Practice Labs - Ethical Hacker v10

Session Hijacking

Introduction

Burp
Session Hijacking
Ethical Hacking
Cookies

Welcome to the **Session Hijacking** Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 - Capture Session Cookies

After completing this lab, you will be able to:

- Install Burp Suite on PLABWIN10
- Install Firefox
- Configure Burp Suite on PLABWIN10
- Configure Firefox to Use Burp Suite Proxy Listeners
- Capture Cookies

Exam Objectives

The following exam objectives are covered in this lab:

- **3.2** Information Security Attack Detection
- **3.3** Information Security Attack Prevention

> ***Note:*** *Our main focus is to cover the practical, hands-on aspects of the exam objectives. We recommend referring to course material or a search engine to research theoretical topics in more detail.*

Lab Duration

It will take approximately **1 hour** to complete this lab.

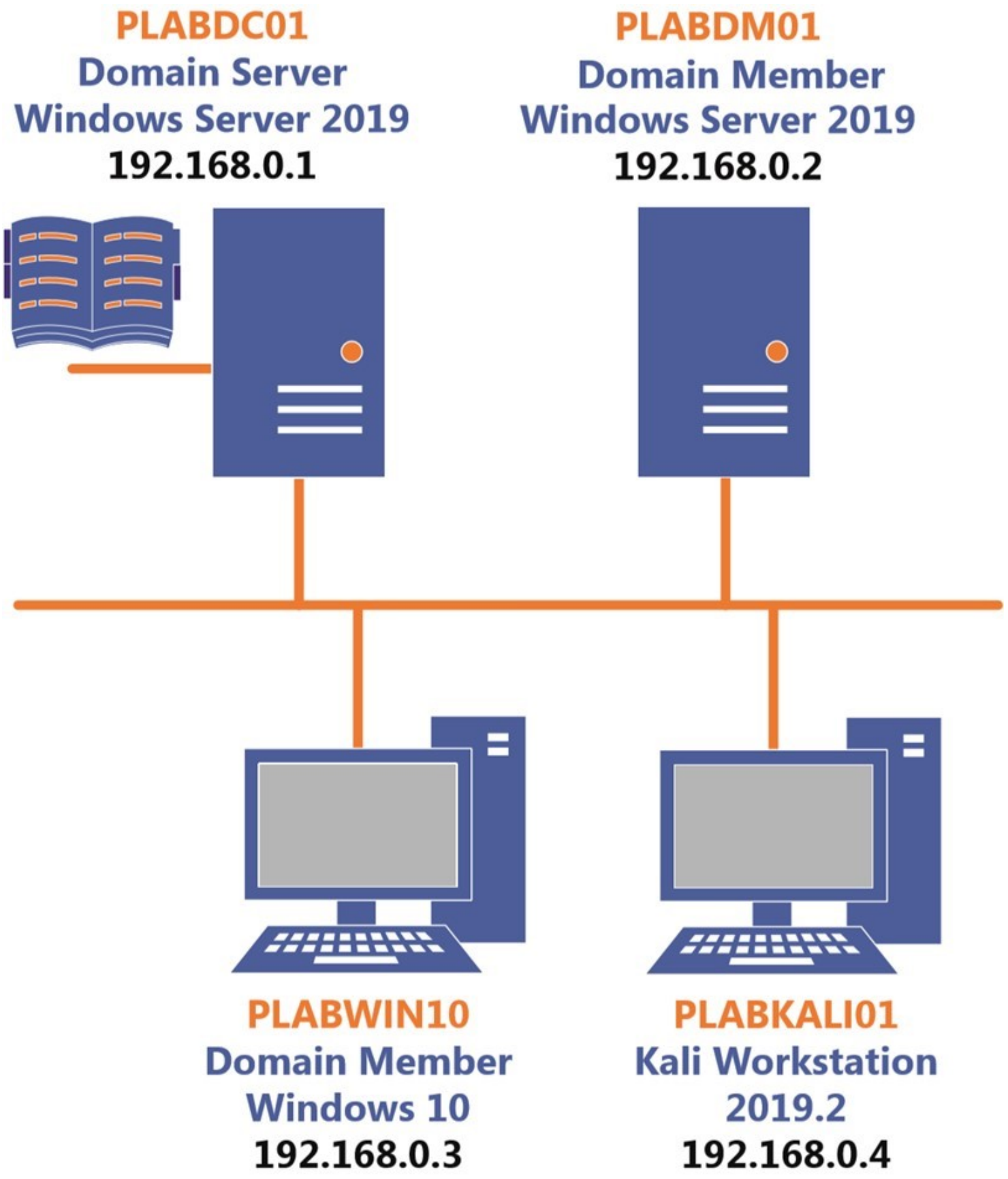
Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

> Click **Next** to view the Lab topology used in this module.

Lab Topology

During your session, you will have access to the following lab configuration.



Depending on the exercises, you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.

- **PLABDC01 -** (Windows Server 2019 - Domain Server)
- **PLABDM01 -** (Windows Server 2019 - Domain Member)
- **PLABWIN10 -** (Windows 10 - Workstation)
- **PLABKALI01 -** (Kali 2019.2 - Linux Kali Workstation)

Click **Next** to proceed to the first exercise.

Exercise 1 - Capture Session Cookies

You can view cookie information from unencrypted sites using session hijacking, also known as cookie hijacking. Session hijacking occurs at the network and application level. At the application level session hijacking, you will intercept the session ID of a particular session with the help of cookies and use it to gain unauthorized access to sensitive or critical data.

In this exercise, you will perform the following tasks to perform application-level session hijacking:

- Enable HTTP web service on PLABSA01
- Configure Burp Suite on PLABWIN10
- Configure Firefox to use Burp Suite proxy listeners
- Capture cookies
- Hijack the session

Learning Outcomes

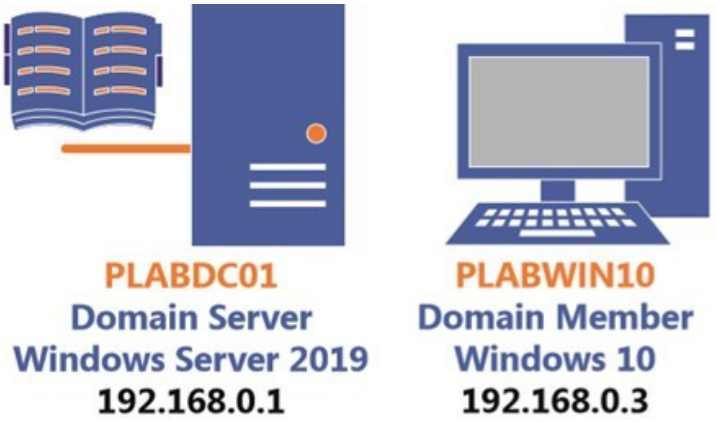
After completing this exercise, you will be able to:

- Install Burp Suite on PLABWIN10
- Install Firefox
- Configure Burp Suite on PLABWIN10
- Configure Firefox to Use Burp Suite Proxy Listeners
- Capture Cookies

Your Devices

You will be using the following devices in this lab. Please power these on now.

- **PLABDC01 -** (Windows Server 2019 - Domain Server)
- **PLABWIN10 -** (Windows 10 - Workstation)



Task 1 - Install Firefox

Firefox is a Web browser developed by Mozilla. It is mainly used for surfing the web, and it is also used with Burp Suite for intercepting traffic.

In this task, you will learn to install Firefox. 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** text box on the taskbar, type the following:

```
Internet Explorer
```

From the search results, select **Internet Explorer**.

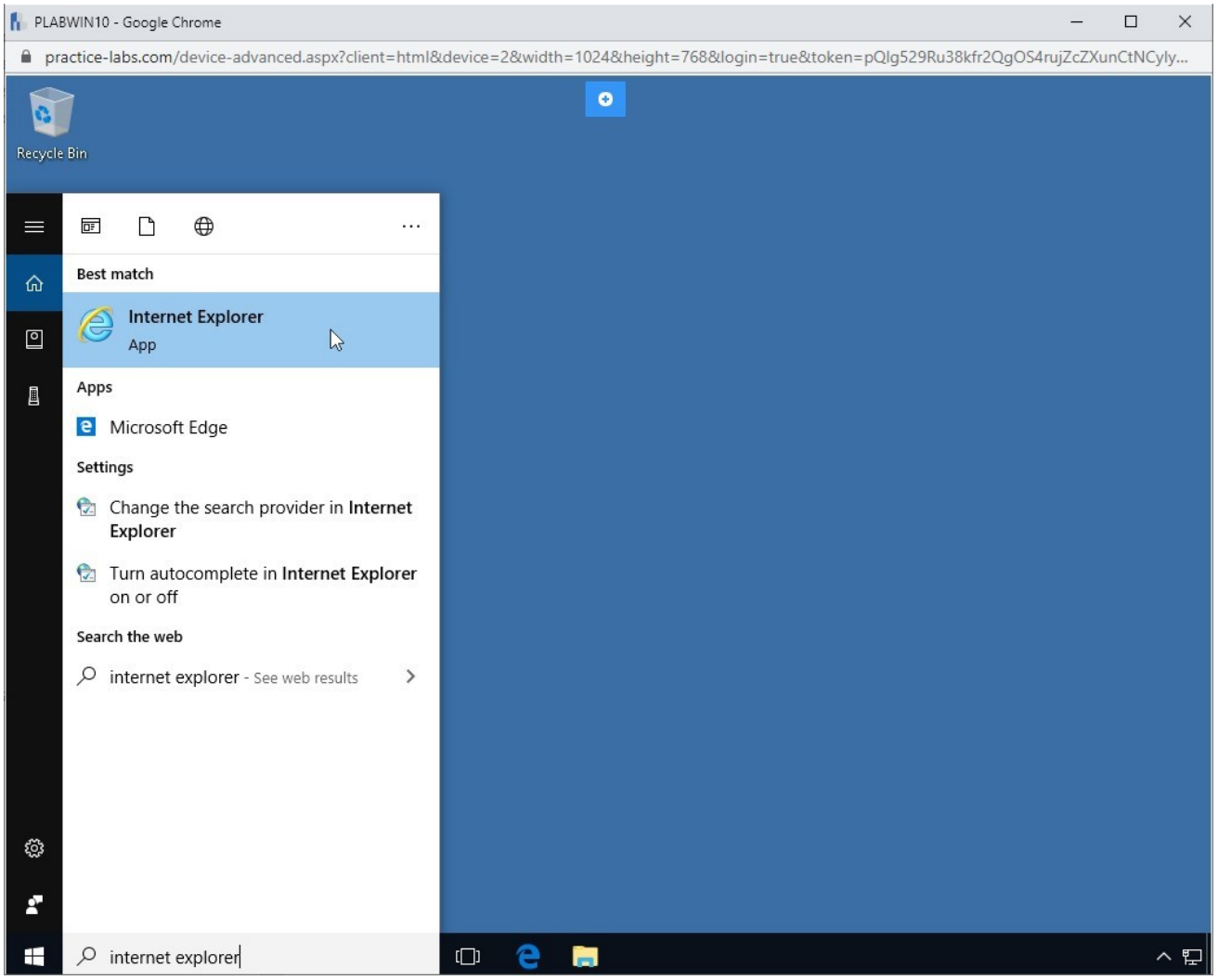


Figure 1.1 Screenshot of PLABWIN10: Desktop, searching the system for Internet Explorer.

Step 2

Internet Explorer is now opened.

The **Intranet** page should be automatically opened, if not,

In the address bar, type the following URL:

```
http://intranet
```

Press **Enter**.

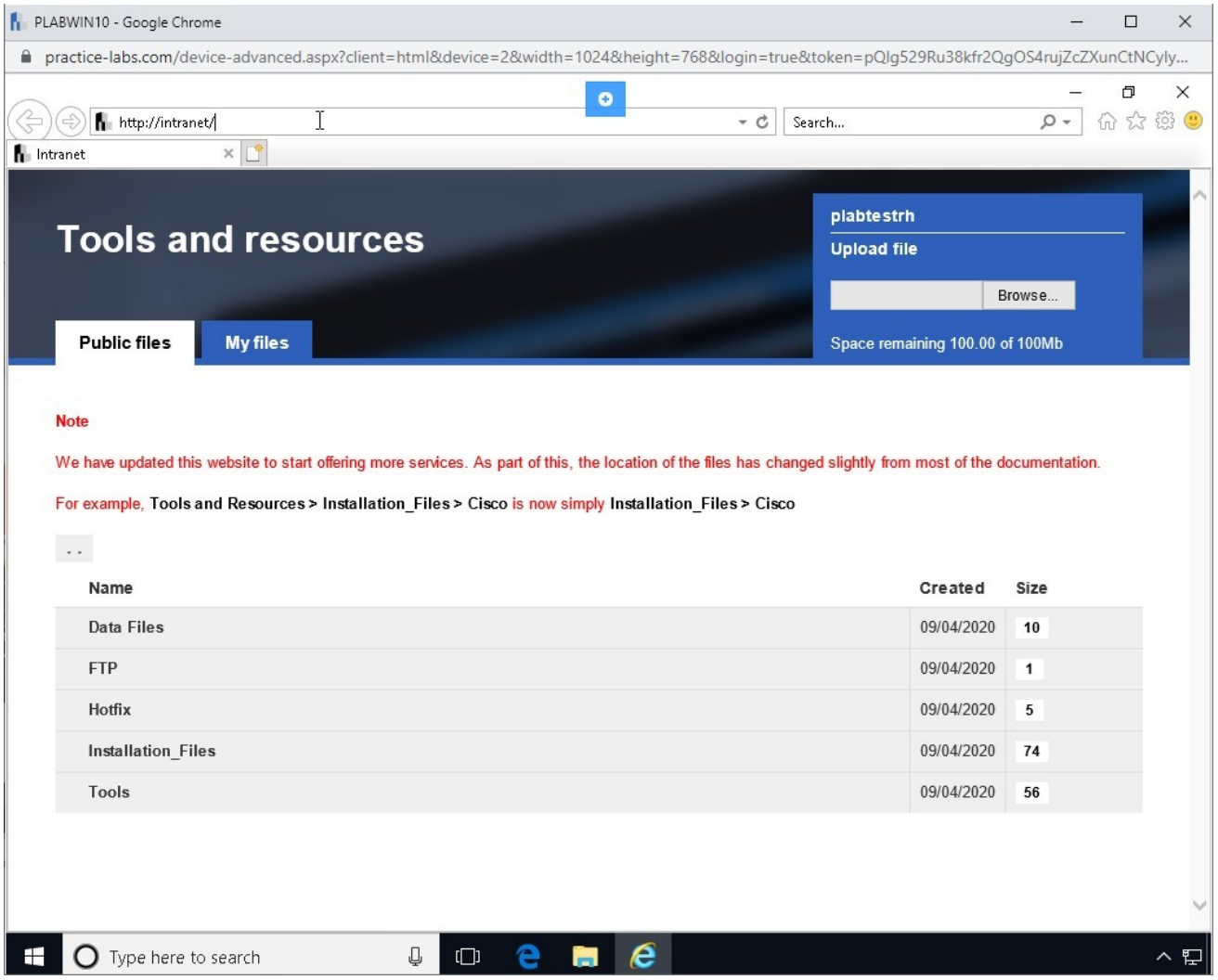


Figure 1.2 Screenshot of PLABWIN10: Entering the URL in the address bar of Internet Explorer.

Step 3

After the **Intranet** Website has loaded, click **Installation_Files**.

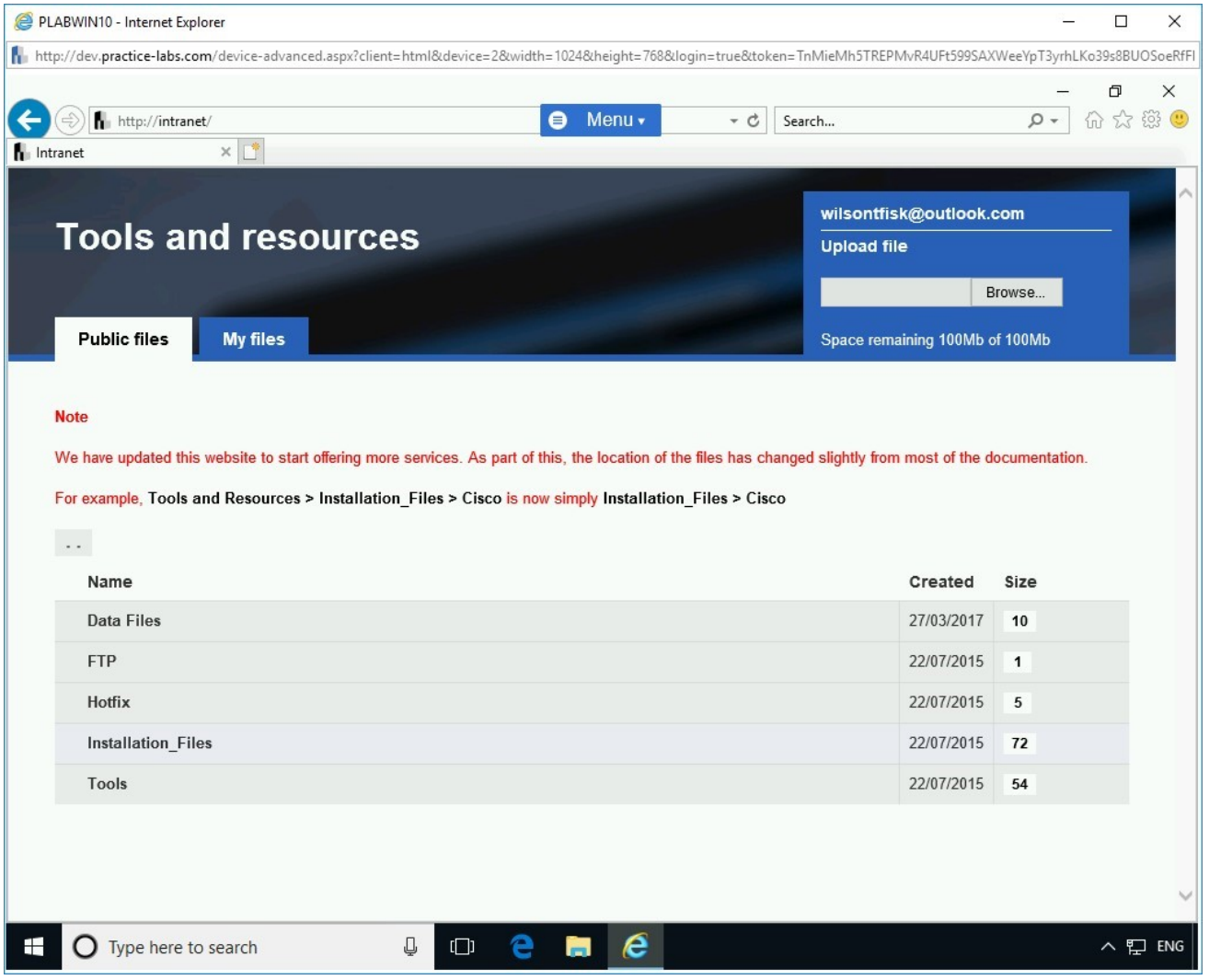


Figure 1.3 Screenshot of PLABWIN10: Clicking the Installation_Files link.

Step 4

On the **Installation_Files** page, click **Firefox**.

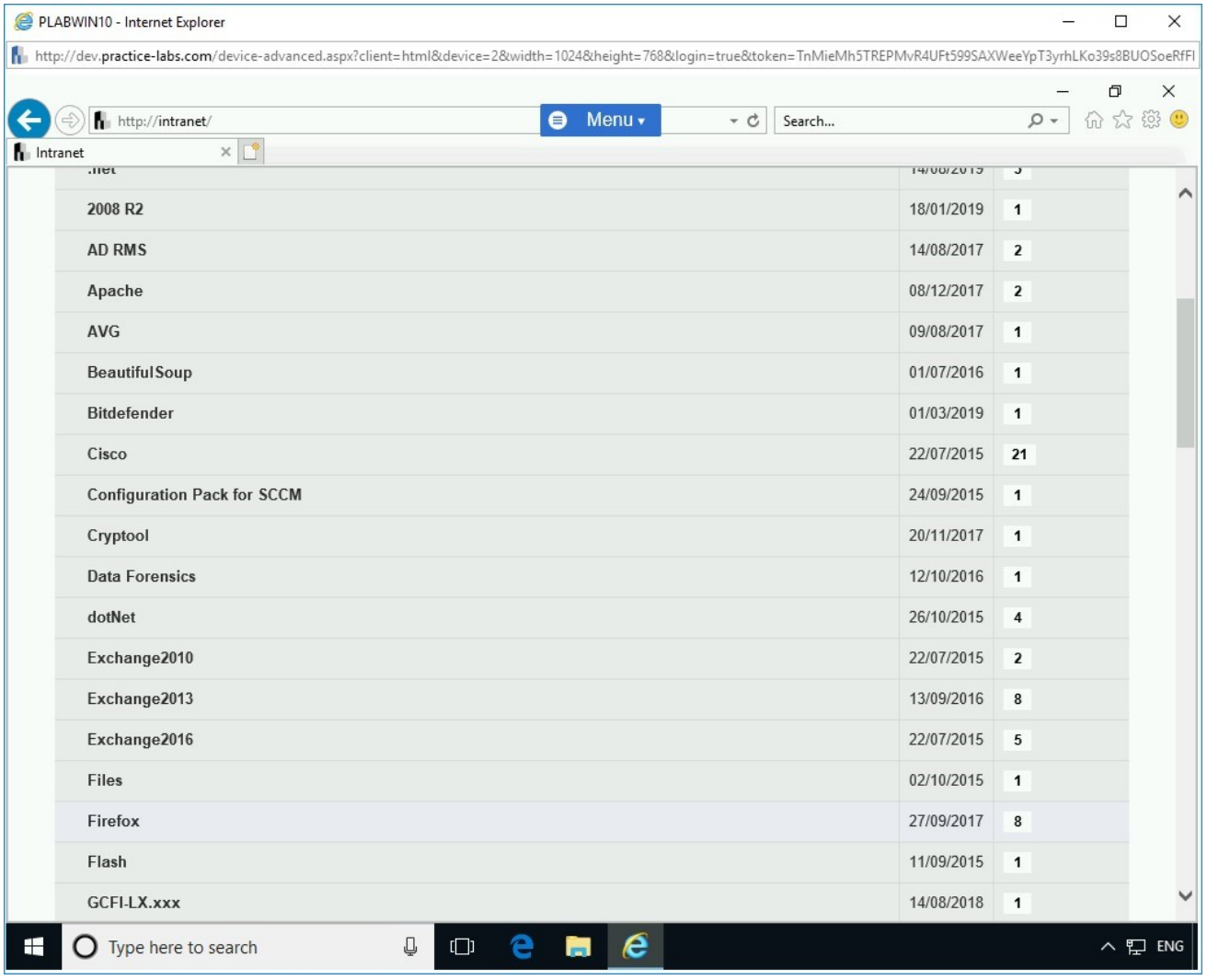


Figure 1.4 Screenshot of PLABWIN10: Clicking the Firefox link.

Step 5

On the **Firefox** page, click **Firefox Setup 67.0.exe**.

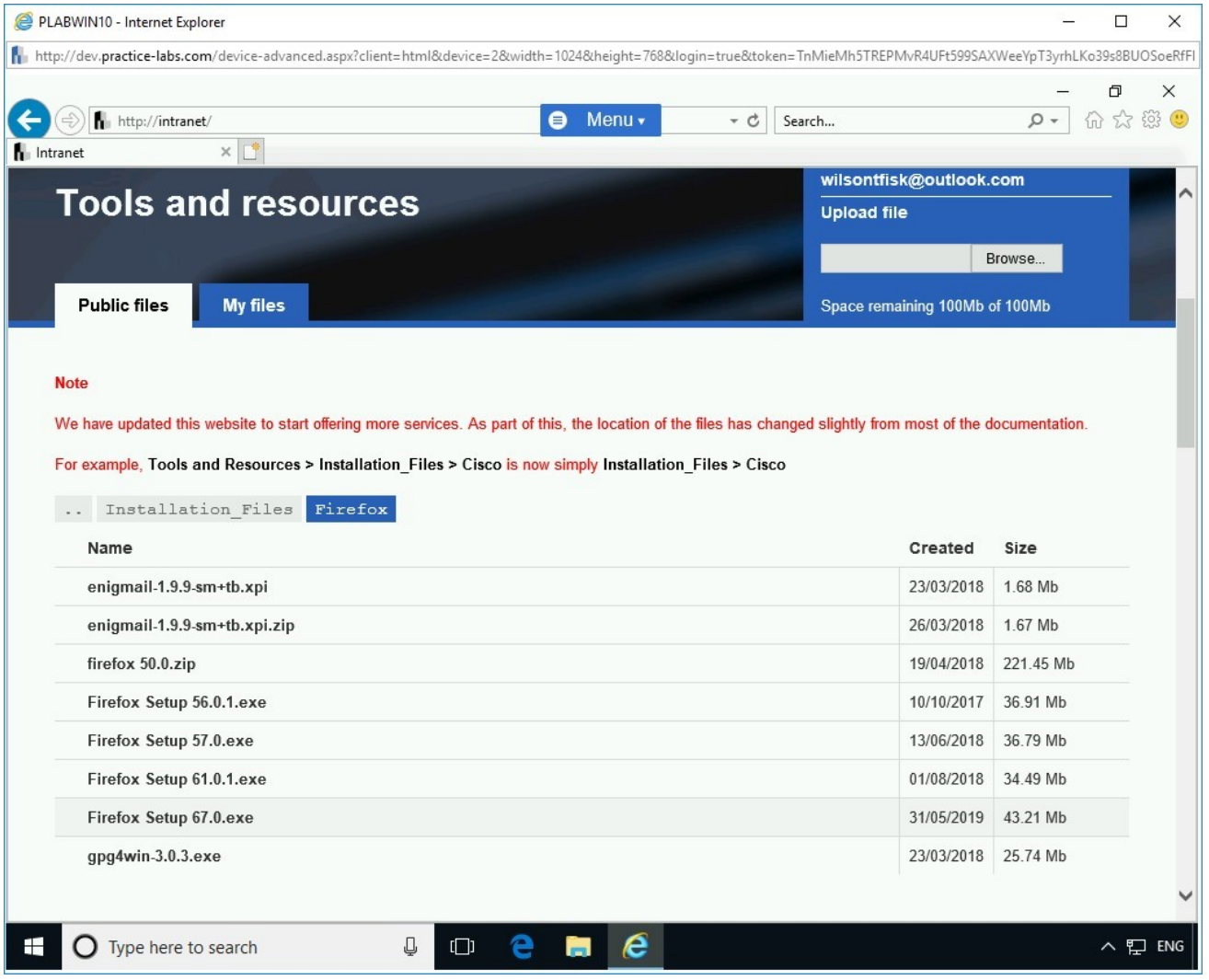


Figure 1.5 Screenshot of PLABWIN10: Clicking the Firefox Setup 67.0.exe link.

Step 6

In the notification bar, click **Run**.

