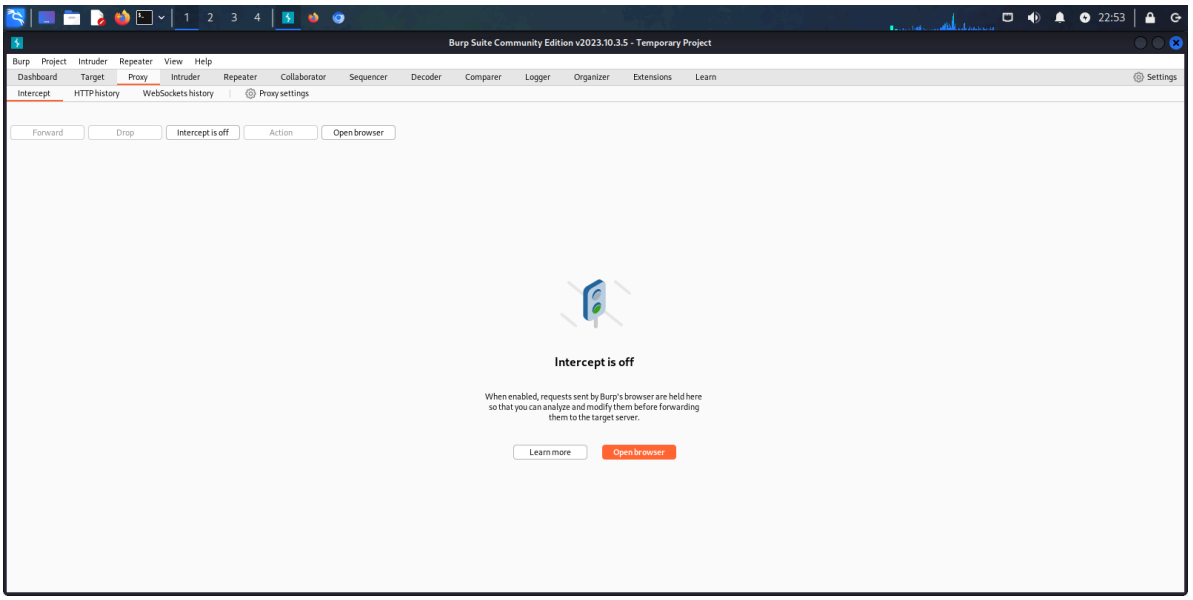
Week7: Perform various attacks using burpsuite and Portswigger

1. Intercepting HTTP Traffic

Step1: Go to the Proxy > Intercept tab.

Click the Intercept is off button, so it toggles to Intercept is on.

Then Click **Open Browser**.



