Security+[SY0–601] Lab Walkthrough

Lab 7 – How to use Burp Suite to intercept client-side requests

Hassen Hannachi

November 24, 2025

Contents

List of Figures

1 Introduction

Burp Suite is an especially useful tool when testing web applications. Burp Suite has many uses, but for this lab, we will be focusing on the local proxy feature, which allows us to intercept the requests being sent from our machine to a server. This provides us with the ability to alter the requests being sent the server.

2 Environment Setup

Please follow these labs to get hands-on experience for CompTIA Security+ exam [SY0–601]. All the labs use free tools. I STRONGLY suggest you use a virtual machine[1] such as VMware or Virtualbox for these labs to avoid exposing your home PC or laptop. [2]

3 Lab Walkthrough

3.1 Task 1

Run "burpsuite" command in Kali terminal screen as "kali" user. Accept and update as required.

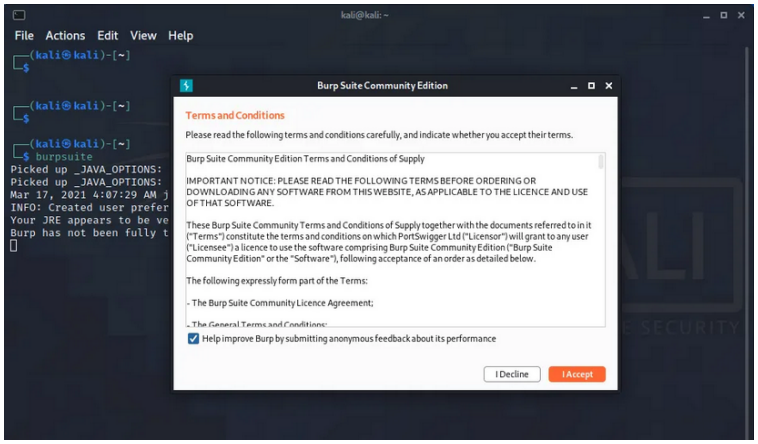

Figure 1: brutsuite -Kali Linux

Once Burp is opened, choose "Temporary Project" from the list of options and click next.

In the next screen, choose the option to setup Burp using Burp defaults, and then press "Start Burp".

[1] You can use Kali Linux amd64 version in a virtual machine for the purpose of this lab.

[2] NEVER configure these labs at work using your employers' PCs.