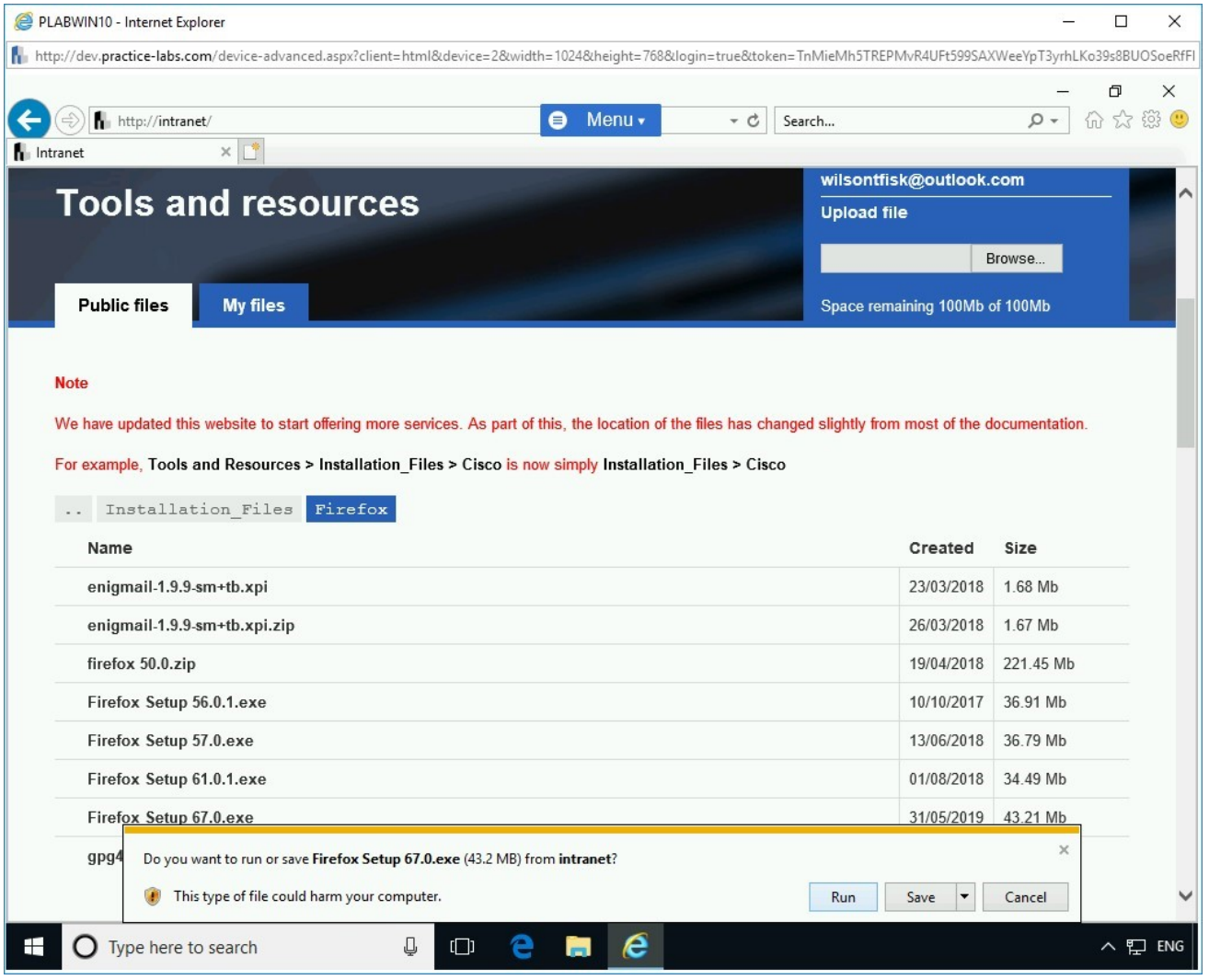


Figure 1.6 Screenshot of PLABWIN10: Clicking Run in the notification bar.

Step 7

A dialog box displays the file extraction in progress.

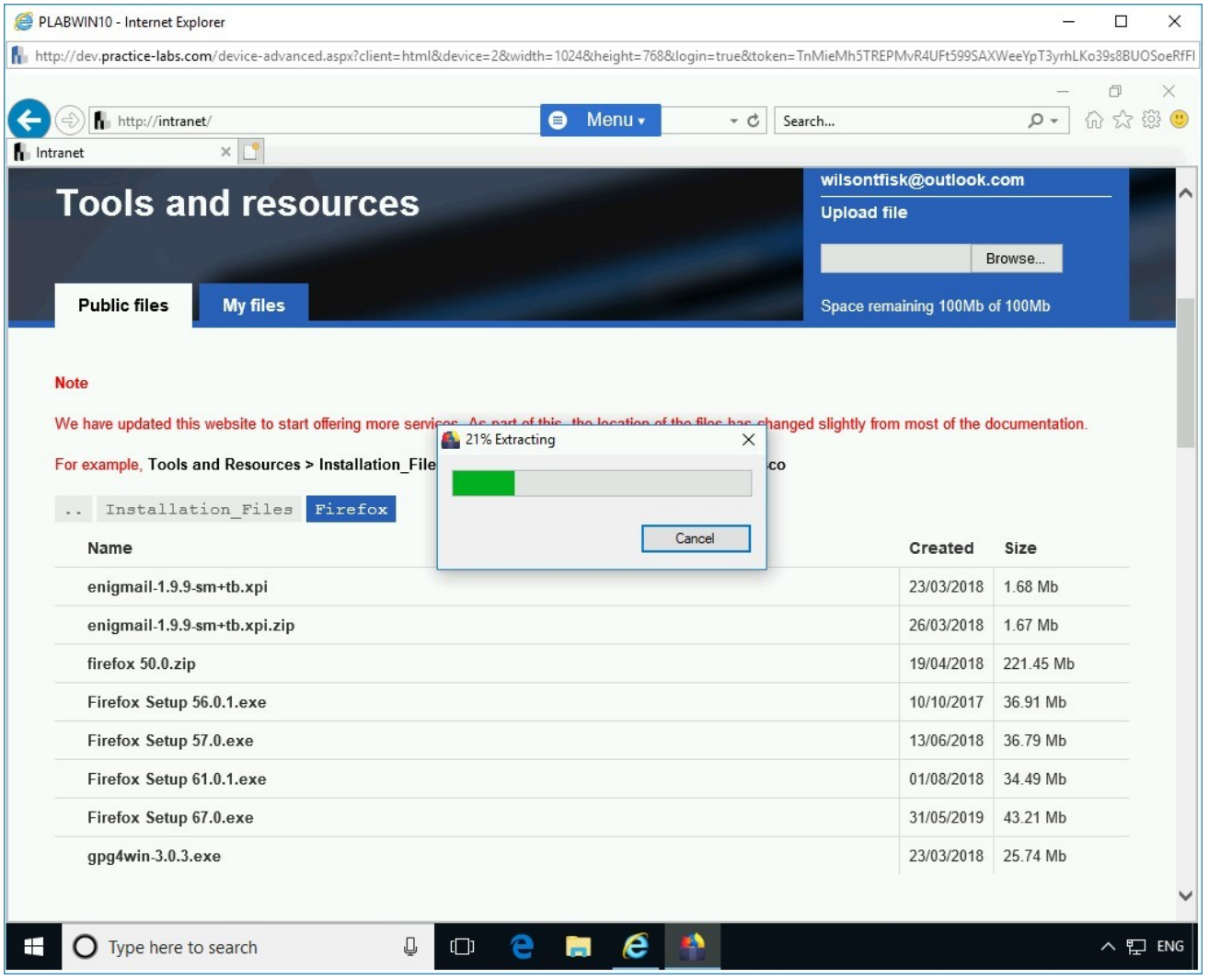


Figure 1.7 Screenshot of PLABWIN10: Showing a dialog box with the file extraction progress.

Step 8

The **Mozilla Firefox Setup** dialog box is displayed. On the **Welcome to the Mozilla Firefox Setup Wizard** page, click **Next**.

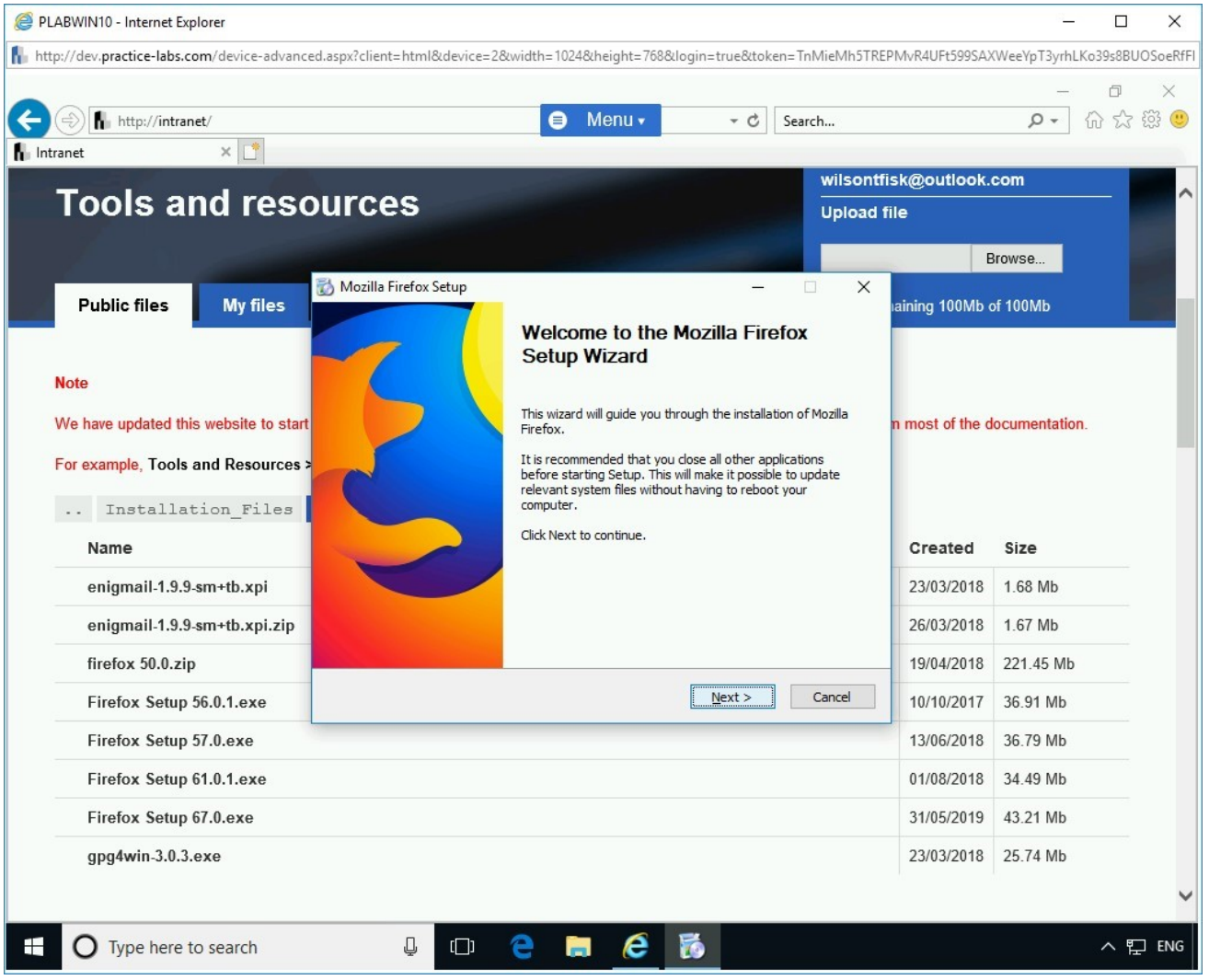


Figure 1.8 Screenshot of PLABWIN10: Clicking Next on the Welcome to the Mozilla Firefox Setup Wizard page.

Step 9

On the **Setup Type** page, keep the default selection and click **Next**.

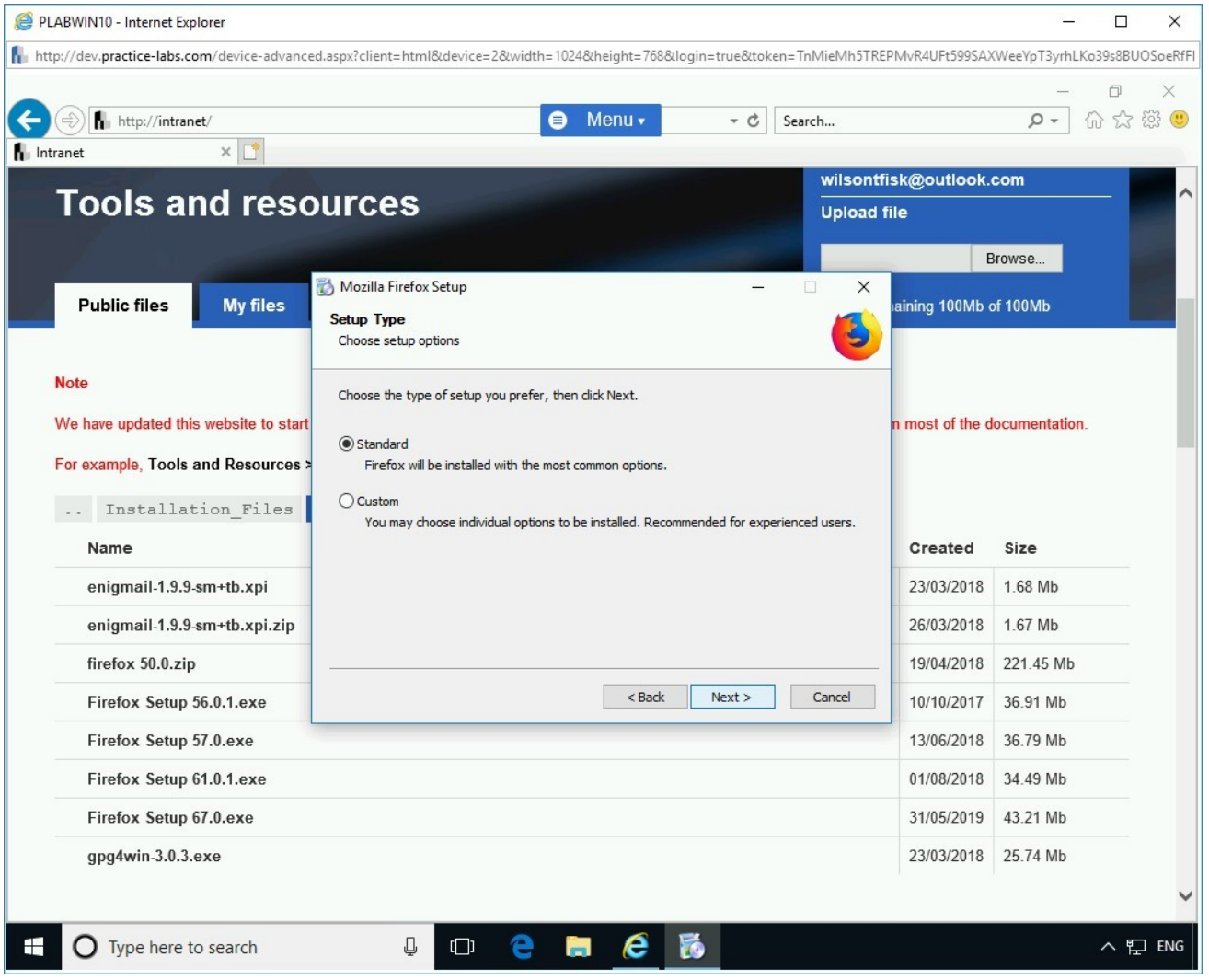


Figure 1.9 Screenshot of PLABWIN10: Clicking Next on the Setup Type page.

Step 10

On the **Summary** page, click **Install**.

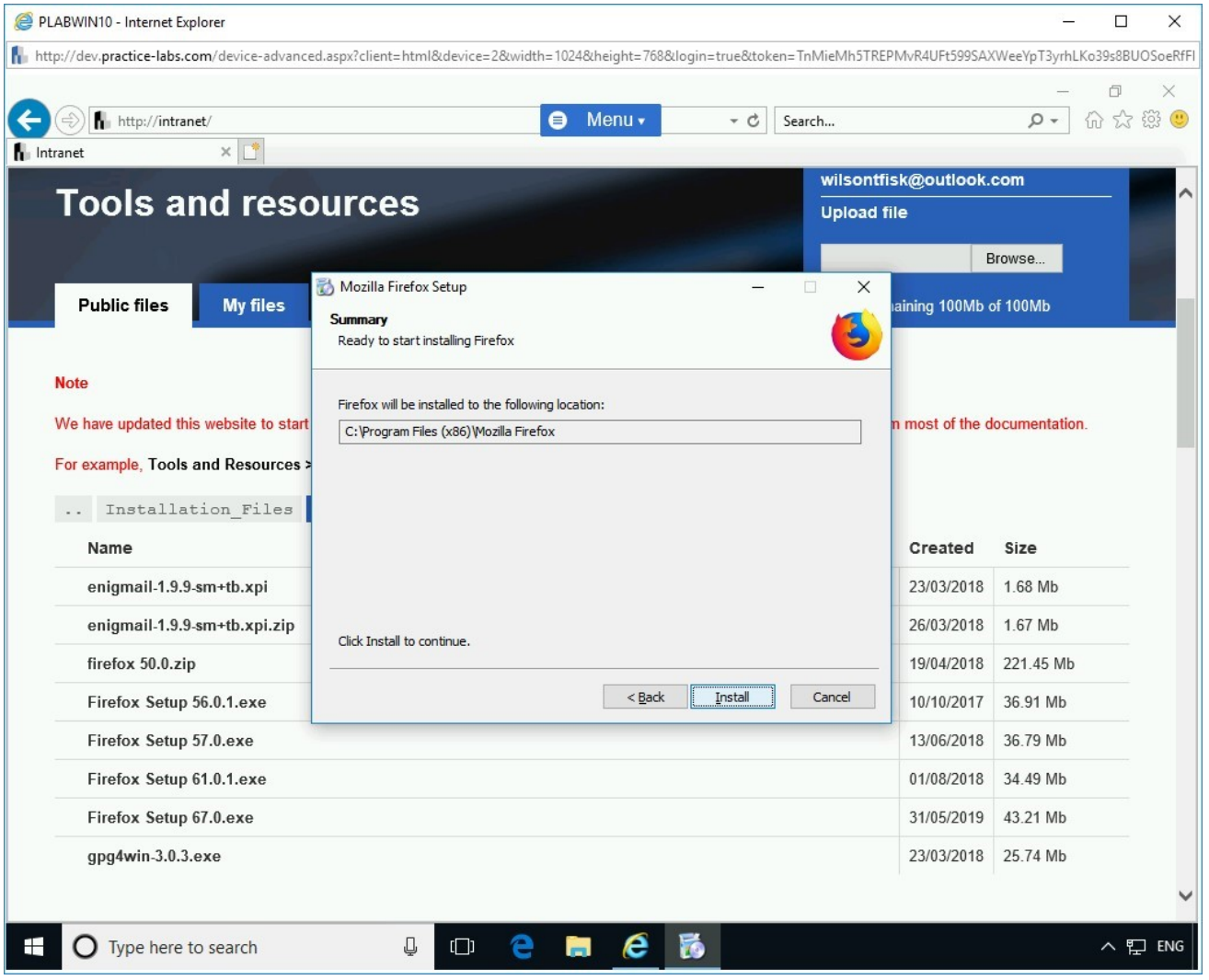


Figure 1.10 Screenshot of PLABWIN10: Clicking Install on the Summary page.

Step 11

On the **Installing** page, the installation progress is displayed.

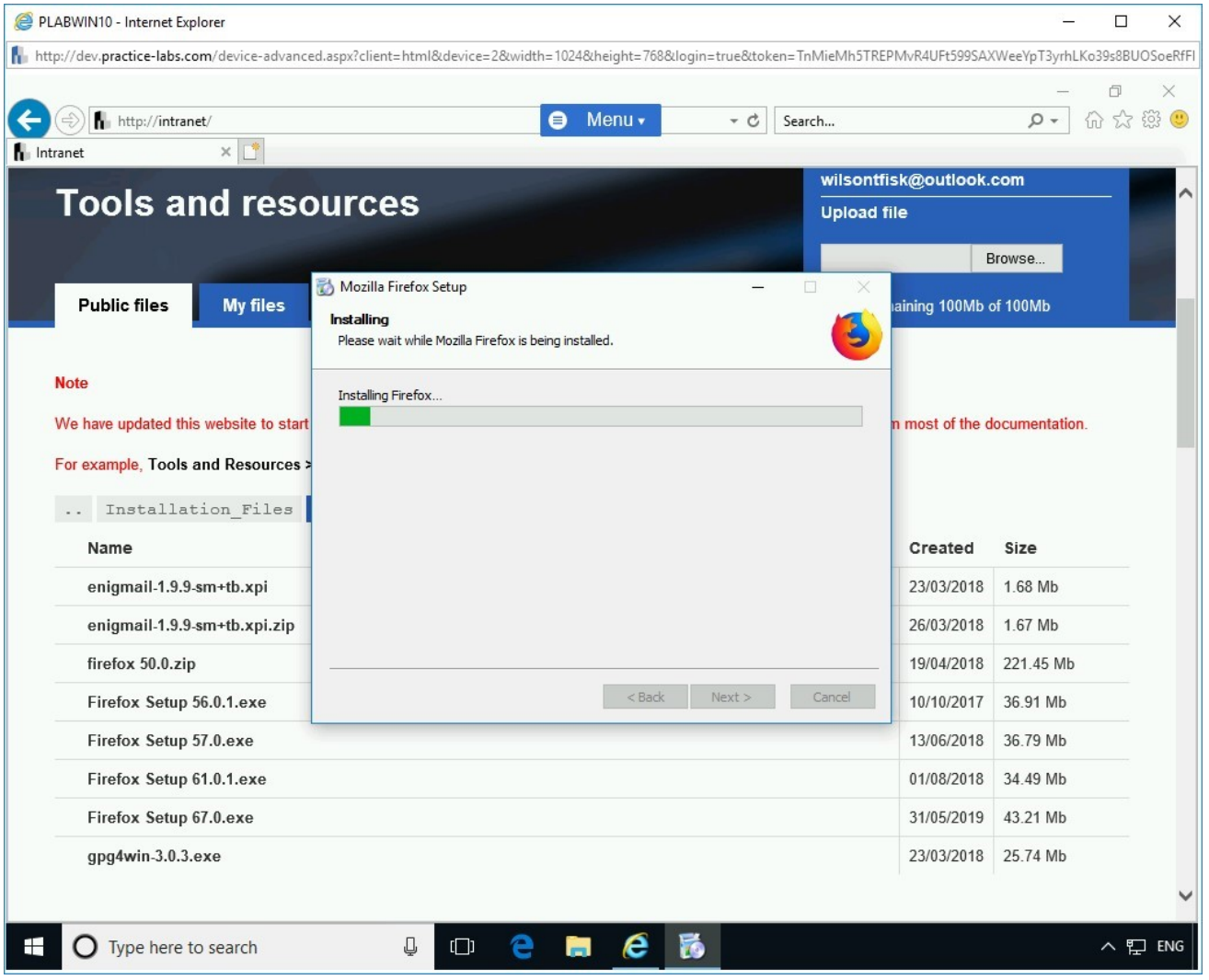


Figure 1.11 Screenshot of PLABWIN10: Showing the installation progress on the Installing page.

Step 12

On the **Completing the Mozilla Firefox Setup Wizard** page, de-select **Launch Firefox now** and click **Finish**.

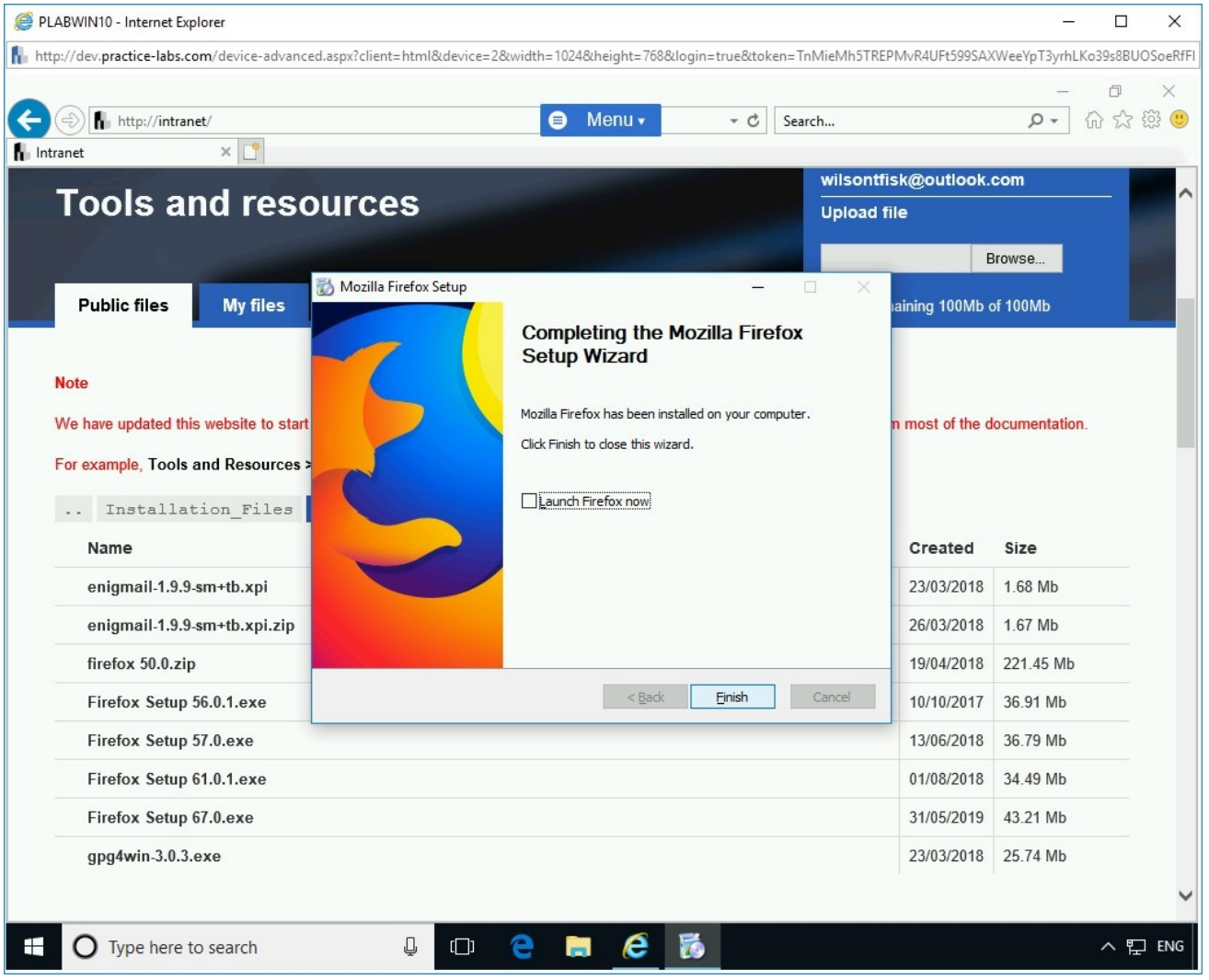


Figure 1.12 Screenshot of PLABWIN10: Clicking Finish on the Completing the Mozilla Firefox Setup Wizard page.

Step 13

Close the **Internet Explorer** window.