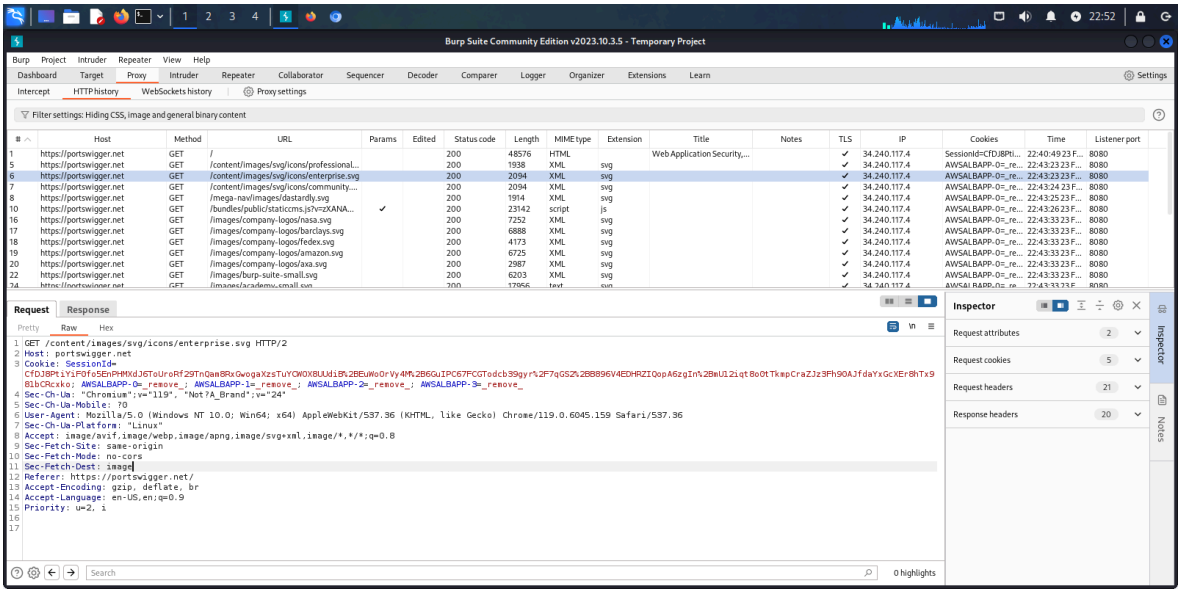
Step 2: Intercept a request: Using Burp's browser, try to visit https://portswigger.net and observe that the site doesn't load. Burp Proxy has intercepted the HTTP request that was issued by the browser before it could reach the server. You can see this intercepted request on the Proxy > Intercept tab.\

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.

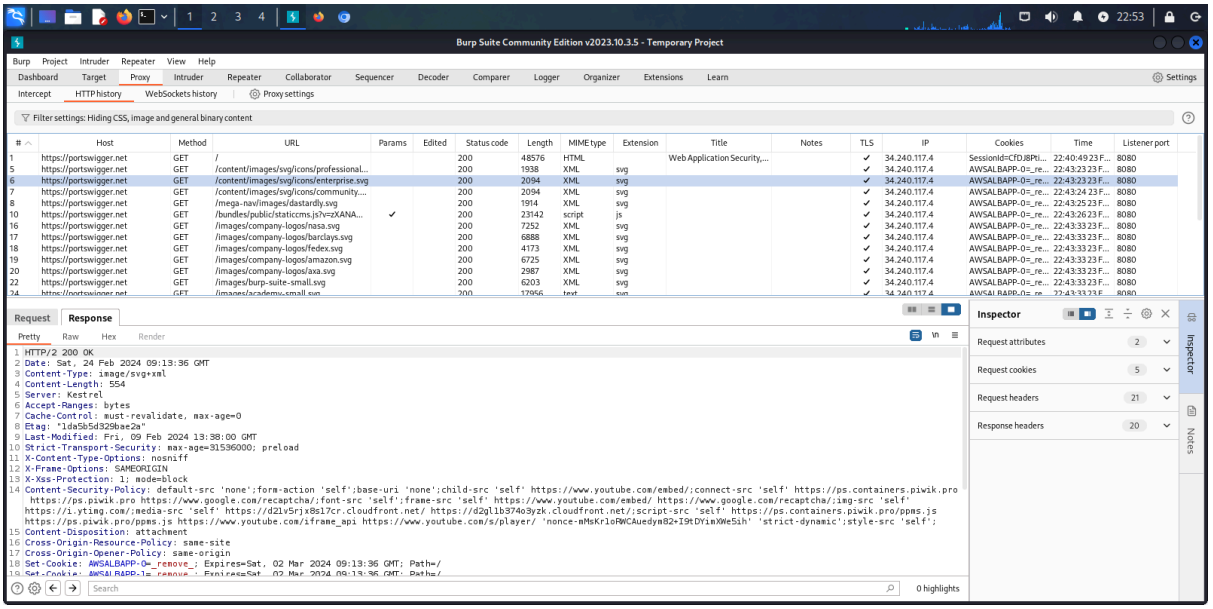
Step 4: Switch off interception: Due to the number of requests browsers typically send, you often won't want to intercept every single one of them. Click the Intercept is on button so that it now says Intercept is off.
Go back to the browser and confirm that you can now interact with the site as normal.

