Burp Suite Lab

Low-Level Logic Flaw

IS 401/501

09/18/2023

Group Members:

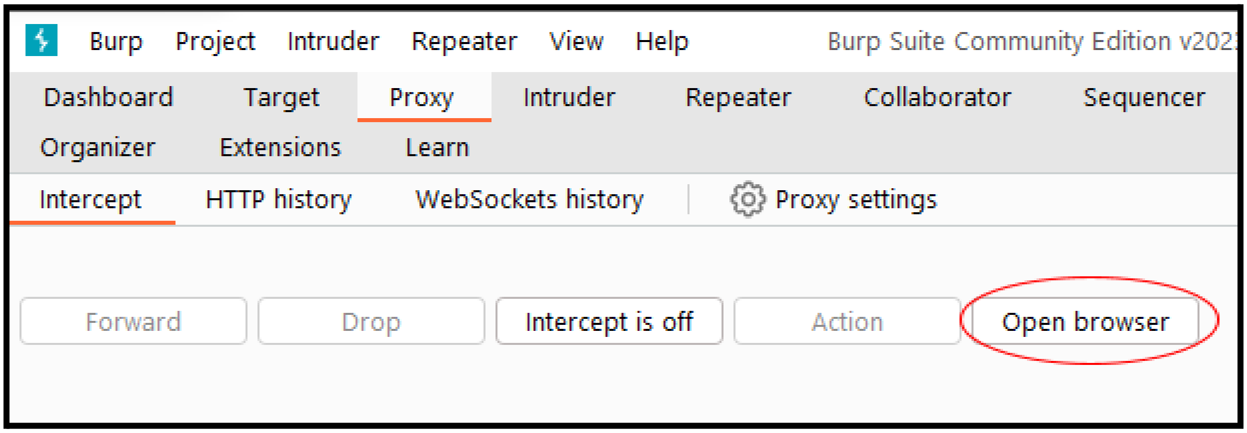
Patrick Doolin, Casen Woody, Isaac Vaillancourt, Josh Catterall,

Isaac Falero, Aaron Thammavongsa

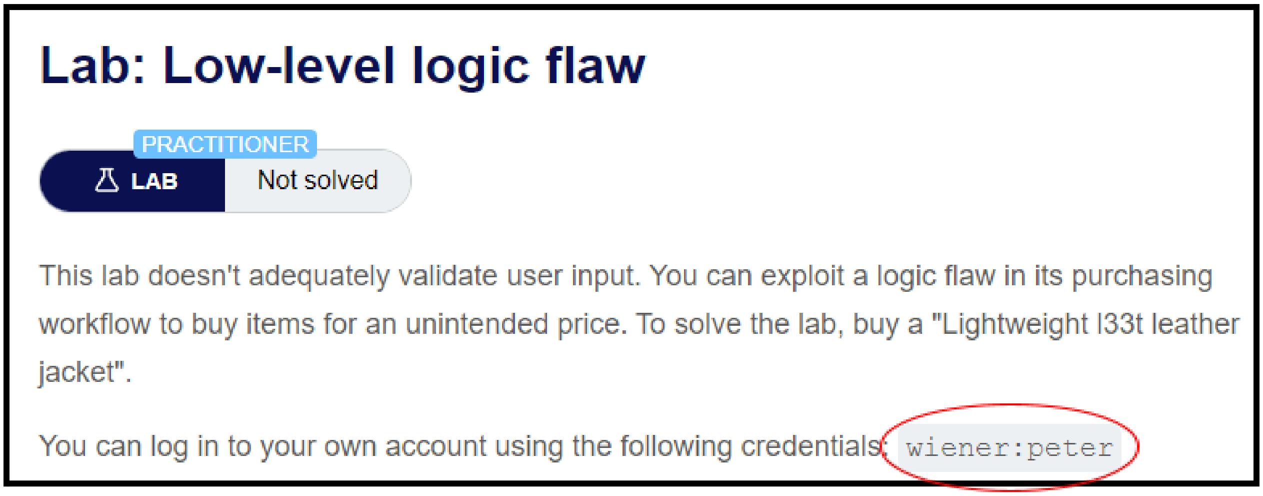
Preface

This lab illustrates a website vulnerability due to a low-level logic flaw. Every programming language has different variable types, with each type possessing a maximum value. In this scenario, we exploit the integer variable’s maximum value to manipulate and bypass the total cart amount using the “quantity” parameter of an HTTP POST request. The following steps demonstrate how we used this strategy to purchase a "Lightweight ‘l33t’ Leather Jacket” for an unintended price:

1. Open Burp Suite, click the “Proxy” tab and then “Open browser.”



2. Log in to your Portswigger account and access the Low-level Logic Flaw Lab. Once the lab is open, click “My Account” and log in using the given credentials.



Lab: Low-level logic flaw

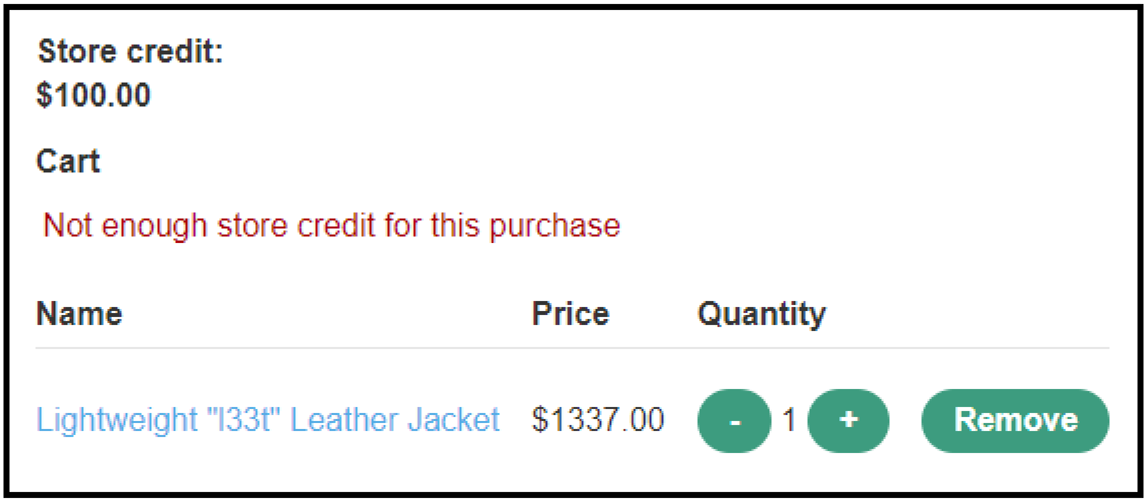
PRACTITIONER

LAB Not solved

This lab doesn't adequately validate user input. You can exploit a logic flaw in its purchasing workflow to buy items for an unintended price. To solve the lab, buy a "Lightweight l33t leather jacket".

You can log in to your own account using the following credentials: `wiener:peter`

3. Go to the main page and add the “Lightweight ‘l33t’ Leather Jacket” to your cart, go to checkout, and press “Place Order”
   - An error message that says “Not enough store credit for this purchase” will pop up.



