Experiment – 6

Aim: Implement Burp proxy to test web applications.

Requirement : PC, Internet, burpsuite_pro_windows-x64_v2022_8_4

Thoery:-

What is Burp Suite?

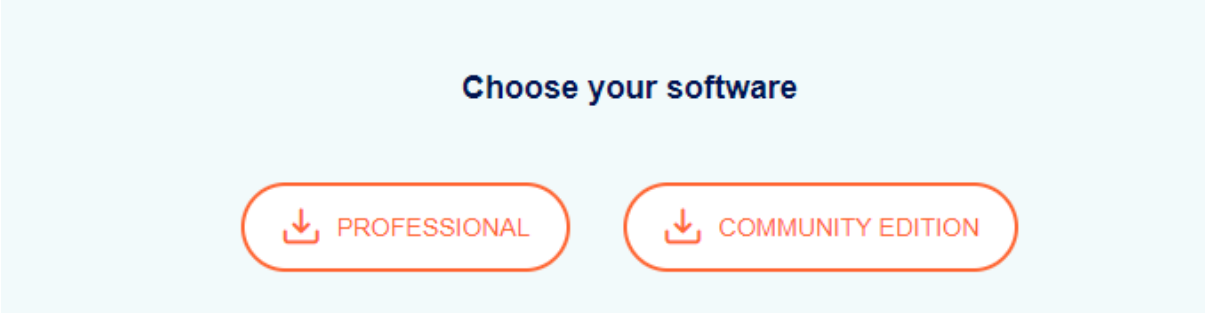
Burp or Burp Suite is a set of tools used for penetration testing of web applications. It is developed by the company named Portswigger, which is also the alias of its founder DafyddStuttard. BurpSuite aims to be an all in one set of tools and its capabilities can be enhanced by installing add-ons that are called BApps.
It is the most popular tool among professional web app security researchers and bug bounty hunters. Its ease of use makes it a more suitable choice over free alternatives like OWASP ZAP. Burp Suite is available as a community edition which is free, professional edition that costs $399/year and an enterprise edition that costs $3999/Year. This article gives a brief introduction to the tools offered by BurpSuite. If you are a complete beginner in Web Application Pentest/Web App Hacking/Bug Bounty, we would recommend you to just read through without thinking too much about a term.

- **Steps to Download and Install Burp Suite:-**

Download and install

- Step 1: Download

Use the links below to download the latest version of Burp Suite Professional or Community Edition.
https://portswigger.net/burp/releases/professional-community-2022-8-4?requestededition=community&requestedplatform=



- Step 2: Install

Run the installer and launch Burp Suite.
When asked to select a project file and configuration, just click **Next** and then **Start Burp** to skip this for now.

- Step 3: Start exploring Burp Suite

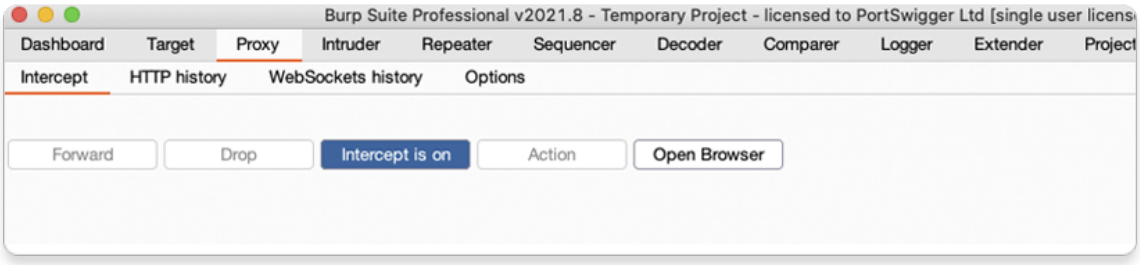
If you're completely new to Burp Suite, follow the rest of this tutorial for an interactive, guided tour of the core features.

