

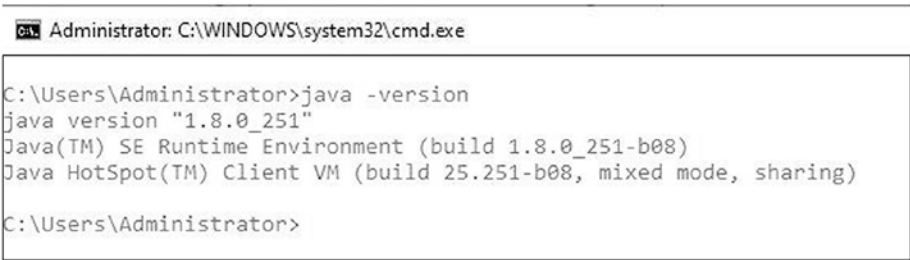
CHAPTER 2

Setting Up the Environment

In the last chapter, we discussed some basics of application security and the need for tools like Burp Suite. In this chapter we'll get started with setting up our environment for Burp Suite.

Burp Suite Installation

Before we attempt to either install or run the Burp Suite, we need to ensure that Java is installed on the system. It is an essential prerequisite to run Burp Suite. On a Windows system, you can simply open up the command prompt and type command “java -version” to check if Java is installed, as shown in Figure 2-1.



```
Administrator: C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator>java -version
java version "1.8.0_251"
Java(TM) SE Runtime Environment (build 1.8.0_251-b08)
Java HotSpot(TM) Client VM (build 25.251-b08, mixed mode, sharing)
C:\Users\Administrator>
```

Figure 2-1. Check if Java is installed

If you don't have Java installed on your system, you can download and install Java from <https://www.oracle.com/java/technologies/javase-jre8-downloads.html>

Once we are sure that Java is installed on our system, we can now proceed with Burp Suite. We first need to download the Burp Suite from <https://portswigger.net/burp/releases/community/latest> as shown in Figure 2-2.

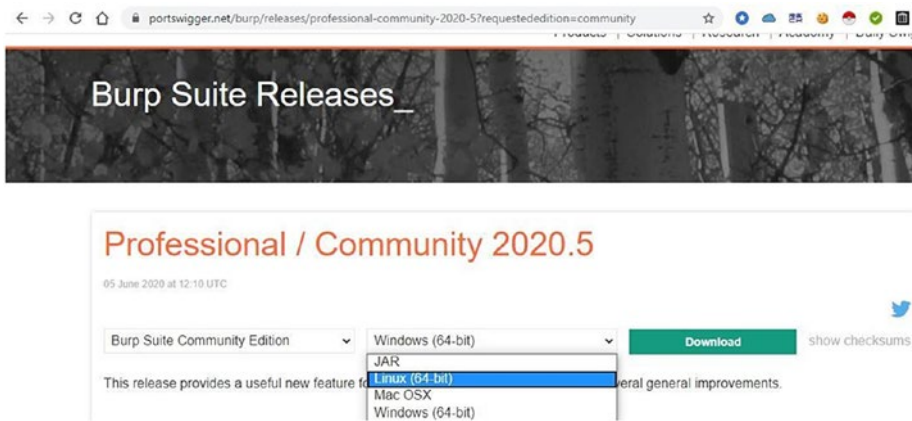


Figure 2-2. Types of Burp Suite downloads

You'll notice there are several forms in which you can download the Burp Suite. There are individual installers for Linux, Mac OSX, and Windows. There's also an option to download a JAR file, which can be used directly to launch Burp Suite without installing. Downloading the JAR file is the easiest way to get started. If you choose to download the installer, it is just like any other software installer and installs the Burp Suite in a few clicks. However, Java is required to be installed in both cases. Once the JAR file is downloaded, you can simply double-click it to launch the Burp Suite.

At times, while running large projects, it might happen that Burp Suite runs out of memory. To solve this problem, it is possible to launch Burp Suite by allocating a fixed amount of memory at startup. This will ensure that it doesn't run out of memory once launched. This can be done using command "java -jar -Xmx2G /path/to/burp.jar" where 2G indicates 2GB of memory. This step is completely optional. We can skip it and directly execute the JAR file to launch Burp Suite with the default configuration.

If all prerequisites are met correctly, we get a startup screen as shown in Figure 2-3.

