CEH v12 Lesson 5 : Session Hijacking Implementation & Prevention

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 — Network Level Hijacking — Capturing Cookie Sessions

After completing this module, you will be able to:

- Disable captive portal detection in Firefox
- Configure Burp Suite for session hijacking
- Configure proxy settings in Firefox
- Use Burp Suite to capture a cookie session

Lab Duration

It will take approximately **30 minutes** to complete this lab.

Exercise 1 — Network Level Hijacking — Capture Cookie Sessions

In network level hijacking, you are looking to identify the session id or cookie that identifies a user's session with a server. This information can be used later in application level hijacking to take over a session.

In this exercise, you will take capture cookies.

Learning Outcomes

After completing this exercise, you will be able to:

- Configure Burp Suite
- Configure Firefox for use as a Burp Suite listener
- Capture cookies

Task 1 — Disable Captive Portal Detection in Firefox

Firefox's captive portal detection tests if a network connection requires a logon. It does this by checking the following URL:

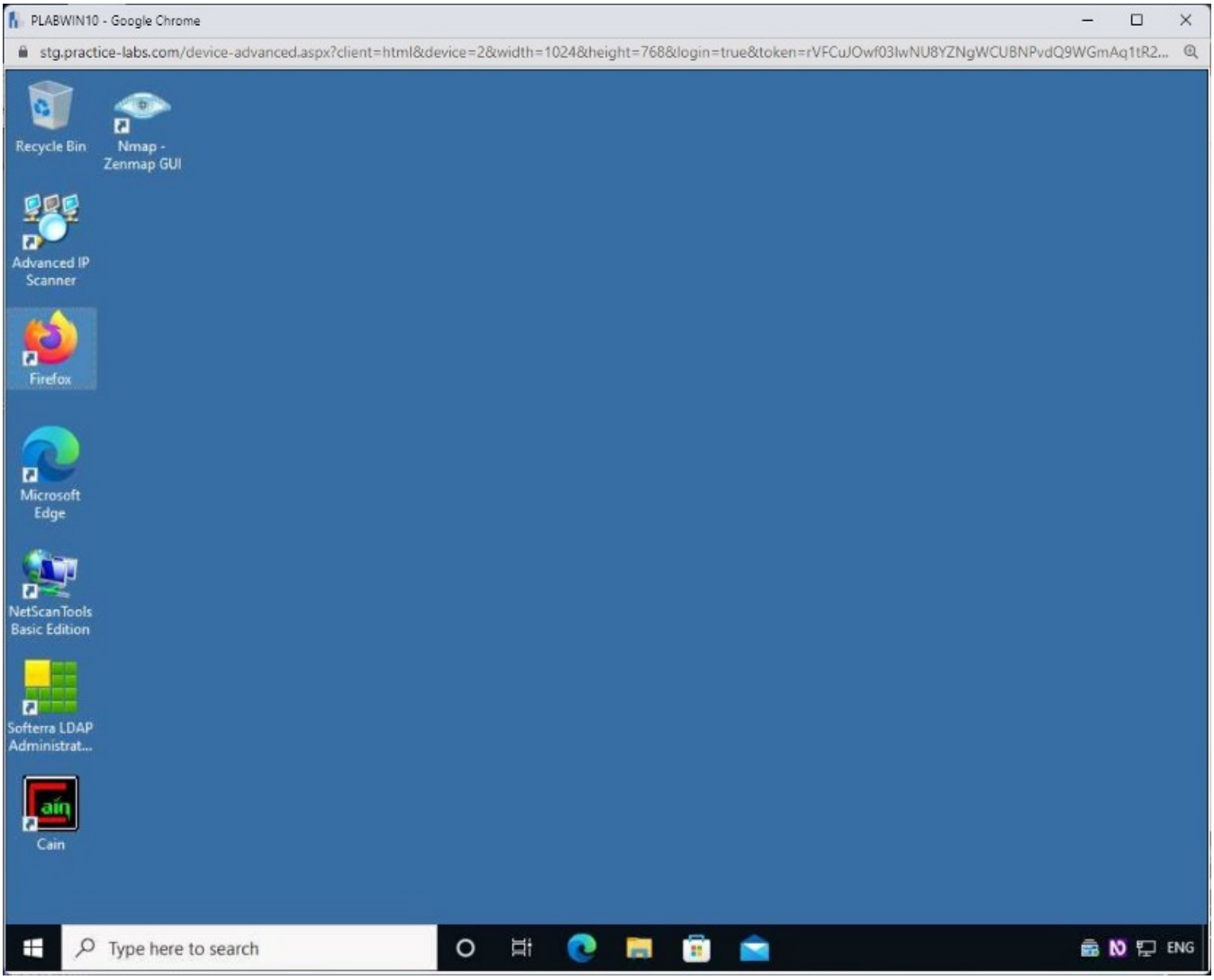
```
http://detectportal.firefox.com
```

This adds a tremendous amount of manually forwarding **HTTP** requests in Task 5. To reduce this, turn off this functionality by doing the following.

Step 1

Power on **PLABWIN10**.

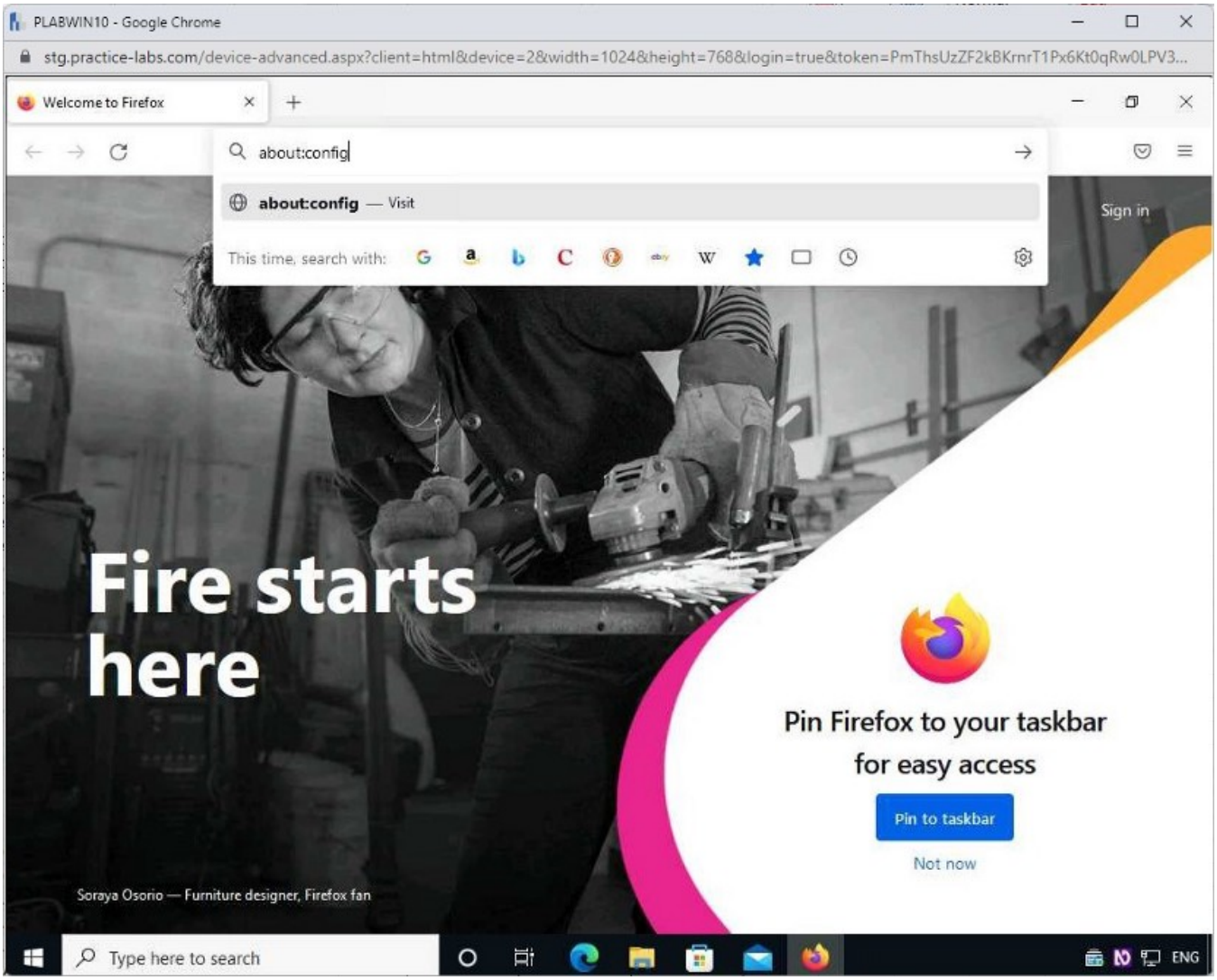
Open **Firefox** by double-clicking the **Firefox** icon on the desktop.



Step 2

In the address bar, type the following:

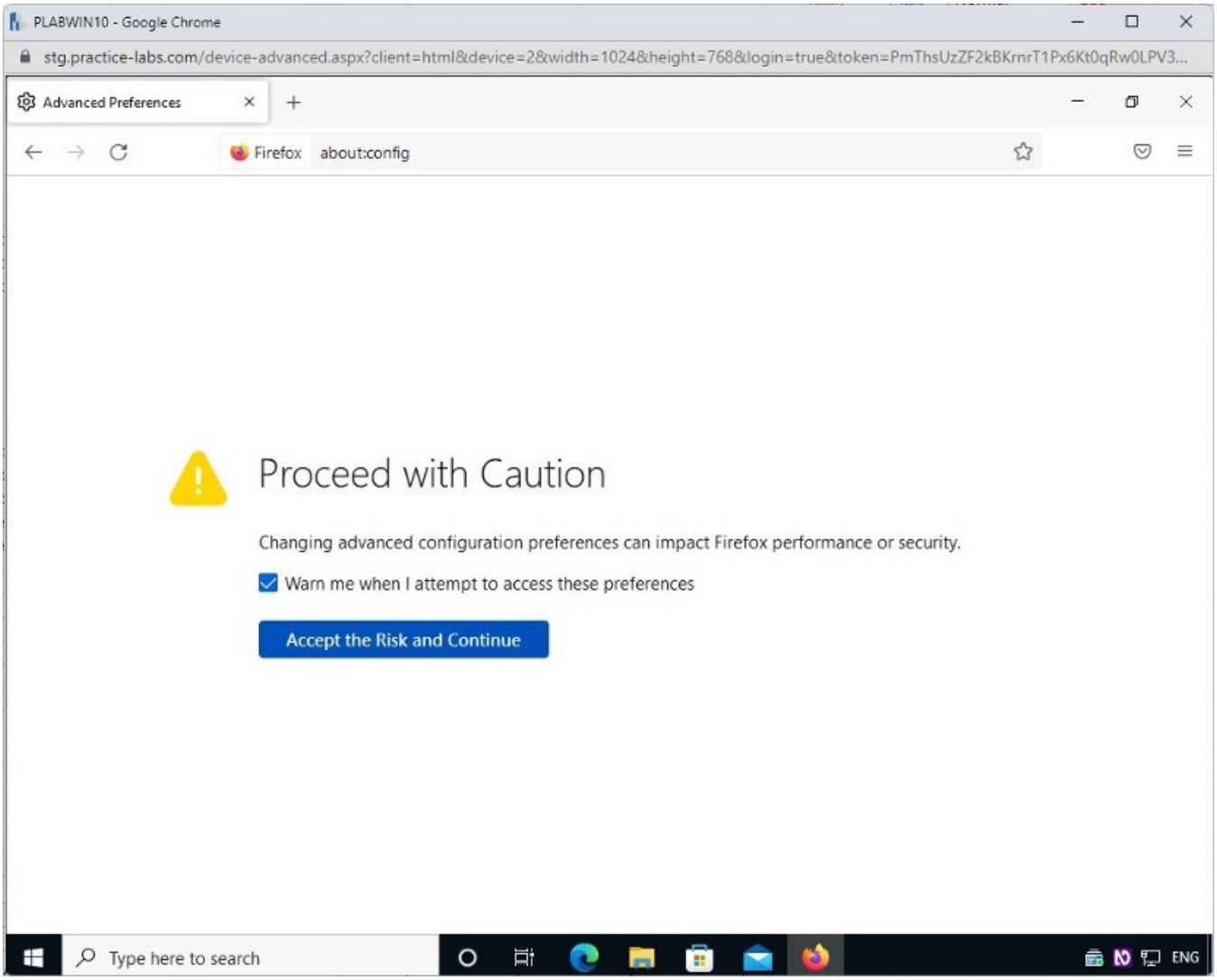
```
about:config
```



Step 3

The **Proceed with Caution** warning page appears.