- **Steps fpr intercepting HTTP traffic with Burp Proxy**

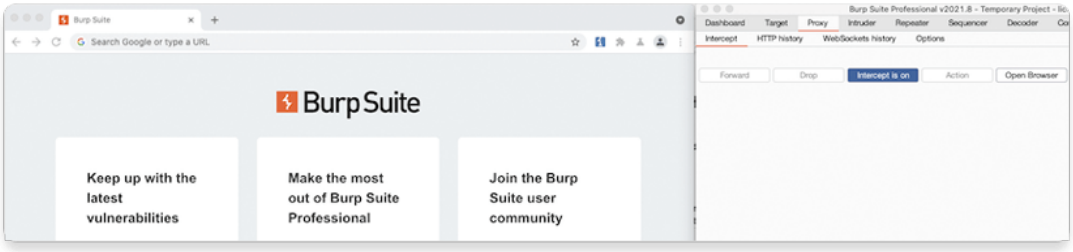
Intercept HTTP traffic with Burp Proxy
In this tutorial, you'll use a live, deliberately vulnerable website to learn how to intercept requests with Burp Proxy.
Intercepting a request
Burp Proxy lets you intercept HTTP requests and responses sent between Burp's browser and the target server. This enables you to study how the website behaves when you perform different actions.

- Step 1: Launch Burp's browser

Go to the **Proxy > Intercept** tab.
Click the **Intercept is off** button, so it toggles to **Intercept is on.**

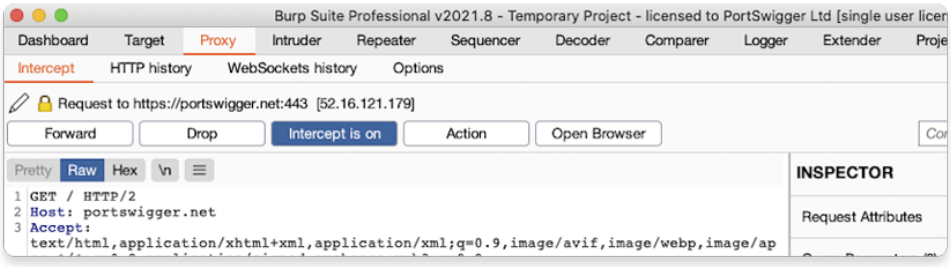


Click **Open Browser**. This launches Burp's browser, which is preconfigured to work with Burp right out of the box.
Position the windows so that you can see both Burp and Burp's browser.



- Step 2: Intercept a request

Using Burp's browser, try to visit `https://portswigger.net` and observe that the site doesn't load. Burp Proxy has intercepted the HTTP request that was issued by the browser before it could reach the server. You can see this intercepted request on the **Proxy > Intercept** tab.



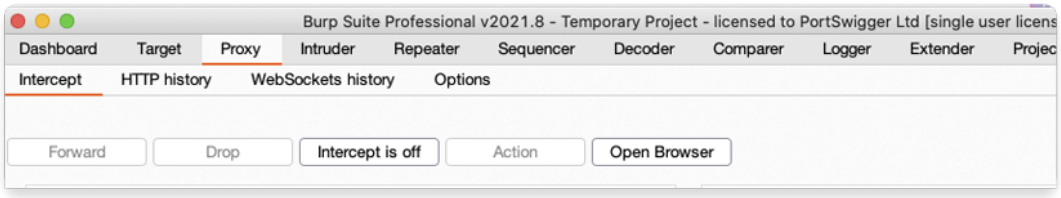
The request is held here so that you can study it, and even modify it, before forwarding it to the target server.

- Step 3: Forward the request

Click the **Forward** button several times to send the intercepted request, and any subsequent ones, until the page loads in Burp's browser.