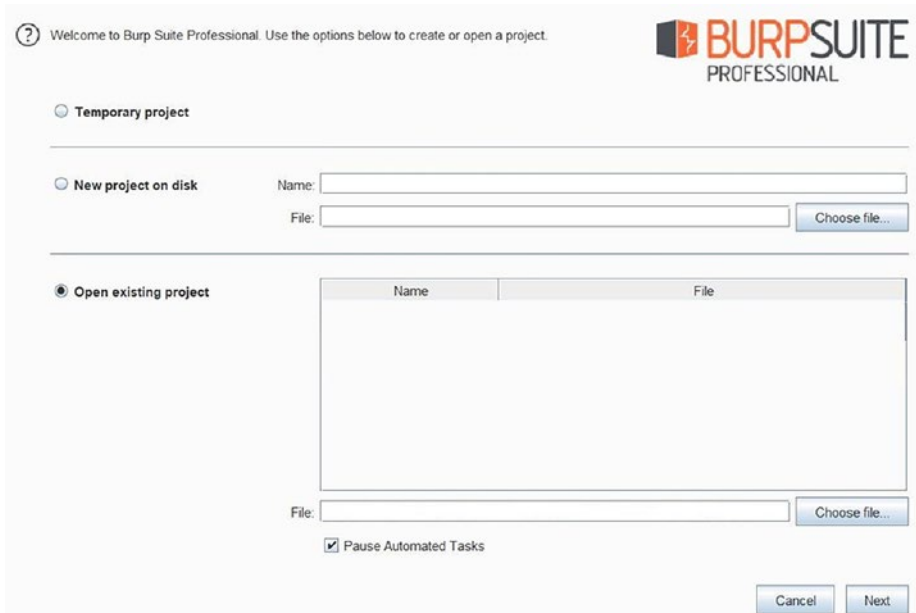


Figure 2-3. Burp Suite Startup Screen

Setting Up Vulnerable Target Web Application

While we set up the Burp Suite on our system, it's important to have a target application on which you will be using the tool. If you are a professional working on application security testing and penetration testing then you would be authorized to use Burp Suite on the application under the test. However, if you are just a beginner trying to get started with learning Burp Suite, then you would need to have some target application on which you could test your skills. Remember, running Burp Suite on an application on which you are not authorized can invite legal troubles. So, from a learning perspective, it's important to try your Burp Suite skills only on a test application. There are several alternatives available as shown below:

1. **Set Up OWASP Juice Shop locally** – OWASP Juice Shop is a modern web application that is deliberately made vulnerable. This can be an excellent starting point. The easiest way to get OWASP Juice Shop up and running is using its docker image. The docker image is available at <https://hub.docker.com/r/bkimminich/juice-shop>. You can simply pull the image and run it in the docker engine on any platform (Windows / Linux / MacOS).
2. **Try out online version of OWASP Juice Shop** – As a beginner, it is always recommended to set up your own copy of Juice Shop; however if you want to quickly try it out before setting it up, you can try the online version at <https://juice-shop.herokuapp.com/#/>

Referring to the image above, at a very high level and in simple terms, the following sequence of events happens:

1. The end user opens up any browser of choice.
2. The user then enters the URL of website he/she wishes to browse.
3. The browser processes the URL of the website and renders the website for the user (a series of request and response happens in the background).

Now let's consider another scenario wherein we have configured Burp Suite with the browser as shown in Figure 2-5.

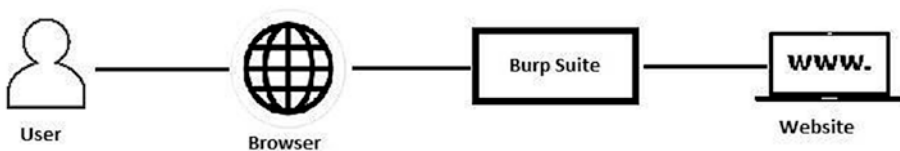


Figure 2-5. A user accessing a website with Burp Suite

Referring to the image above, at a very high level and in simple terms, the following sequence of events happens:

1. The end user opens up any browser of choice.
2. The user then enters the URL of the website he/she wishes to browse.
3. The browser redirects the request to Burp Suite, which then forwards the request to the target website.
4. The target website responds to the request and sends a response back to Burp Suite, which then passes on the response to be rendered in the browser.

So in this scenario, Burp Suite is acting as ‘Man-in-the-Middle’ between the browser and the target website. Burp Suite is able to intercept and tamper all the traffic passing through it.