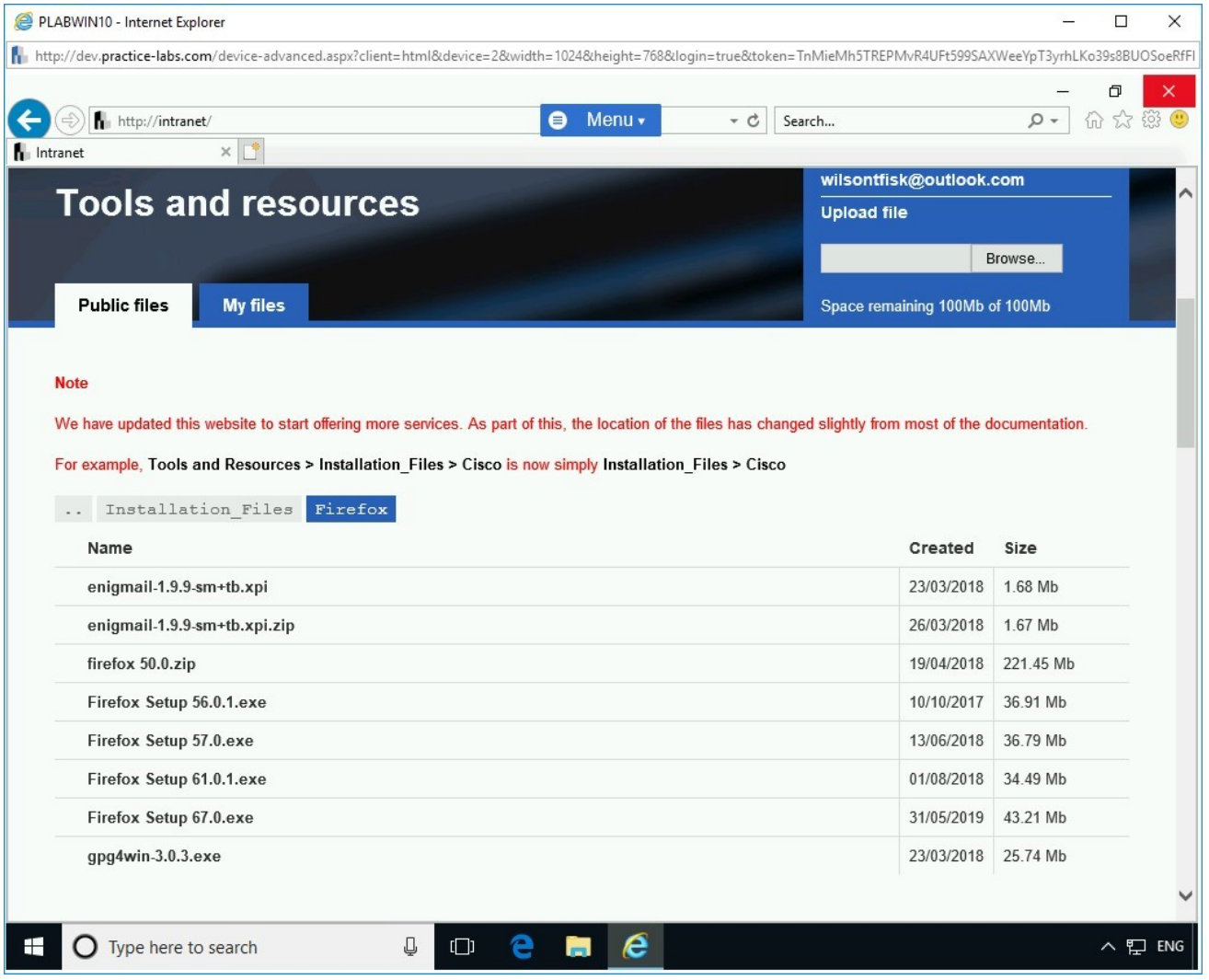


Figure 1.13 Screenshot of PLABWIN10: Closing the Internet Explorer window.

Task 2 - Install Burp Suite on PLABWIN10

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 learn to install Burp Suite. To do this, perform the following steps:

Step 1

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

Double click **Mozilla Firefox** located on the desktop.

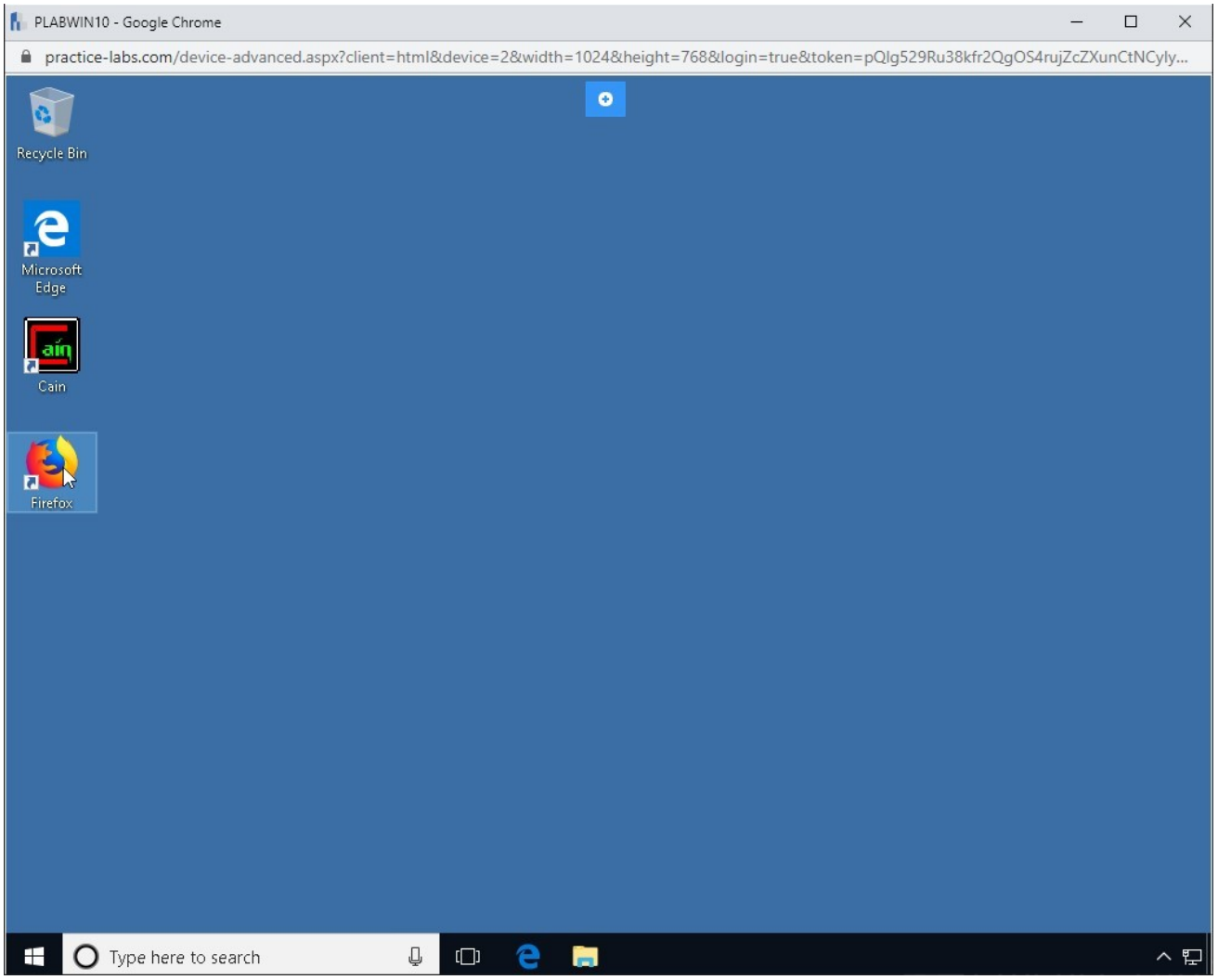


Figure 1.14 Screenshot of PLABWIN10: Selecting Firefox from the Windows Desktop.

Step 2

The **Mozilla Firefox** window opens. Notice that two tabs are opened. You can close the **Firefox Privacy Notice** tab.

On the update notification, click **Not Now**.

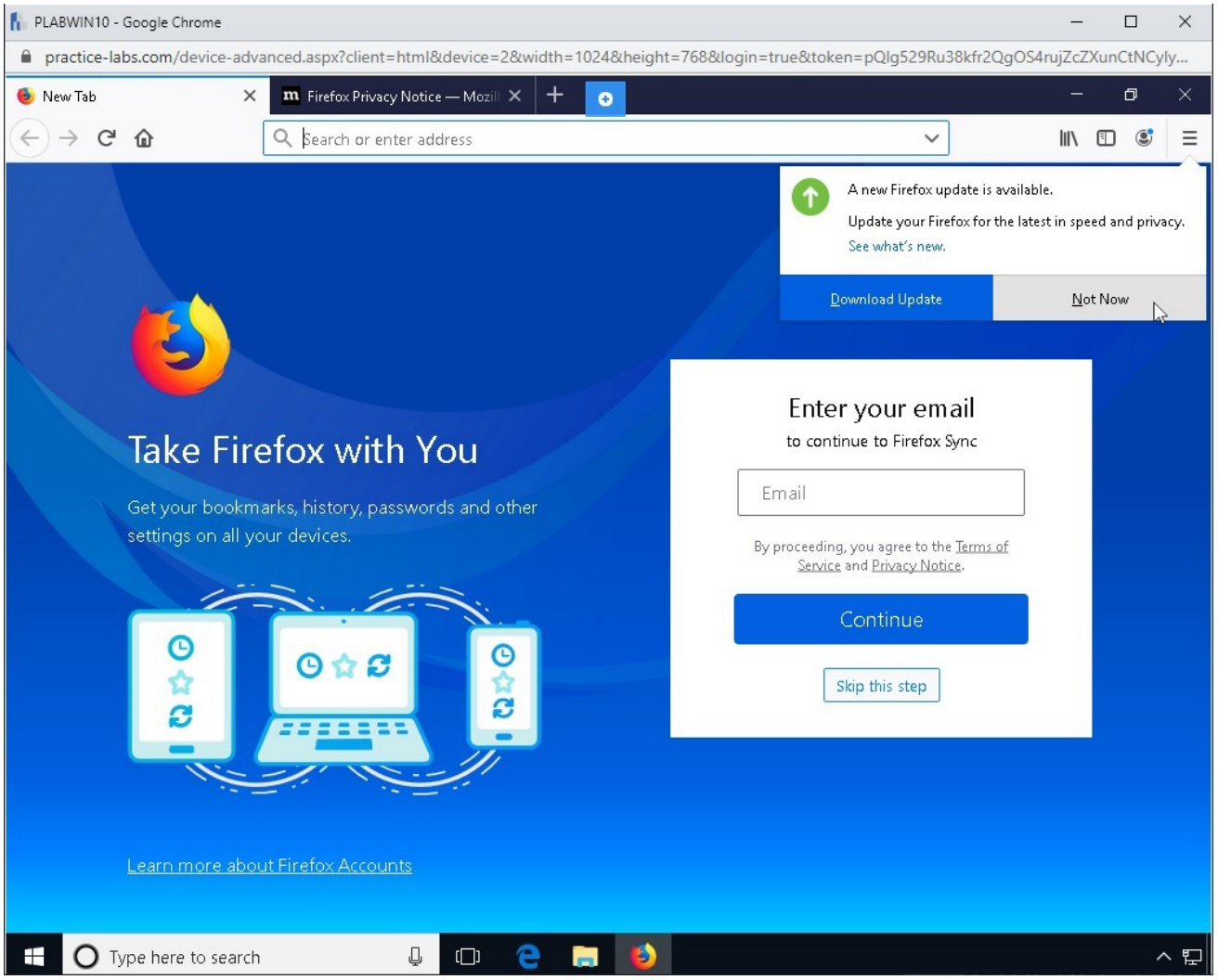


Figure 1.15 Screenshot of PLABWIN10: Firefox opened and displaying the home page.

Step 3

You will need to download **Burp Suite** from its Website. In the address bar of **Mozilla Firefox,** type the following:

```
https://portswigger.net/burp/communitydownload
```

Press **Enter**.

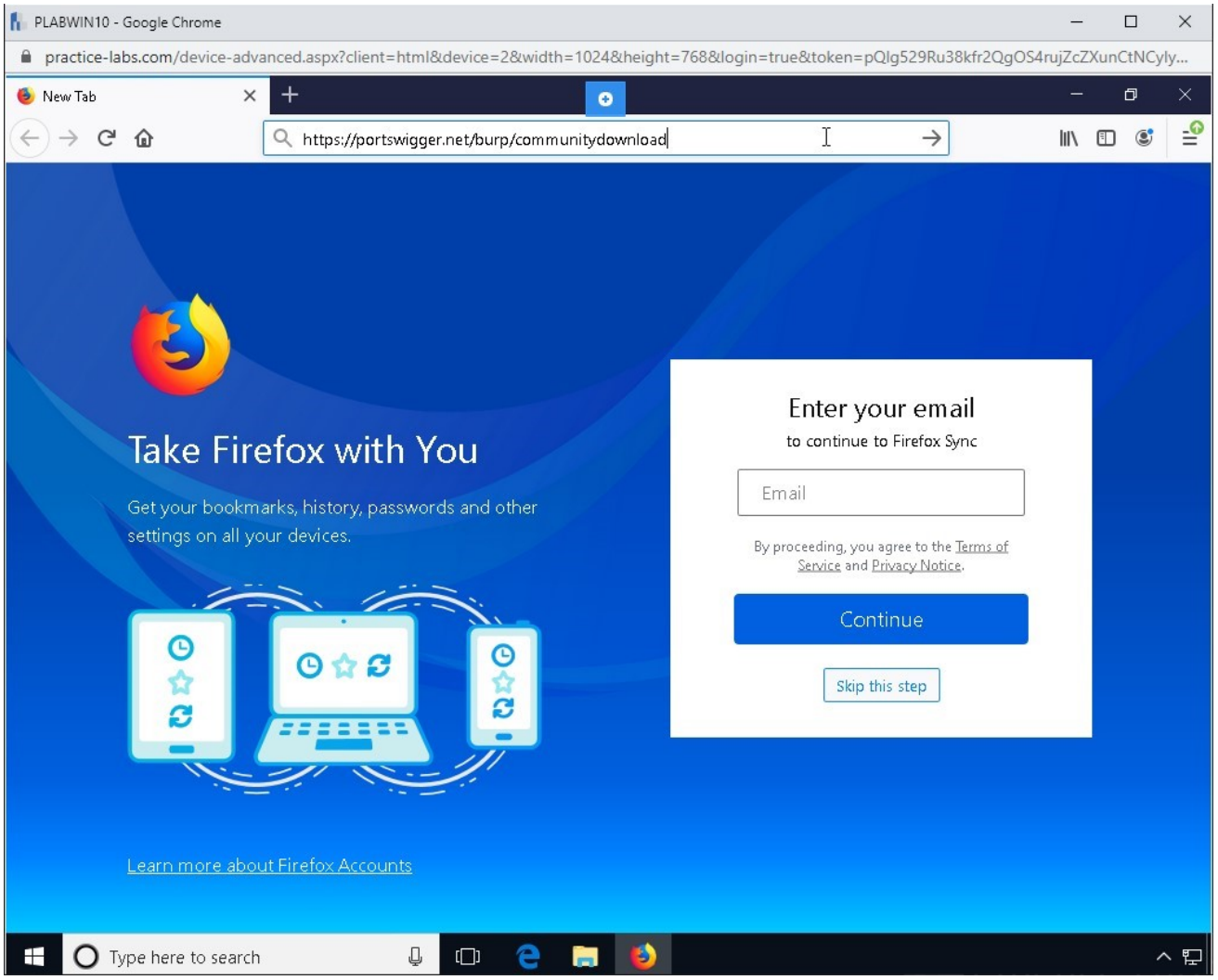


Figure 1.16 Screenshot of PLABWIN10: Firefox home page, showing the URL required for Burp Suite entered.

Step 4

On the **Burp Suite** website, select **Download the latest version.**

> ***Note:*** *The version of Burp Suite may change over time.*

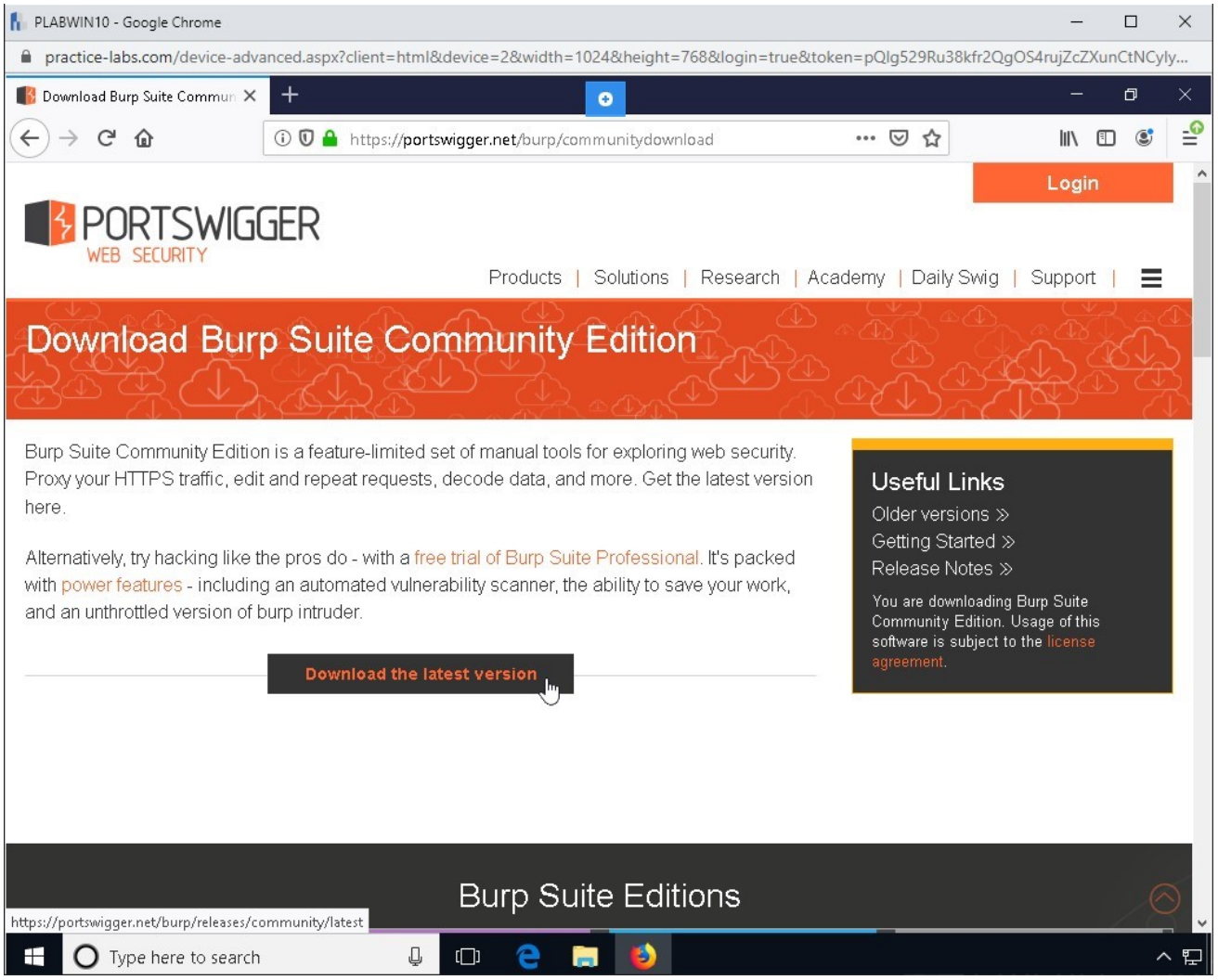


Figure 1.17 Screenshot of PLABWIN10: Clicking the Burp Suite download for the latest version button.

Step 5

You will be shown the download page for the latest version of **Burp Suite.**

Ensure that the drop down menus show **Burp Suite Community Edition** and **Windows (64-bit).**

Click the **Download** button.

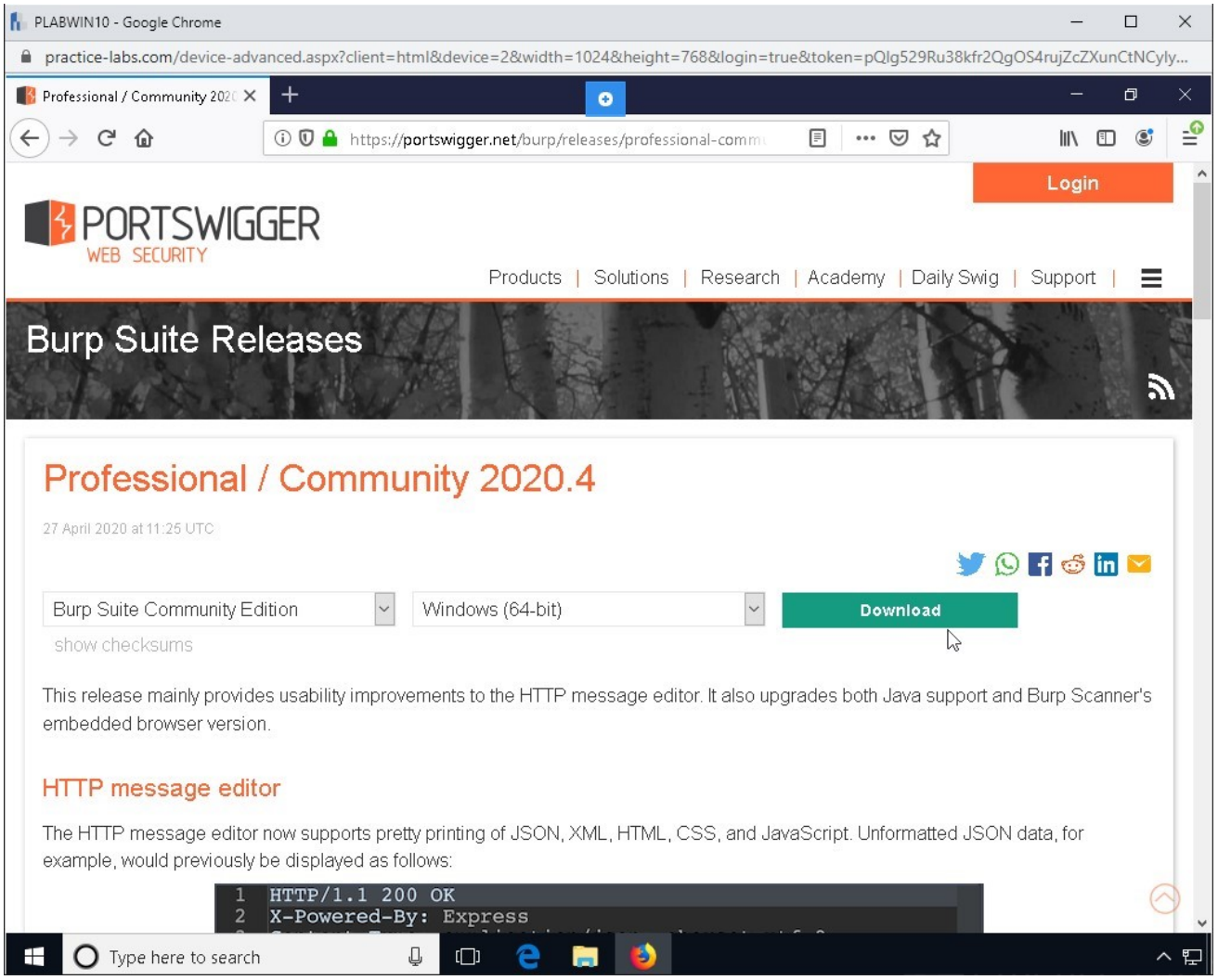


Figure 1.18 Screenshot of PLABWIN10: Showing the Burp Suite download button.

Step 6

A dialogue box will then be shown.

Select **Save File.**

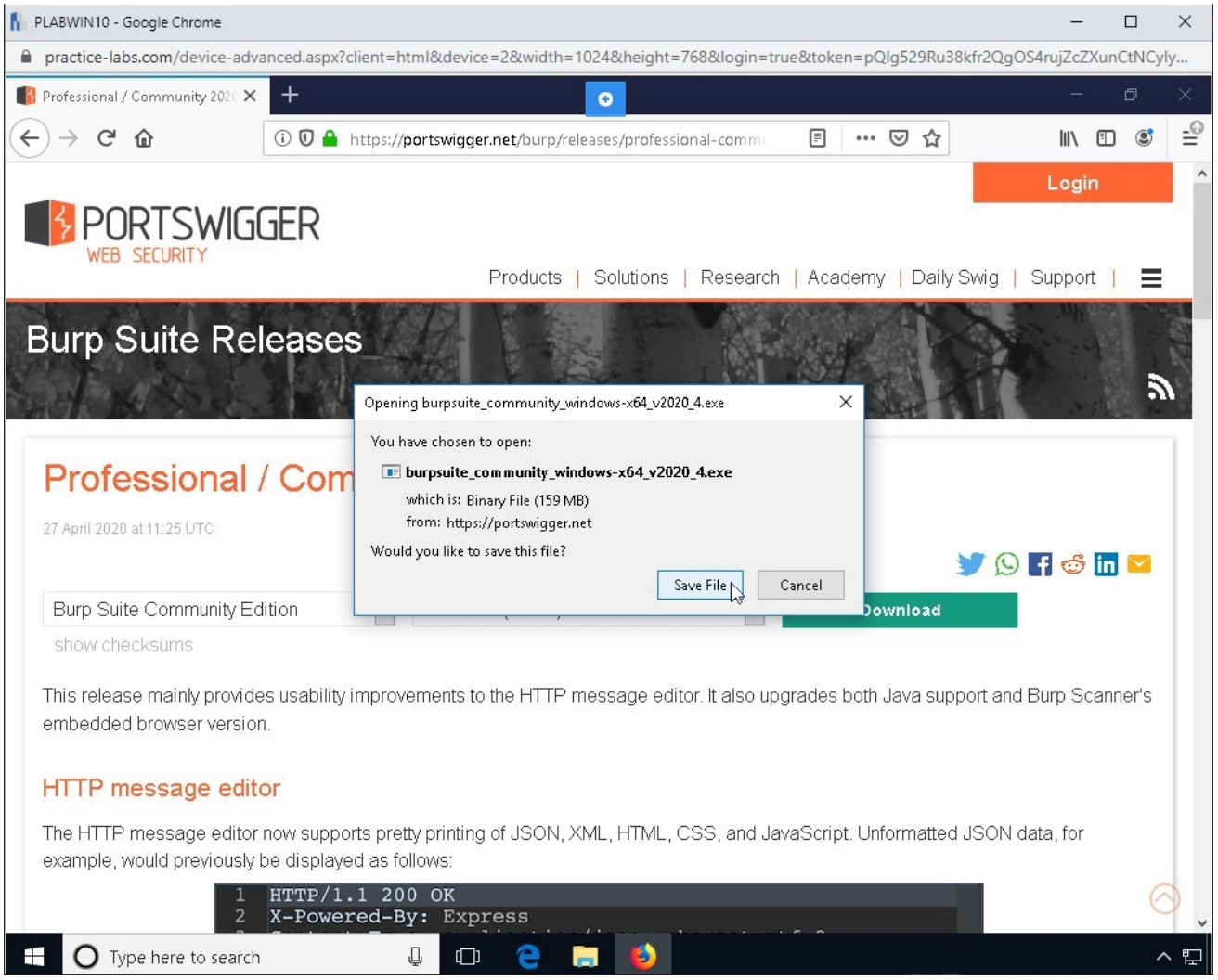


Figure 1.19 Screenshot of PLABWIN10: Clicking Save File on the opened dialogue box.

Step 7

Press the button towards the top of the browser to display the progress of ongoing downloads.