- Step 4: Switch off interception

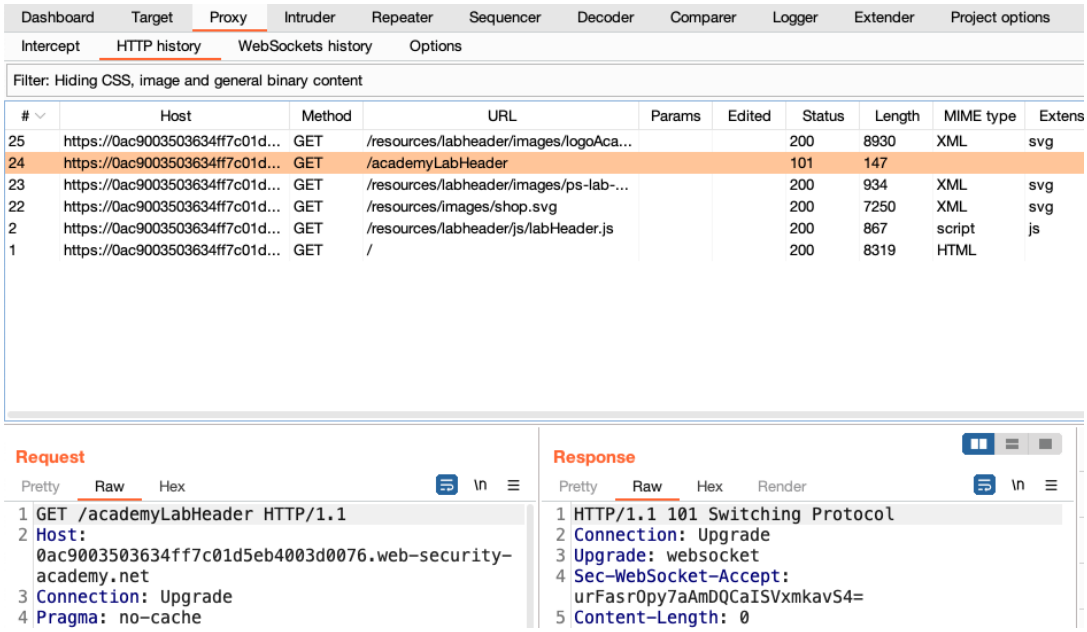
Due to the number of requests browsers typically send, you often won't want to intercept every single one of them. Click the **Intercept is on** button so that it now says **Intercept is off**.



Go back to the browser and confirm that you can now interact with the site as normal.

- Step 5: View the HTTP history

In Burp, go to the **Proxy > HTTP history** tab. Here, you can see the history of all HTTP traffic that has passed through Burp Proxy, even while interception was switched off.
Click on any entry in the history to view the raw HTTP request, along with the corresponding response from the server.



This lets you explore the website as normal and study the interactions between Burp's browser and the server afterward, which is more convenient in many cases.

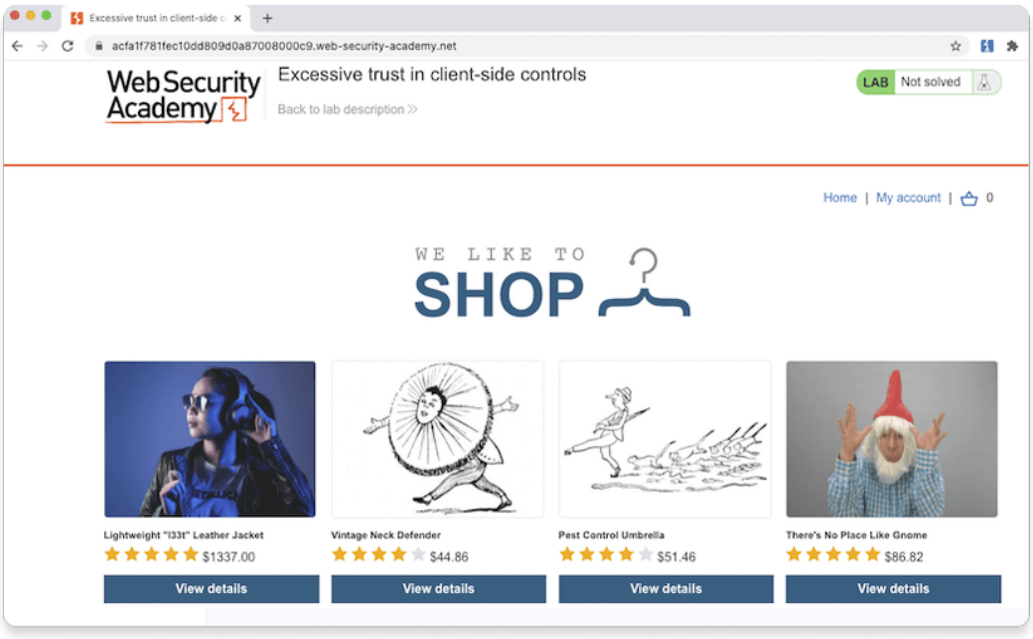
- **Steps for Modiying HTTP requests with Burp Proxy**

Modifying HTTP requests with Burp Proxy

In this tutorial, you'll learn how to modify an intercepted request in Burp Proxy. This enables you to manipulate the request in ways that the website isn't expecting in order to see how it responds. Using one of our deliberately vulnerable websites, known as "labs", you'll see how this can help you identify and exploit real vulnerabilities.