We’ll now see how we can configure the most popular browsers to work with Burp Suite.

Firefox

For configuring Firefox with Burp Suite:

Go to Tools ► Options as shown in Figure 2-6.

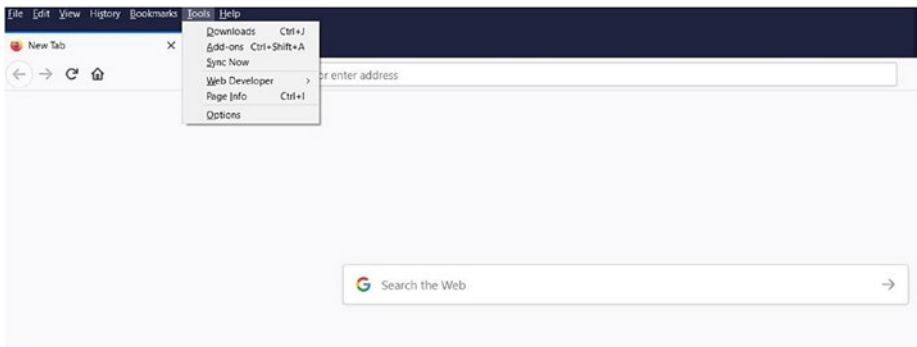


Figure 2-6. Navigating the Tools ► Options menu in Firefox

In the search field, enter the keyword ‘network’ as shown in Figure 2-7 and click on ‘Settings.’

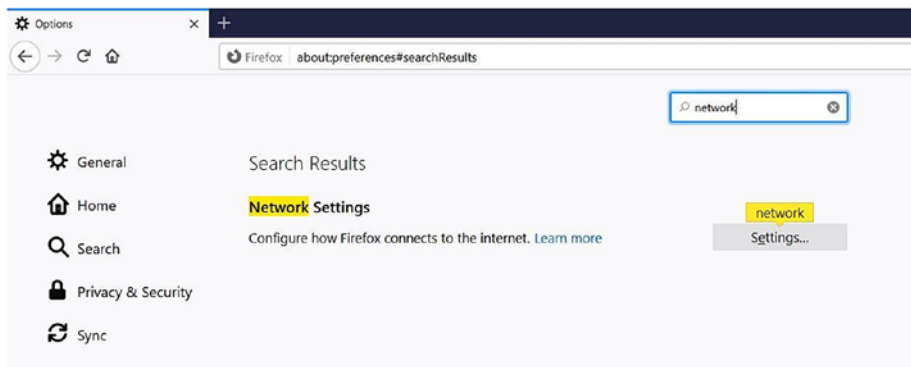


Figure 2-7. Searching for ‘Network Settings’ within Firefox options

Select ‘Manual proxy configuration’ as shown in Figure 2-8 and enter the IP as 127.0.0.1 (or localhost) and port as 8080.

Note: By default the Burp Suite proxy listens on port 8080. This can be customized and we’ll see that in the next chapter. However, the same port number must be entered both in the browser as well as in the Burp Suite in case you wish to change the same.

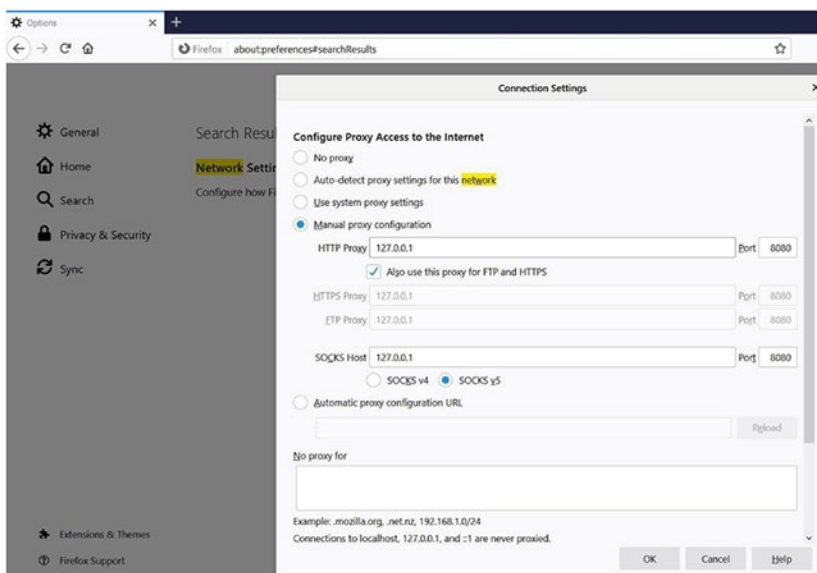


Figure 2-8. Setting up the manual proxy configuration

Simply click ‘OK’ once the proxy details have been configured.