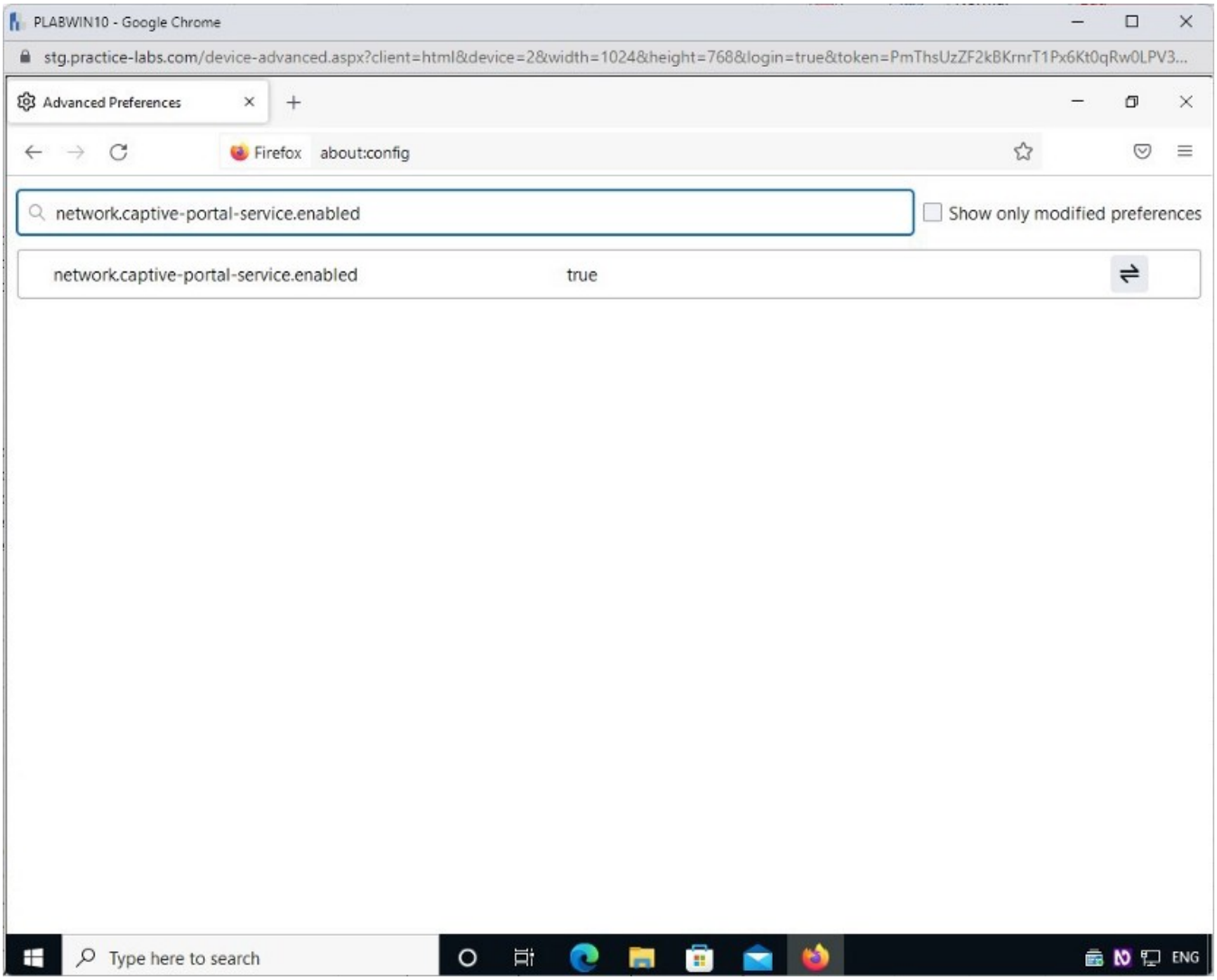
Keep the default settings, and select **Accept the Risk and Continue**.



Step 4

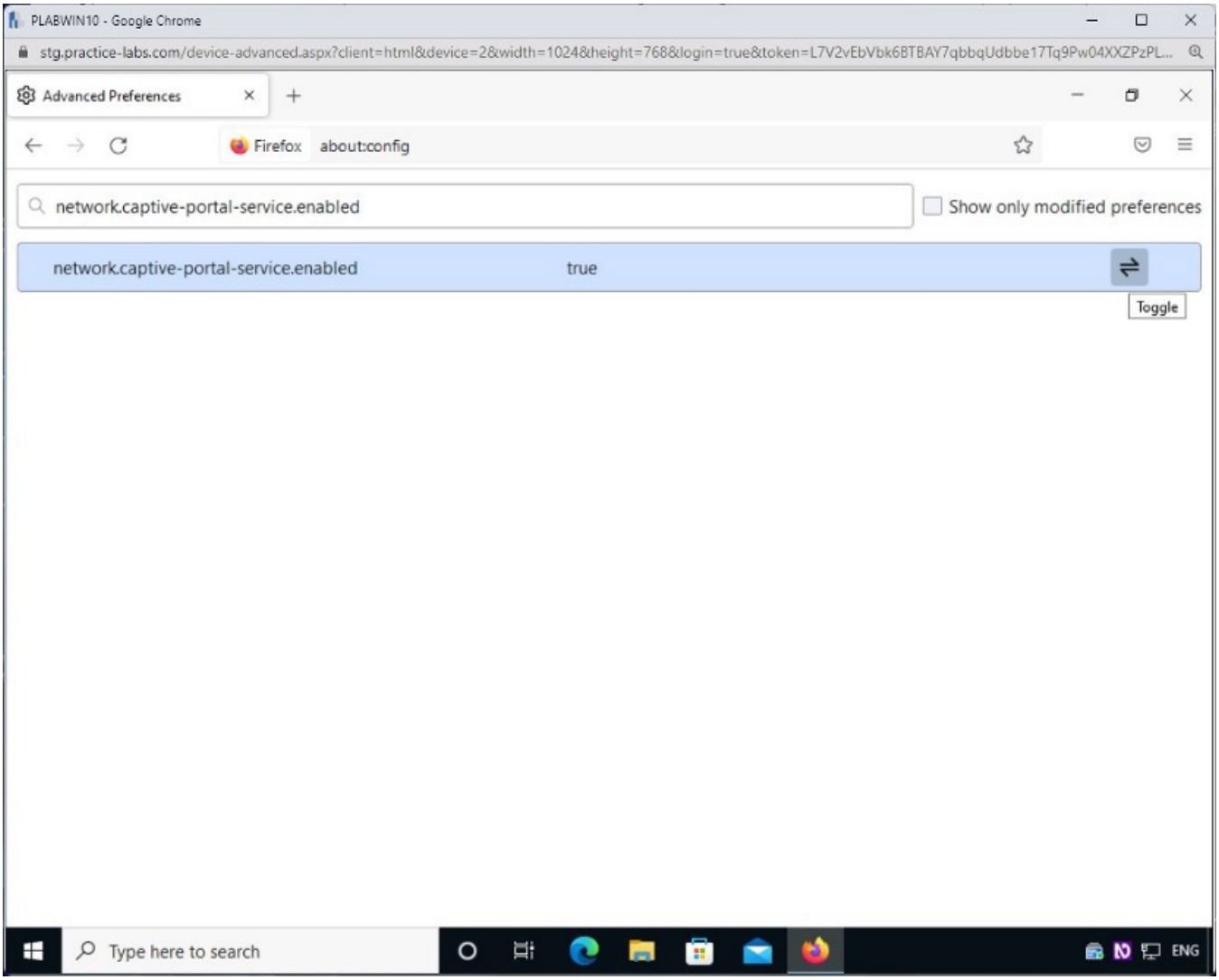
In the **Search** bar, type the following:

```
network.captive-portal-service.enabled
```



Step 5

Click the **Toggle** icon **enabled** to change the status from **true** to **false**.



Once complete, minimize the **Firefox** window.

Task 2 — Configure Burp Suite

You need to configure Burp Suite to intercept traffic from Mozilla Firefox. Burp Suite is one of the most used applications when it comes to intercepting traffic. It has a proxy that can intercept and modify Web traffic. In this task, you will configure Burp Suite to capture cookie sessions. To do this, perform the following steps:

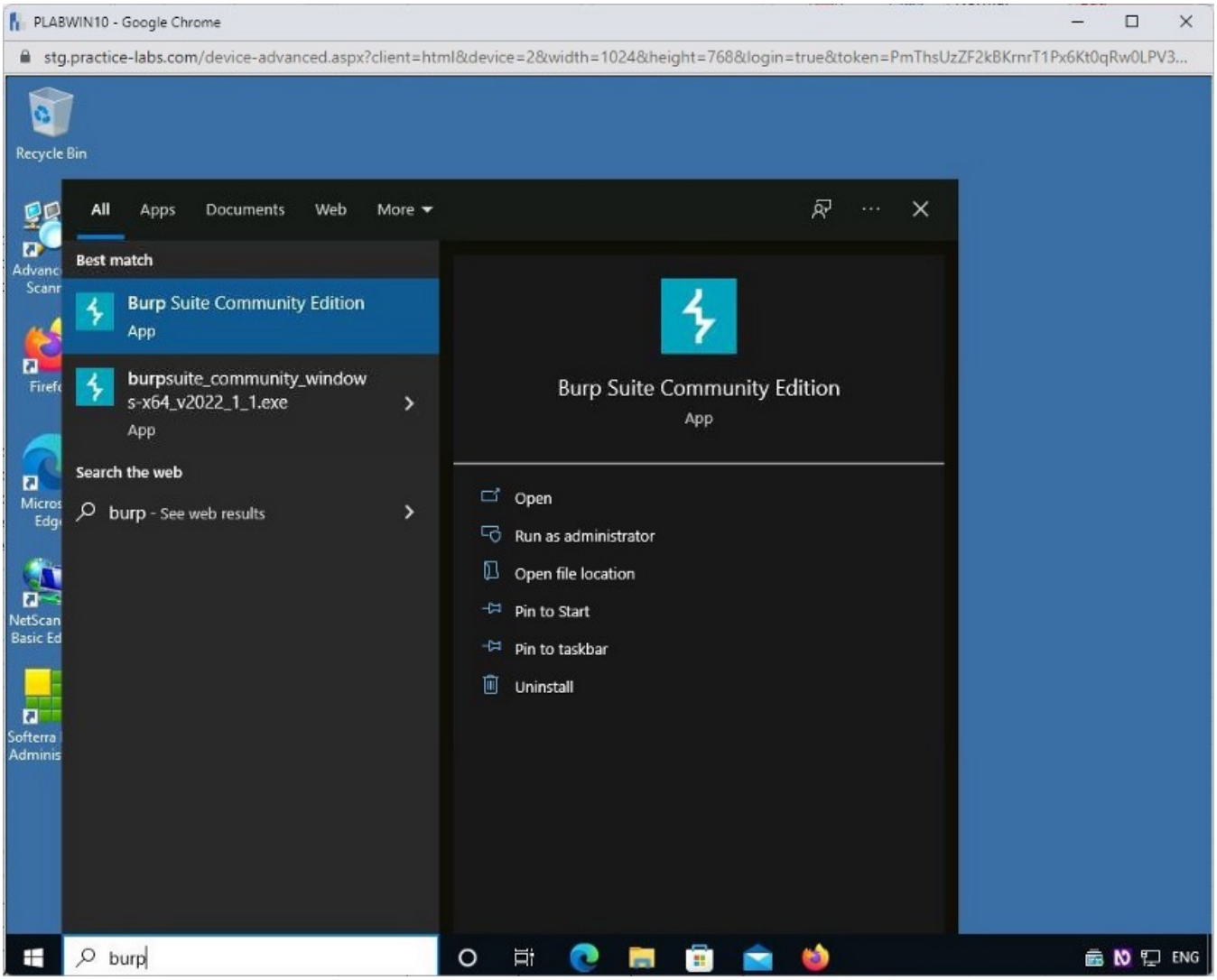
Step 1

Ensure you have powered on all the devices and connect to **PLABWIN10**.

In the **Type here to search** textbox, type the following:

```
burp
```

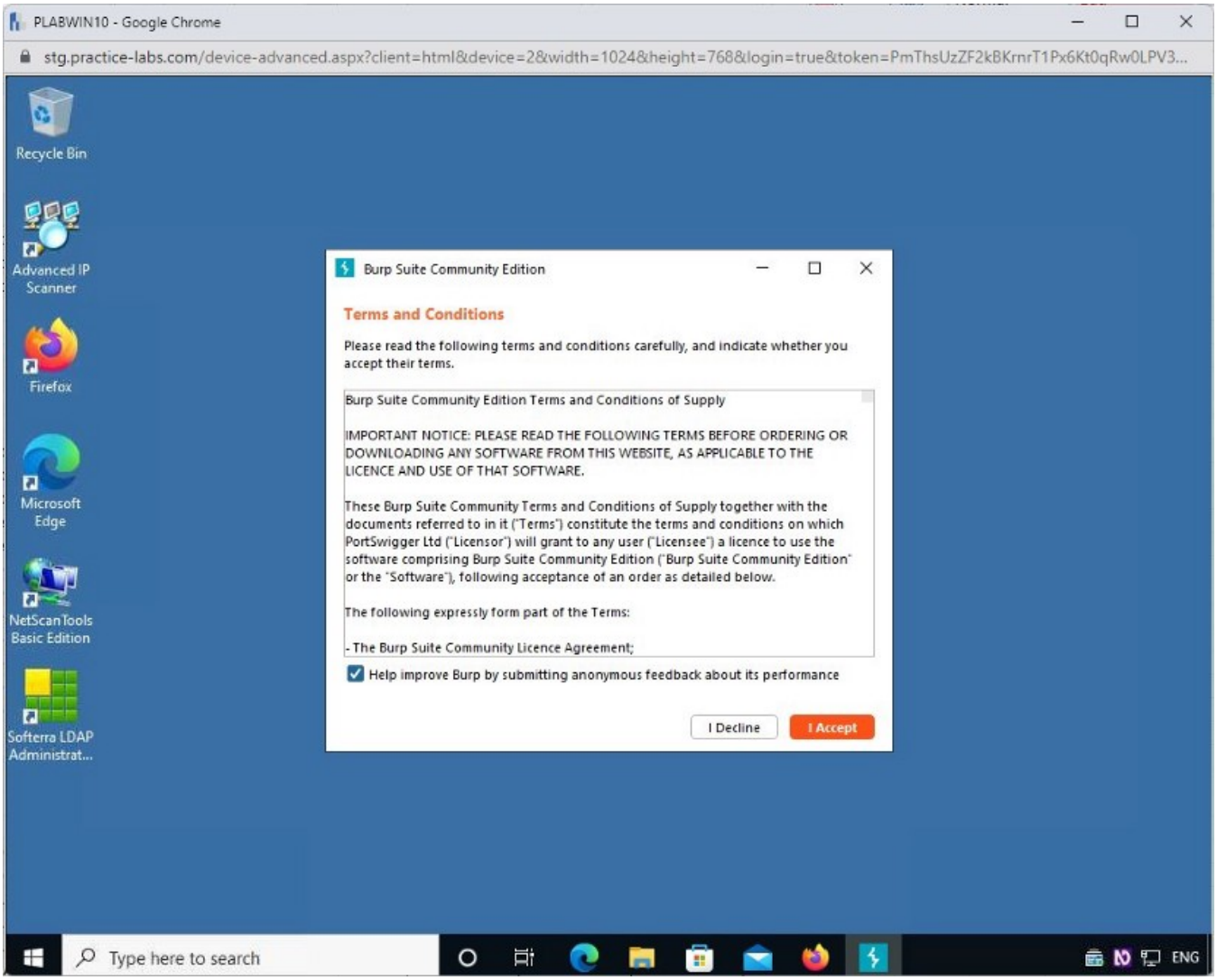
From the search results, select **Burp Suite Community Edition**.



Step 2

The **Burp Suite Community Edition** splash screen is displayed. Wait a few seconds, and the **Terms and Conditions** window appears.

Click **I Accept**.