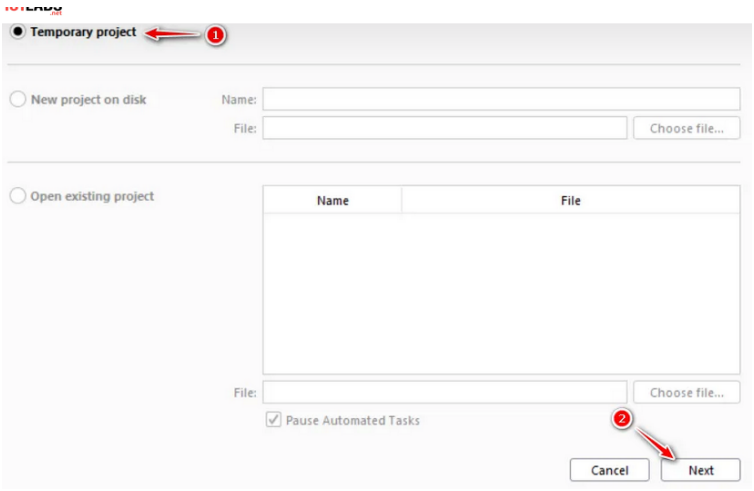

Figure 2: temporary project

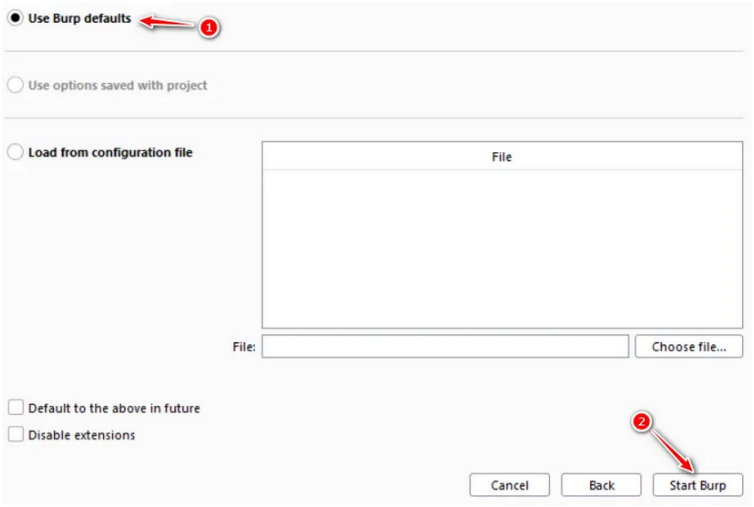

Figure 3: burp defaults

3.2 Task 2

Once Burp Suite is opened, you will see a lot of tabs and other information. For now, all we will be worrying about is the Proxy tab, so you can navigate there now.

Burp Suite recently updated to include its own built-in browser for using the local proxy with, which means we no longer must configure our browser to work with Burp manually. However, we will also consider the use of an external browser in this lab.

Notice that colored button which says, "intercept is on". This means that Burp is currently intercepting traffic sent from our Kali machine to any server. For now, we can press this button to turn intercept mode off.

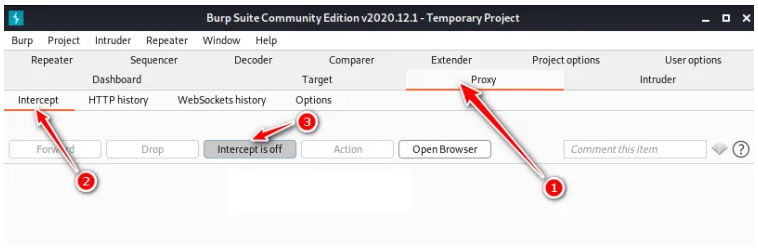

Figure 4: burp suite

3.3 Task 3

We will begin by learning how to use Burp with Firefox. Navigate to the proxy tab, and then to the options tab. Then, click on "Import/export CA Certificate". This is the certificate which will allow our browser to trust Burp Suite.

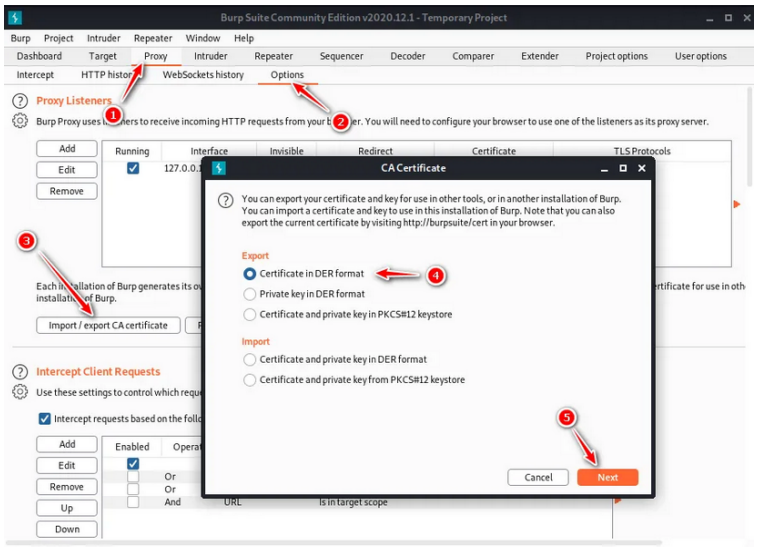

Figure 5: brup with firefox -proxy

Then, browse to a location on your Kali VM where you want to save the file. It is important that, when you are saving the file, you save it with a .der extension, otherwise the file won't import correctly into Firefox.