Select **Show All Downloads.**

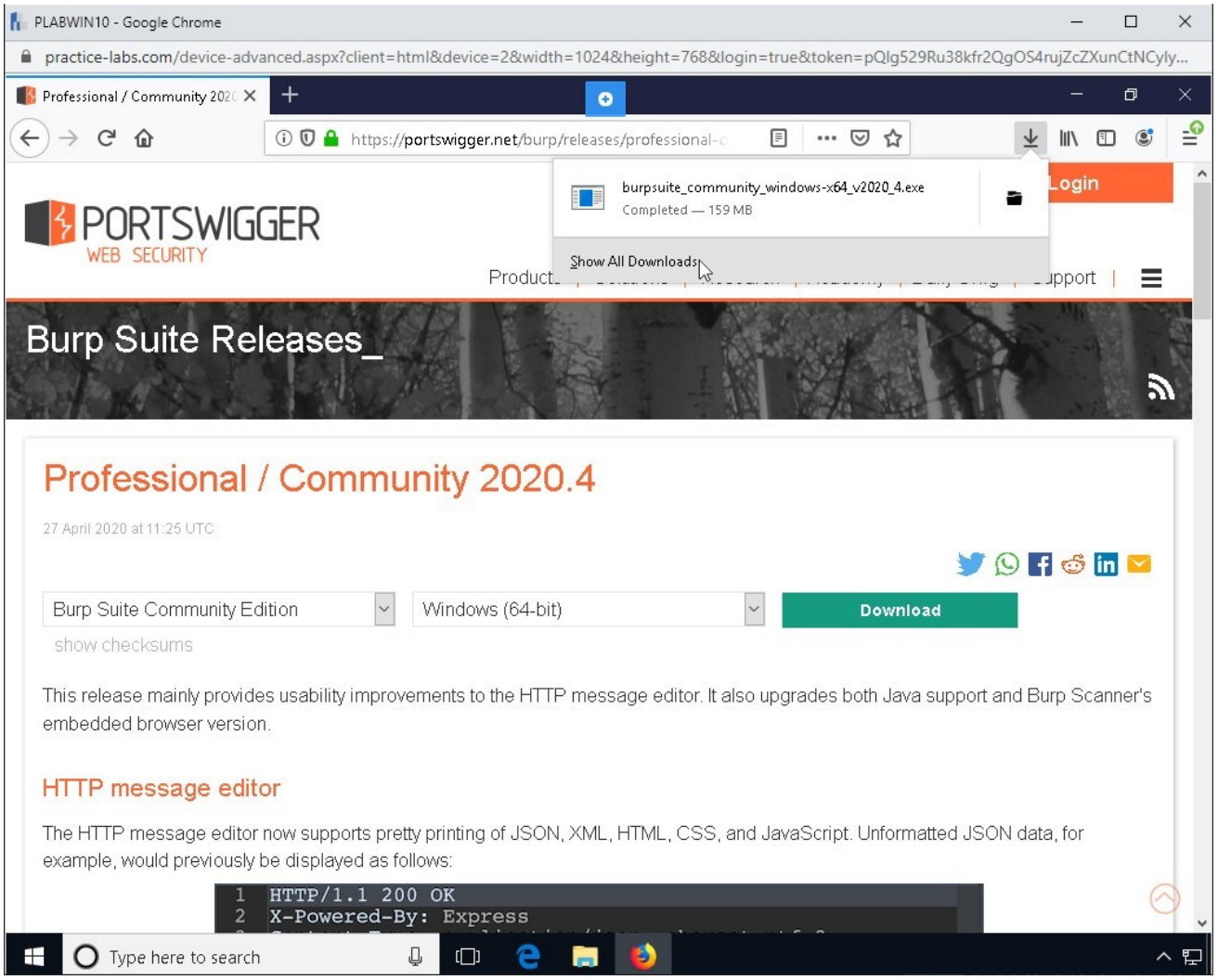


Figure 1.20 Screenshot of PLABWIN10: Clicking Show All Downloads on Firefox.

Step 8

When the download has completed, Double click the downloaded file for **Burp Suite**.

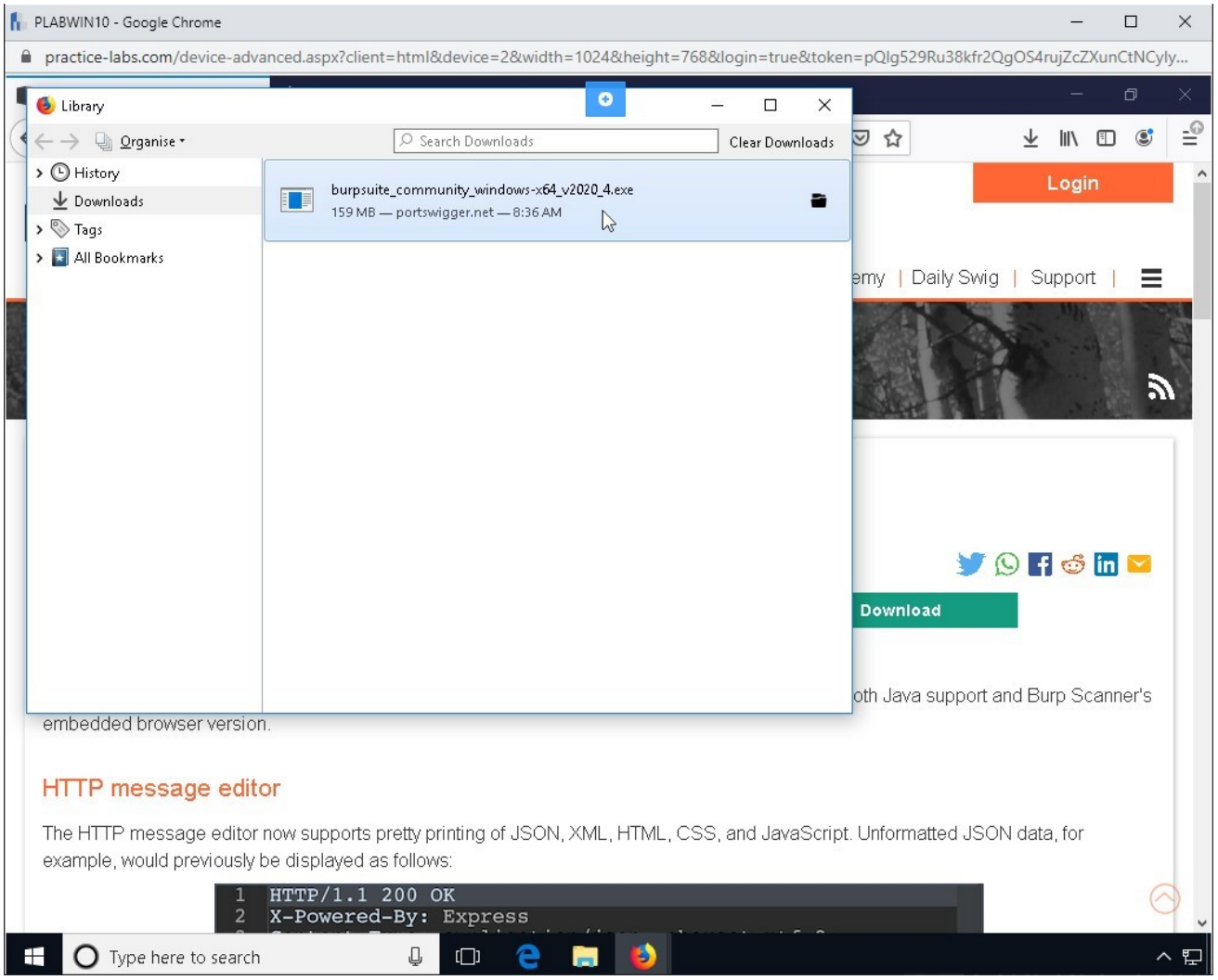


Figure 1.21 Screenshot of PLABWIN10: Double Clicking on the completed Burp Suite download.

Step 9

The **Burp Suite Installation Wizard** is then displayed.

Please wait for this to complete.

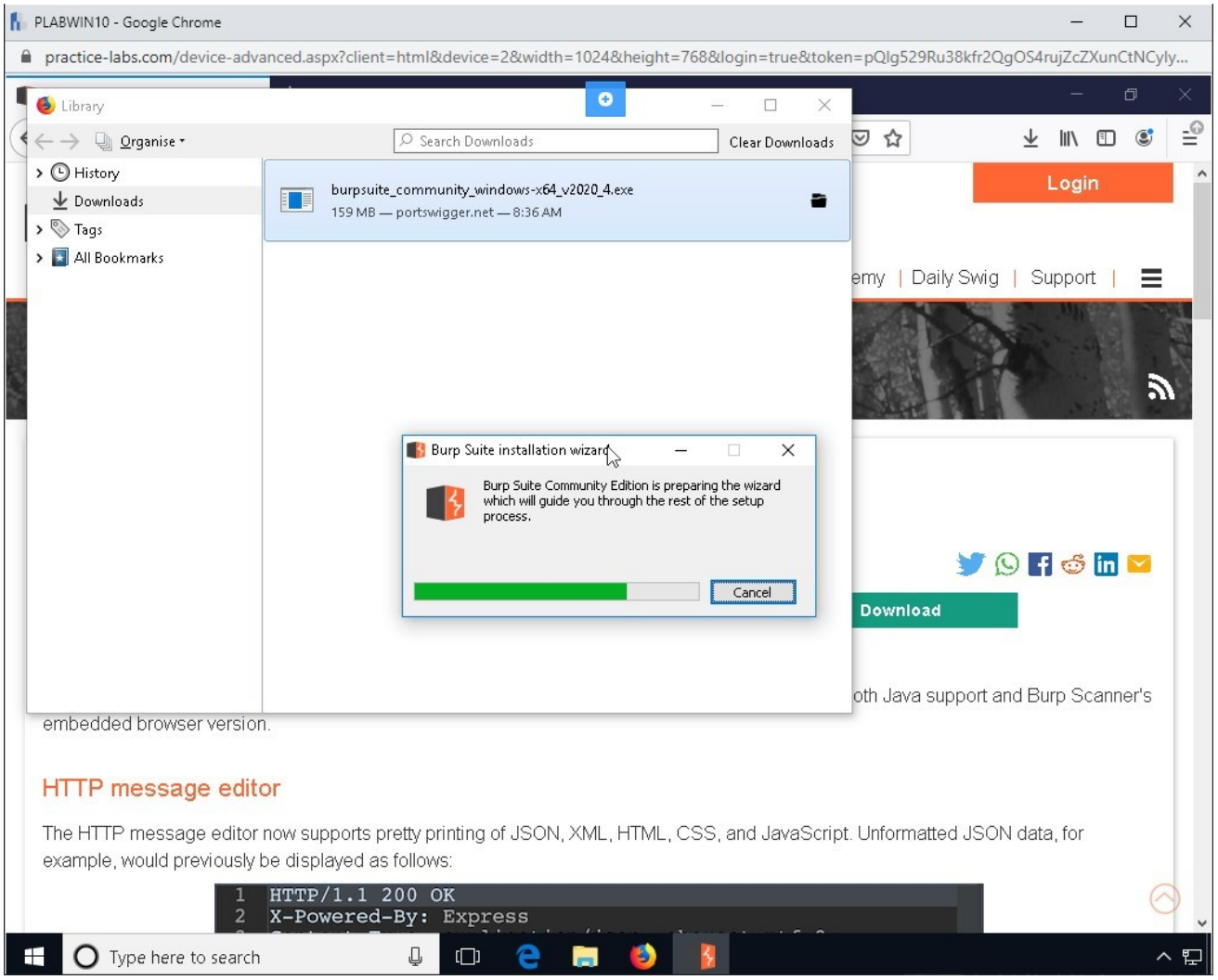


Figure 1.22 Screenshot of PLABWIN10: Showing the Burp Suite Installation wizard dialog box.

Step 10

On the Setup for **Burp Suite Community Edition** Welcome page,

Click **Next.**

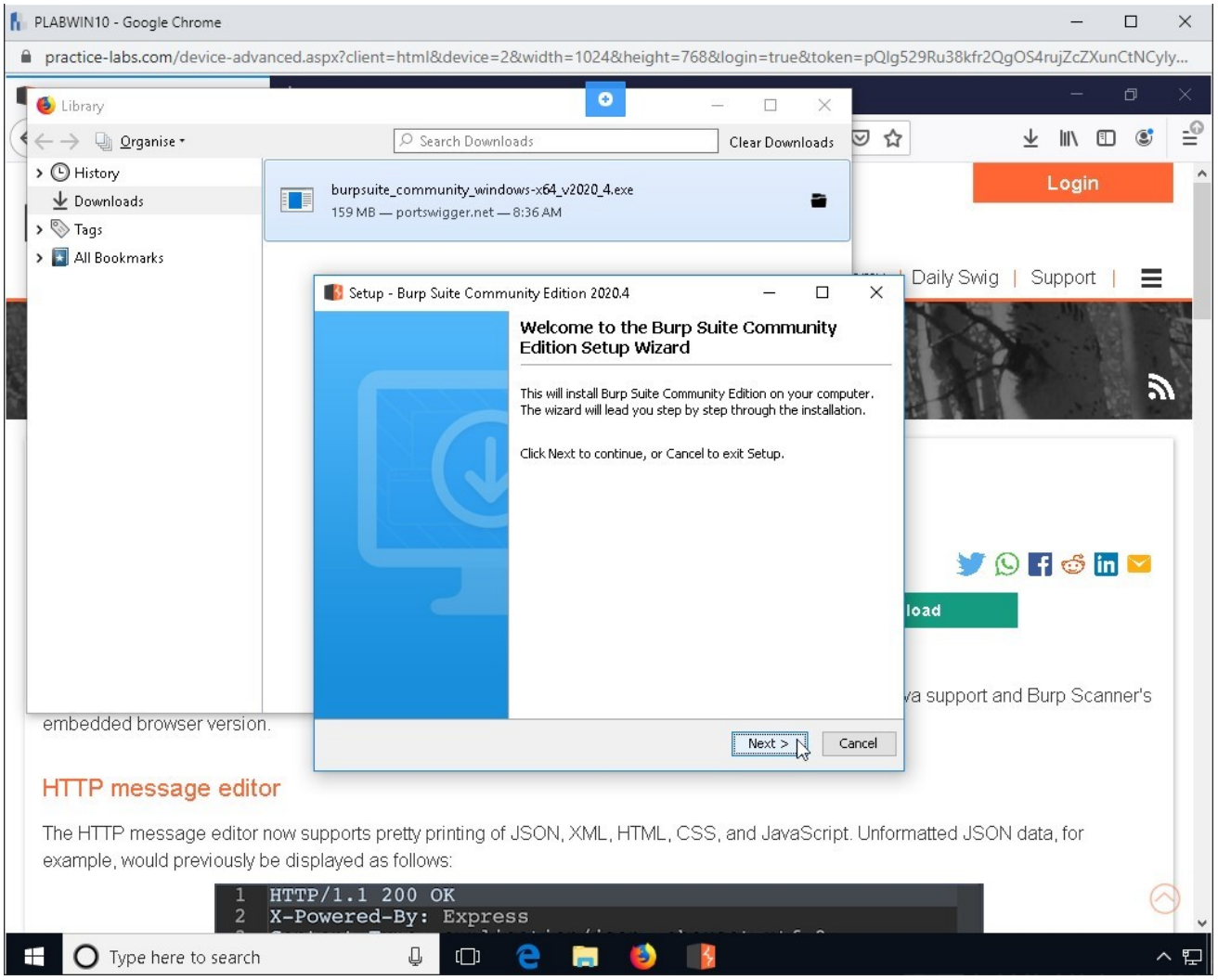


Figure 1.23 Screenshot of PLABWIN10: Clicking Next on the Welcome to the Burp Suite Community Edition Setup Wizard page.

Step 11

On the **Select Destination Directory**

Keep the default selection and press **Next.**

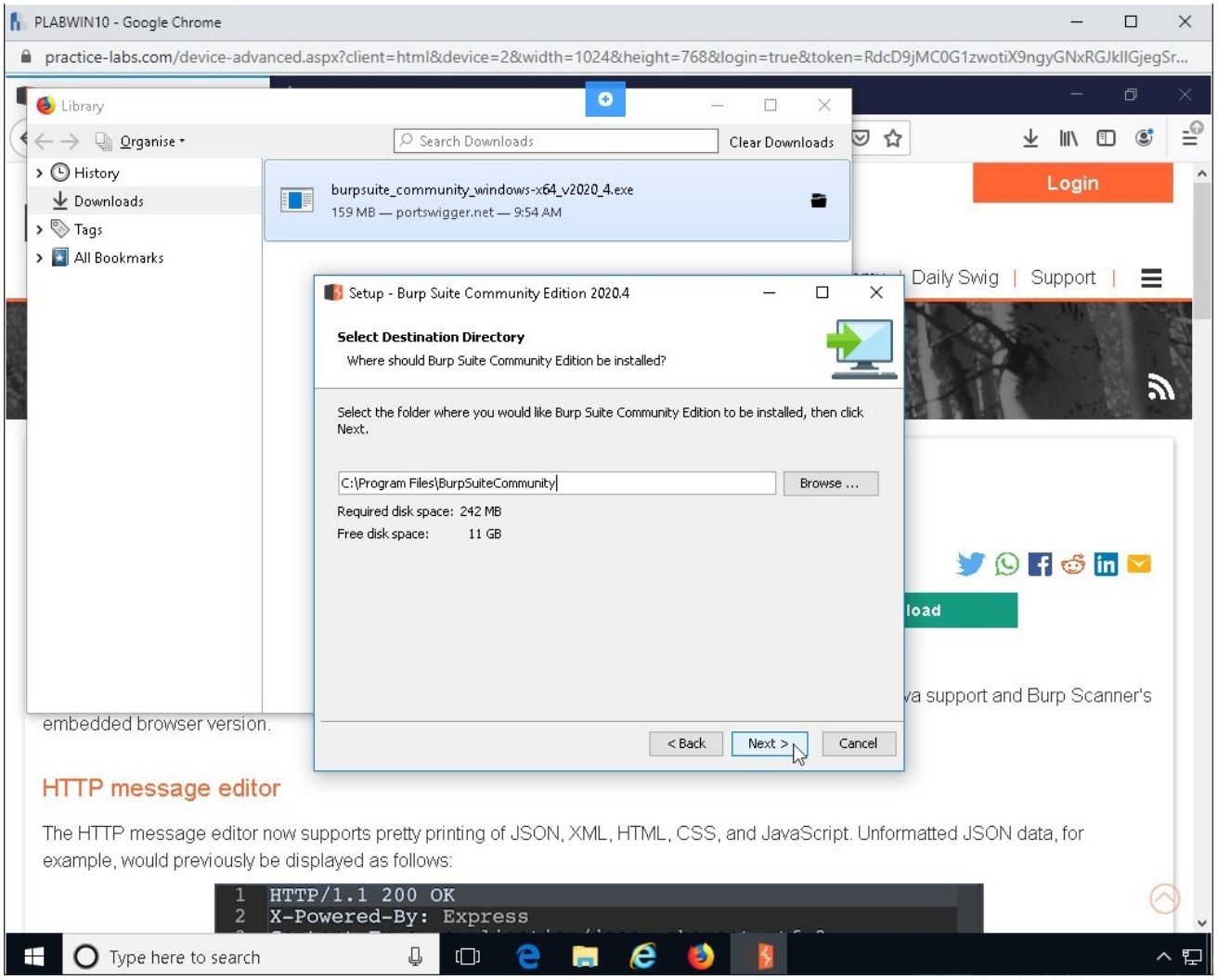


Figure 1.24 Screenshot of PLABWIN10: Clicking Next on the Select Destination Directory page.

Step 12

On the **Select Start Menu Folder** section,

Ensure that **Create shortcuts for all users** is ticked.

Press **Next.**

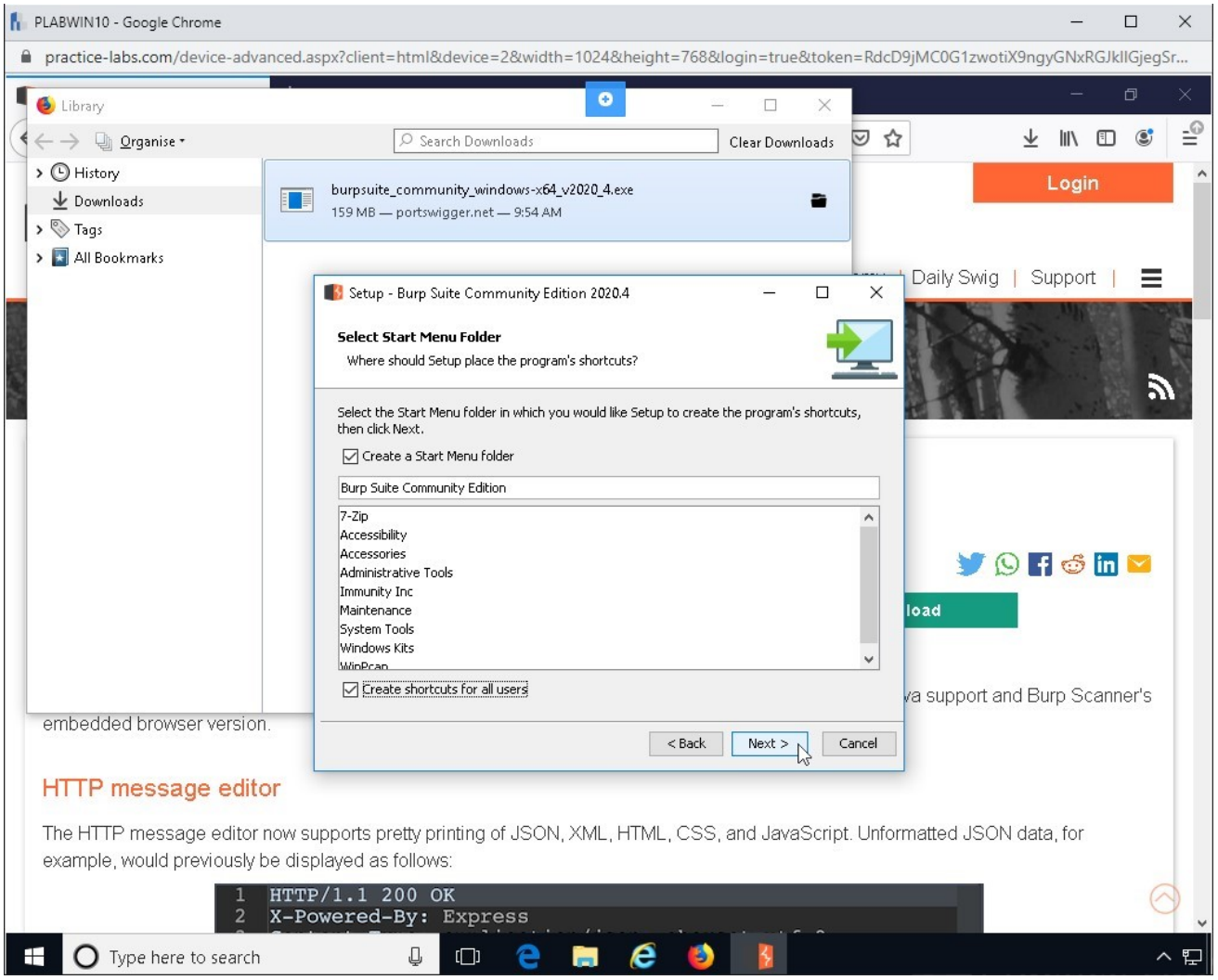


Figure 1.25 Screenshot of PLABWIN10: Clicking Next on the Select Start Menu Folder page.

Step 13

The files for **Burp Suite** are now being extracted.

Please wait for this to complete.

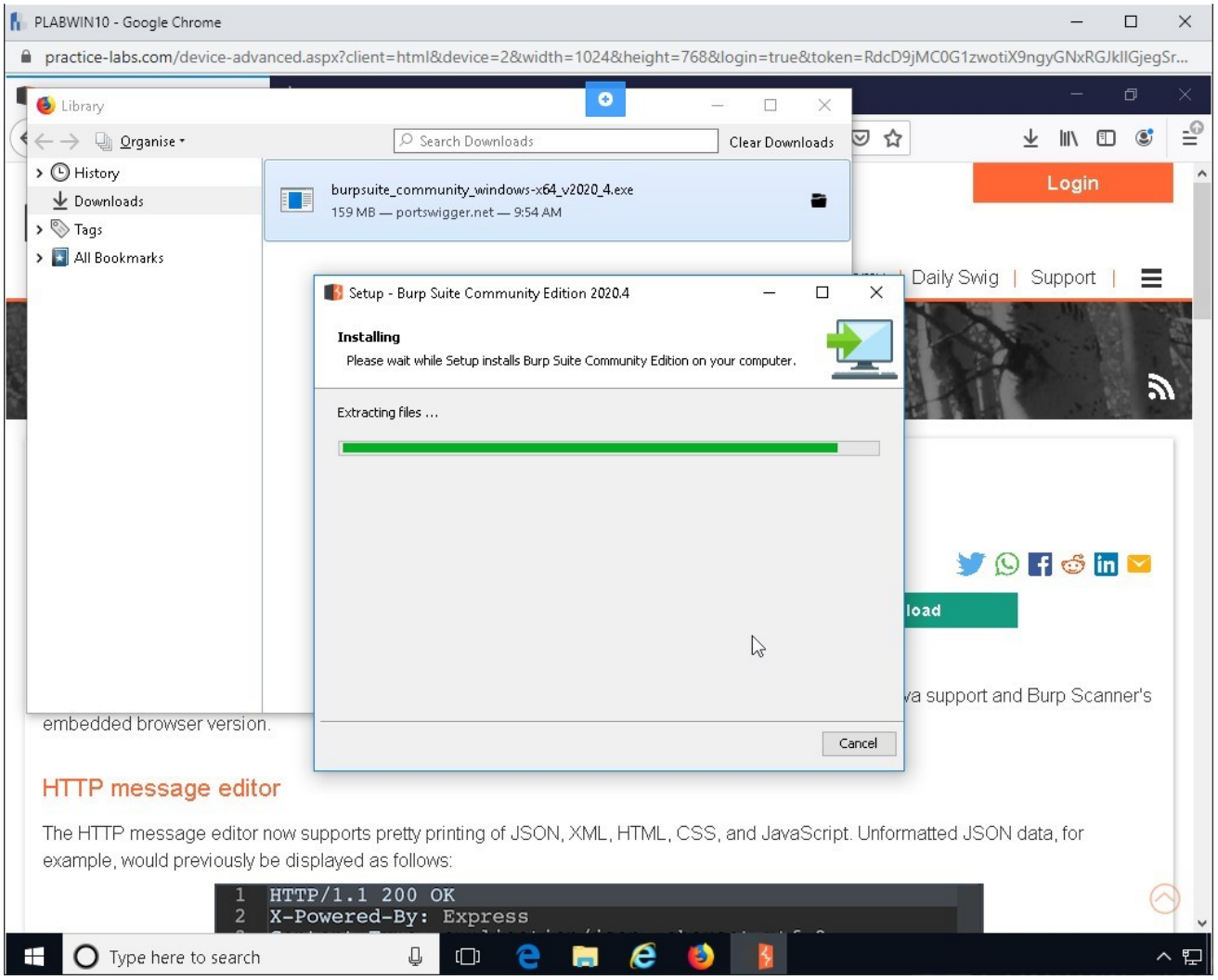


Figure 1.26 Screenshot of PLABWIN10: Showing the installation progress on the Installing page.

Step 14

The Setup for **Burp Suite** is now complete.