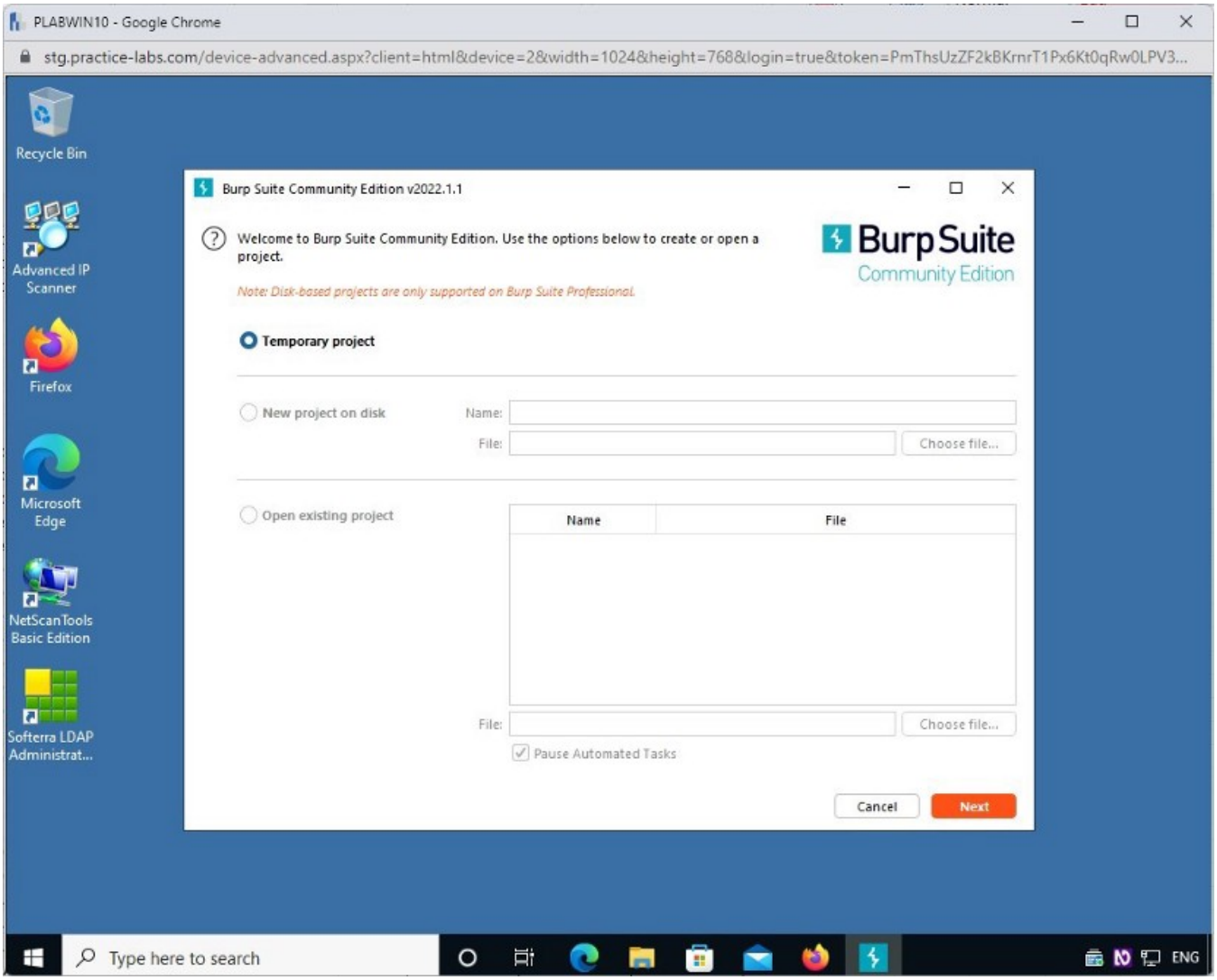


Step 3

The **Burp Suite Community Edition** wizard is displayed.

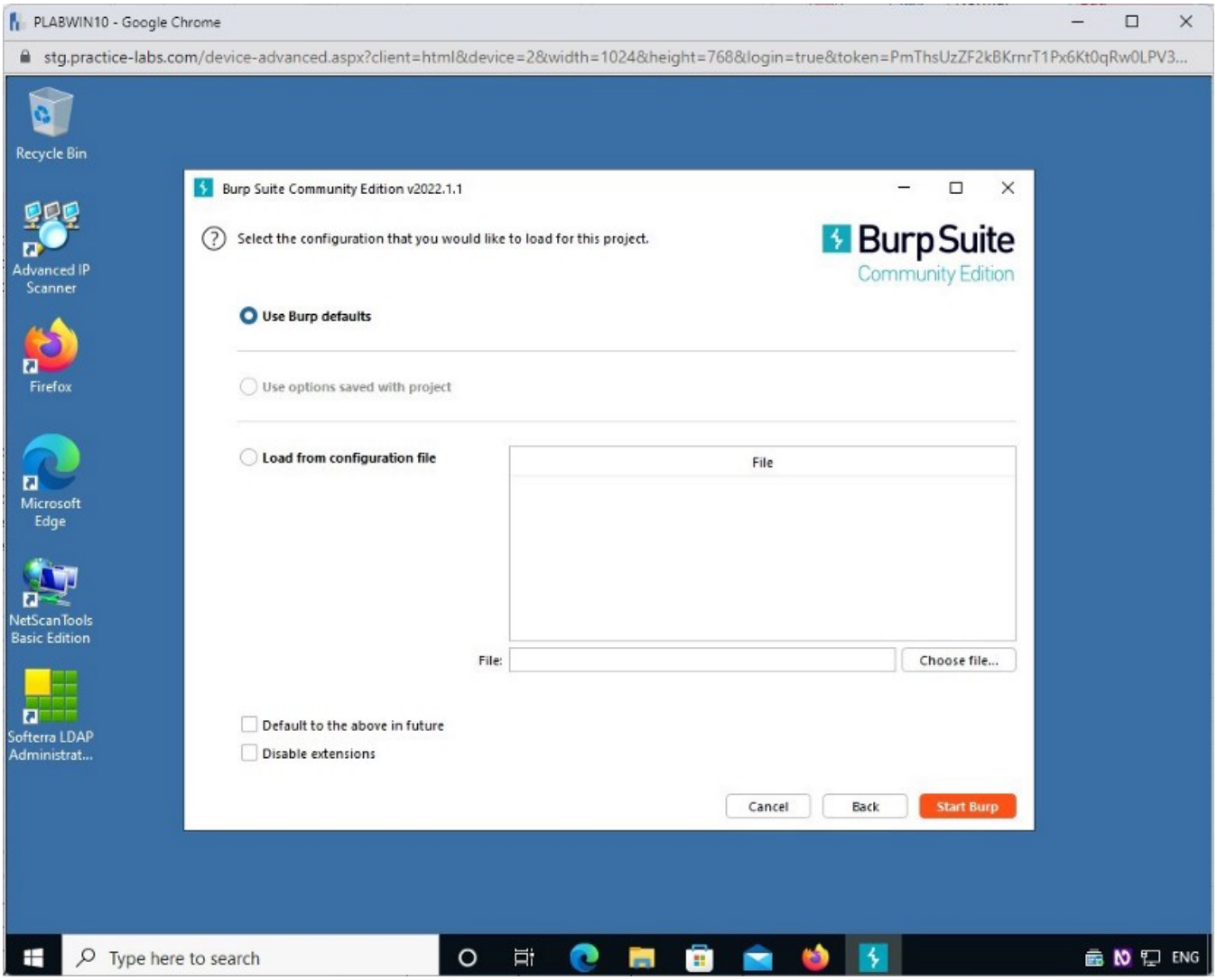
On the **Welcome to Burp Suite Community Edition** window, keep the default selection of **Temporary project** and select **Next**.

***Note**: Depending on the date you installed Burp Suite, your version number and interface may change.*



Step 4

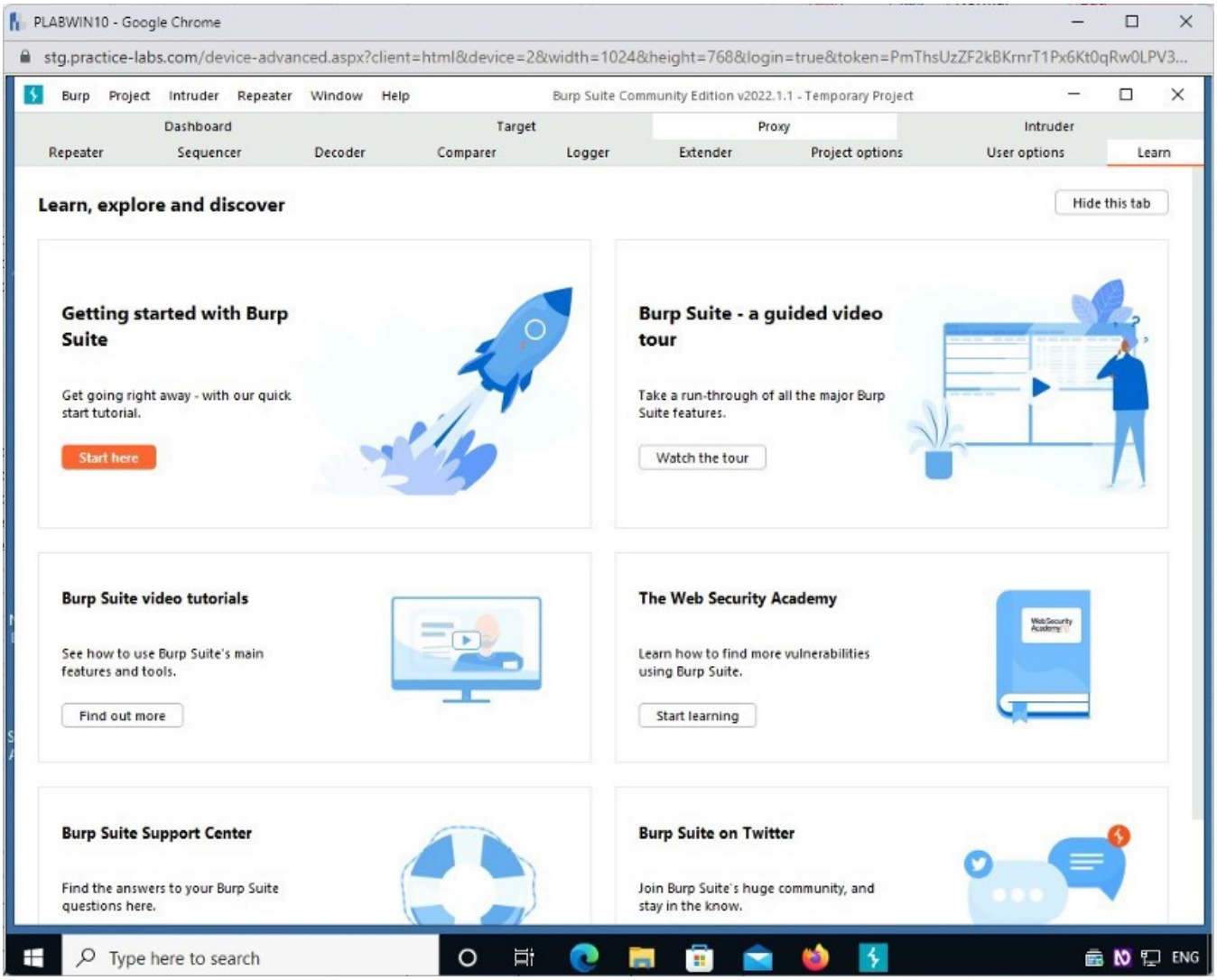
On the **Select the configuration that you would like to load for this project** page, keep the default selection of **Use Burp defaults** and select **Start Burp**.



Step 5

It will take a few seconds for **Burp** to start the project and open the **Burp Suite Community Edition — Temporary Project** page.

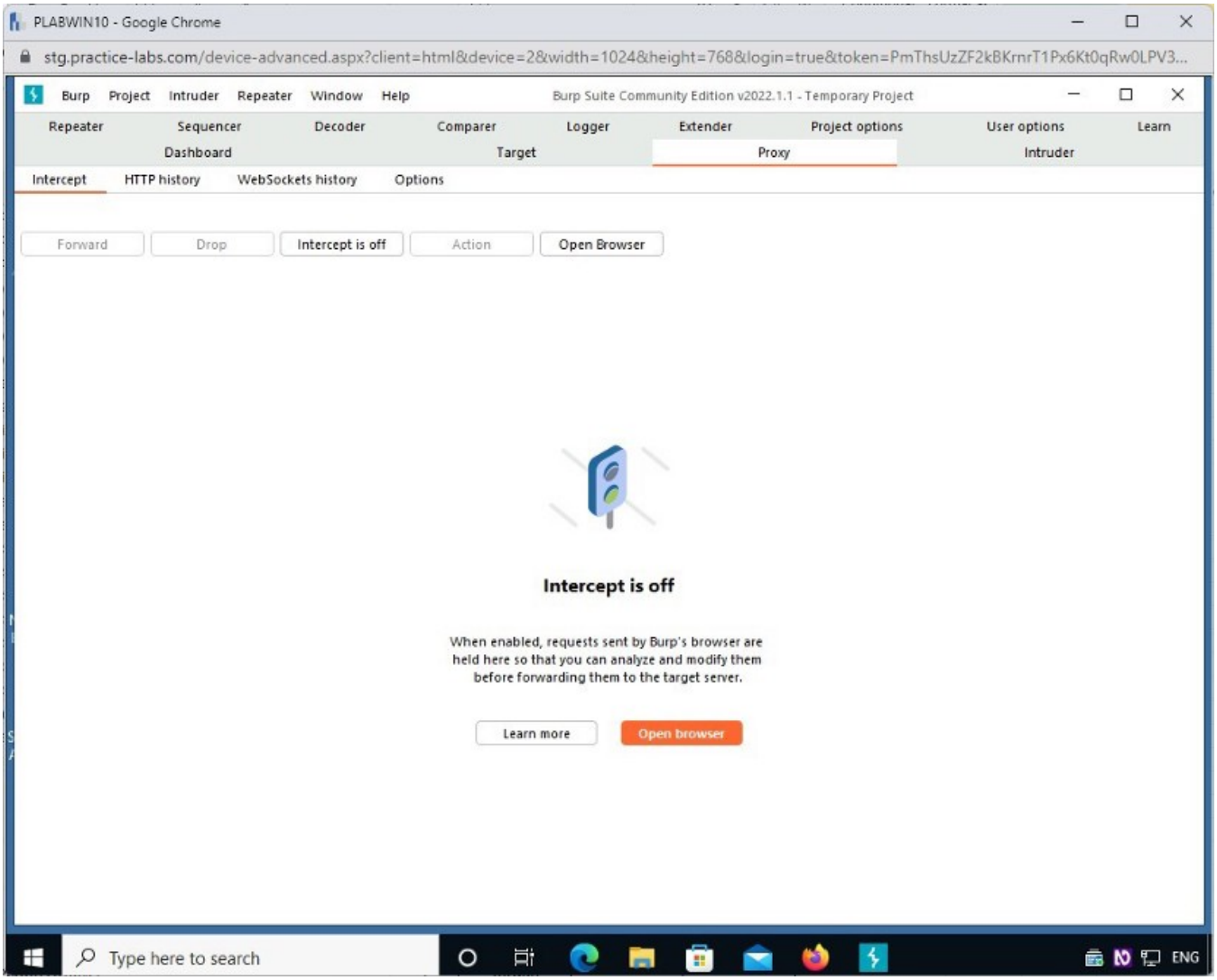
Select the **Proxy** tab from the top of the page.