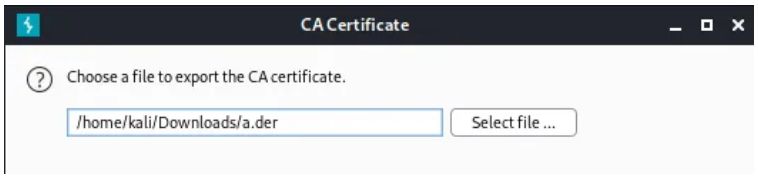

Figure 6: CA certificate

3.4 Task 4

Once this is done, open Web Browser (Firefox) in Kali and navigate to the options. Find "proxy" in Preferences' search box. Click on the button called "Settings" under Network Settings.

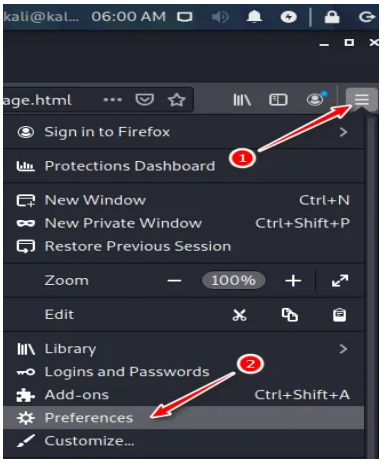

Figure 7: proxy preferences

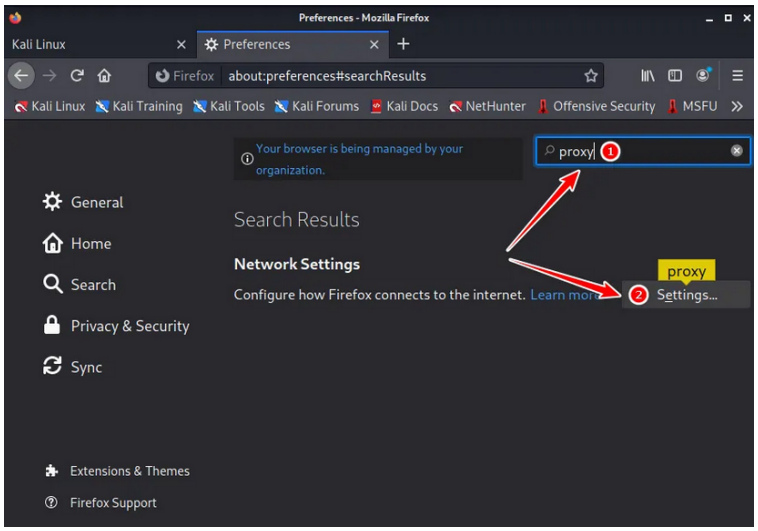

Figure 8: proxy settings

Then, click Manual Proxy Configuration and enter the following details:

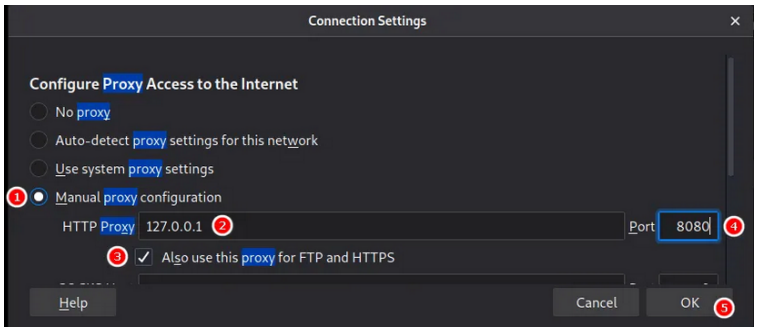

Figure 9: manual proxy configuration

3.5 Task 5

Once this is done, navigate to the Privacy & Security tab and then to the Certificates section. This is where we will import the certificate from Burp we saved earlier. To do this, press on "View Certificates" and click on "Import".