Click **Finish.**

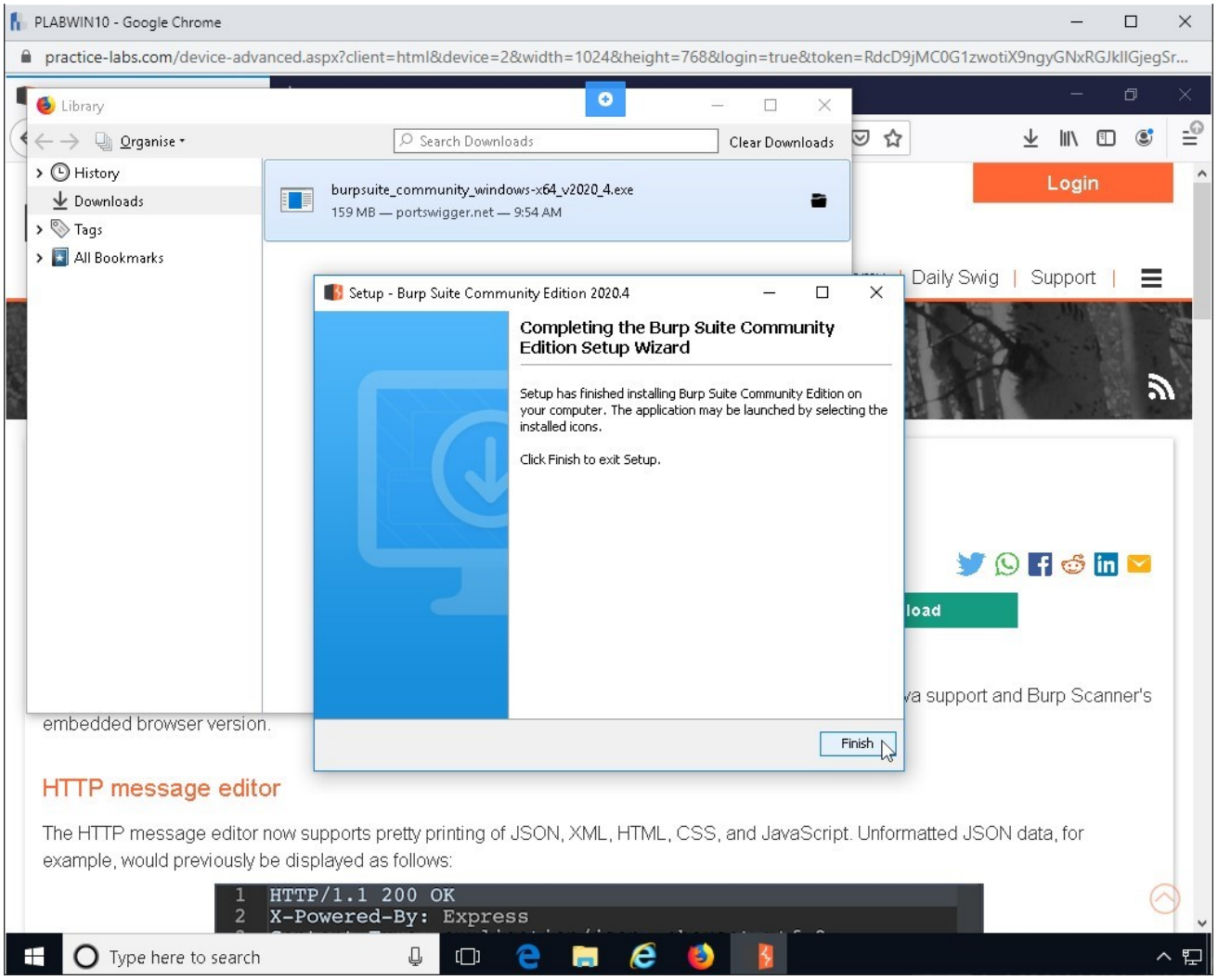


Figure 1.27 Screenshot of PLABWIN10: Clicking Finish on the Completing the Burp Suite Community Edition Setup Wizard page.

Step 15

Close all open Windows to return to the desktop.

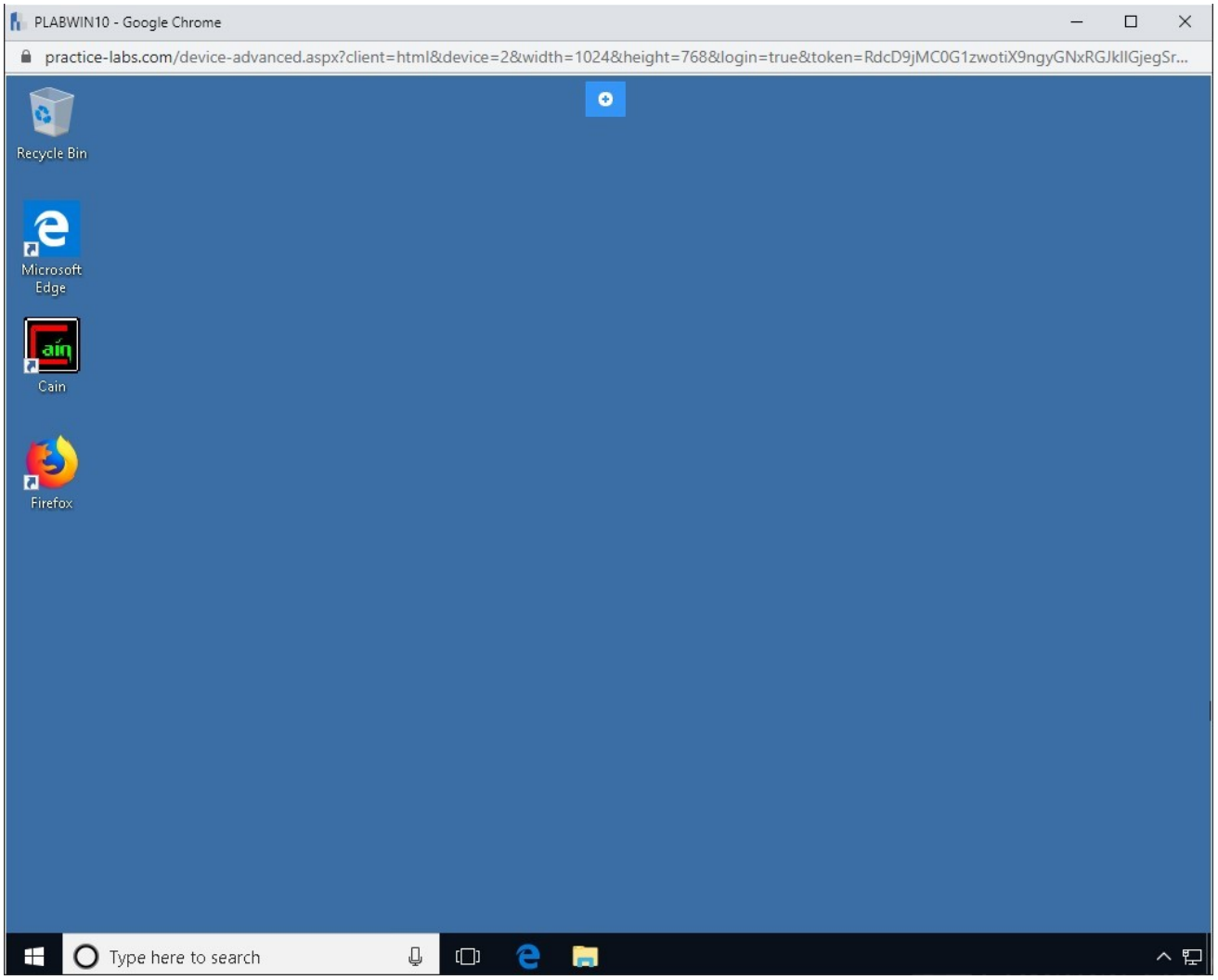


Figure 1.28 Screenshot of PLABWIN10: Desktop showing all open windows have been closed.

Task 3 - Configure Burp Suite on PLABWIN10

After you have installed Burp Suite, you need to configure it to intercept traffic from Mozilla Firefox. In this task, you will configure Burp Suite on **PLABWIN10**. 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**.

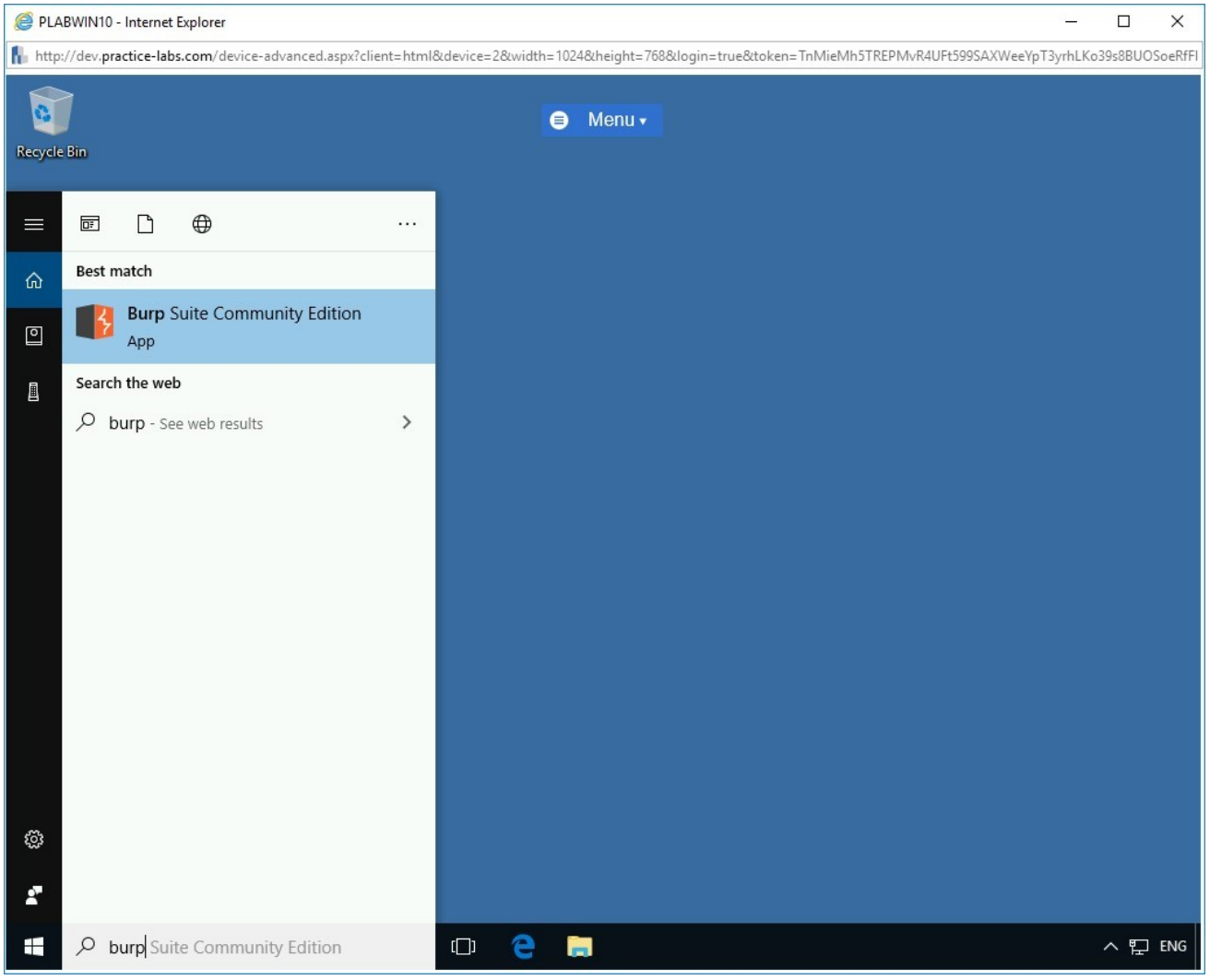


Figure 1.28 Screenshot of PLABWIN10: Selecting Burp Suite Community Edition from the search results.

Step 2

The **BURPSUITE COMMUNITY EDITION** splash screen is displayed.

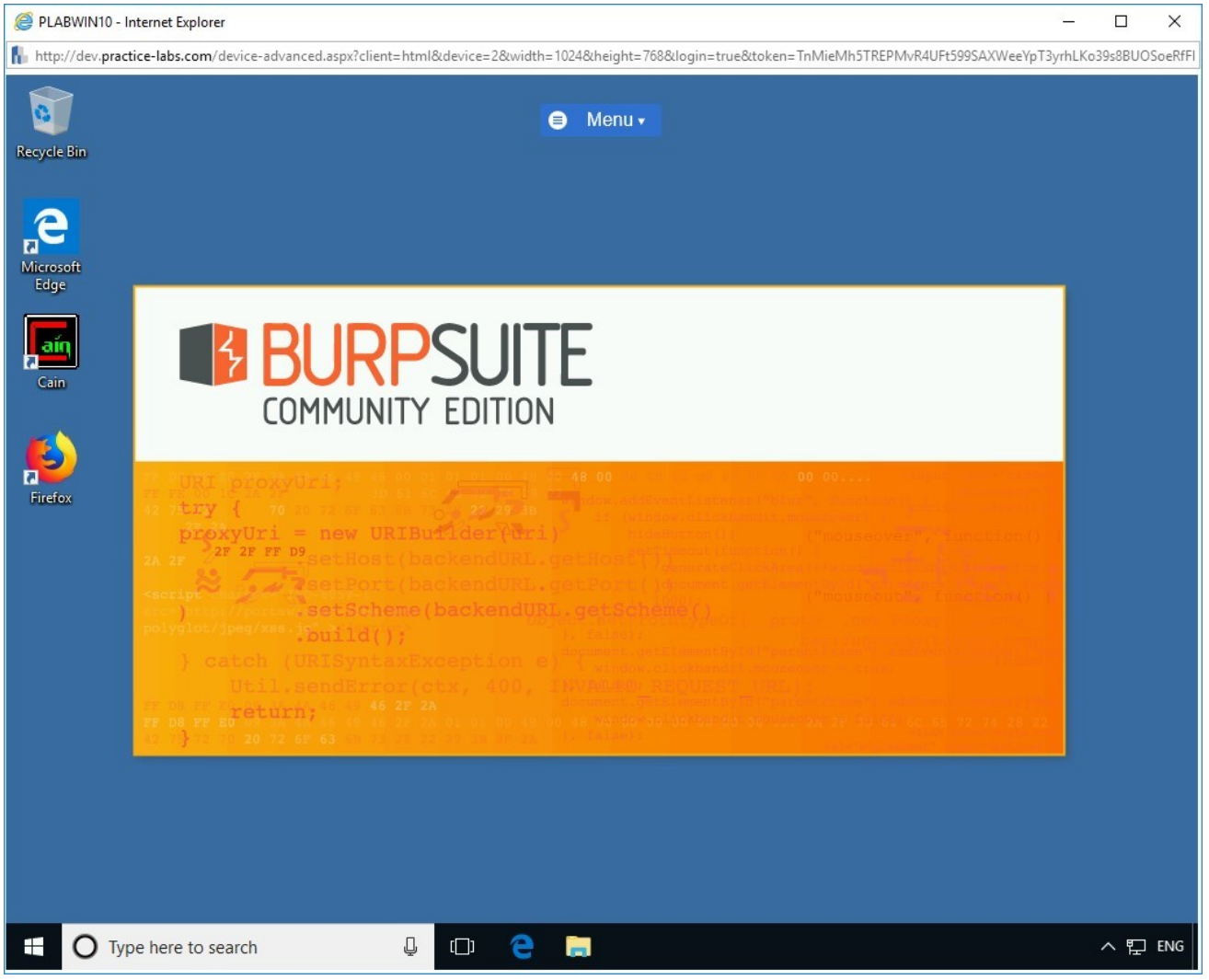


Figure 1.29 Screenshot of PLABWIN10: Showing the splash screen of Burp Suite Community Edition.

Step 3

On the **Terms and Conditions** page, click **I Accept**.

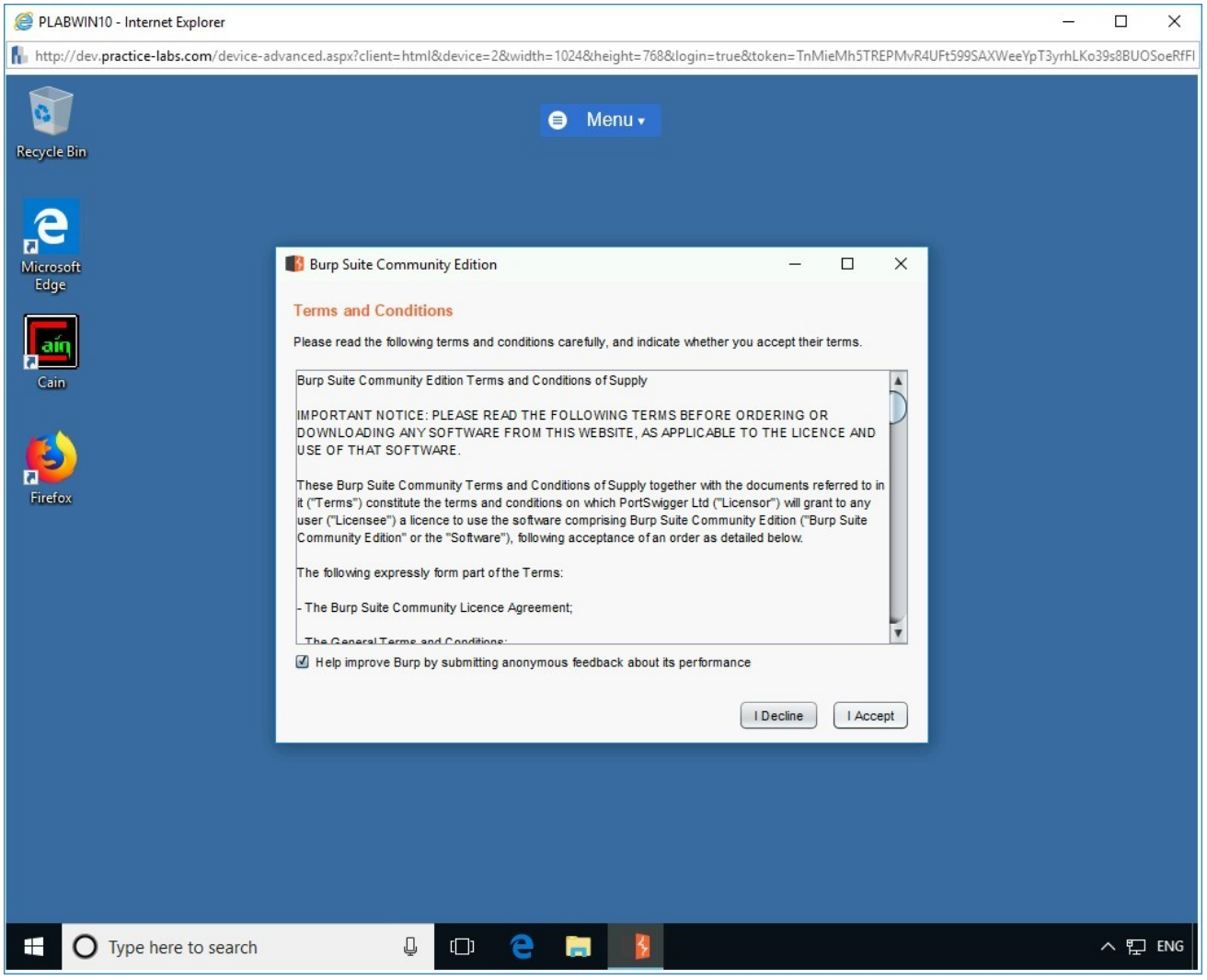


Figure 1.30 Screenshot of PLABWIN10: Clicking the I Accept button on the Terms and Conditions page.

Step 4

The **Burp Suite Community Edition v2.04** wizard is displayed. On the **Welcome to Burp Suite Community Edition** page, select the required options to create or open a project.

For this demonstration, keep the default selection of Temporary project and click Next.

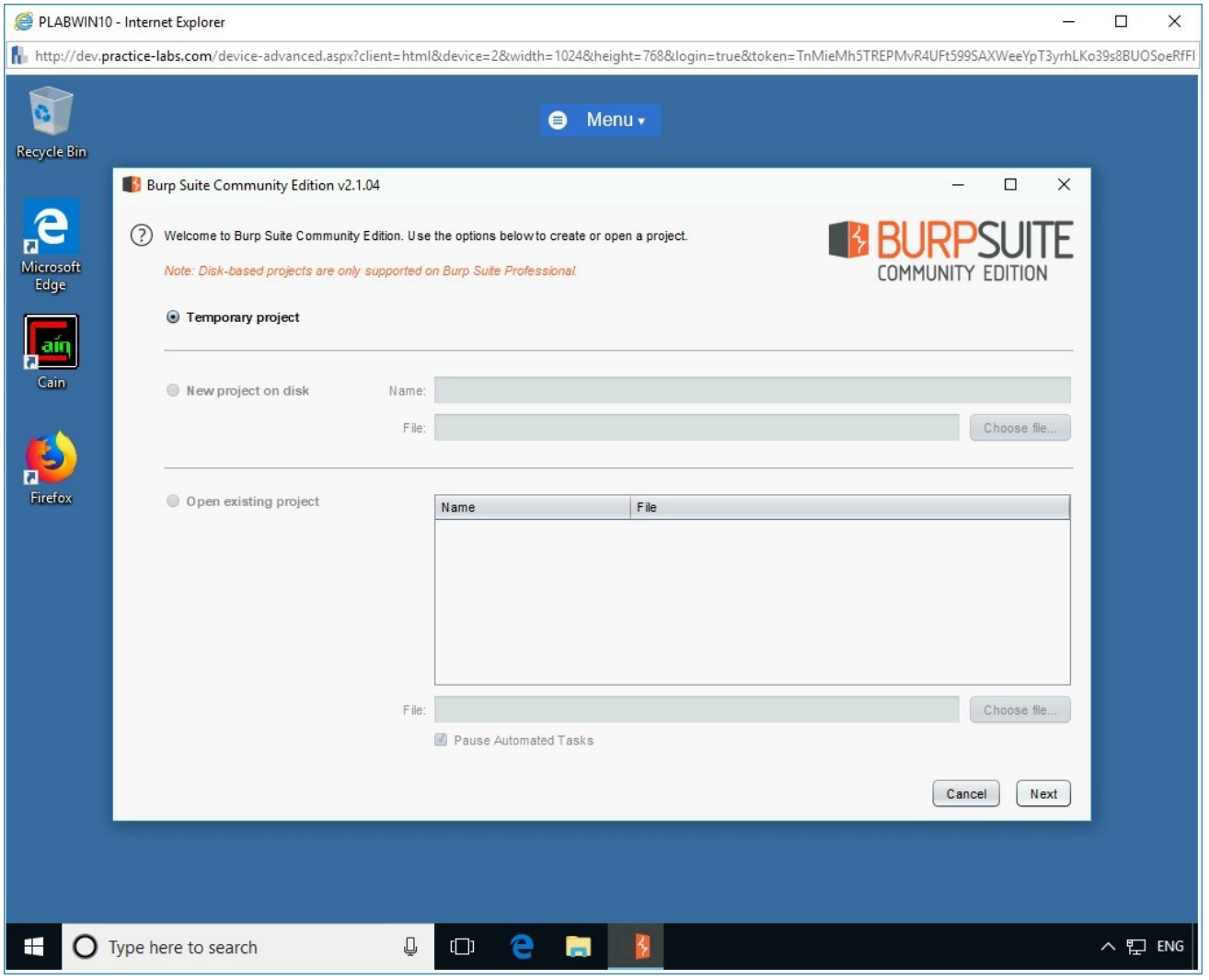


Figure 1.31 Screenshot of PLABWIN10: Selecting the default Temporary project and clicking Next.

Step 5

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

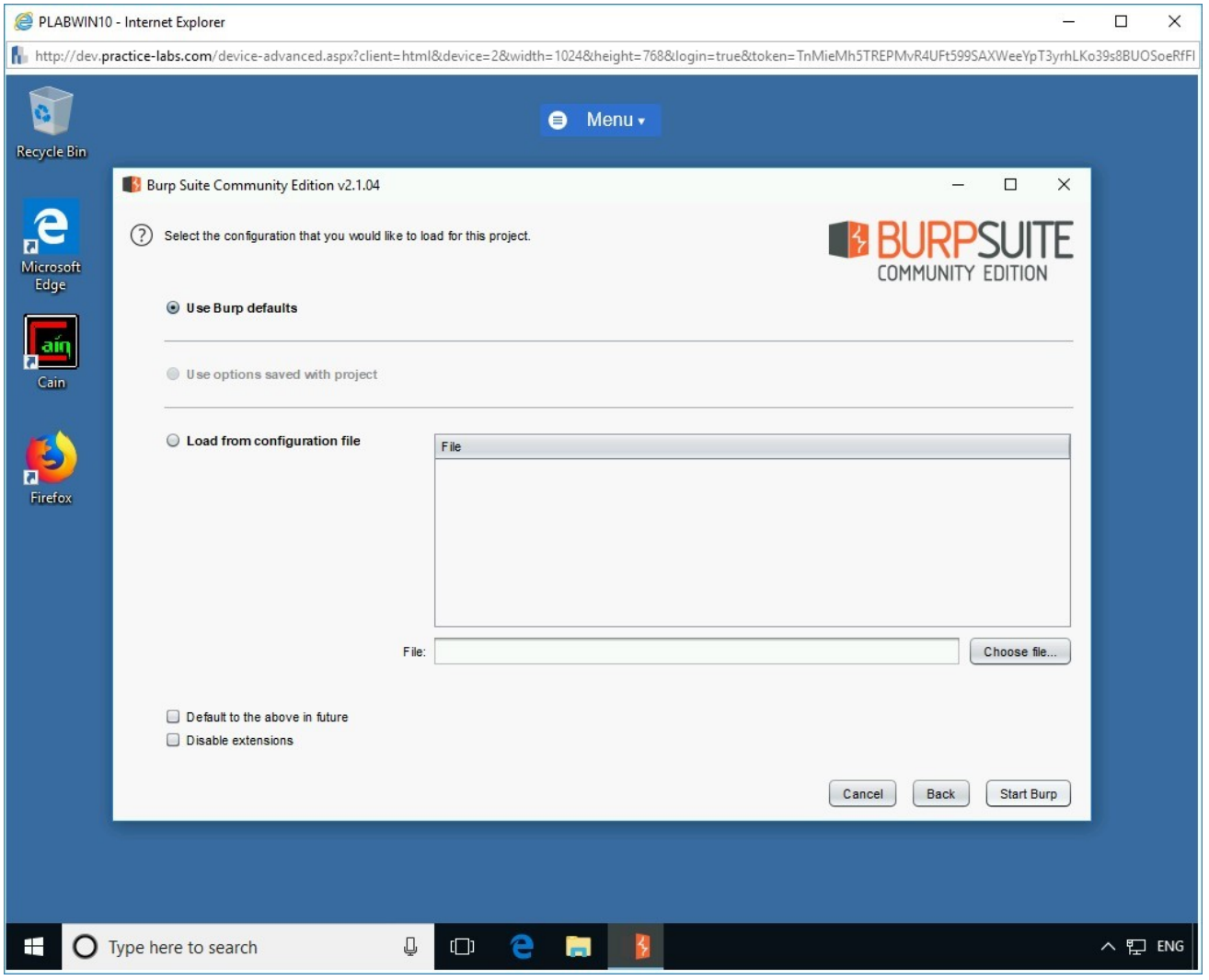


Figure 1.32 Screenshot of PLABWIN10: Keeping the default selection of Use Burp defaults and clicking Start Burp.

Step 6

Burp Suite is starting the project.

It will take a few seconds to complete.