Step 6

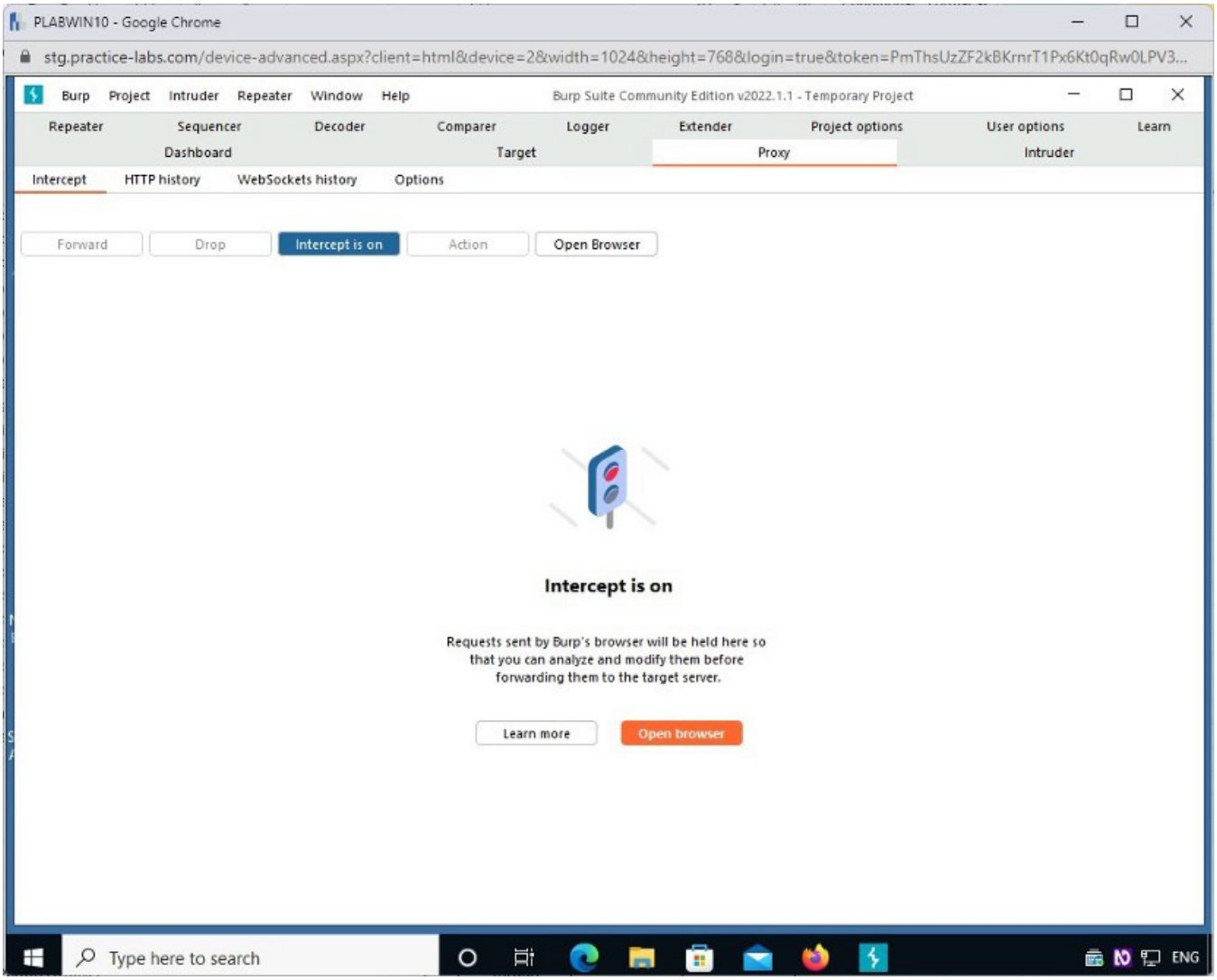
The **Intercept** tab is opened by default.

Firstly, click the Intercept is off button to enable **Intercept**.



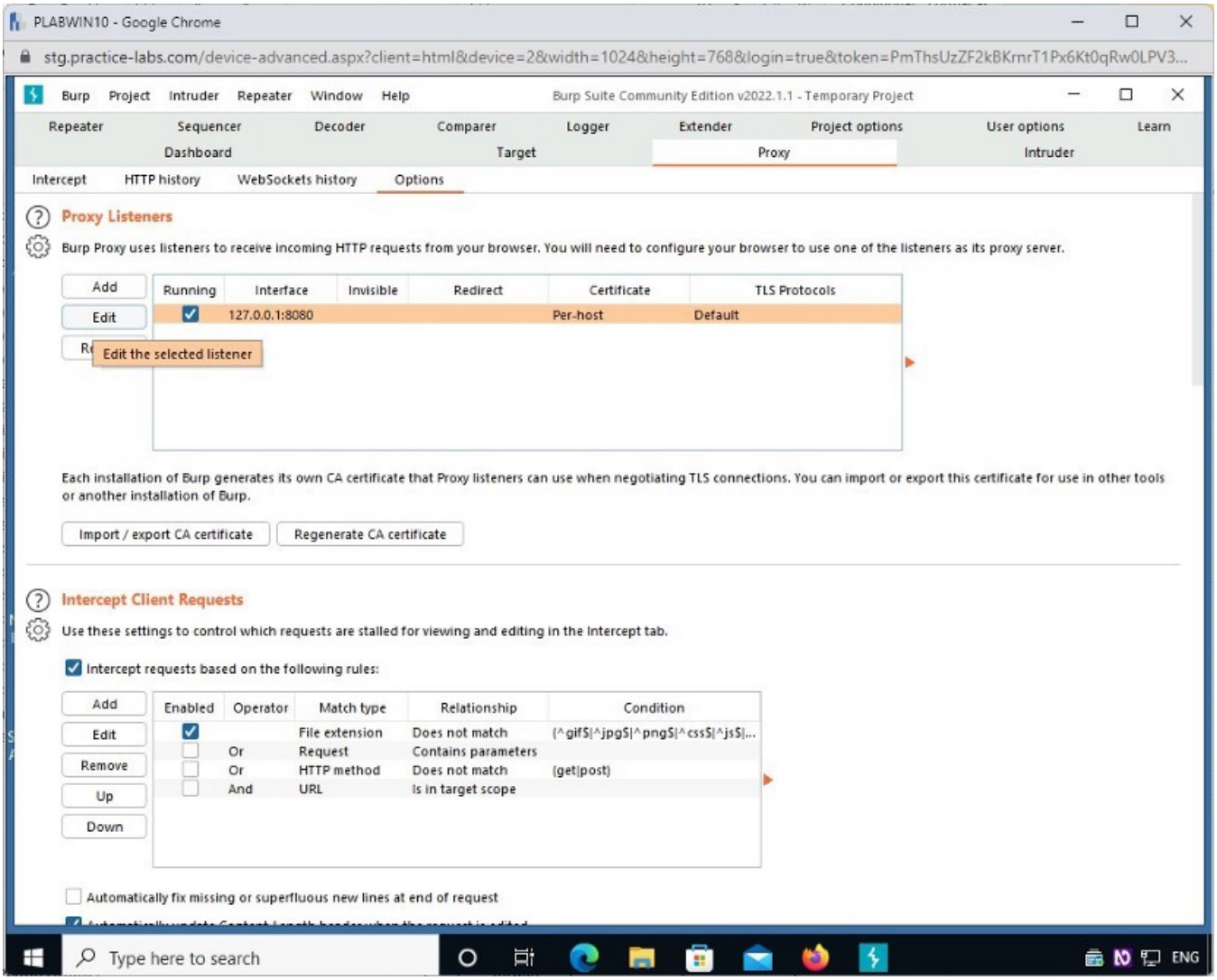
Step 7

Once Intercept has been enabled, click the **Options** tab.



Step 8

In the **Proxy Listeners** section, select the IP address **127.0.0.1:8080** and then select **Edit**.



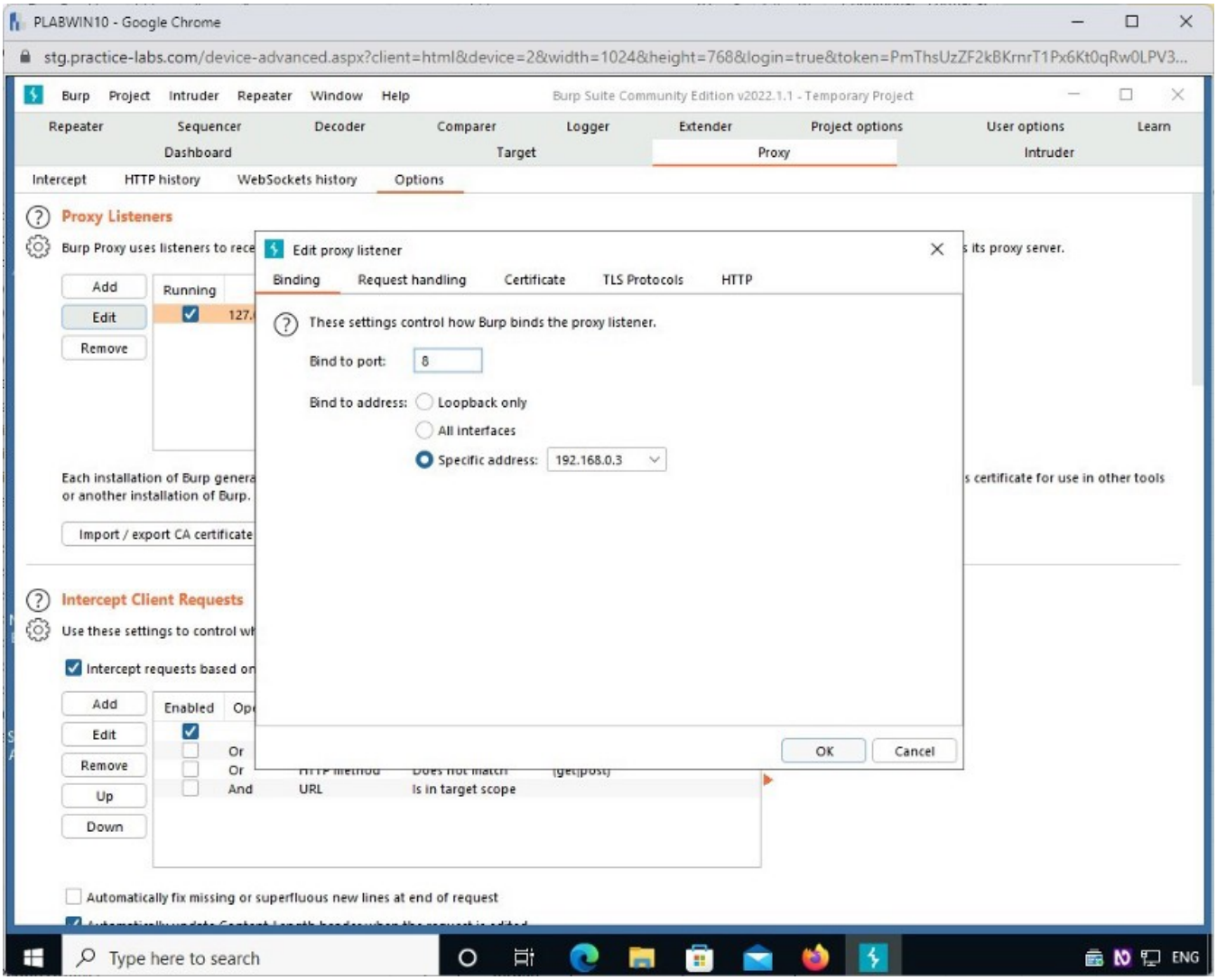
Step 9

The **Edit proxy listener** window appears. In the **Bind to port** box, type the following:

```
8888
```

***Note**: You can use any port number. However, it is recommended not to use well-known ports such as 80, 443, 8080, and 8443.*

In the **Bind to address** section, select **192.168.0.3** from the **Specific address** drop-down. Select **OK**.

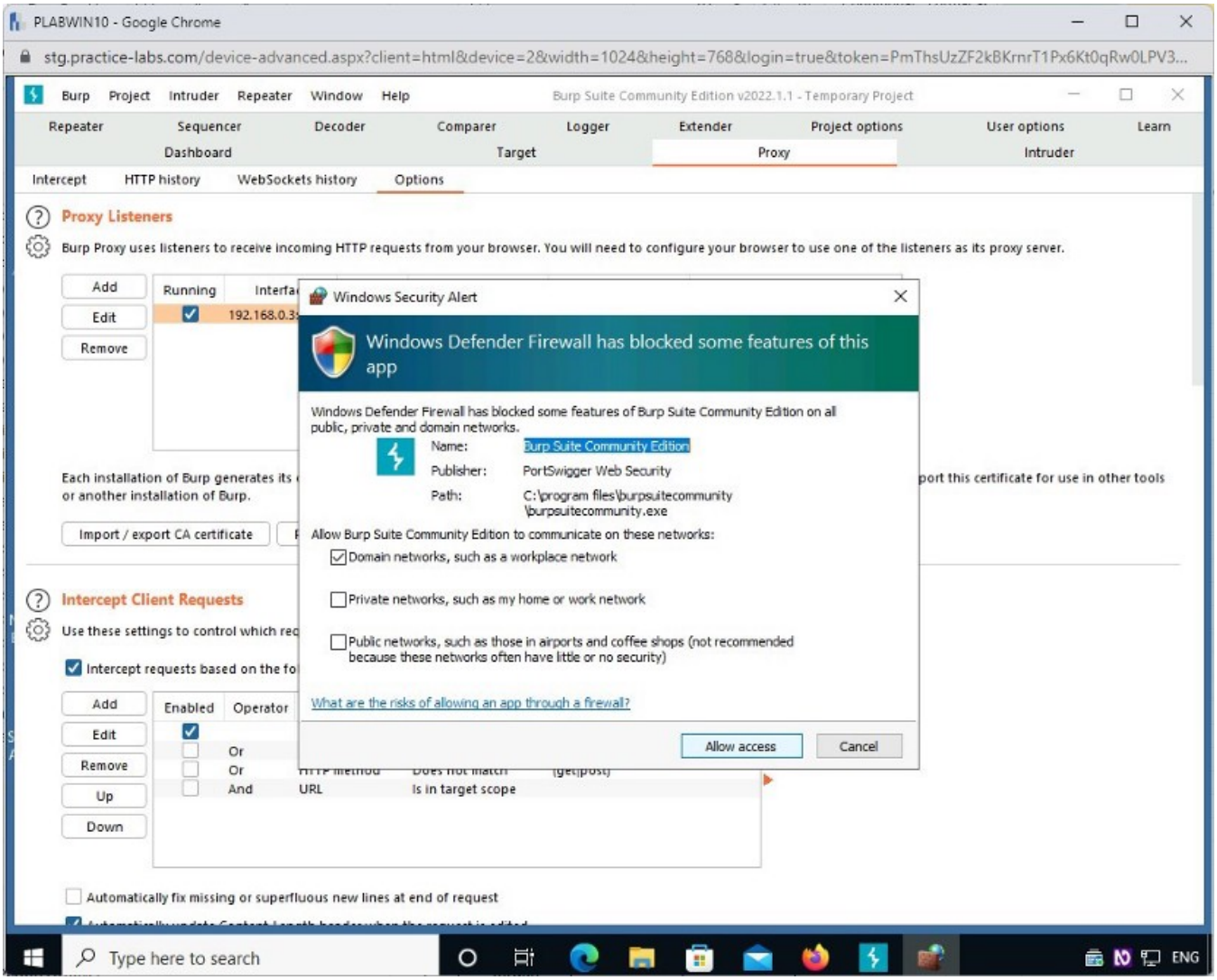


Step 10

You are back to **Proxy Listeners** section on the **Options** tab.