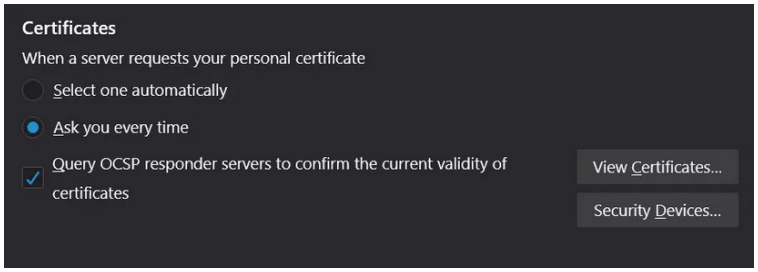

Figure 10: certificates view

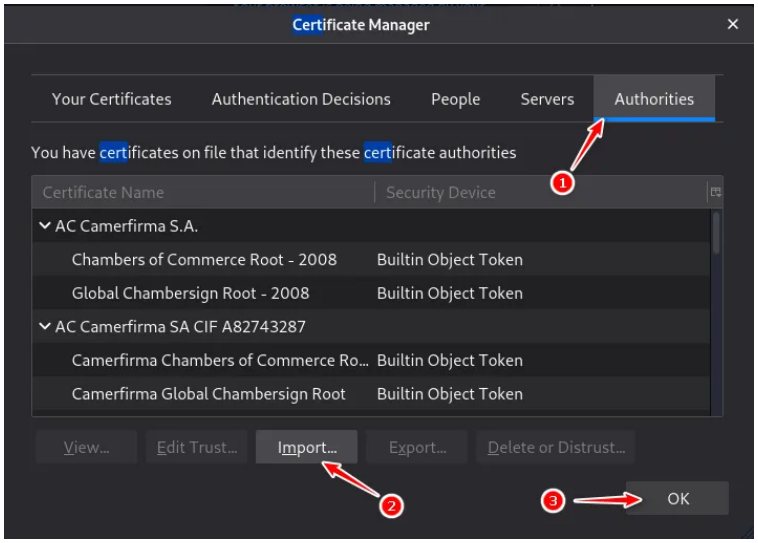

Figure 11: certificate manager

Navigate to the .der file that we saved earlier. Once selected, a box will pop up asking if

you would like Burp Suite to be able to intercept emails and connections to websites. Select both options and click “Ok”.

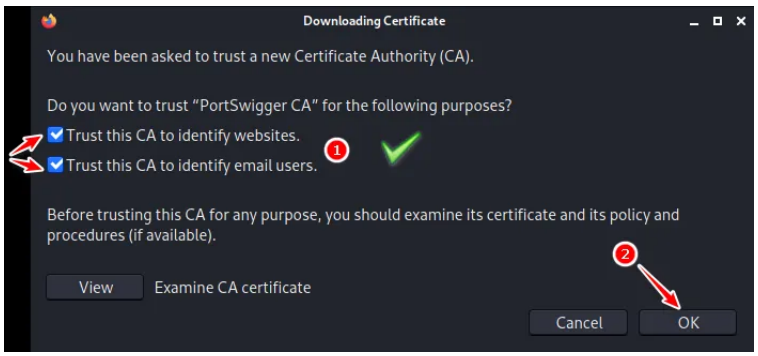

Figure 12: download certificate

Great, Firefox is now configured to work with burp! To test it out, open Burp and Firefox. Ensure Intercept mode is turned ON, and search something in Firefox. If Burp Suite is not intercepting requests, you may have to navigate back to the proxy page. A pop-up might appear asking you to set up a listener. Simply press enable and Burp should then work properly.

Your request should be captured in Burp Suite for you to manipulate or examine.

3.6 Task 6

Now, we will learn how to use Burp to intercept browser network traffic.

Once the web browser opens, navigate to the following site:

http://testasp.vulnweb.com/Login.asp?RetURL=

Once there, go back to Burp and turn ON intercept mode. Then, enter any username and password combination into the site and click “Login”. As you will see, the page will remain in a loading state. This is because Burp has now intercepted the request we sent to the server, and is holding it for us to manipulate.