Chrome

For configuring Chrome with Burp Suite:

Click on the three vertical dots in the right-hand corner and select ‘Settings’ as shown in Figure 2-9.

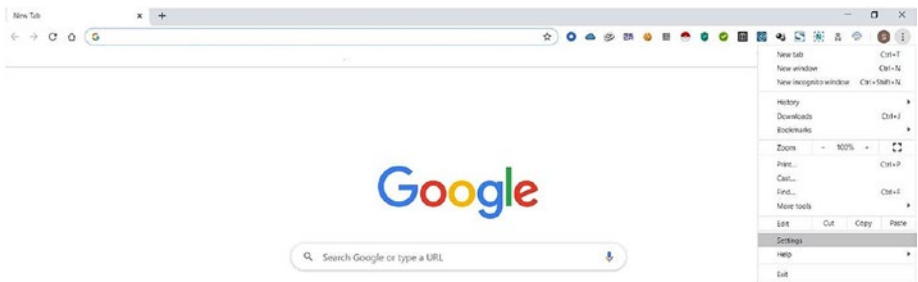


Figure 2-9. Navigating to the Chrome Settings

Search for the keyword ‘proxy’ as shown in Figure 2-10, and click on the ‘Open your computer’s proxy settings’ option.

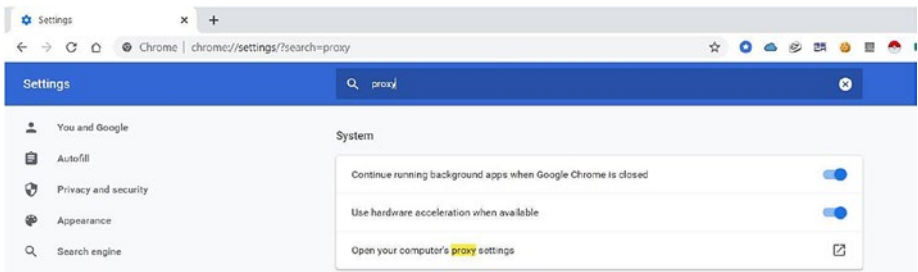


Figure 2-10. Opening the proxy settings in Chrome

Now enable the ‘Use a proxy server’ option and enter the address and port number as shown in Figure 2-11.