***Note**: Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You need to configure a browser to use one of the listeners as its proxy server.*

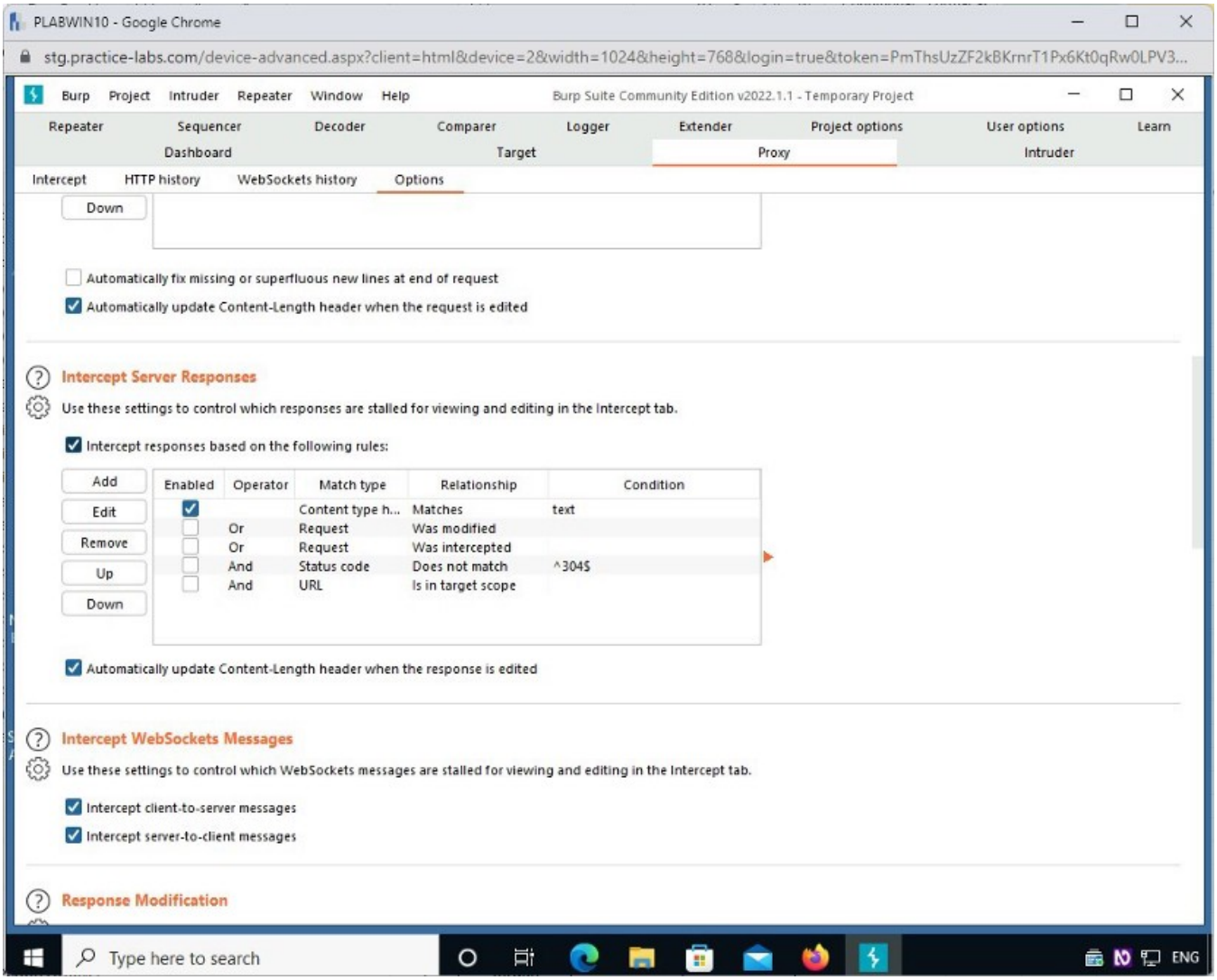
The **Windows Security Alert** dialog box is displayed. Keep the default settings and select **Allow access**.



Step 11

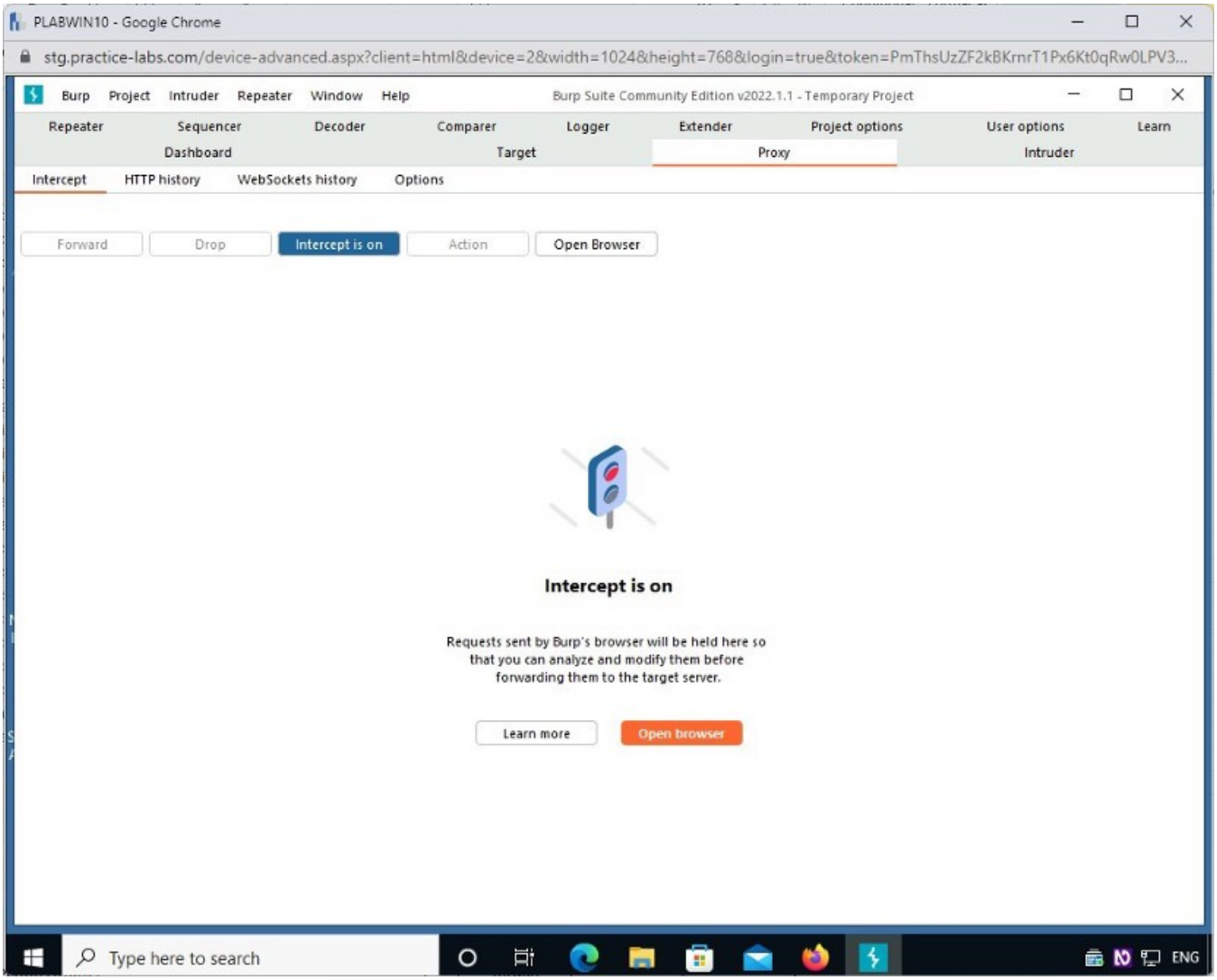
You now need to configure **Burp Suite** to intercept responses.

In the **Options** tab, scroll down to **Intercept Server Responses** section and select the **Intercept responses based on the following rules** checkbox.



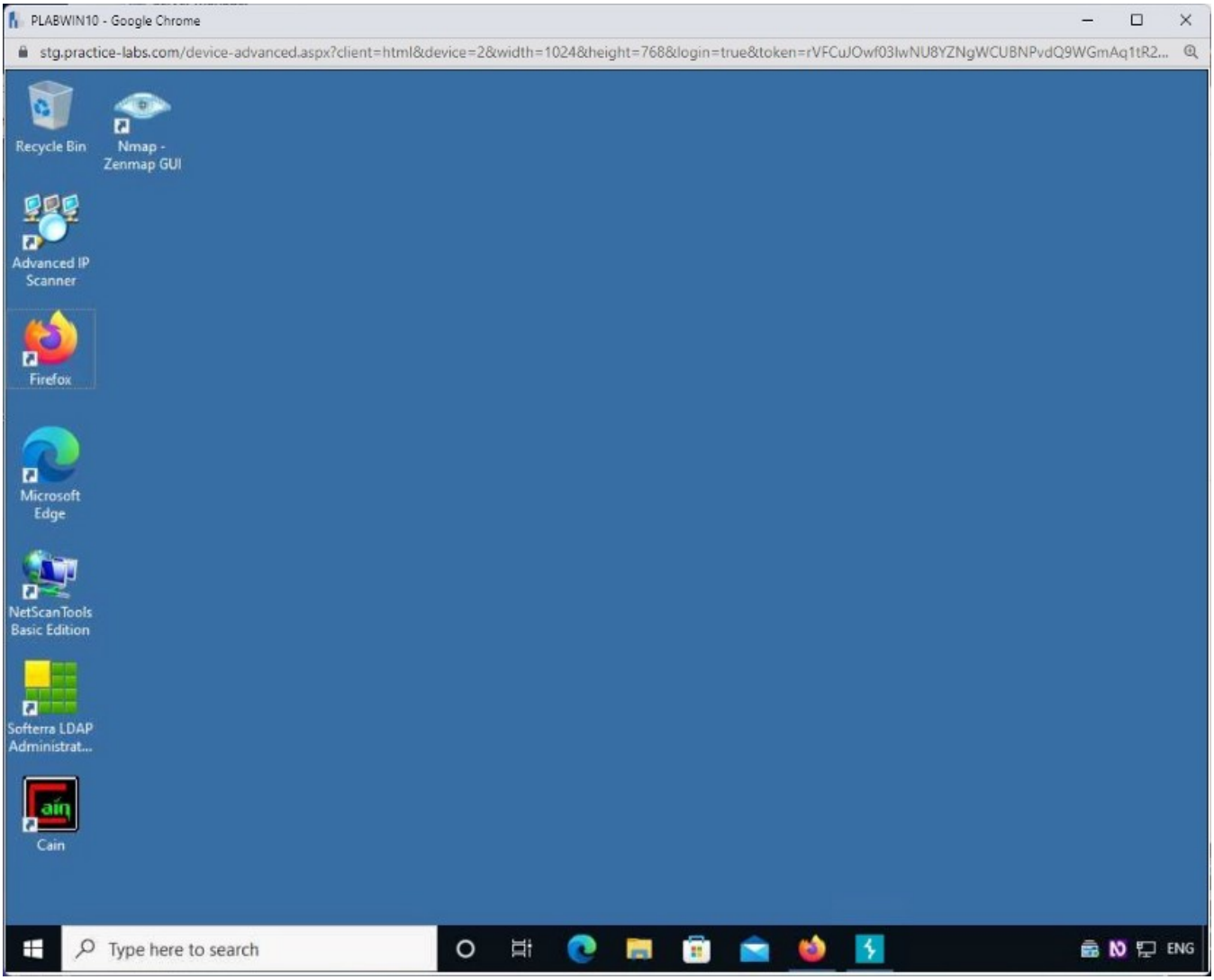
Step 12

Select the **Intercept** tab to the far left of the **Options** tab.



Step 13

Minimize the **Burp Suite** window, so your desktop appears again.