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.



Screenshot of HTTP request code



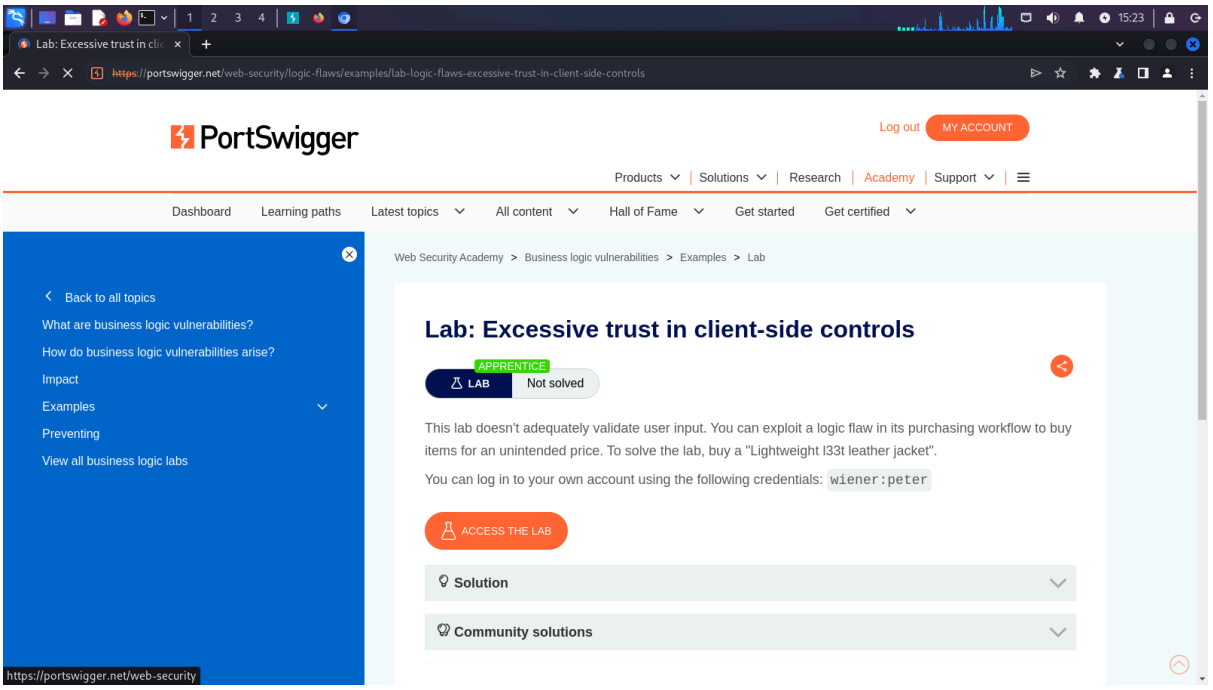
Screenshot of HTTP response code

2. Modifying Requests

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:

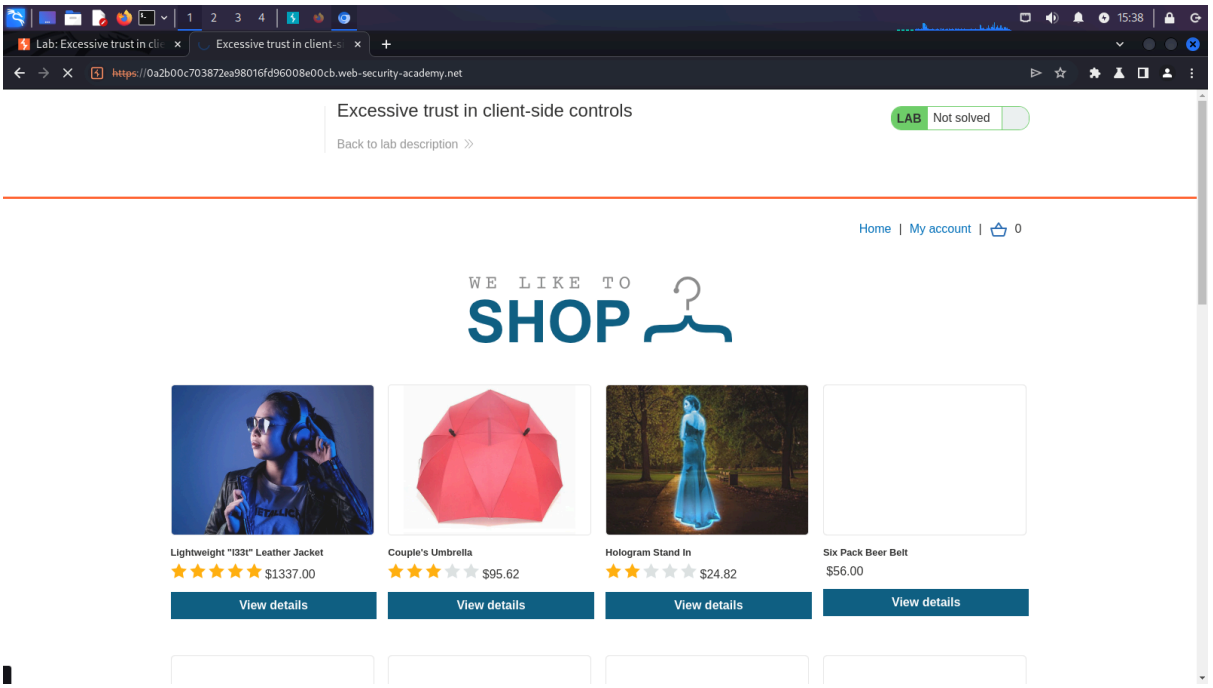
https://portswigger.net/web-security/logic-flaws/examples/lab-logic-flaws-excessive-trust-in-client-side-controls



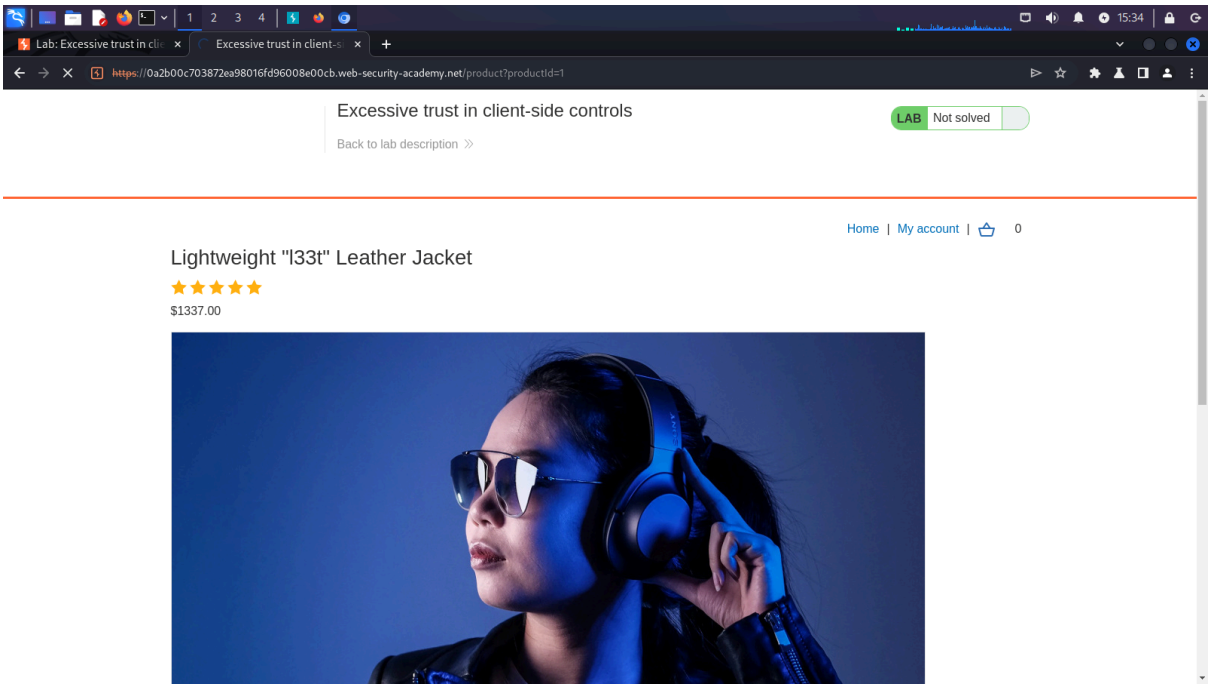
When the page loads, click Access the lab. If prompted, log in to your portswigger.net account. After a few seconds, you will see your own instance of a fake shopping website.