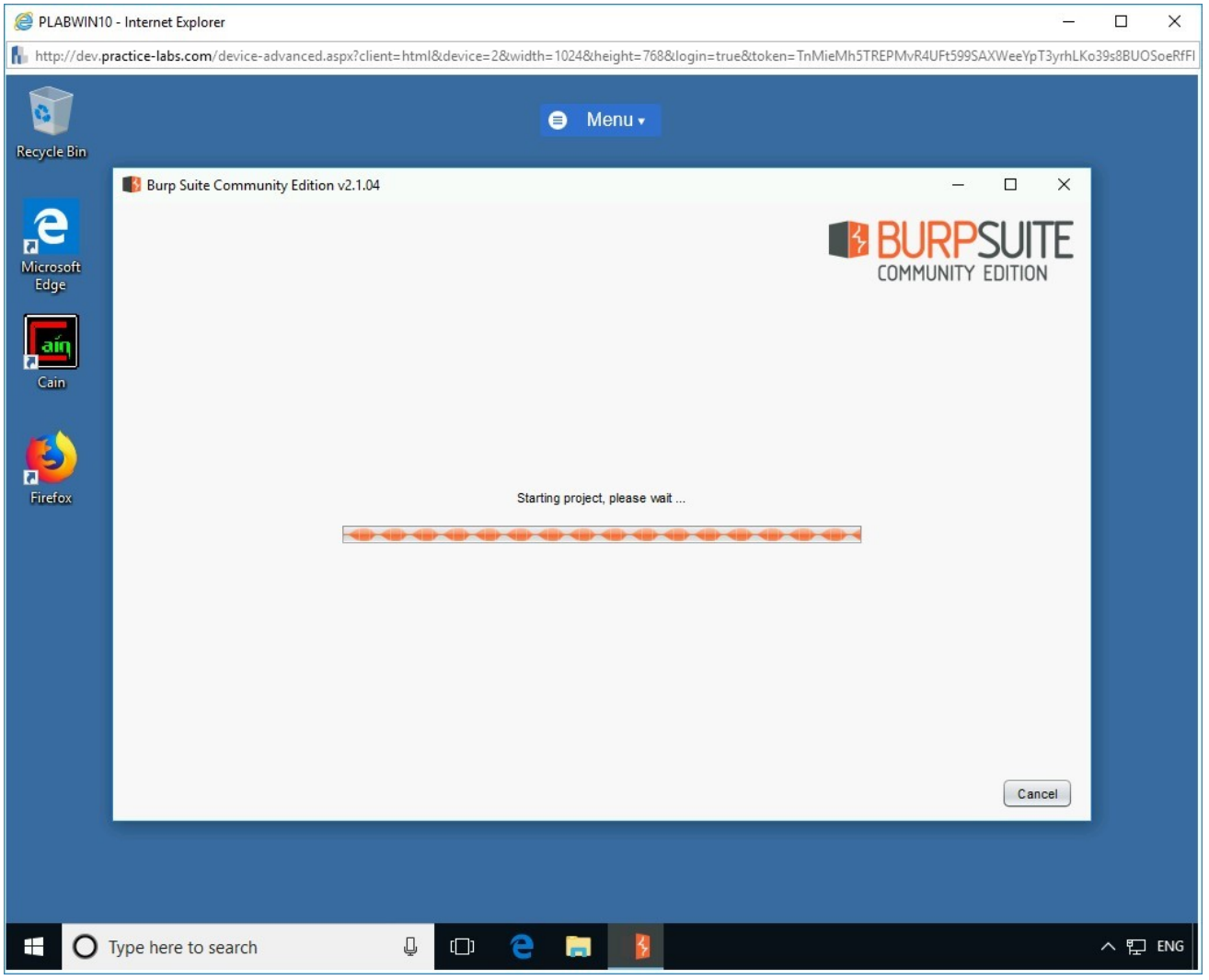


Figure 1.33 Screenshot of PLABWIN10: Showing the starting of Burp Suite project.

Step 7

The **Burp Suite Community Edition 2.1.04 - Temporary Project** window displays.

Click the **Proxy** tab.

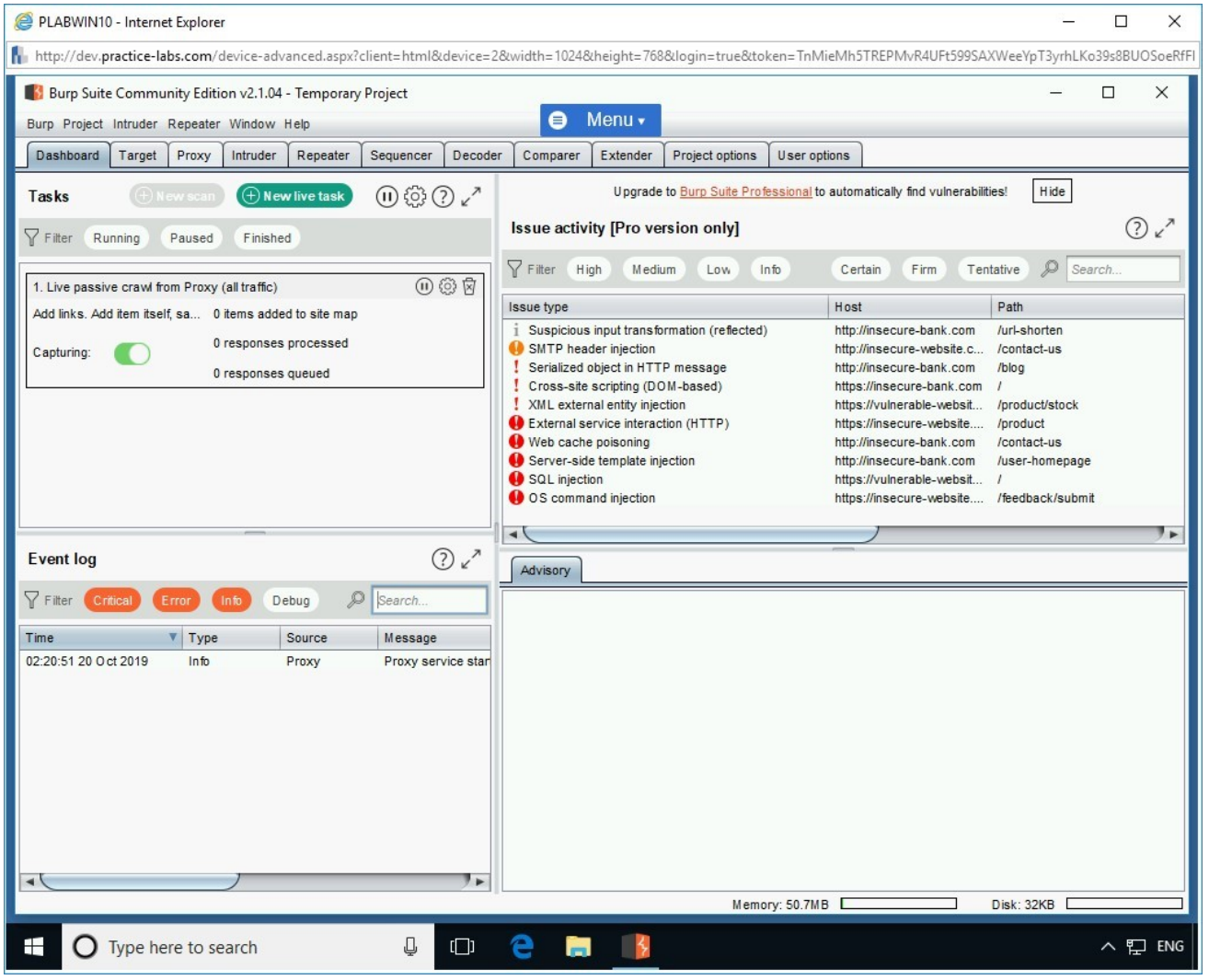


Figure 1.34 Screenshot of PLABWIN10: Clicking the Proxy tab.

Step 8

Under the **Proxy** tab, click the **Options** tab.

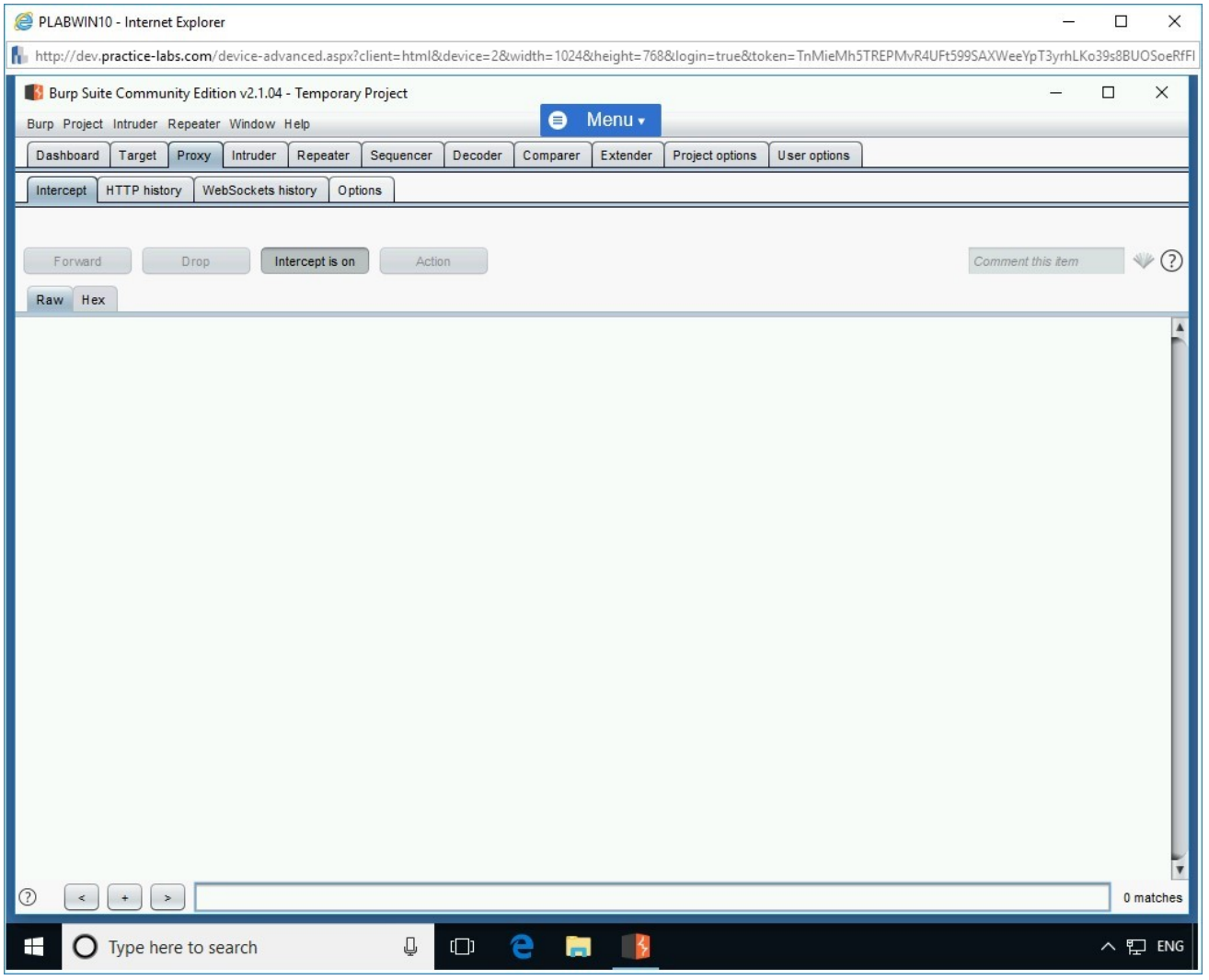


Figure 1.35 Screenshot of PLABWIN10: Clicking the Options tab under the Proxy tab.

Step 9

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

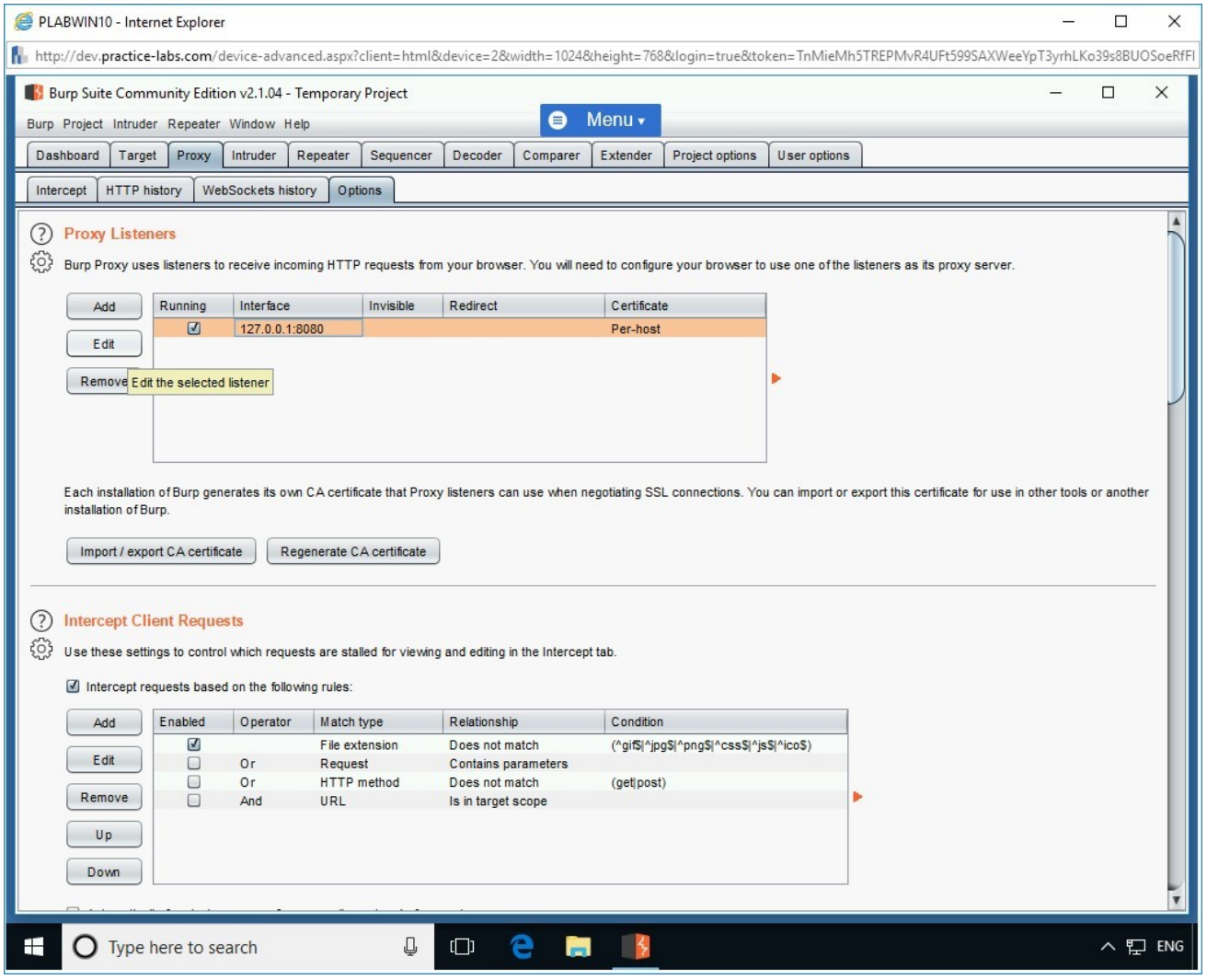


Figure 1.36 Screenshot of PLABWIN10: Selecting the default proxy listener's IP address and clicking Edit.

Step 10

The **Edit proxy listener** dialog box 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.

Click **OK**.

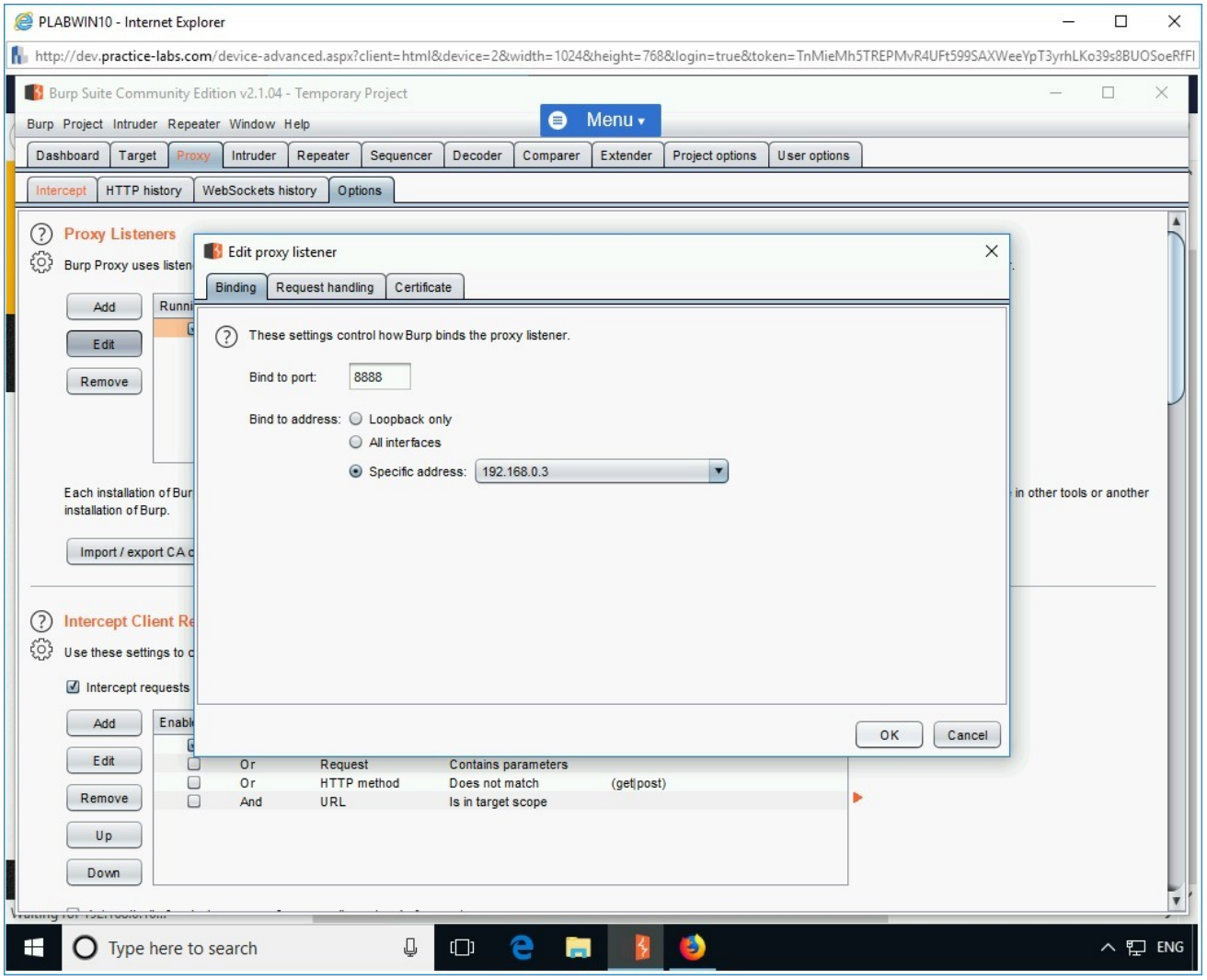


Figure 1.37 Screenshot of PLABWIN10: Entering the port number and then selecting a specific interface as proxy listener.

Step 11

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 will 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 click **Allow access**.

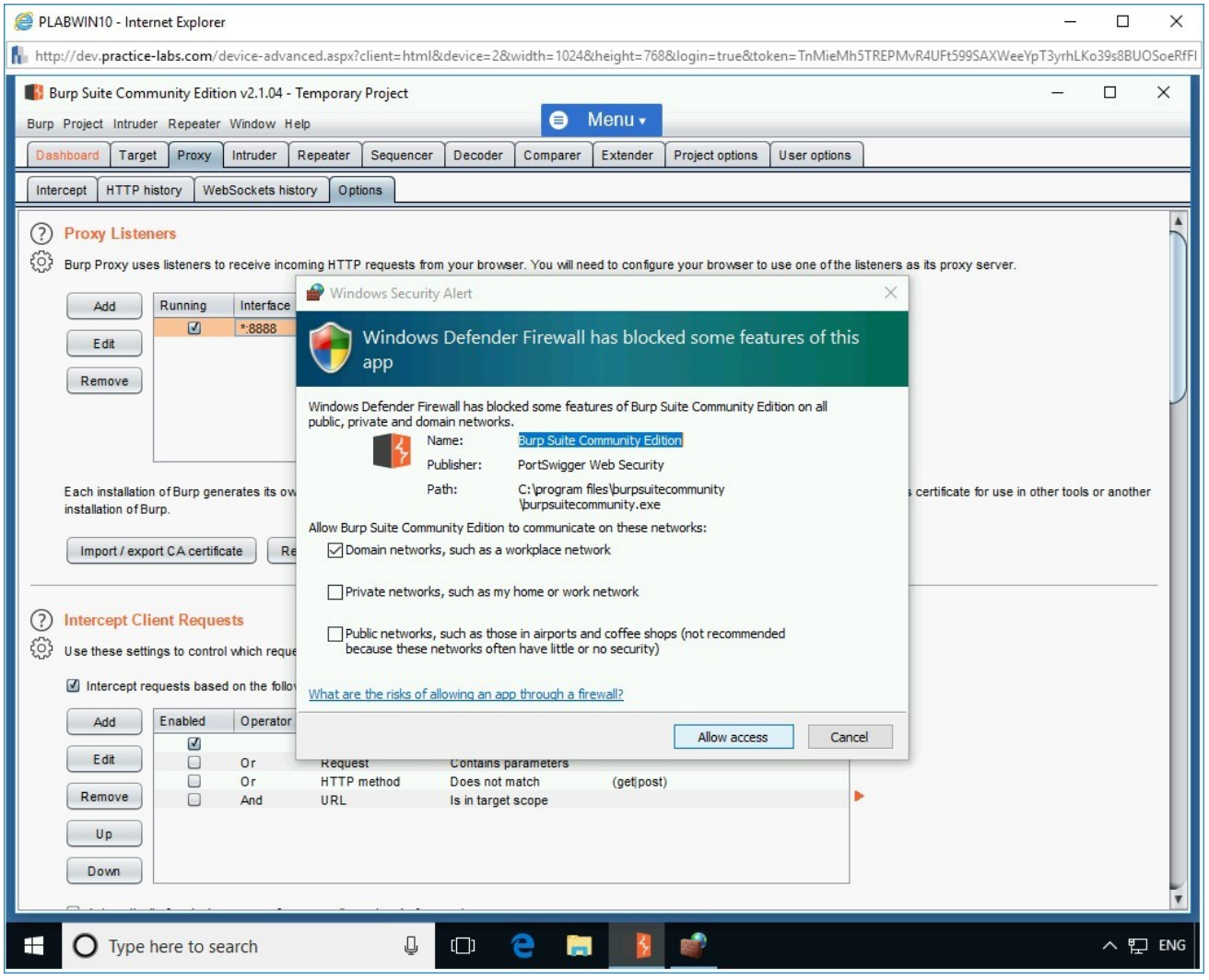


Figure 1.38 Screenshot of PLABWIN10: Clicking Allow access on the Windows Security Alert dialog box.

Step 12

You now need to configure Burp Suite to intercept responses.

In the **Options** tab, scroll down to **Intercept Server Responses** section.

Click to select the checkbox **Intercept responses based on the following rules**.

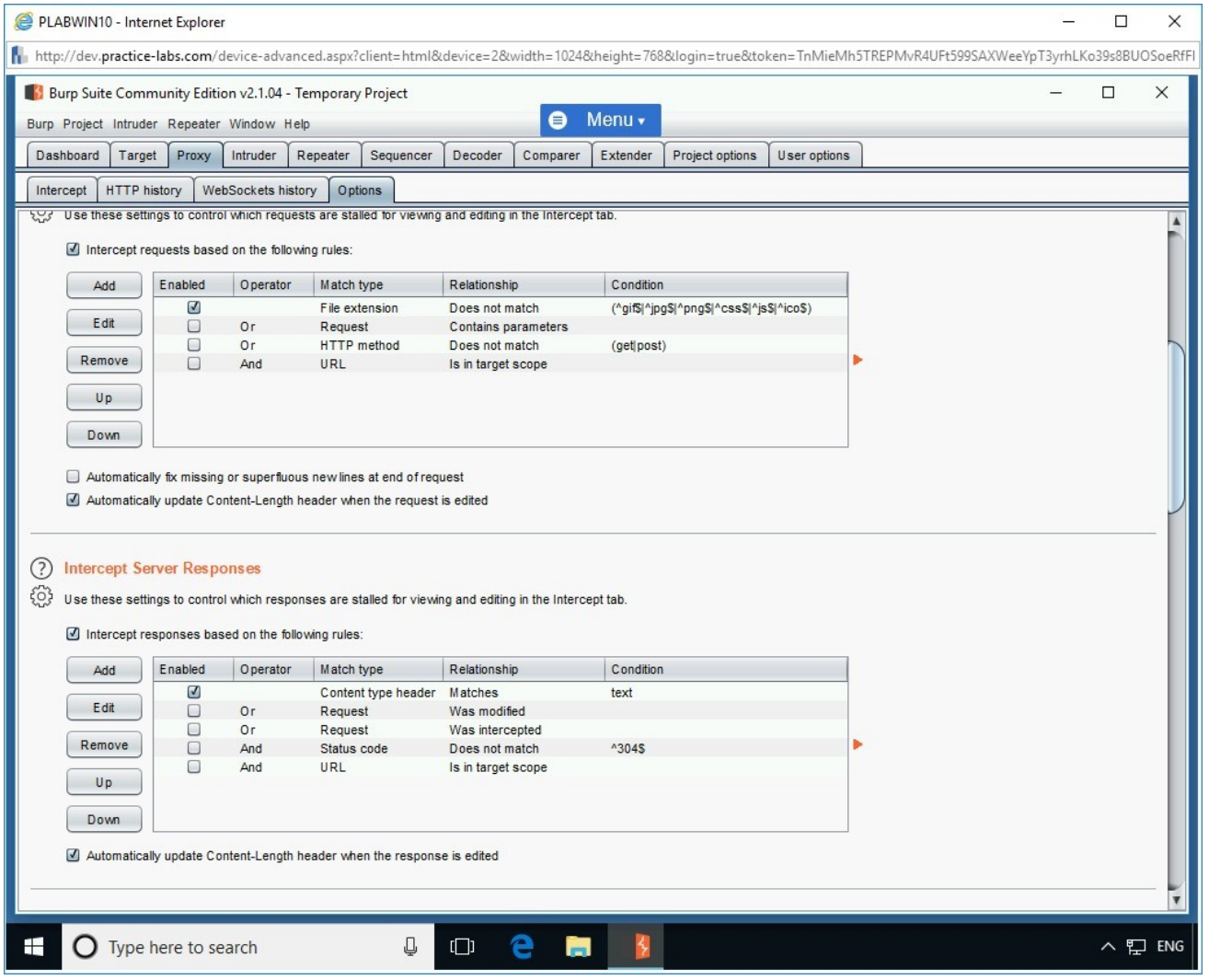


Figure 1.39 Screenshot of PLABWIN10: Selecting the “Intercept responses based on the following rules” checkbox in the Intercept Server Responses section.

Step 13

Click the **Intercept** tab under the **Proxy** tab.

