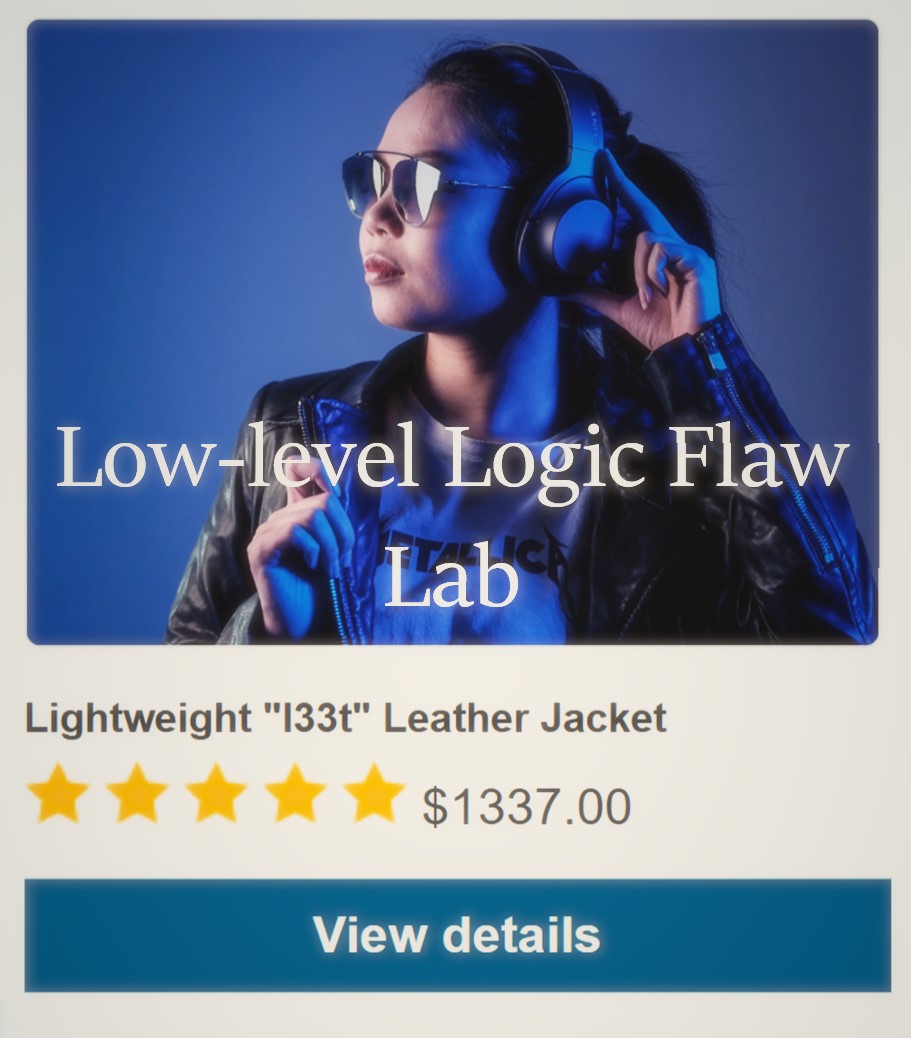
**September 20th’**

**(IS 401/501-01 