Step 2: Log in to your shopping account

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

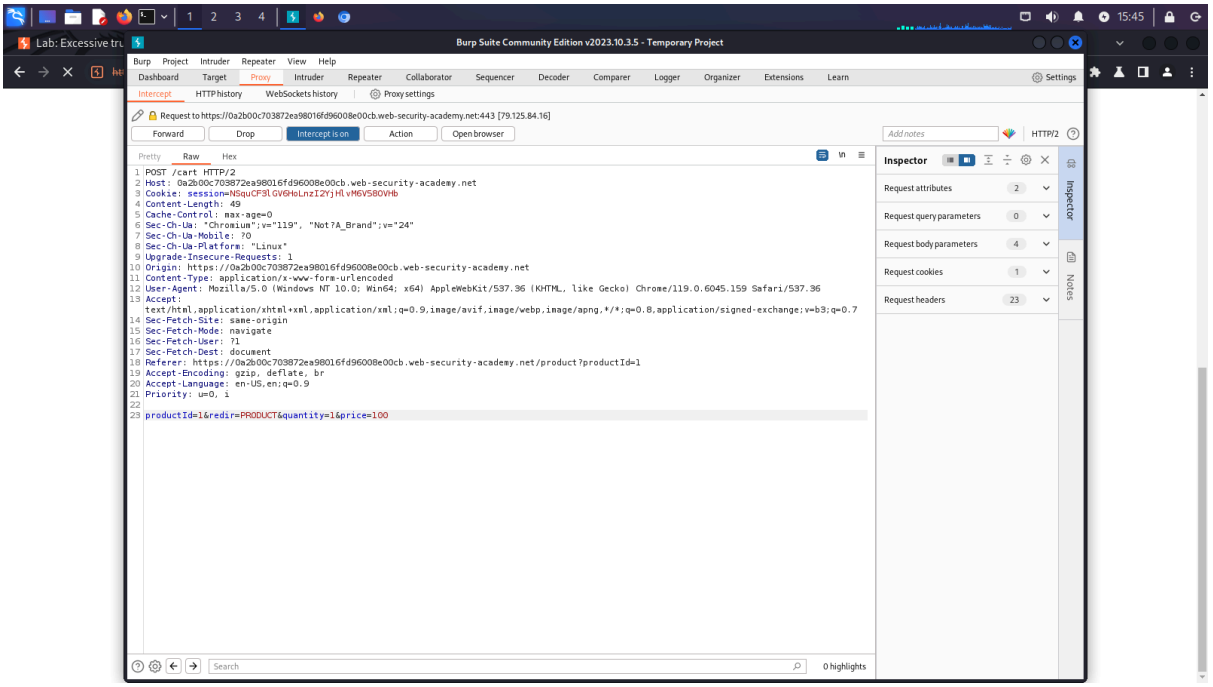


Step 3: Find something to buy: Click Home to go back to the home page. Select the option to view the product details for the Lightweight "l33t" leather jacket.



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.

Step 5: Modify the request: Change the value of the price parameter to 100(1$) and click Forward to send the modified request to the server.
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.
Click the Place order button to purchase the jacket for an extremely reasonable price.