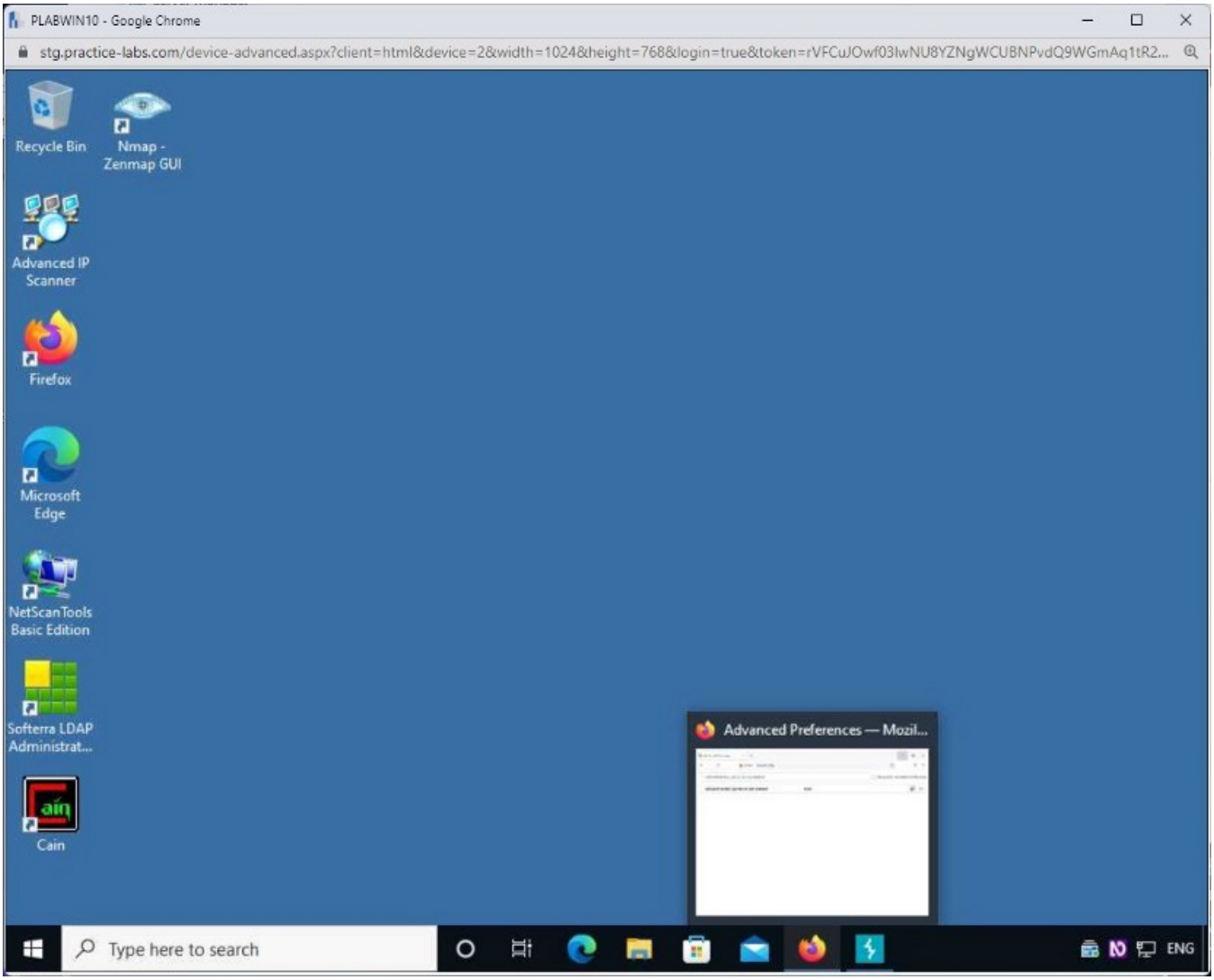
Task 3 — Configure Firefox to Use Burp Suite Proxy Listeners

Now that Burp Suite is configured to intercept traffic, you need to configure Firefox to use proxy listeners. In this task, you will perform the following steps to configure Mozilla Firefox to use Burp Suite proxy listeners.

Step 1

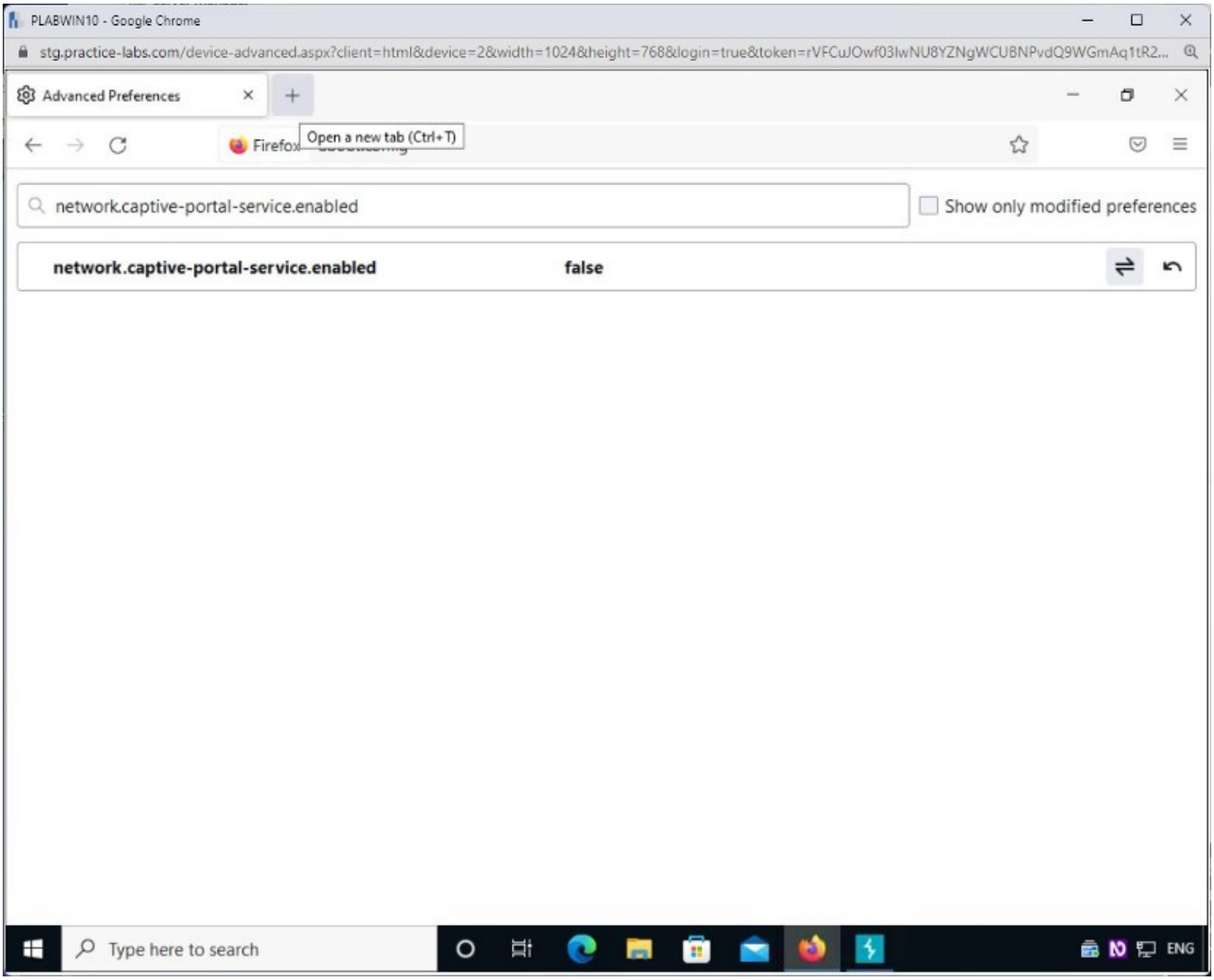
Ensure you have powered on all the devices and connect to **PLABWIN10**.

Reopen **Firefox** from the taskbar.



Step 2

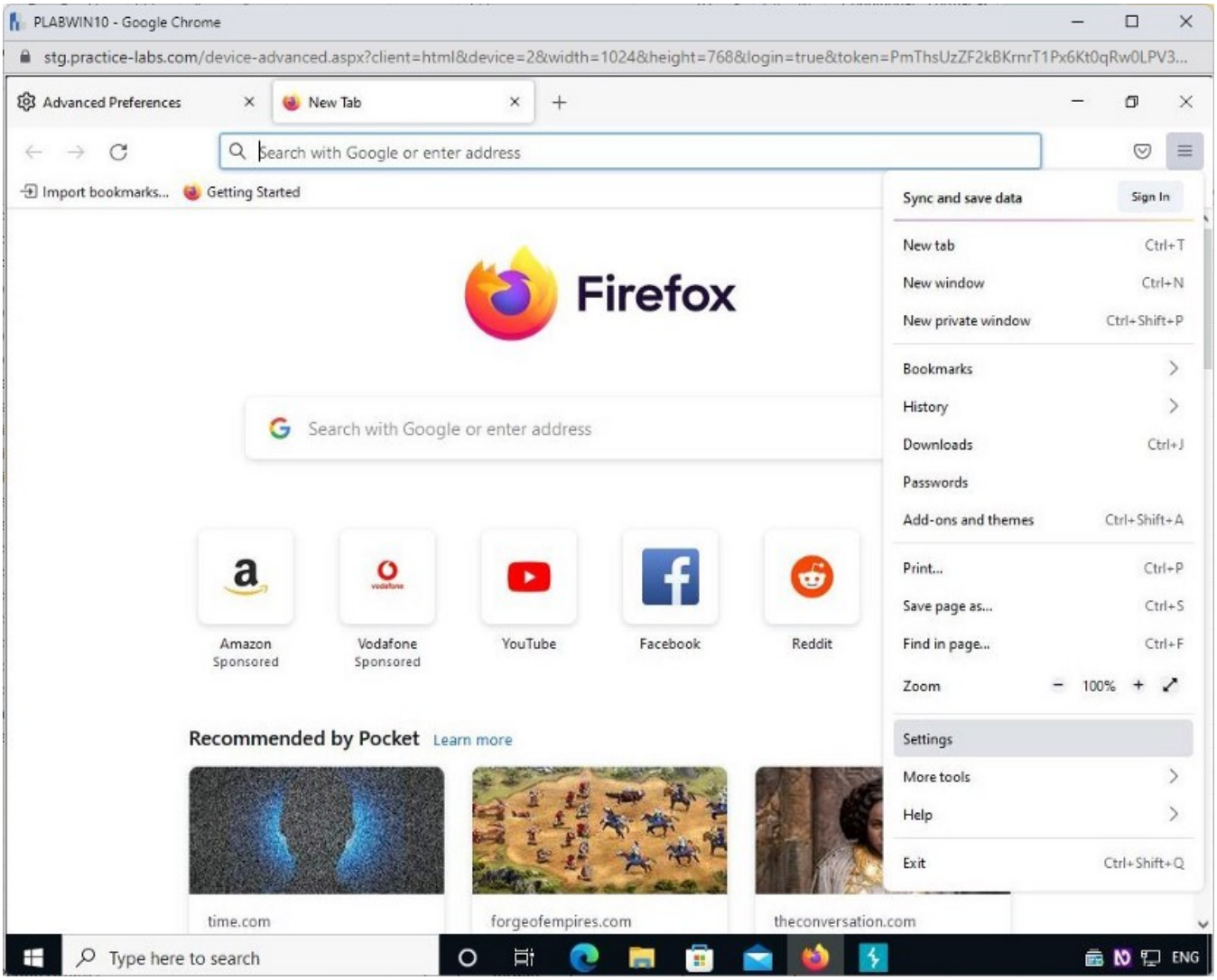
Open a new tab by clicking the **Plus** icon.



Step 3

Click the **Open menu** icon from the upper right-hand corner.

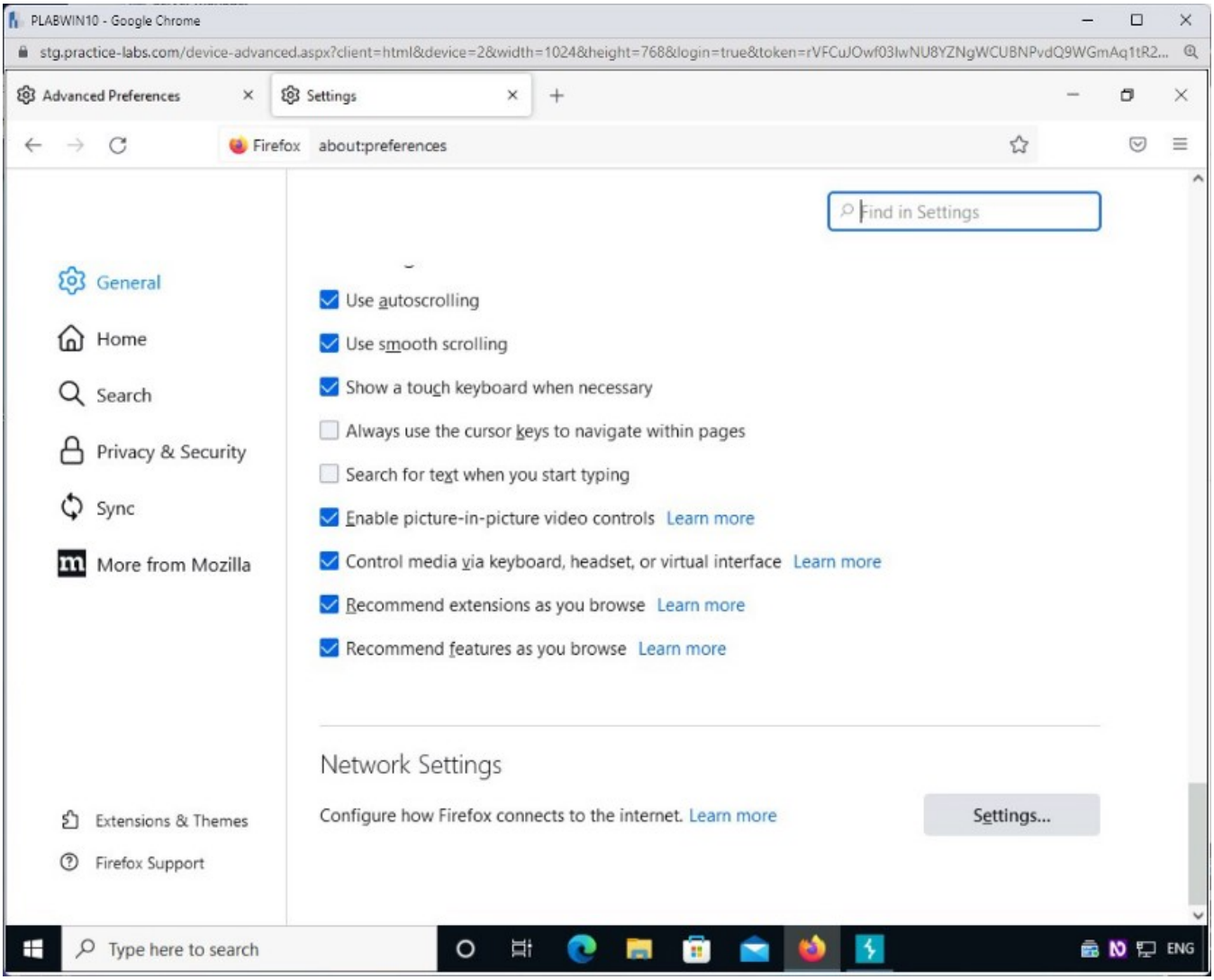
Click **Settings**.