MERGED) (FA23) CYBERSECURITY PRINCIPLES**

**Burp Suite: Lab: Low-level Logic Flaw**

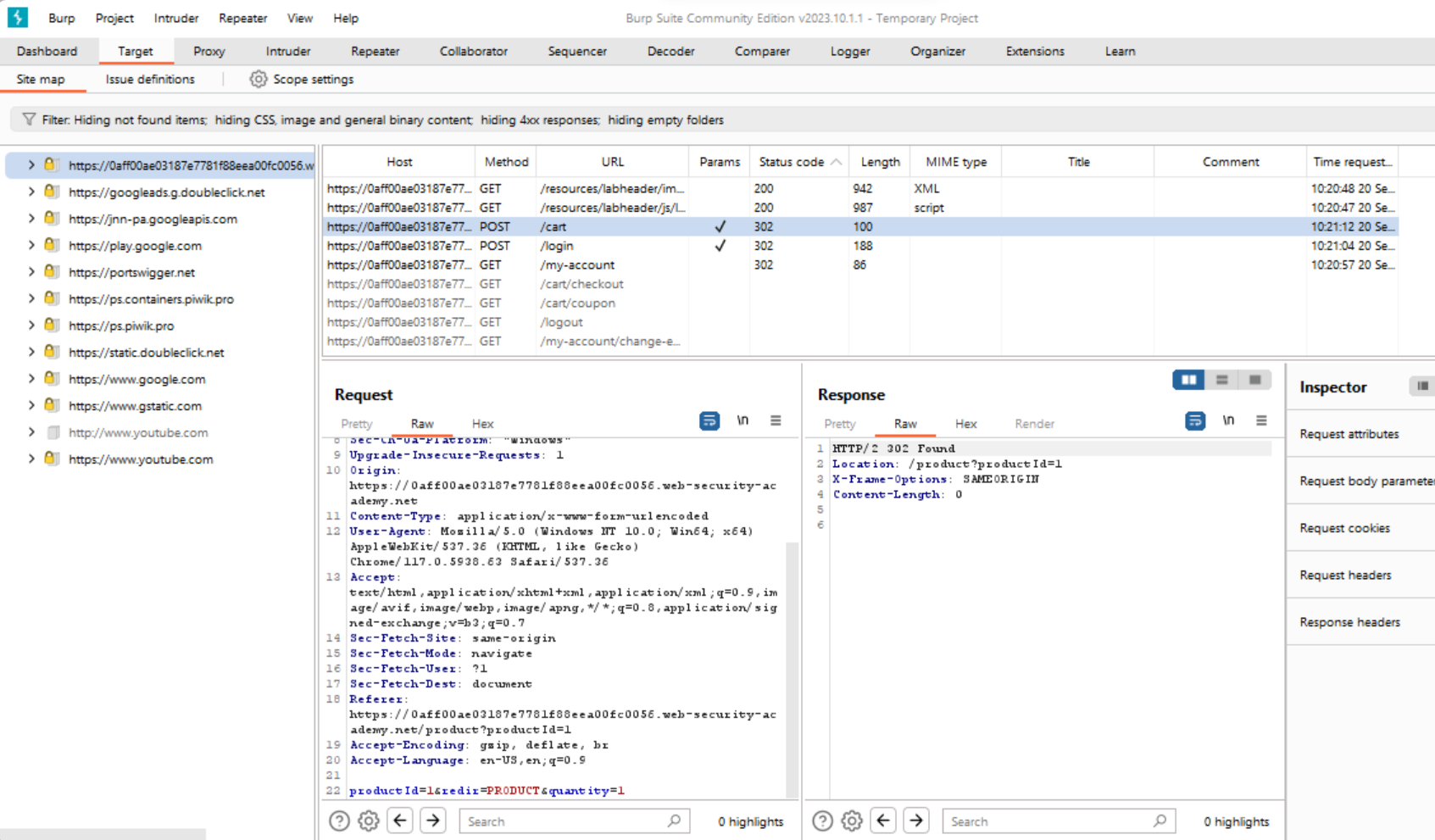
**Pod 6**

**Aayushi Bhatia, Frances Brandofino, Elsa Gilsdorf, Amogh