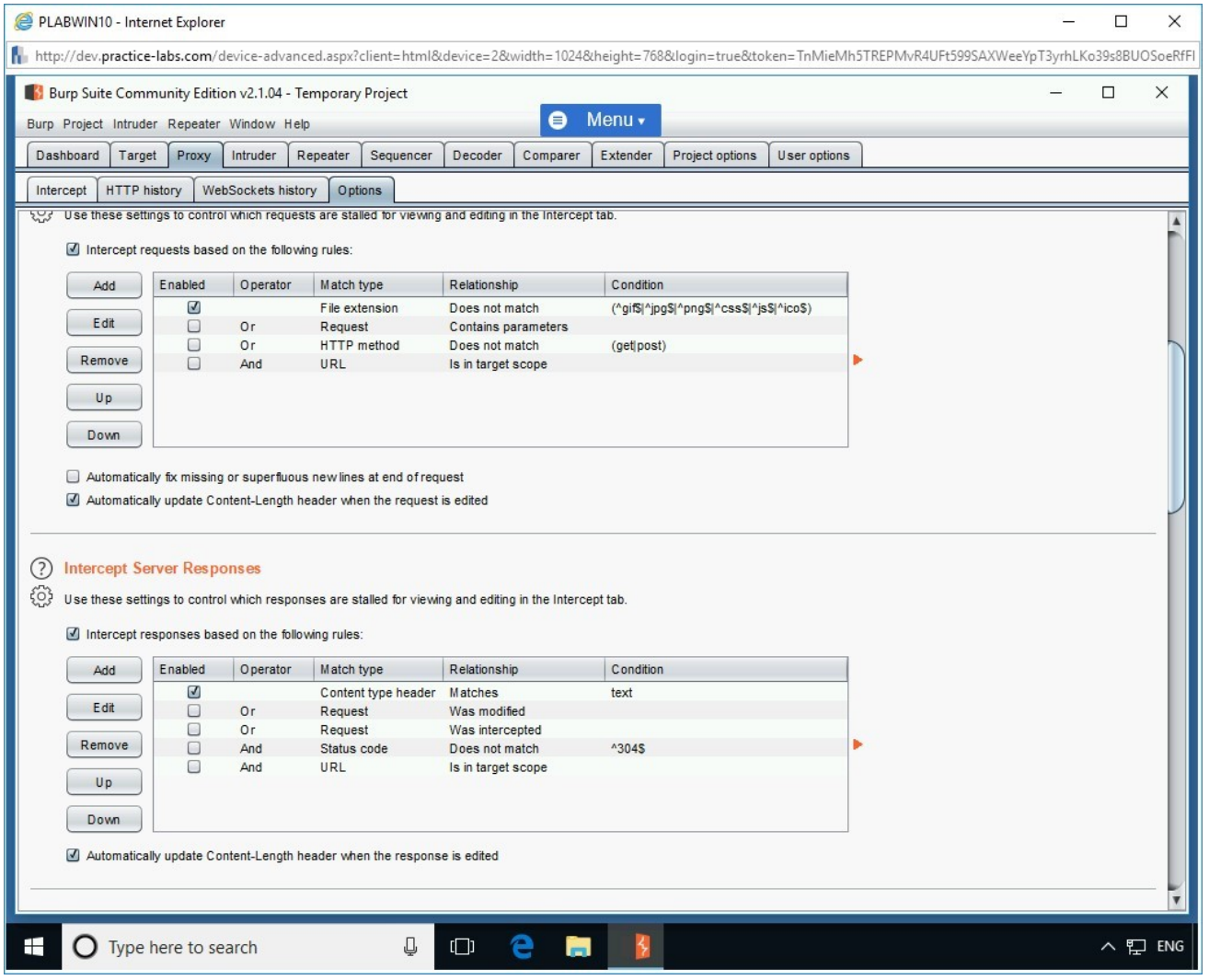


Figure 1.40 Screenshot of PLABWIN10: Clicking the Intercept tab under the Proxy tab.

Step 14

Ensure that the **intercept** button is set to: **Intercept is on**.

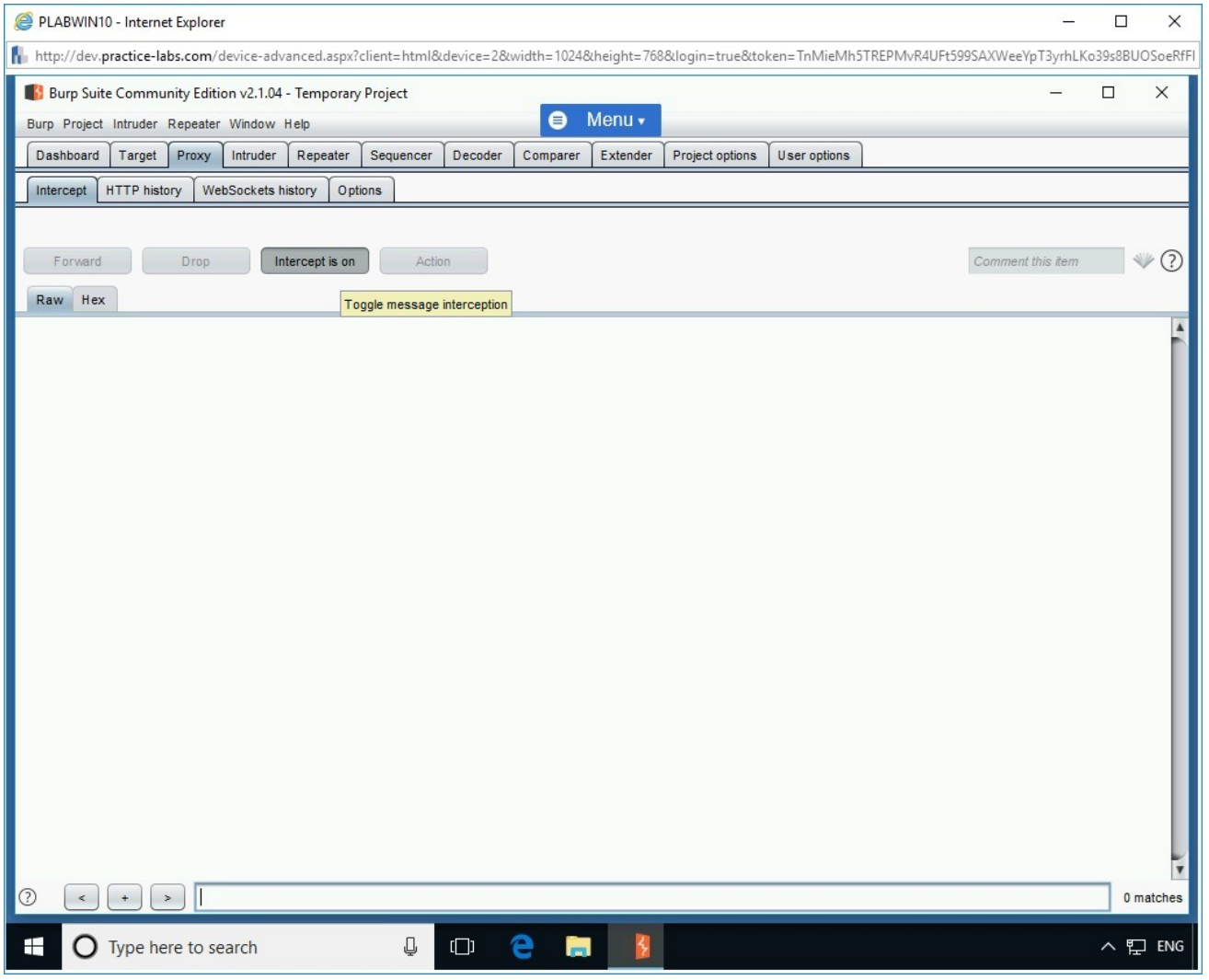


Figure 1.41 Screenshot of PLABWIN10: Ensuring that the intercept option is on the Intercept tab.

Step 15

Minimize the **Burp Suite** window.

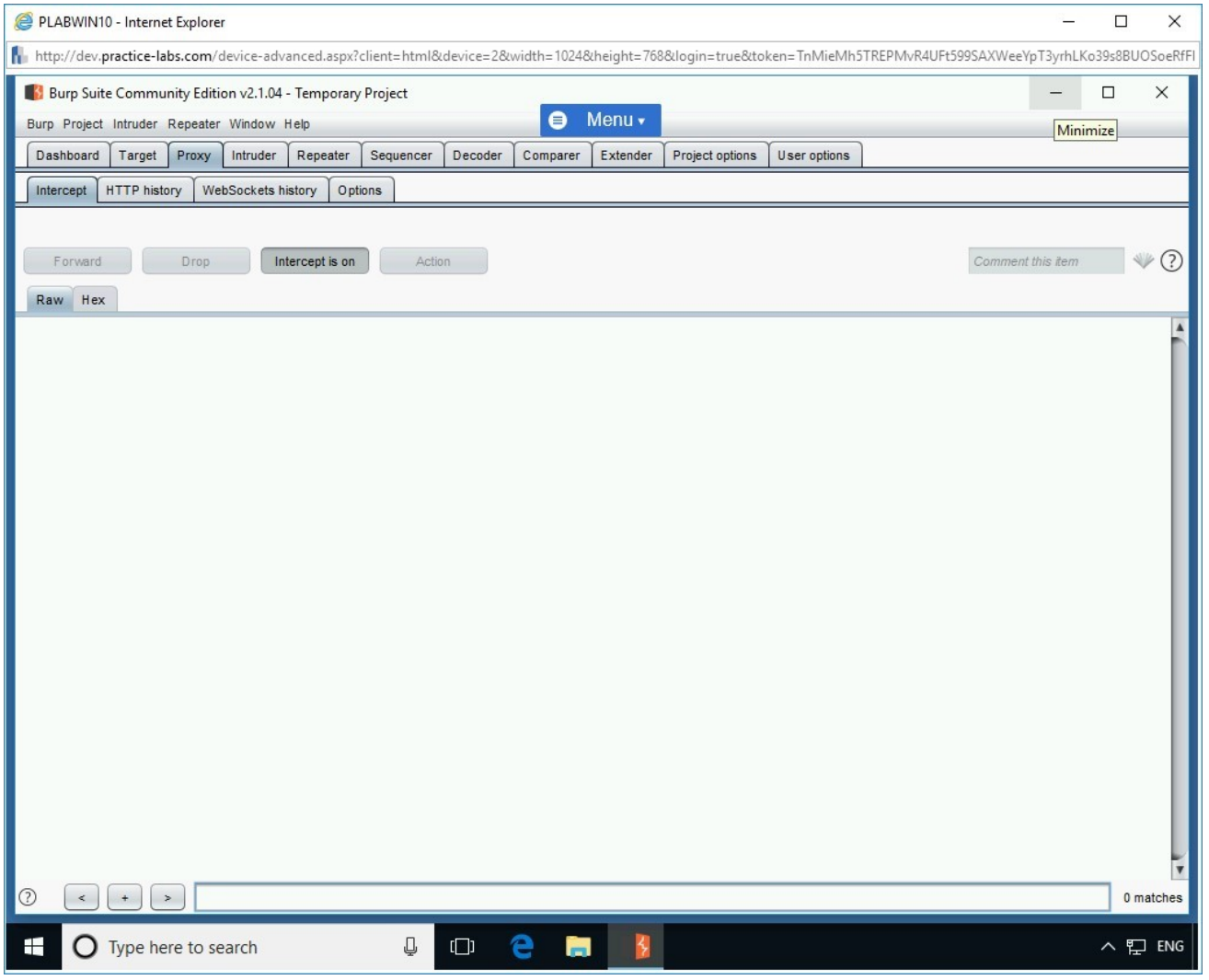


Figure 1.42 Screenshot of PLABWIN10: Minimizing the Burp Suite window.

Task 4 - Configure Firefox to Use Burp Suite Proxy Listeners

After you have configured Burp Suite to intercept traffic, you need to now configure Firefox to use proxy listeners. In this task, you will configure Mozilla Firefox to use Burp Suite proxy listeners. To do this, perform the following steps:

Step 1

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

From **PLABWIN10** desktop, double-click **Mozilla Firefox**.

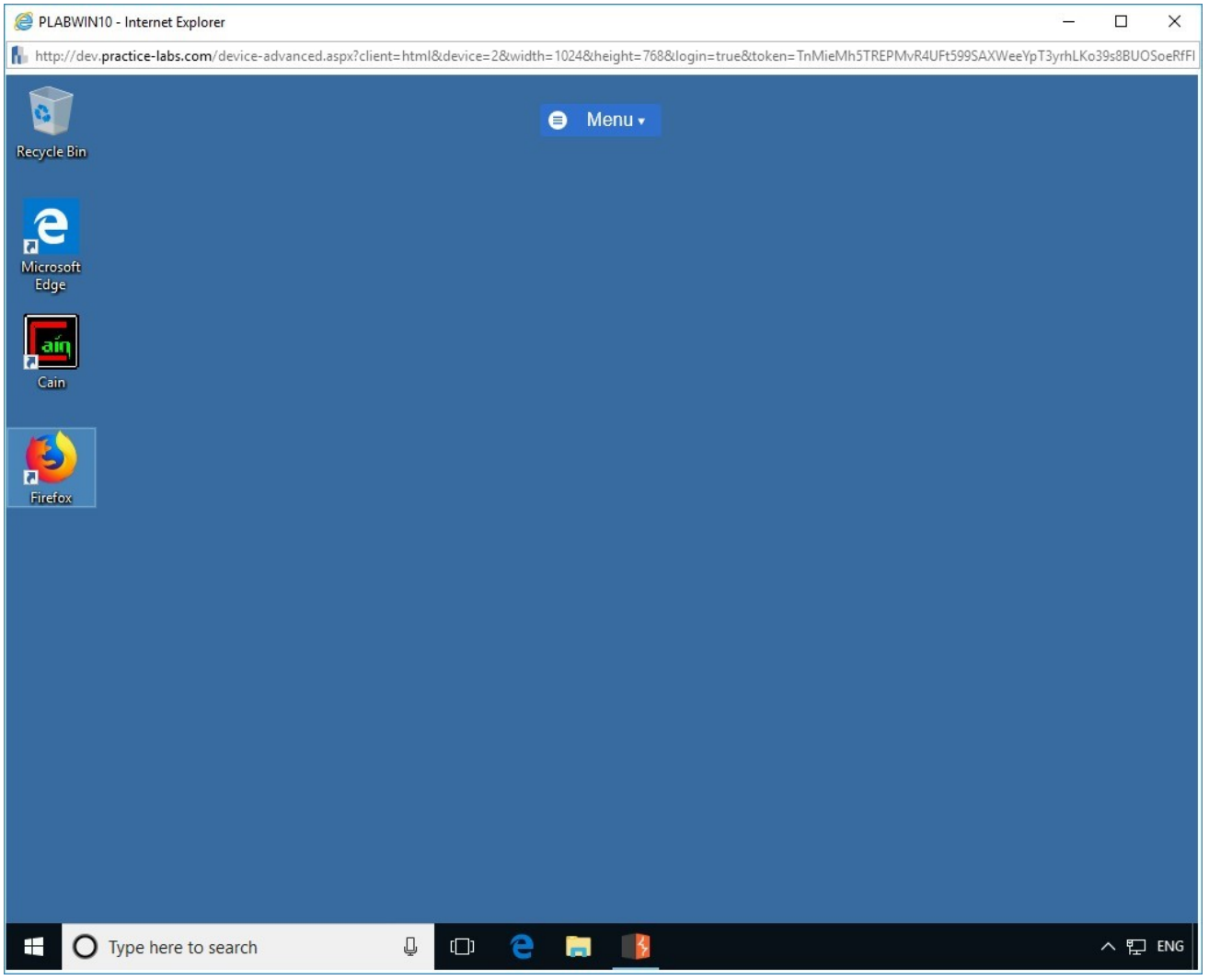


Figure 1.43 Screenshot of PLABWIN10: Double-clicking the Firefox icon on the desktop.

Step 2

The **Mozilla Firefox** window opens.

A **Default Browser** dialogue box appears.

Click **Not now.**

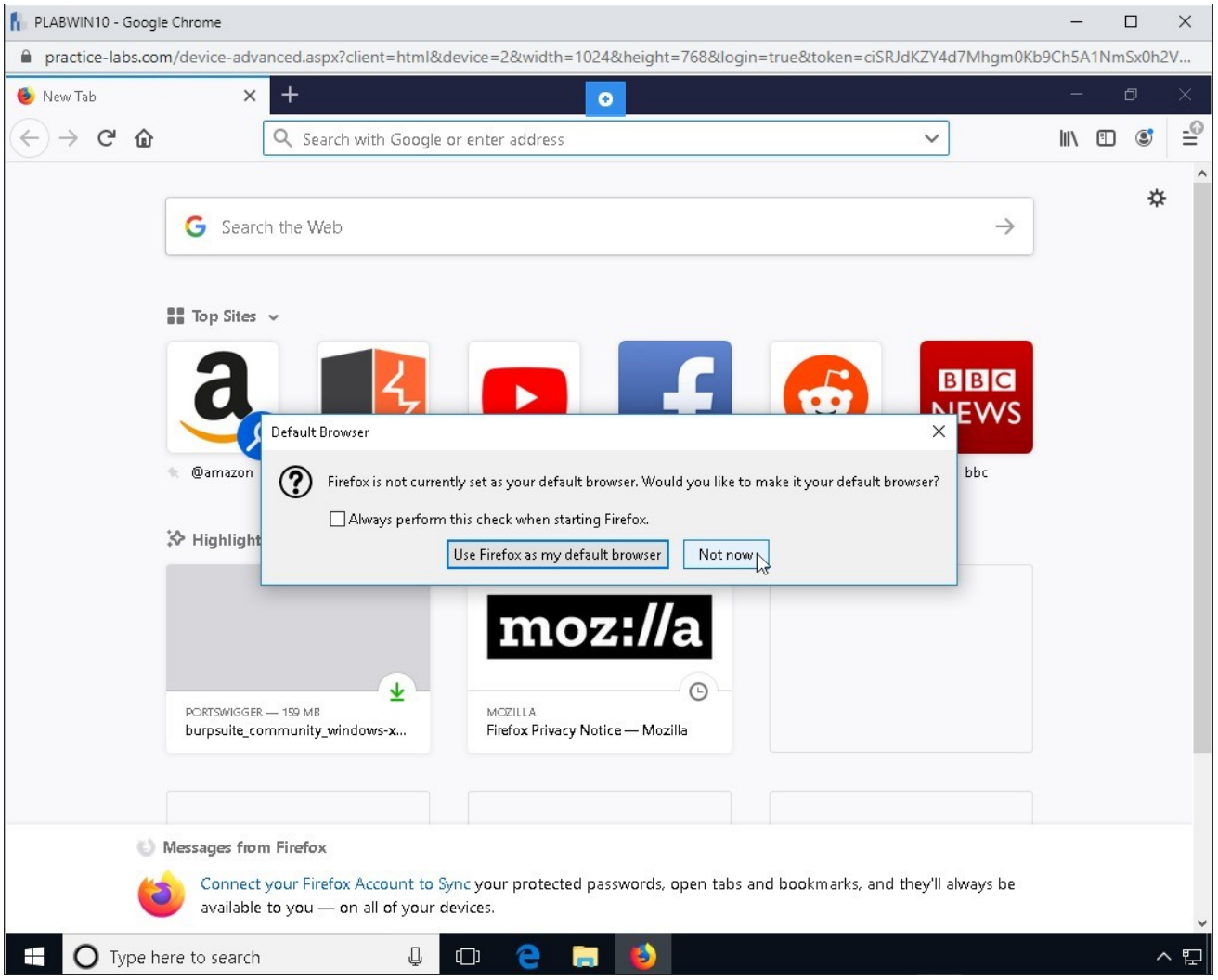


Figure 1.44 Screenshot of PLABWIN10: Pressing Not now on the Default Browser dialogue box..

Step 3

On the update notification, click **Not Now**.

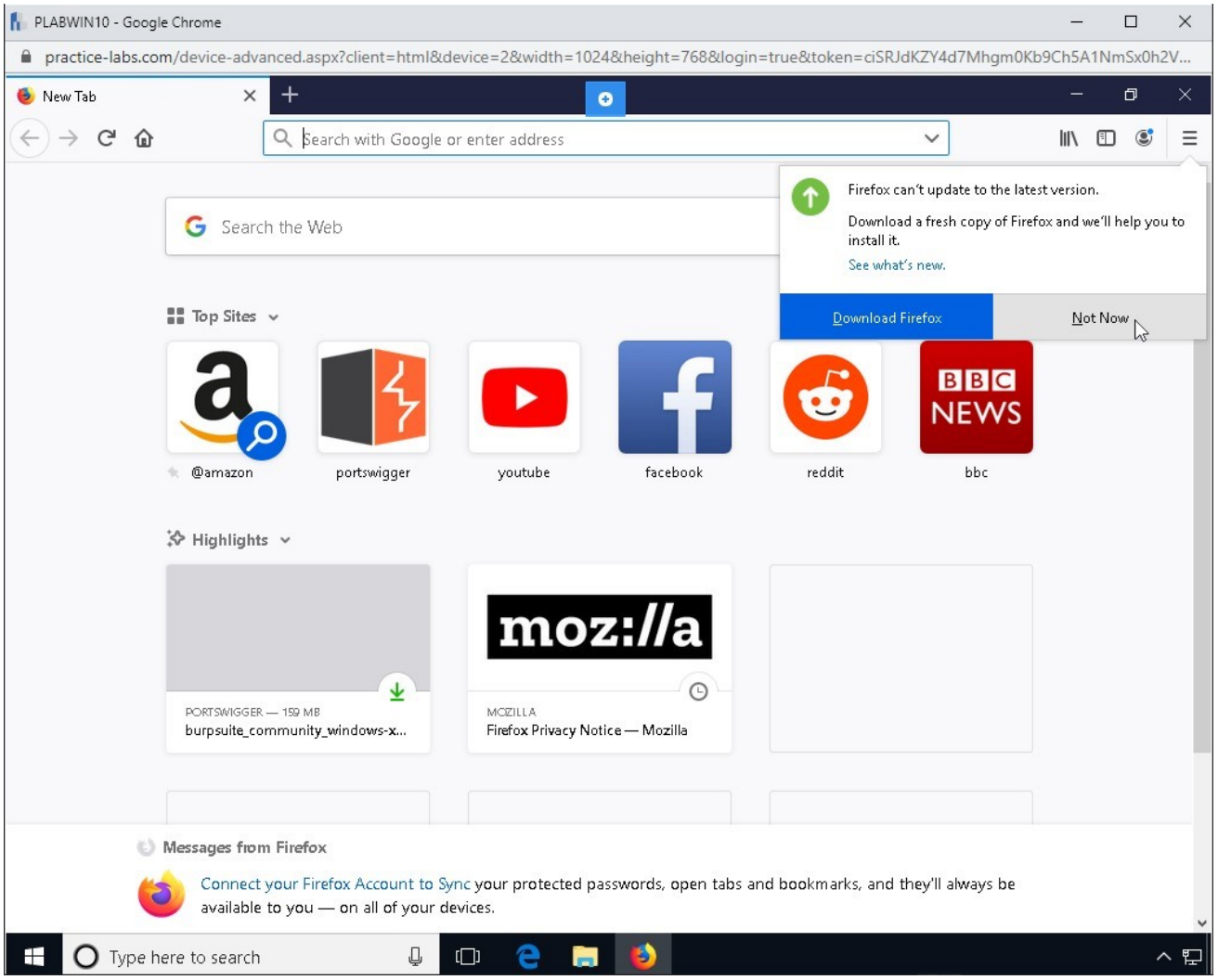


Figure 1.45 Screenshot of PLABWIN10: Clicking the Not Now option on the update notification.

Step 4

In the **Mozilla Firefox** window, click the **Open menu** icon from the upper right corner, and select **Options**.

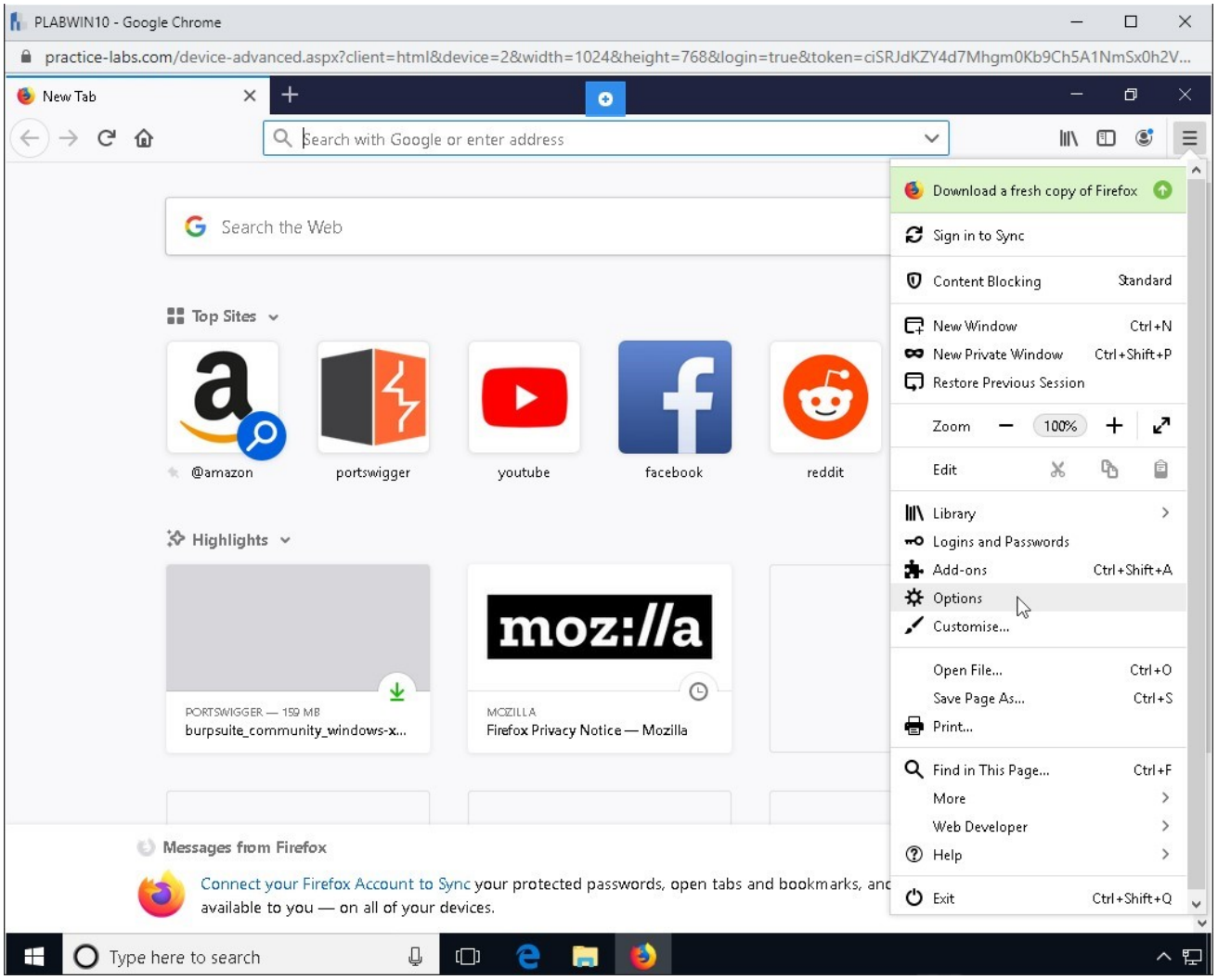


Figure 1.46 Screenshot of PLABWIN10: Selecting Options from Open menu.

Step 5

The **Options** page opens. The update notification is displayed again. Click **Not Now**.