Step 4

In the **Settings** page, the **General** tab opens by default.

Scroll to the bottom of the page to the **Network Settings** section and click **Settings** on the right-hand pane.



Step 5

The **Connection Settings** dialog box opens.

Change the manual proxy address to the Burp listener address. Select **Manual proxy configuration**.

In the **HTTP Proxy** box, type the following IP address:

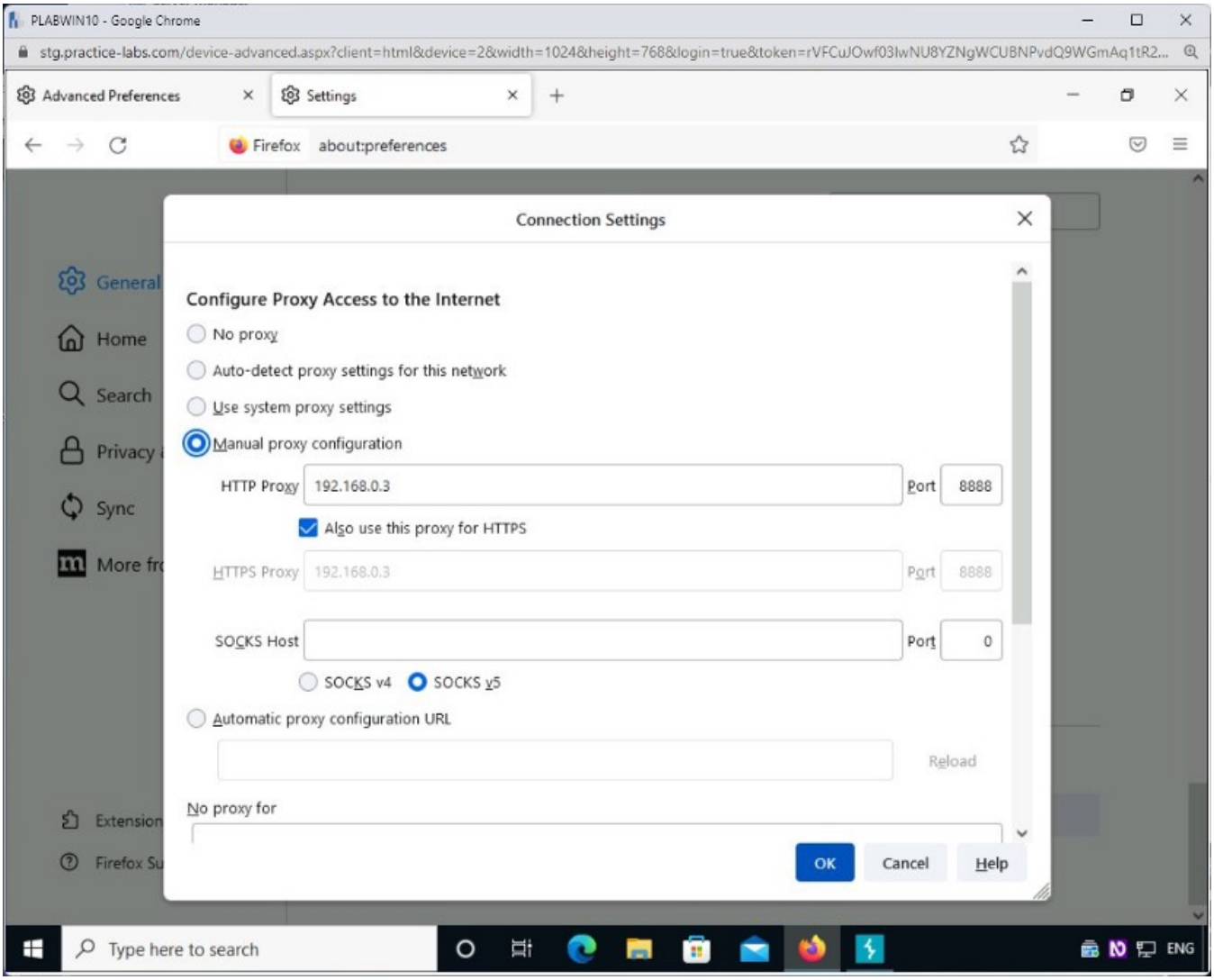
```
192.168.0.3
```

In the **Port** box, type the following port number:

```
8888
```

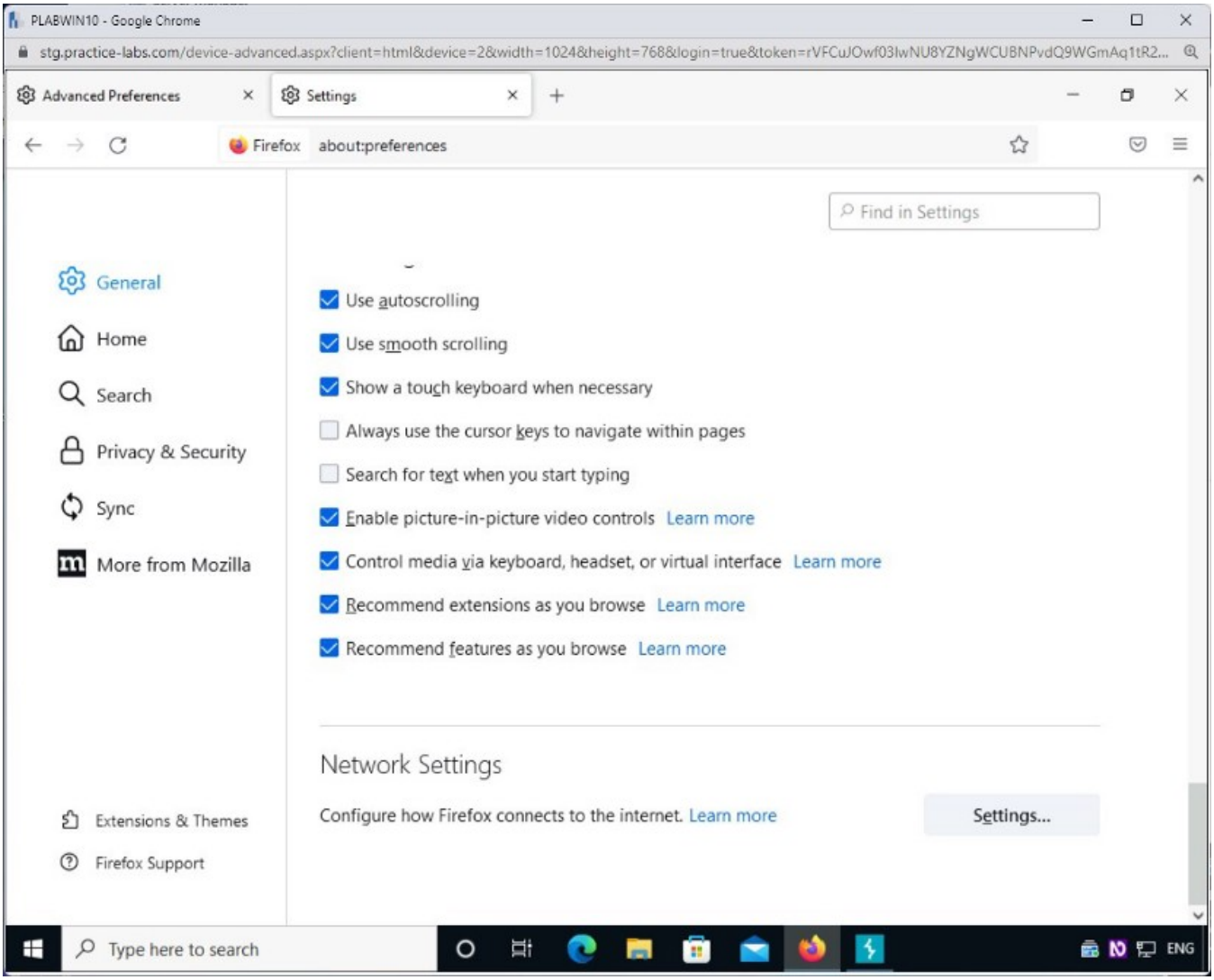
Select the checkbox **Use this proxy server for HTTPS**.

Select **OK** and close the **Connection Settings** page.



Step 6

You should now be back on the **Firefox Options** page.



Task 4 — Capture Cookies

In this task, you will be using the Extremely Buggy Web Application (bWAPP). The proxy listener configuration you previously set up in Firefox will send all the packets to Burp Suite. You will capture the login information as it is sent from the client (browser) to the server (web application) through the proxy. You will also need to forward each HTTP request from Burp Suite to the web application so it can send HTTP responses and web HTML page data, so the user will not know you have captured the packets.

An important point that needs to be noted in this task is that for each action in the Mozilla Firefox application, you must forward the associated request in Burp Suite. This will allow Burp Suite to intercept each and every request.

In this session, you will capture cookies. To do this, perform the following steps:

Step 1

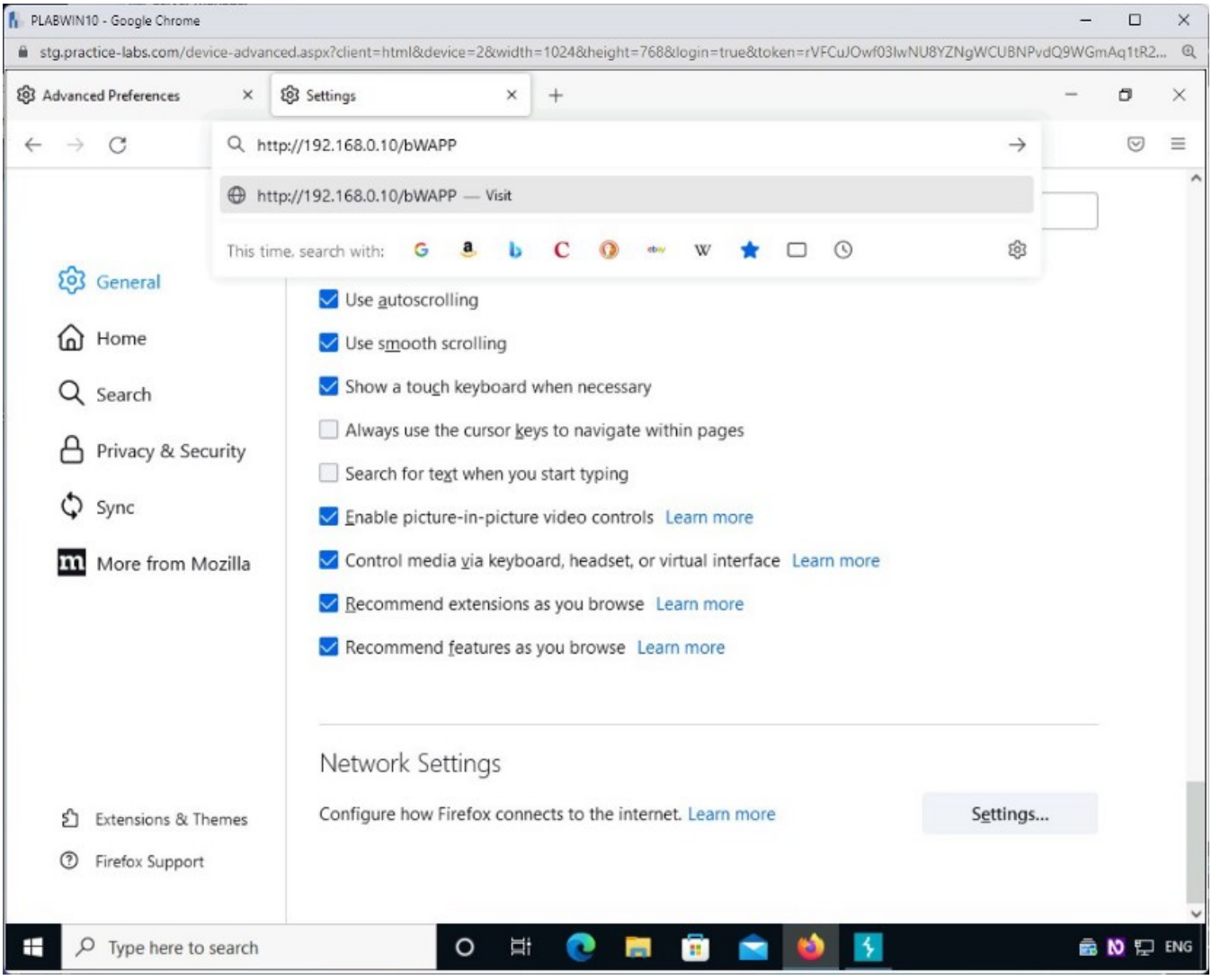
Ensure you have powered on all the devices and connect to **PLABWIN10**.

To access the **bWAPP** application, type the following URL in the address bar of **Firefox**:

```
http://192.168.0.10/bWAPP
```

Press **Enter**.