Patel**

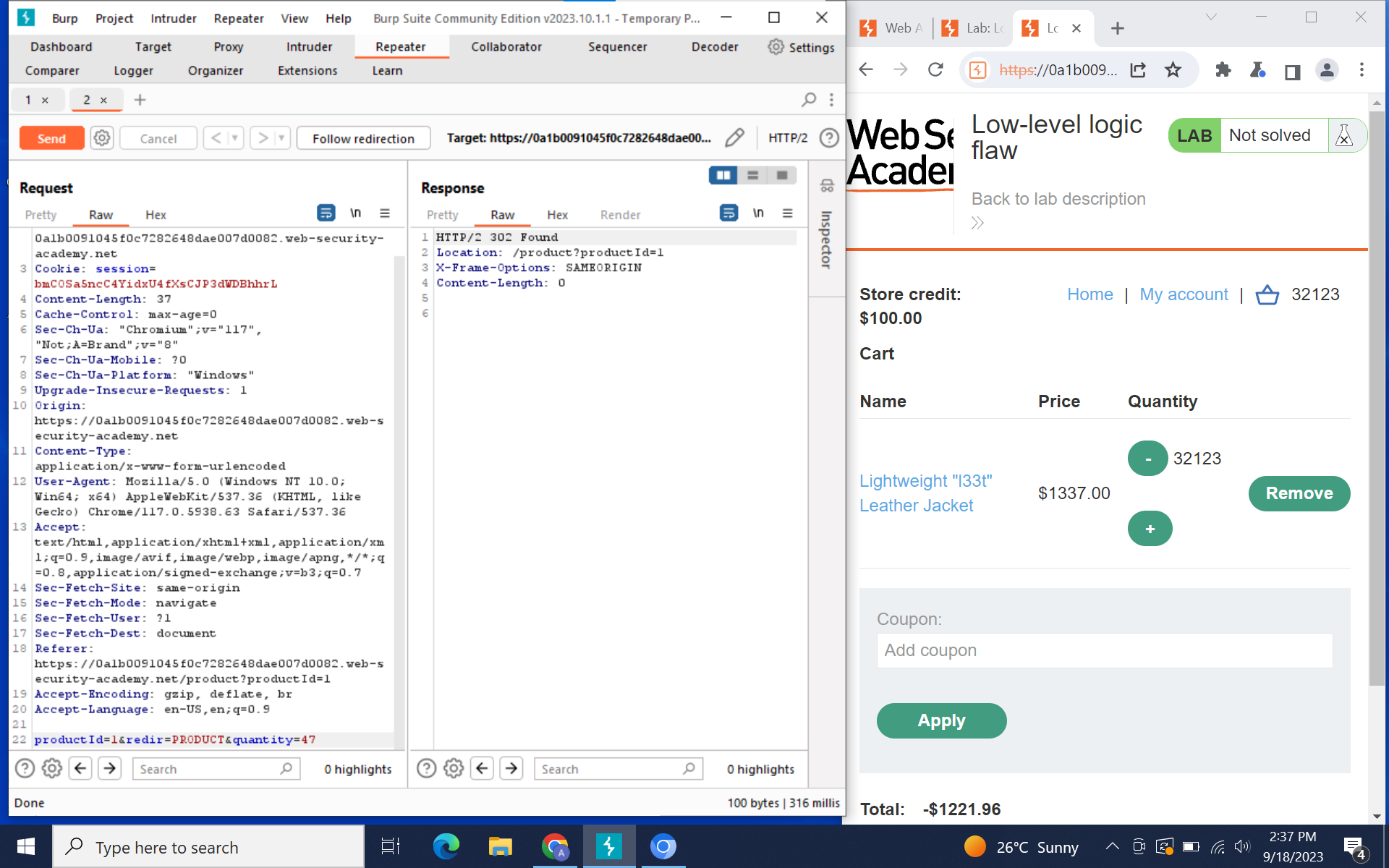
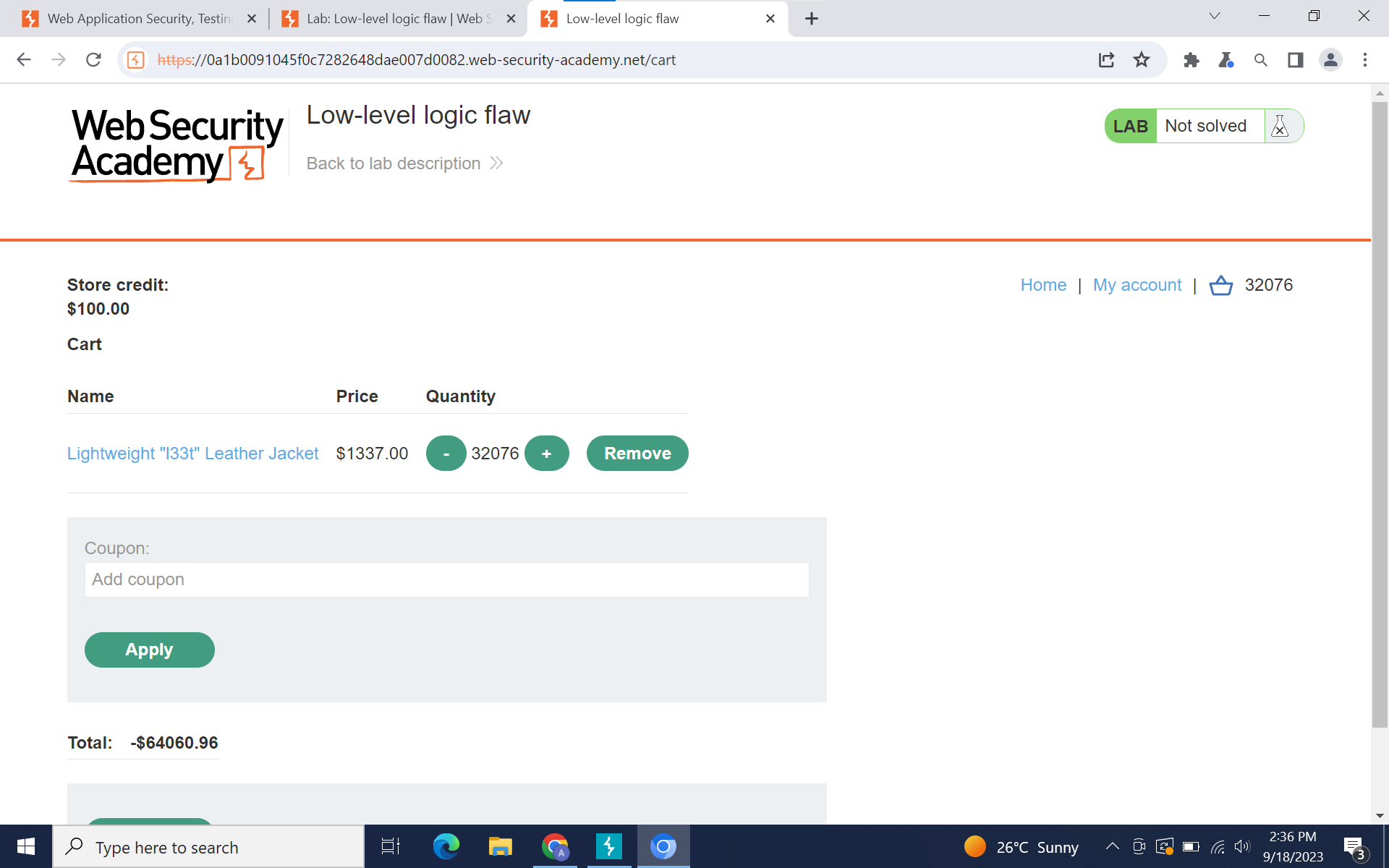