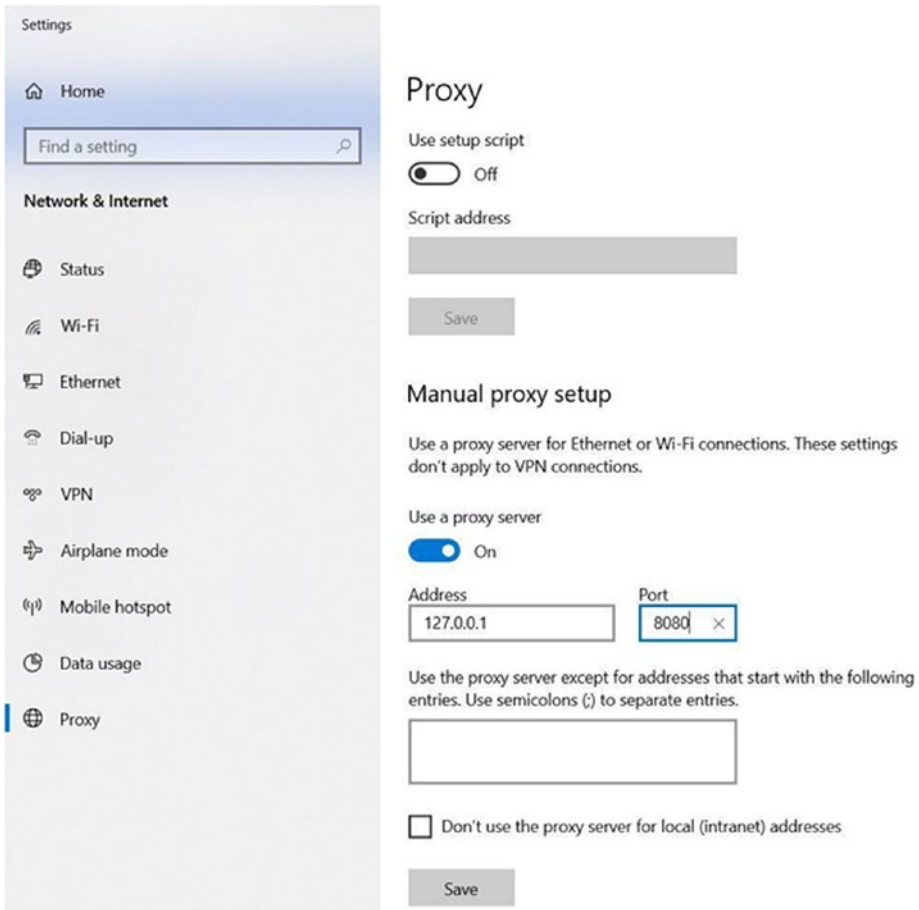


Figure 2-11. *Configuring the system proxy*

Once the proxy is configured, simply click on the ‘Save’ option.

Edge

For configuring Edge with Burp Suite:

Click on the three horizontal dots in the right-hand corner and select the ‘Open proxy settings’ as shown in Figure 2-12.

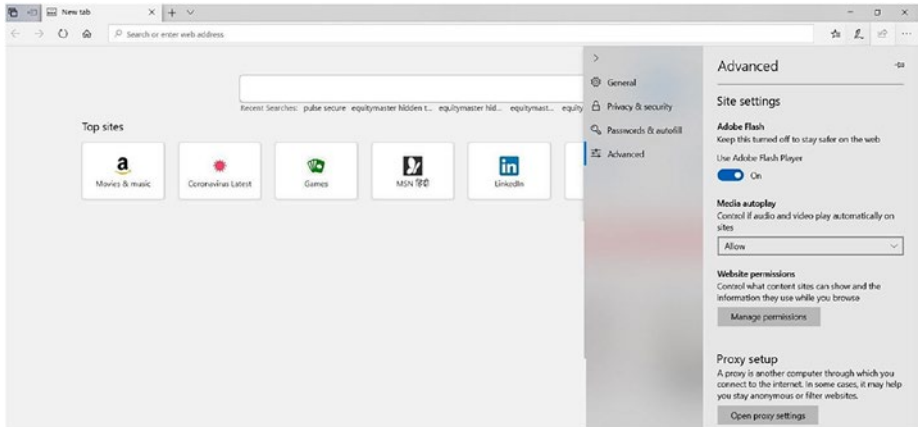


Figure 2-12. *Opening the Proxy Settings in Edge browser*

Now enable the ‘Use a proxy server’ option and enter the address and port number as shown in Figure 2-13.