- Step 1: Access the vulnerable website in Burp's browser

In Burp, go to the **Proxy > Intercept** tab and make sure interception is switched off.
Launch Burp's browser and use it to visit the following URL:
`https://portswigger.net/web-security/logic-flaws/examples/lab-logic-flaws-excessive-trust-in-client-side-controls`
When the page loads, click **Access the lab**. If prompted, log in to your portswigger.net account. After a few seconds, you will see your own instance of a fake shopping website.



- Step 2: Log in to your shopping account

On the shopping website, click **My account** and log in using the following credentials:

Username: `wiener`

Password: `peter`

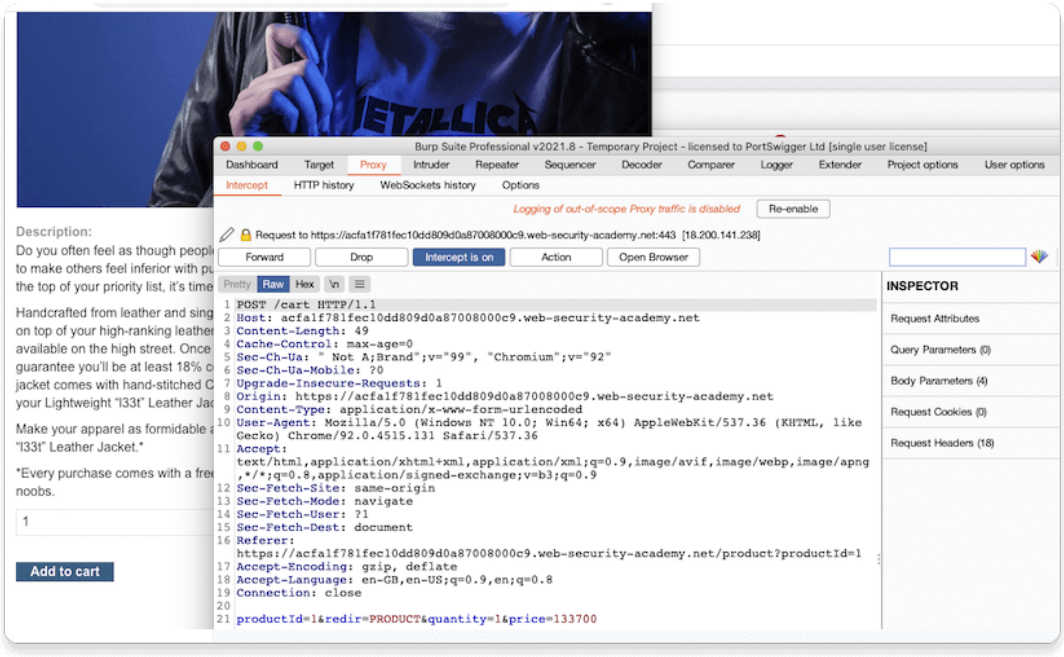
Notice that you have just $100 of store credit.

- Step 3: Find something to buy

Click **Home** to go back to the home page. Select the option to view the product details for the **Lightweight "l33t" leather jacket**.

- Step 4: Study the add to cart function

In Burp, go to the **Proxy > Intercept** tab and switch interception on. In the browser, add the leather jacket to your cart to intercept the resulting `POST /cart` request.



You may initially see a different request on the **Proxy > Intercept** tab if the browser is doing something else in the background. In this case, just click **Forward** until you see the `POST /cart` request as shown in the screenshot above.
Study the intercepted request and notice that there is a parameter in the body called `price`, which matches the price of the item in cents.

- Step 5: Modify the request

Change the value of the `price` parameter to 1 and click **Forward** to send the modified request to the server.

```
20
21 productId=1&redir=PRODUCT&quantity=1&price=1
```

Switch interception off again so that any subsequent requests can pass through Burp Proxy uninterrupted.

- Step 6: Exploit the vulnerability

In Burp's browser, click the basket icon in the upper-right corner to view your cart. Notice that the jacket has been added for just one cent.
Note
There is no way to modify the price via the web interface. You were only able to make this change thanks to Burp Proxy.
Click the **Place order** button to purchase the jacket for an extremely reasonable price.
Congratulations, you've also just solved your first Web Security Academy lab! You've also learned how to intercept, review, and manipulate HTTP traffic using Burp Proxy.
Conclusion