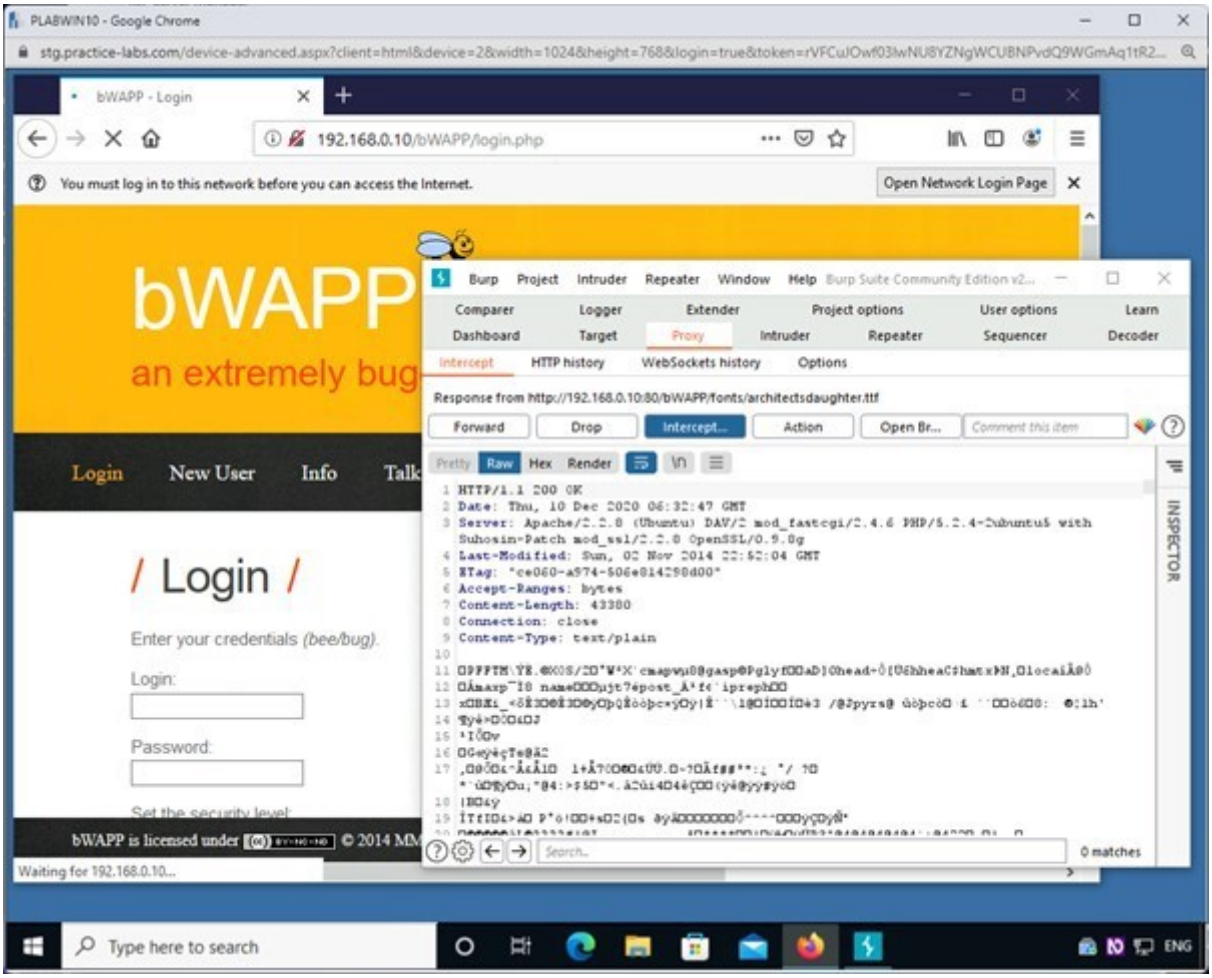
Alert: Ensure to select **Forward** in **Burp Suite** for each and every request made in **Mozilla Firefox**, as the intercept is **ON** in **Burp Suite**.



Step 2

Resize the **Firefox** and **Burp Suite** windows so you can see both.

Continue to select the **Forward** button in **Burp Suite** until the login page on the **bWAPP** app appears in **Firefox**.



Note*: It may take 30–40 forwards to get to the bWAPP login page.*

Step 3

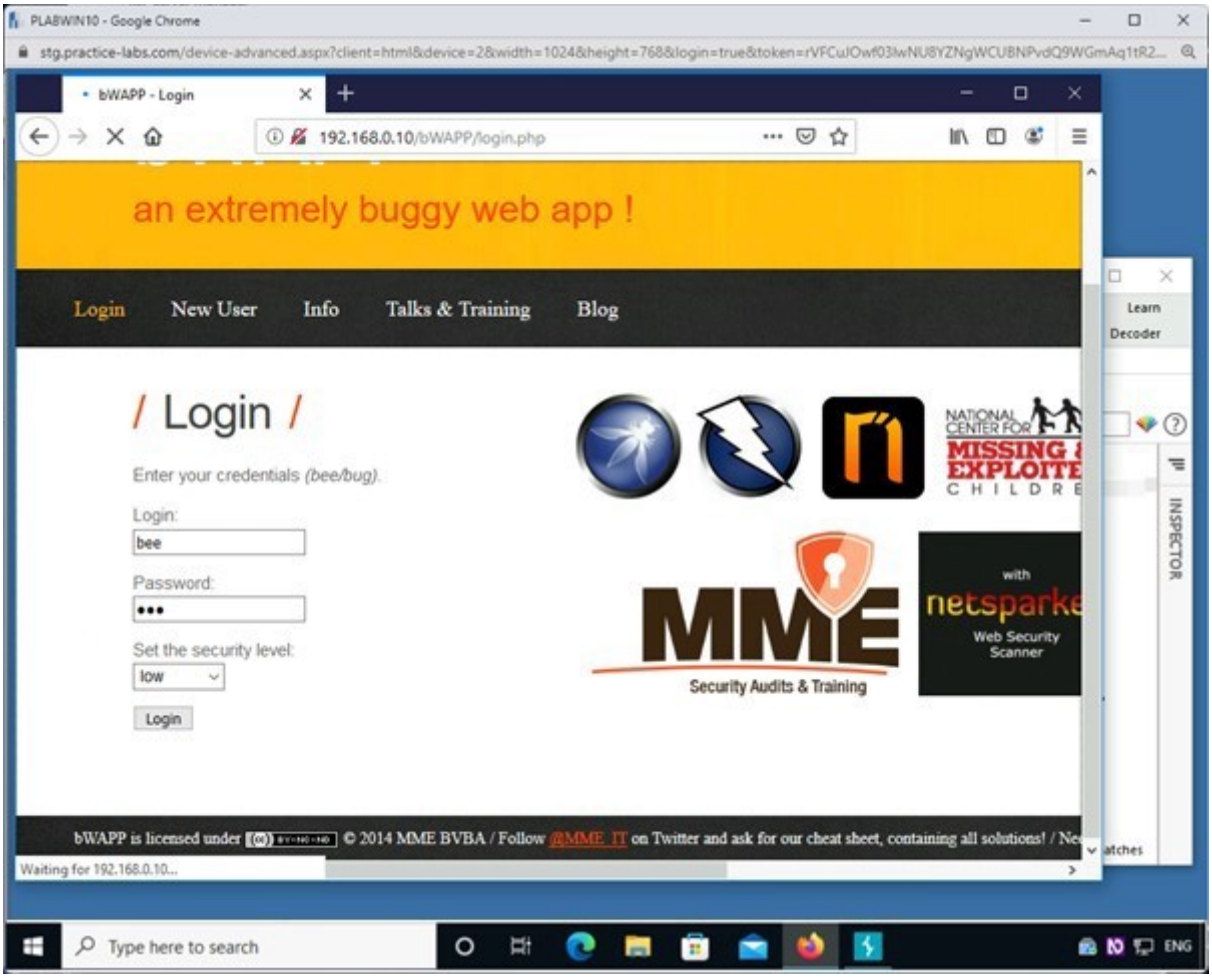
In the **Username** box on the **bWAPP** login page, type the following username:

```
bee
```

In the **Password** box, type the following password:

bug

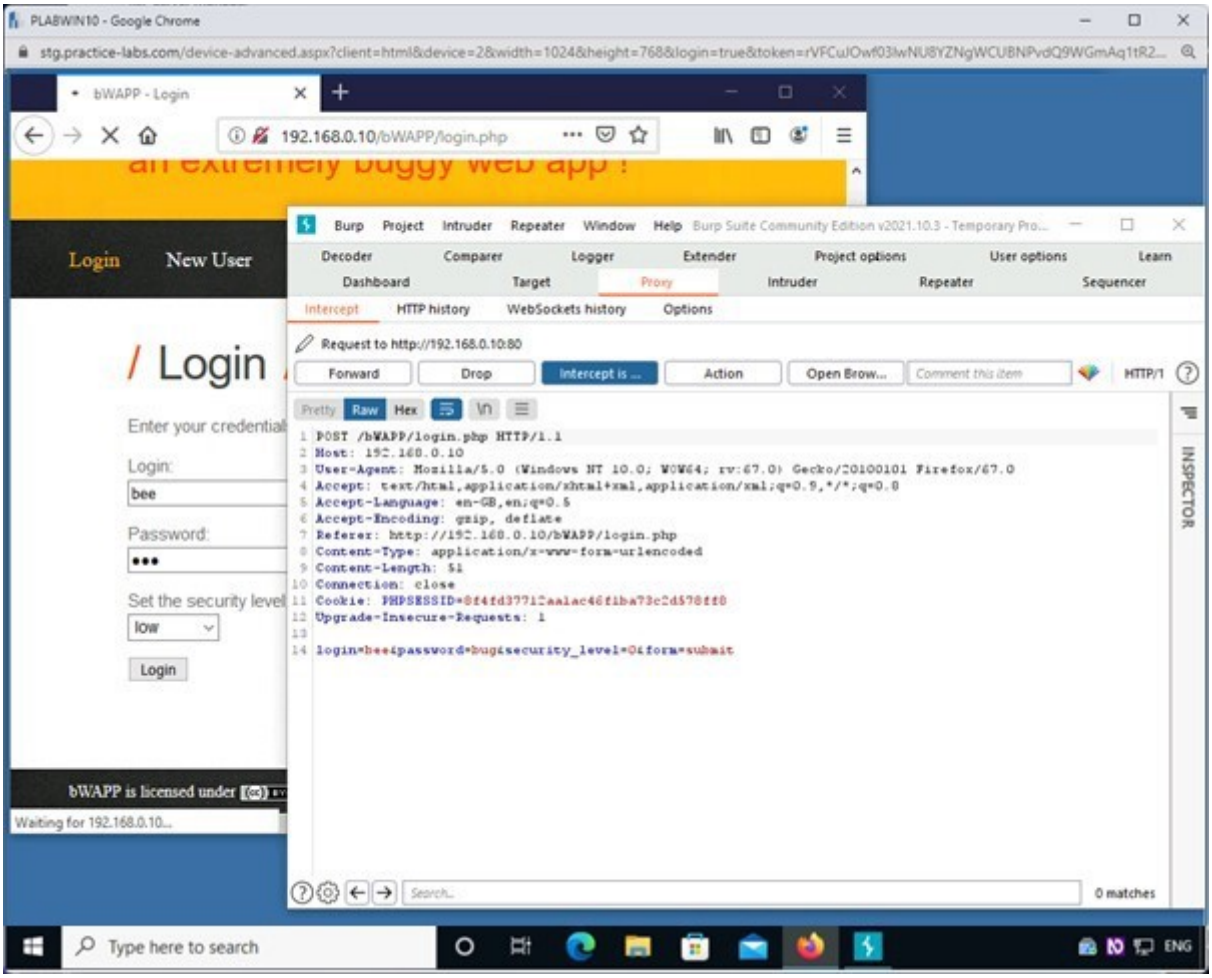
Select **Login**.



Step 4

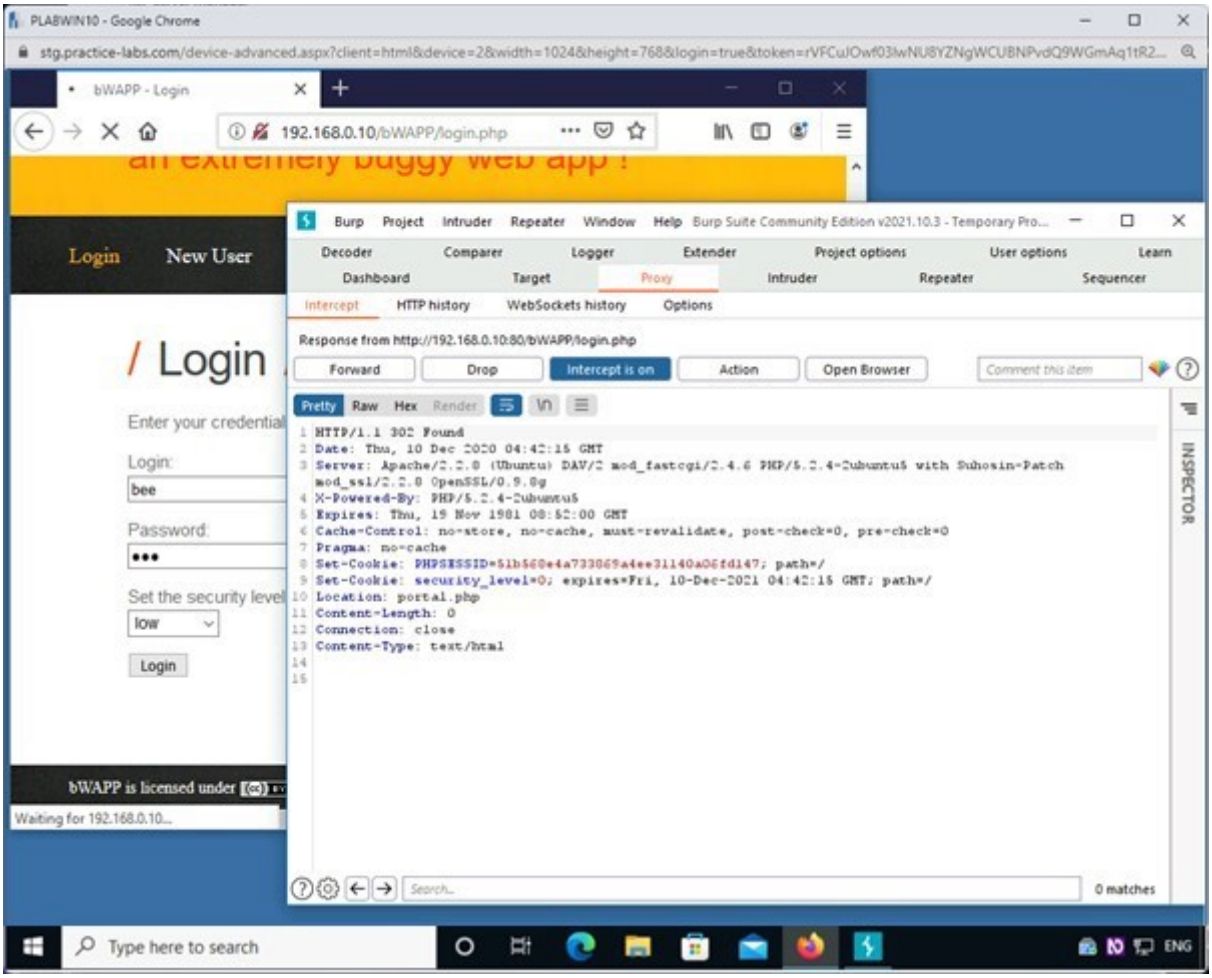
Switch to the **Burp Suite** window. Select the **Forward** button. Analyze the displayed information. Here you can see the username and password you entered as well as a cookie session id.

***Note**: You may have to select the forward button several times. It should not take too many since Firefox is no longer trying to detect a captive portal.*



Step 5

Continue selecting the forward button to see additional HTTP requests being captured. Even though the **bWAPP** has not returned a completed login screen to the browser, you see a newly created cookie session id along with its validity time.



Step 6

Continue clicking the forward button until **Burp Suite** shows a blank screen.

Notice the **bWAPP** screen changed and you are now completed logged in.