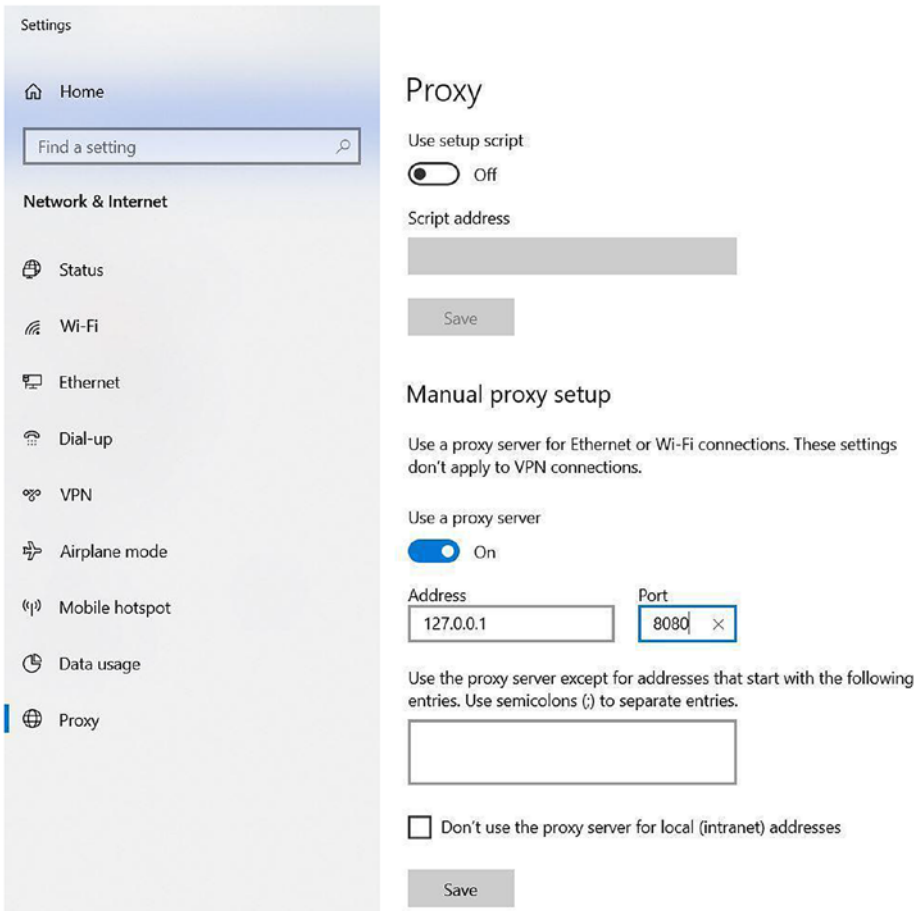


Figure 2-13. *Configuring the system proxy*

Once the proxy is configured, simply click on the ‘Save’ option.

Opera

For configuring Opera with Burp Suite:

Click on the settings in the top right-hand corner and select the option ‘Go to browser settings’ as shown in Figure 2-14.

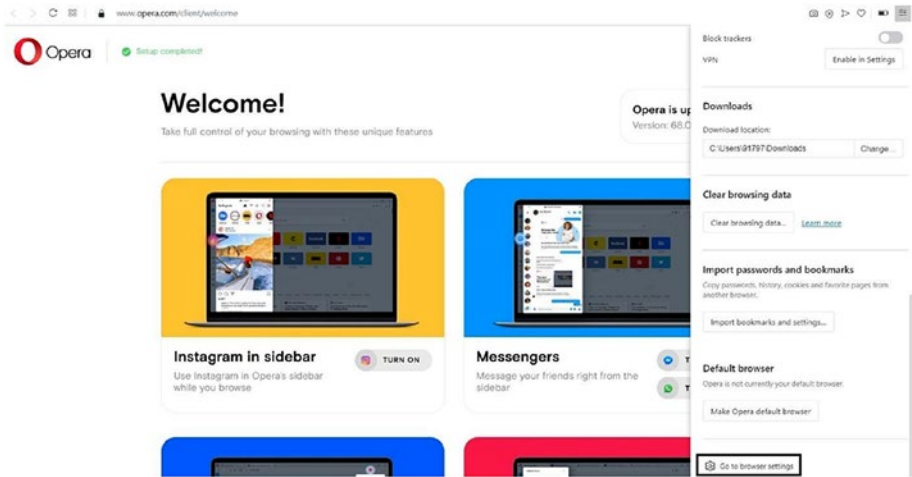


Figure 2-14. Opening the browser settings in Opera

In the search field, type proxy and then select the option ‘Open your computer’s proxy settings’ as shown in Figure 2-15.

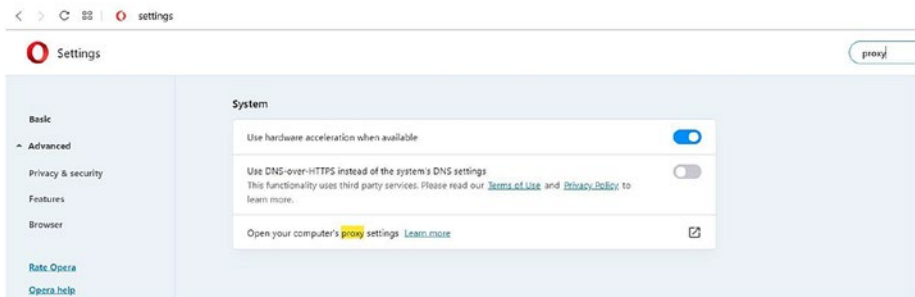


Figure 2-15. Opening up the system proxy settings

Now enable the ‘Use a proxy server’ option and enter the address and port number as shown in Figure 2-16.