**Instructions:**

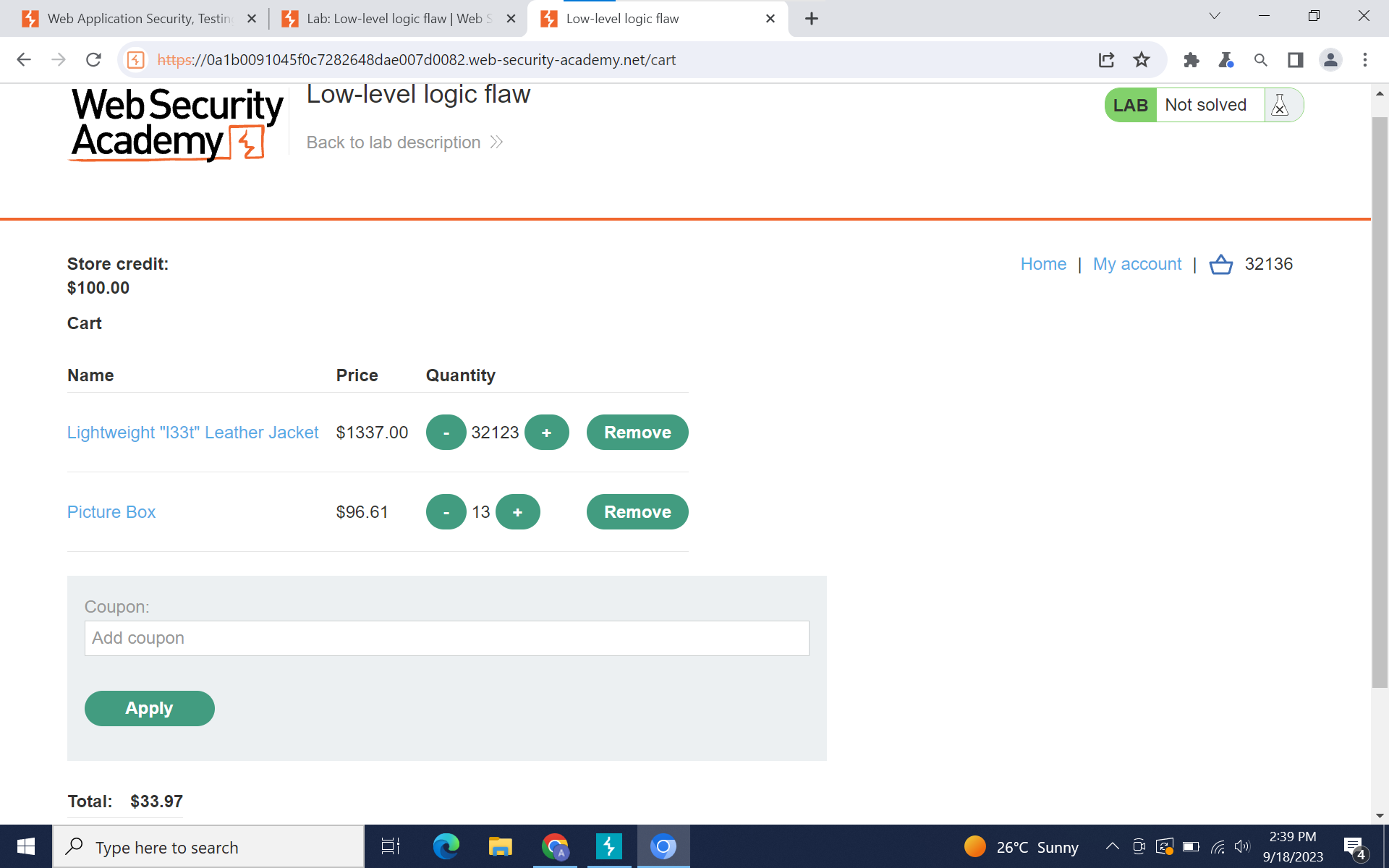
Download the Burp Suite program and open the ‘Target’ tab in Burp Suite. Then to solve the lab, open the browser in the ‘Target’ tab and paste in the URL to access the “Low-level Logic Flaw Lab”. Once you have signed into the lab, buy a "Lightweight l33t leather jacket". Click on the “Lightweight l33t leather jacket” and add to cart. Then, return to the ‘Target’ tab and select the first URL listed on the top left side and scroll through the host’s methods until you find the ones that specify “**POST**”. Click on the URL section “**/cart**” and then, left click on the data appearing in the request section and select “**Send to Repeater**”. The next step is to navigate to the ‘Repeater’ tab.