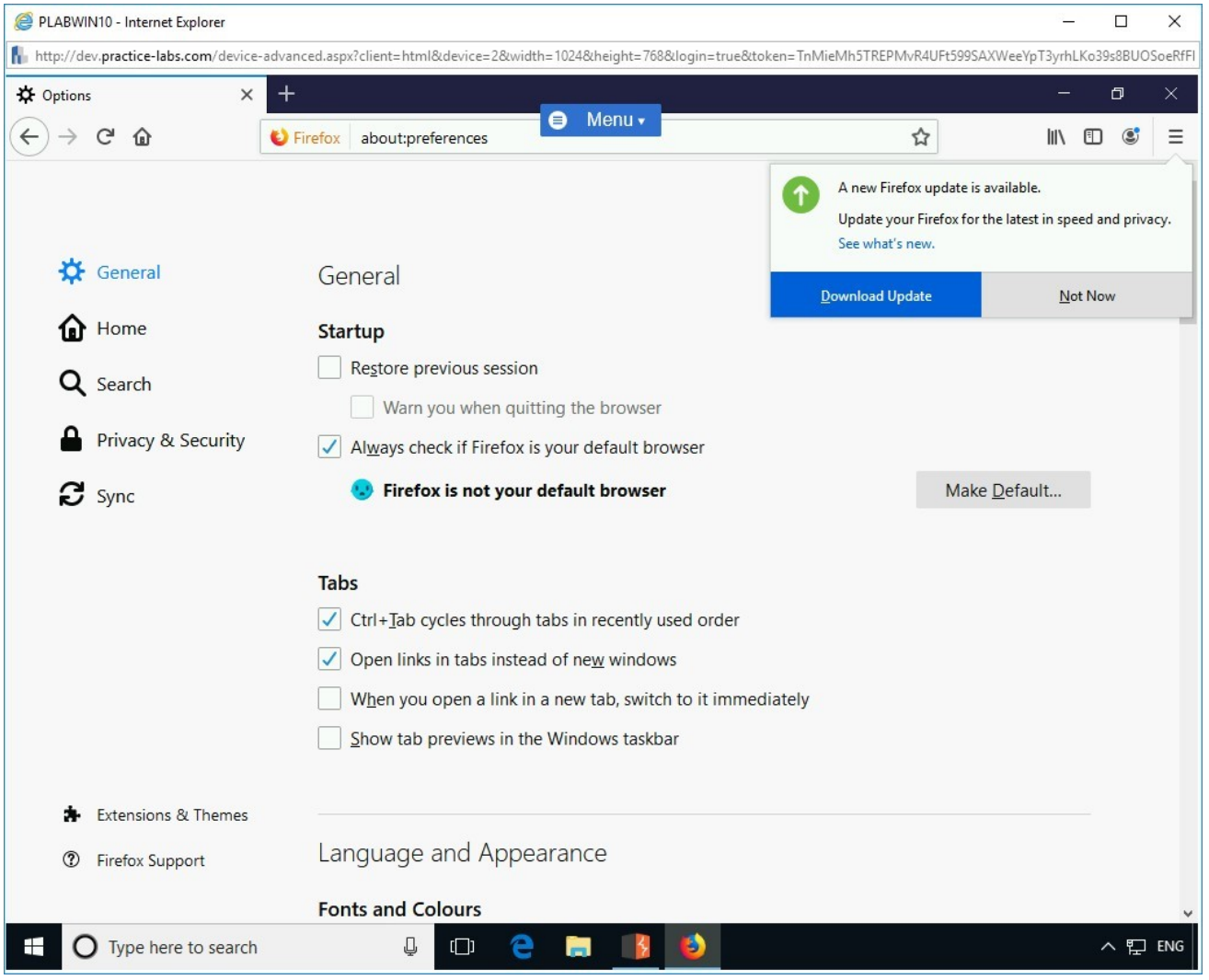


Figure 1.47 Screenshot of PLABWIN10: Showing the Options page and clicking Not now on the update notification.

Step 6

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

Scroll down to configure the network proxy.

Click **Settings** on the right-hand pane.

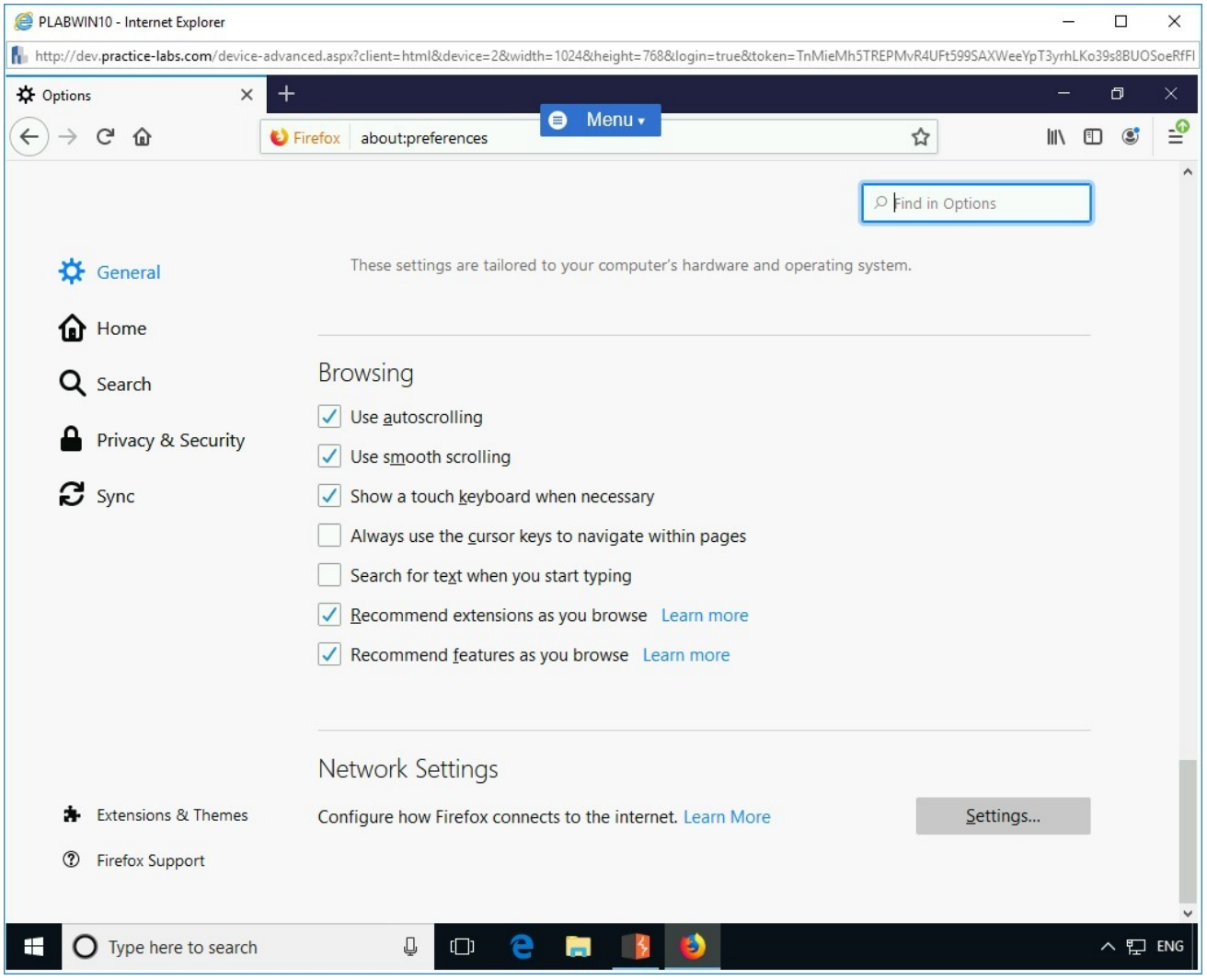


Figure 1.48 Screenshot of PLABWIN10: Clicking the Settings button on the Options page.

Step 7

The **Connection Settings** dialog box opens.

To change the manual proxy address to the Burp listener address, click **Manual proxy configuration**.

In the **Connection Settings** dialog box, under **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
```

Click to select the checkbox **Use this proxy server for all protocols**.

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

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

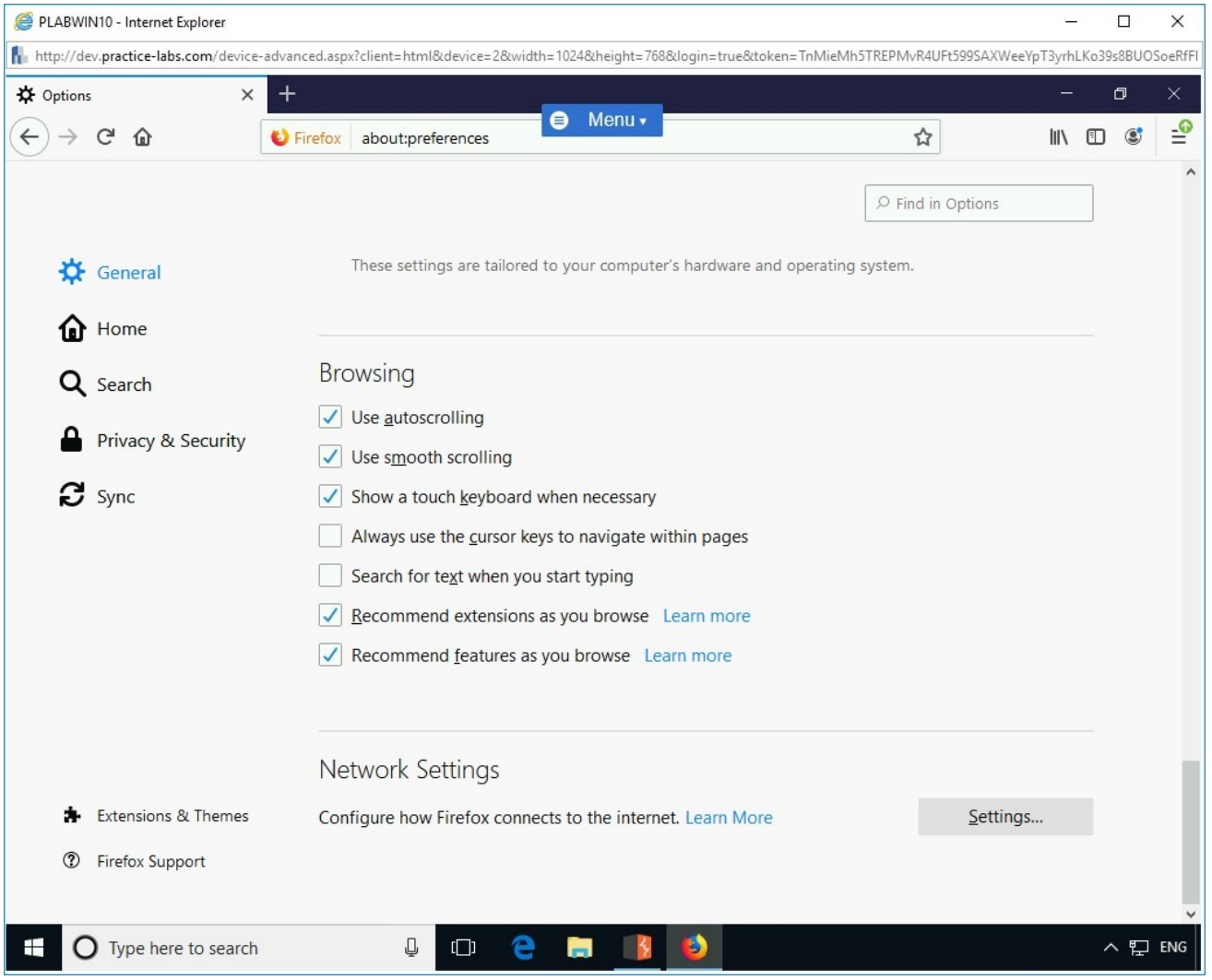


Figure 1.49 Screenshot of PLABWIN10: Showing the Options page.

Task 5 - Capture Cookies

In this task, you will view cookie information in the response and request intercepted by Burp Suite. An important point that needs to be noted in this task is that for each action in 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, in the **Mozilla Firefox** Web browser window, in the new tab, type the following URL in the address bar:

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

Press **Enter**.

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

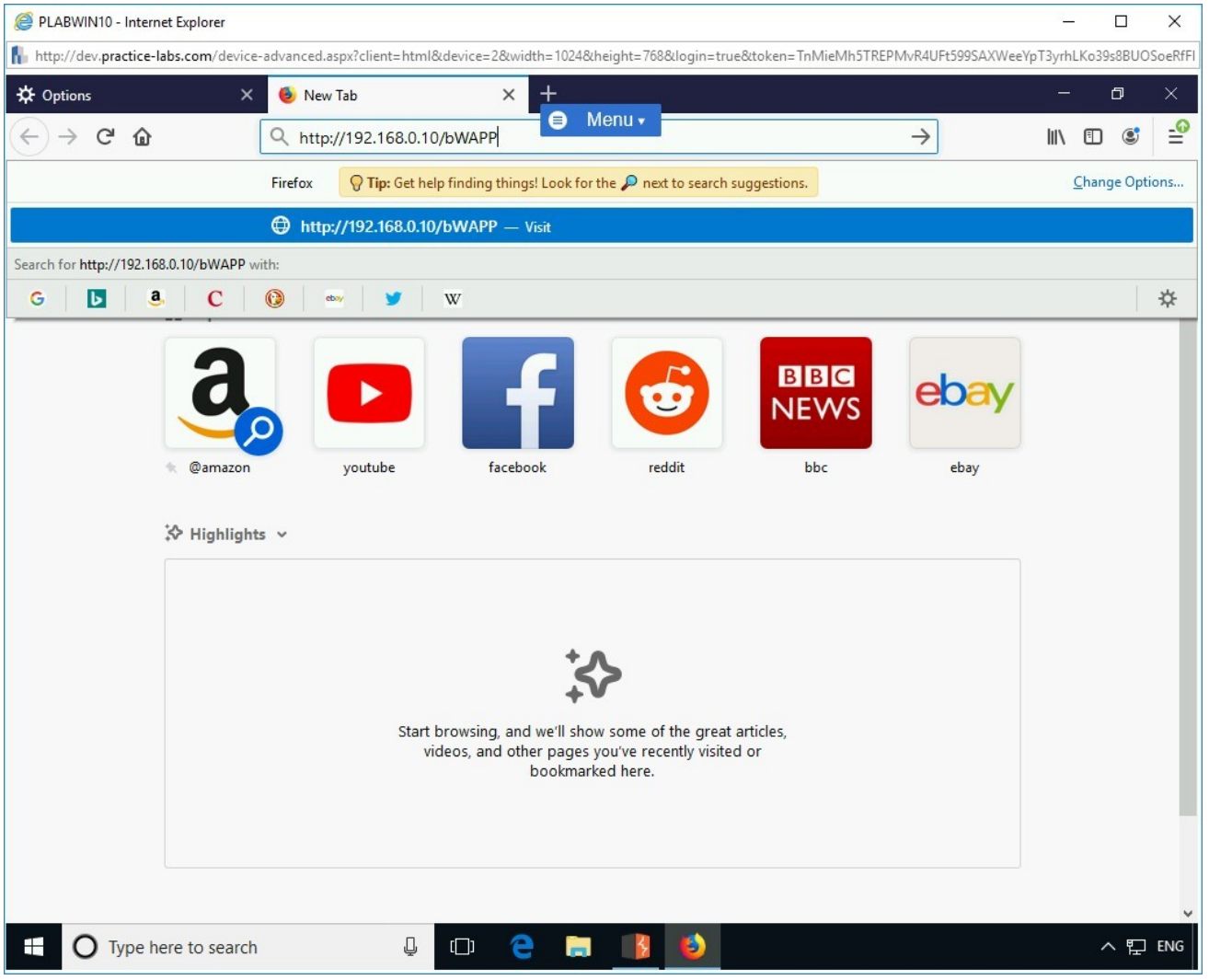


Figure 1.50 Screenshot of PLABWIN10: Entering the URL in the address bar of Internet Explorer.

Step 2

The login page of the bWAPP application is displayed.

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

```
bee
```

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

bug

Click **Login**.

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

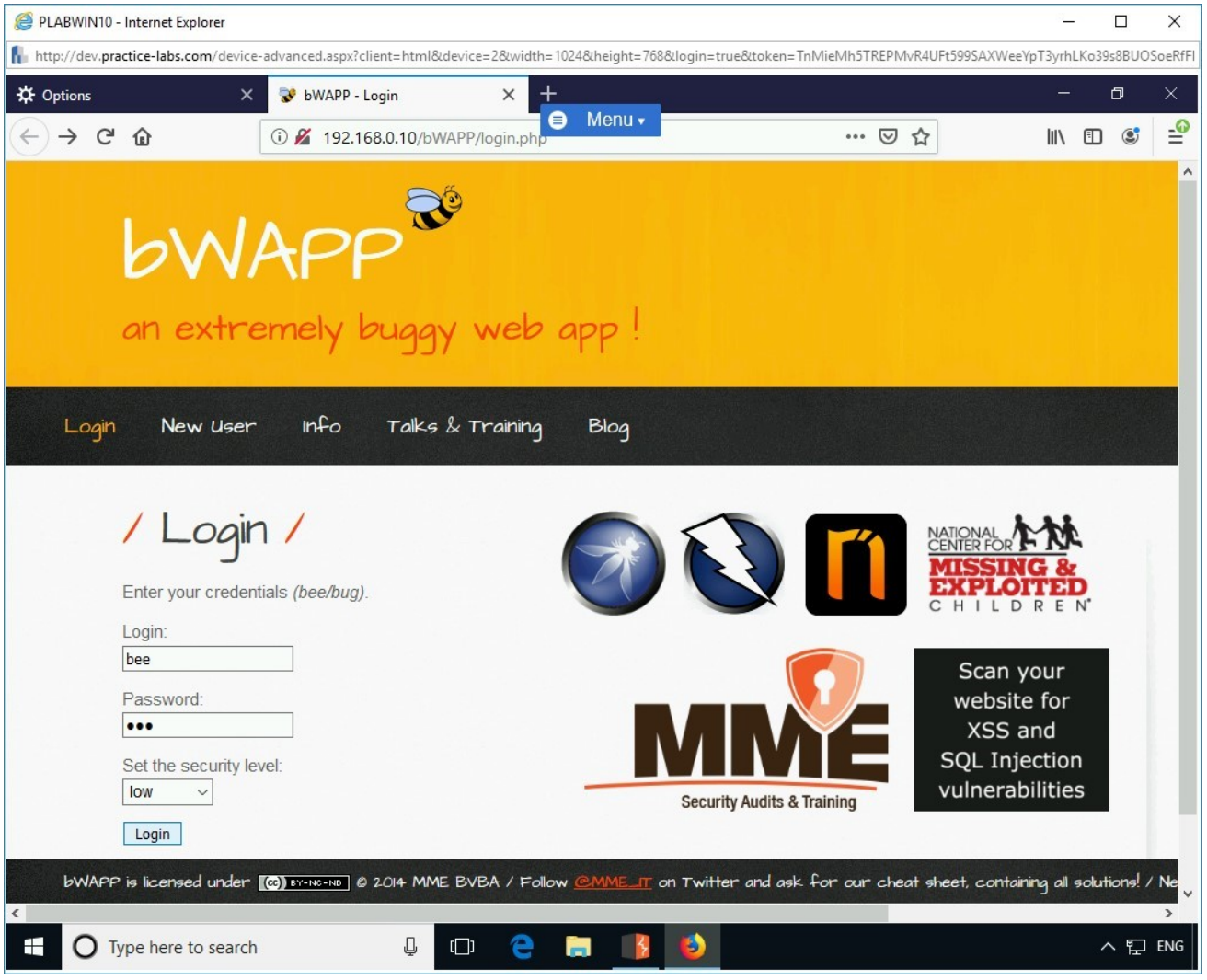


Figure 1.51 Screenshot of PLABWIN10: Entering the username and password in the login page and then clicking Login.

Step 3

The portal page is displayed after login. On the login notification, click **Don't Save.**

Figure 1.52 Screenshot of PLABWIN10: Showing the logged in page after successful login and then clicking Don't Save on the login notification.

Step 4

Switch to the **Burp Suite Free Edition v1.7.27 - Temporary Project** window.

Notice the **Intercept** tab displays the details about the request to the following URL:

```
http://192.168.0.10
```

Analyze the displayed information.

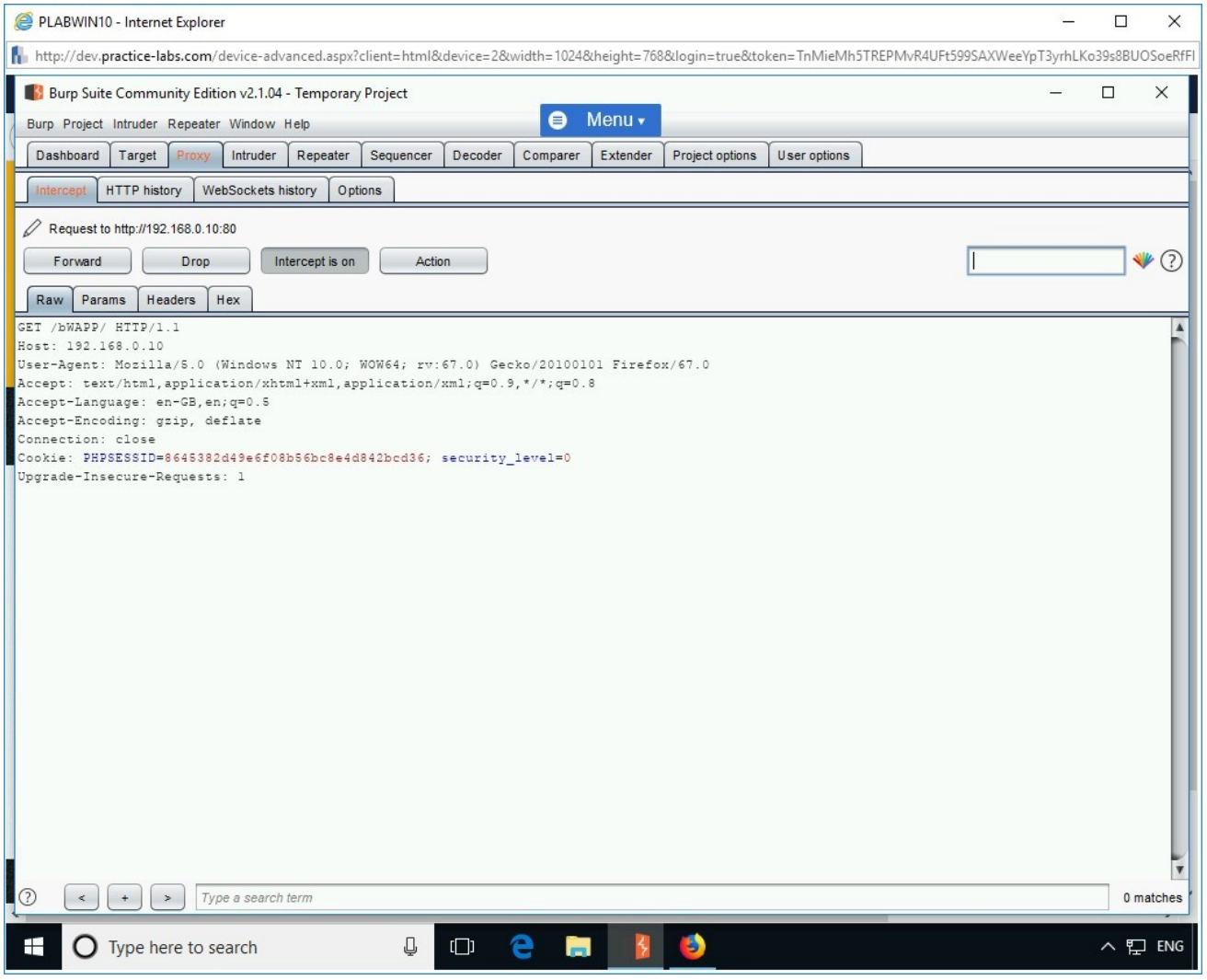


Figure 1.53 Screenshot of PLABWIN10: Showing the cookie information on the Intercept tab.

Step 5

In the **Burp Suite Free Edition v1.7.27 - Temporary Project** window, click **Forward**.

Wait for Burp Suite to intercept the response.

Notice the response being captured.

In the response, observe that the browser sends a **Cookie** parameter. This is the cookie assigned by the browser for the current user session to the BWAPP application.

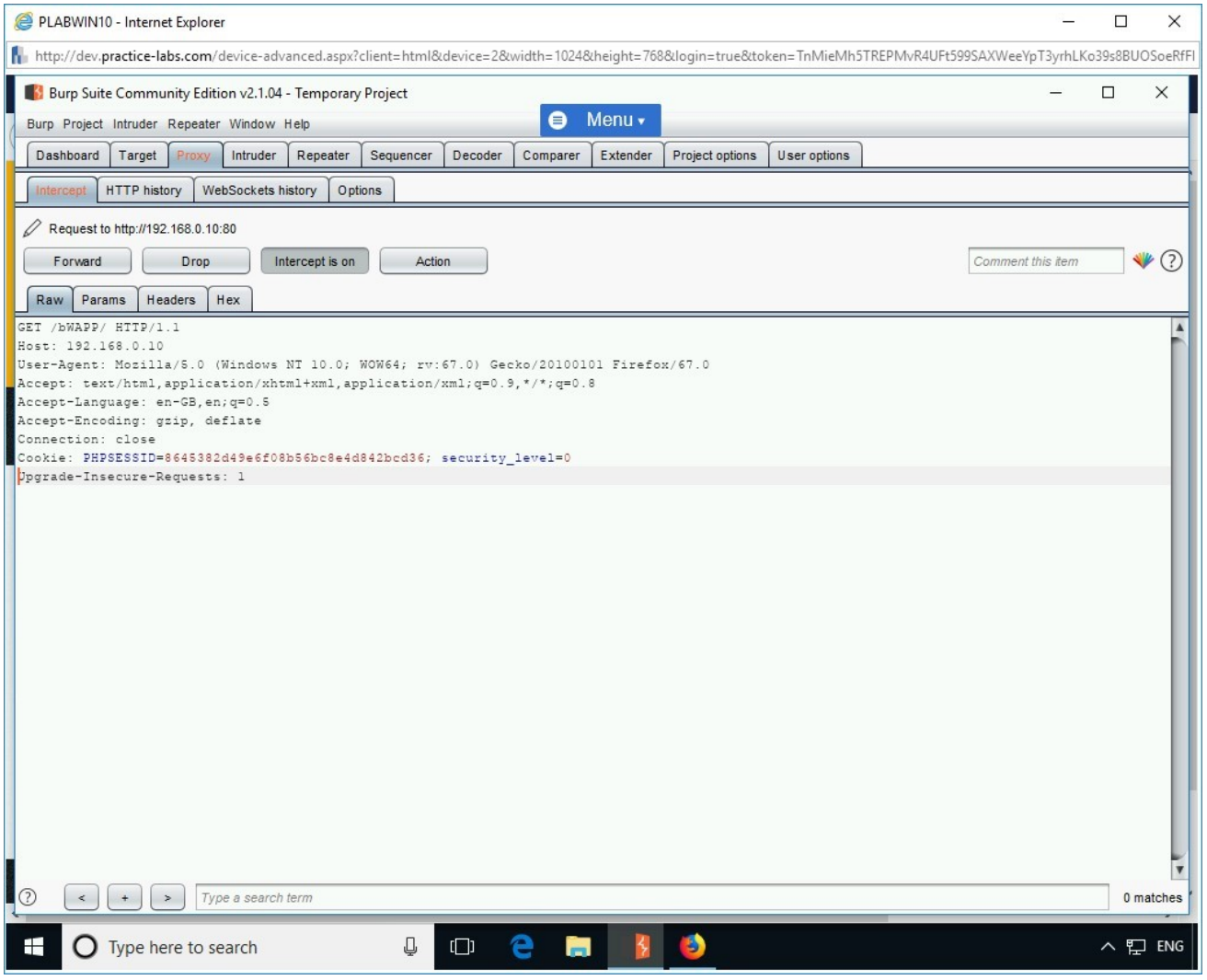


Figure 1.54 Screenshot of PLABWIN10: Showing the cookie information on the Intercept tab.

Review

Well done, you have completed the **Session Hijacking** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Capture Session Cookies

After completing this lab, you will be able to:

- Install Burp Suite on PLABWIN10
- Install Firefox
- Configure Burp Suite on PLABWIN10
- Configure Firefox to Use Burp Suite Proxy Listeners
- Capture Cookies

You should now be able to:

- Install Burp Suite on PLABWIN10
- Install Firefox
- Configure Burp Suite on PLABWIN10
- Configure Firefox to Use Burp Suite Proxy Listeners
- Capture Cookies

Feedback

Shutdown all virtual machines used in this lab. Alternatively, you can log out of the lab platform.