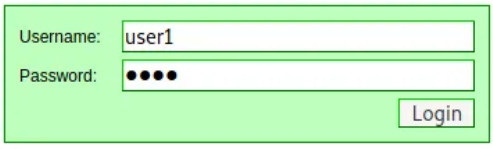

Figure 13: testasp vulnweb login

Go back to Burp and you will find the intercepted request, along with the username and password data that we entered. To navigate through the different requests Burp is intercepting, simply press the “Forward” button to send the request to the server and view the next request.

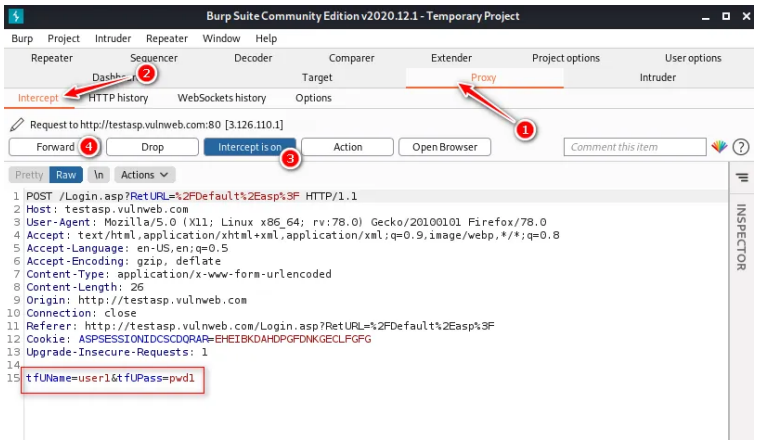

Figure 14: burp interception

3.7 Task 7

You can also alter any text portion of web traffic when Burb interception mode is ON. Try to change "tfUName=admin" and "tfUPass=none" and press the "Forward" button. Those are valid credentials for the green-colored page, and you will be granted access to the next page.

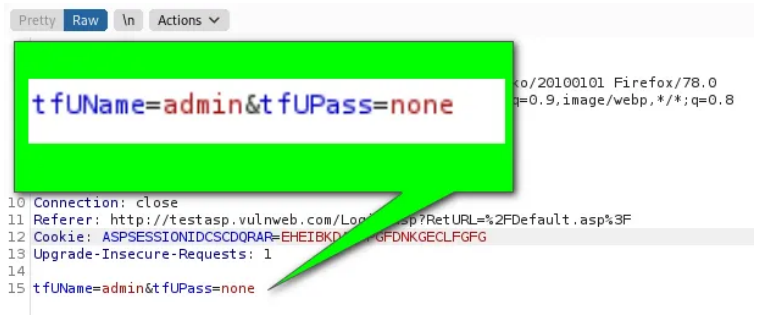

Figure 15: alter text portion

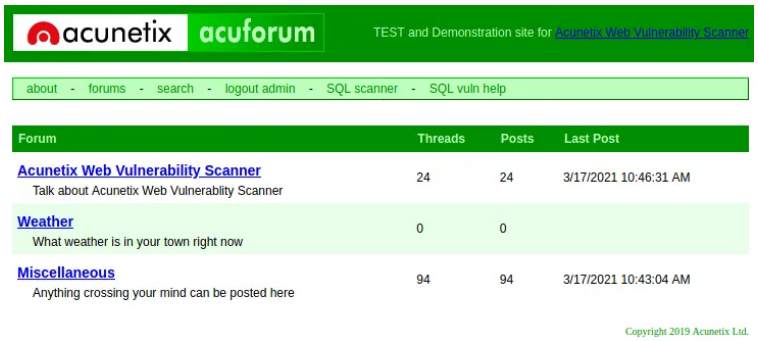

Figure 16: valid credentials

4 Conclusion

This lab demonstrated the power and flexibility of Burp Suite as an essential tool for web application testing. By intercepting and manipulating HTTP requests, Burp Suite enables security professionals to analyze how web applications behave, identify vulnerabilities such as insecure session handling, hidden form fields, and improper input validation.

References

[1] Namp: A Beginner's Guide to Network Mapping and Security

[2] Nmap Port Scanning Options.