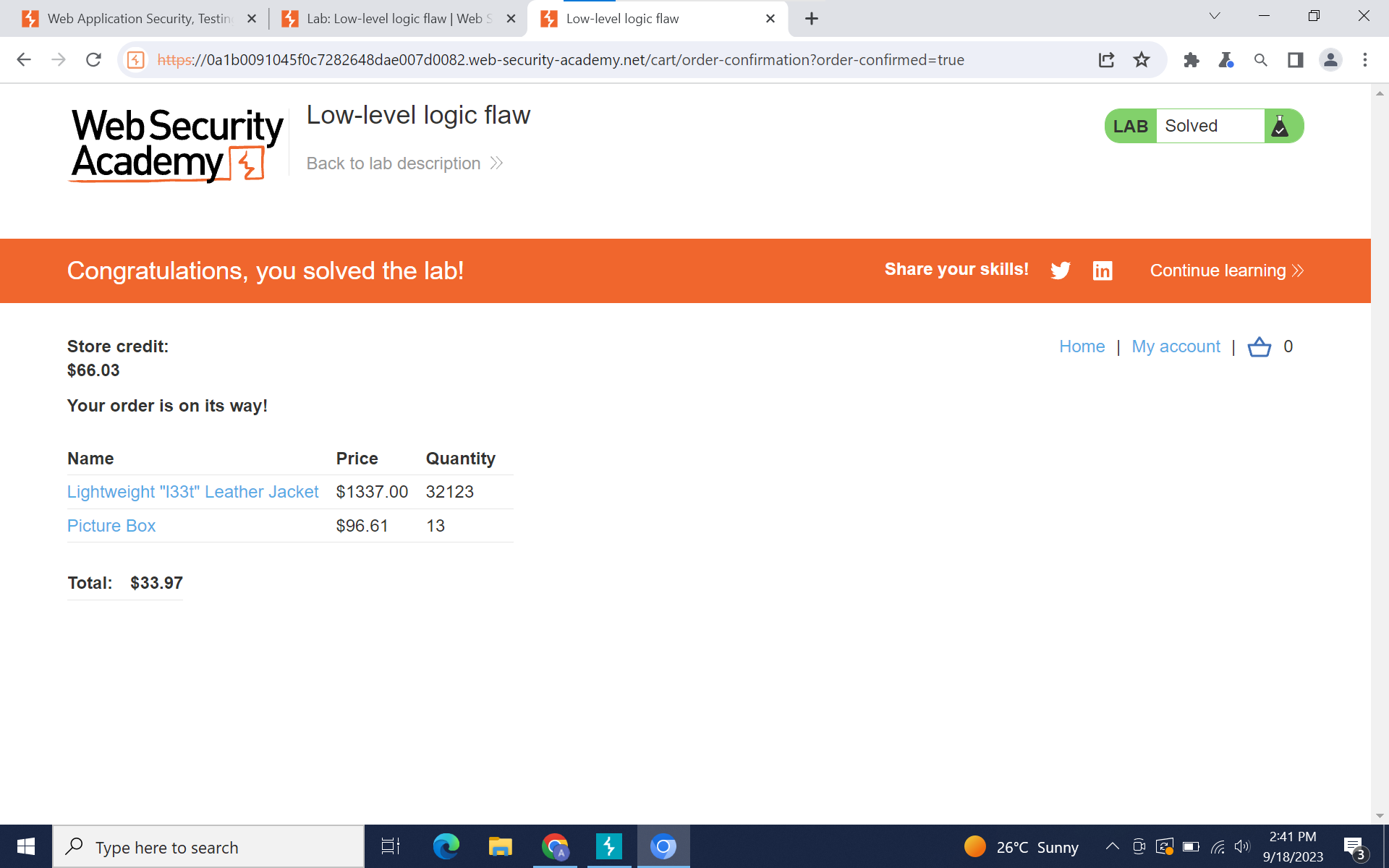
Inside Burp Suite, there should be a tab labeled ‘Repeater’. Inside the request section, find a line labeled ‘**productID=1&redir=PRODUCT&quantity=1**’. After editing the amount, by any number (such as 47), left click and select “**Send to Intruder**”. Then proceed to the ‘Intruder’ tab and to the ‘Payloads’ subtab. In the ‘Payloads type’ section, choose **“Null Payloads”**. Then, choose to have the section run indefinitely (or generate a specific amount of payloads). Once this is done, select the ‘Start attack’ button and begin refreshing the browser page. You will then see the price go up, then fall into the negative numbers.



At this point, return to the store and buy another item that can ‘balance out’ this negative number. The goal is to buy enough that your total is positive, but not above your credit amount (which is $100.00).



Afterwards, select Place Order to complete the lab.



**Help used:**

<https://www.youtube.com/watch?v=KDpzutmW31c>

<https://medium.com/@d.harish008/business-logic-vulnerabilities-low-level-logic-flaw-f308a21a945d>

**Explanation:**

This exploit works on integer overflow. Integer overflow occurs when the result of an arithmetic operation on integers exceeds the range that can be represented by the data type used to store those integers. This typically happens in programming languages that use fixed-size integer types, where there is a maximum and minimum value that an integer can hold.

For example, consider a hypothetical 8-bit signed integer, which can hold values from -128 to 127. If you attempt to add 127 and 2 together, the result would be 129, which is outside the valid range for an 8-bit signed integer. In this case, integer overflow occurs, and the result will "wrap around" or "overflow" back to the minimum value of -128. This behavior can lead to unexpected and incorrect results in your programs.

**Division of Labor Report:**

**Write Up -** Amogh Patel, Frances Brandofino

**Formatter -** Elsa Gilsdorf

**Burp Suite Operator -** Amogh Patel, Aayushi Bhatia