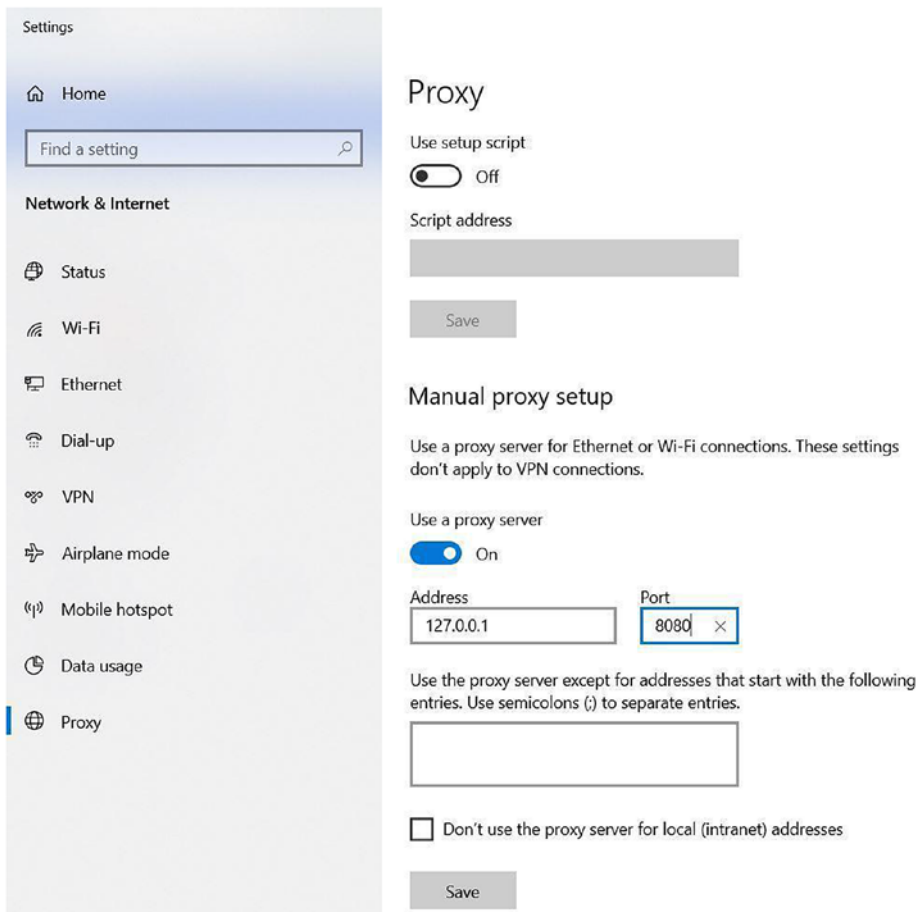


Figure 2-16. *Configuring the system proxy*

Once the proxy is configured, simply click on the ‘Save’ option.

So far we have seen how to configure browsers like Firefox, Chrome, Edge, and Opera to work along with Burp Suite. It simply requires configuring the network proxy option. However, it is important to note that once the browser proxy is configured, all the traffic initiating from the browser will compulsorily pass through Burp Suite. If you are working on multiple tabs within a browser and testing an application in one tab while

accessing email in another, all this traffic will be routed through Burp Suite. In case you wish to pass only selective traffic through Burp Suite, you need to make use of additional browser plugins such as those shown in Table 2-1.

Table 2-1. *Additional Browser Plugins for Proxy*

Firefox	Proxy SwitchyOmega, FoxyProxy
Chrome	Proxy SwitchyOmega, FoxyProxy
Edge	N/A
Opera	Proxy Switcher & Manager

The above plugins are simple to use and allow custom selective traffic to pass through Burp Suite. Using these plugins is completely optional. If you don't wish to use these plugins, you can simply use two separate instances of browser, one for application testing and the other for personal use. Or it is also possible to scope out only the required traffic in Burp Suite that we will be learning in an upcoming chapter.

Summary

In this chapter we saw how to download, install, and get started with the Burp Suite tool. We then explored various options available for setting up vulnerable targets to practice Burp Suite skills. We also learned how to configure different browsers to work along with the Burp Suite.

In the next chapter, we'll see how to configure some of the basic settings in the Burp Suite like the Proxy, User Options, and Project Options.

Exercises

- Download the latest version of the Burp Suite.
- Try to launch Burp Suite from the command line, allocating custom memory size.
- Try and explore how to use the FoxyProxy plugin for Firefox and Chrome.