Edition is a feature-limited set of manual tools for exploring web security. Proxy your HTTPS traffic, edit and repeat requests, decode data, and more.