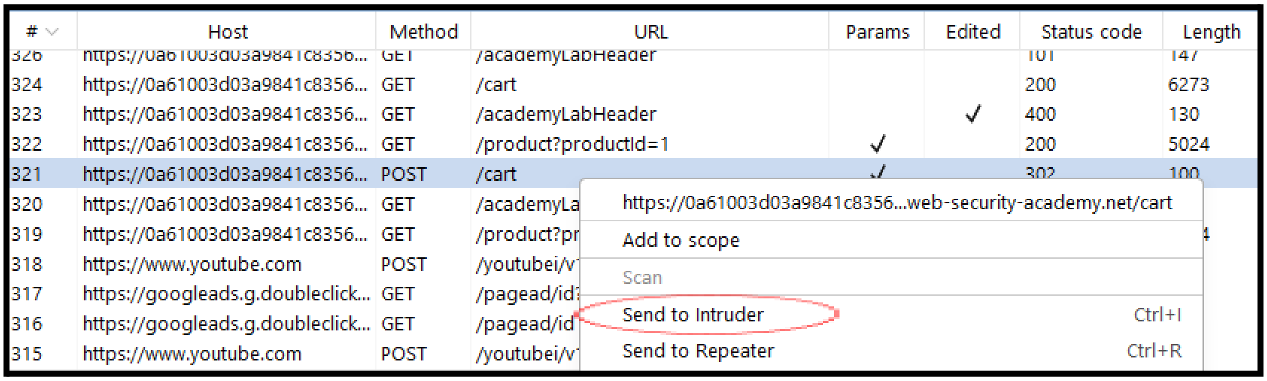
Store credit:
$100.00

Cart

Not enough store credit for this purchase

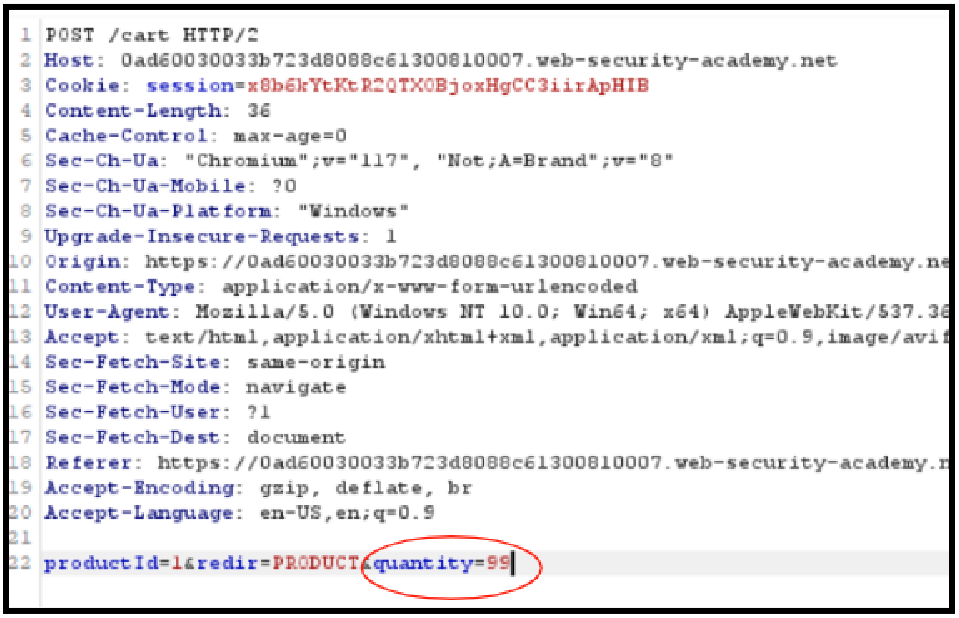
Name	Price	Quantity	
Lightweight "l33t" Leather Jacket	$1337.00	- 1 +	Remove

4. In Burp Suite, open the Proxy tab and send the "POST /cart" request (found within "HTTP history") to Intruder.



#	Host	Method	URL	Params	Edited	Status code	Length
326	https://0a61003d03a9841c8356...	GET	/academyLabHeader			101	147
324	https://0a61003d03a9841c8356...	GET	/cart			200	6273
323	https://0a61003d03a9841c8356...	GET	/academyLabHeader		✓	400	130
322	https://0a61003d03a9841c8356...	GET	/product?productId=1	✓		200	5024
321	https://0a61003d03a9841c8356...	POST	/cart	✓		302	100
320	https://0a61003d03a9841c8356...	GET	/academyLa				
319	https://0a61003d03a9841c8356...	GET	/product?pr				
318	https://www.youtube.com	POST	/youtubei/v				
317	https://googleads.g.doubleclick...	GET	/pagead/id?				
316	https://googleads.g.doubleclick...	GET	/pagead/id				
315	https://www.youtube.com	POST	/youtubei/v				

5. In Intruder:
   a. click the "Positions" tab in payload positions and change value "quantity" from 1 to 99. (99 is the highest value we can change the quantity to, so this change will ensure a more speedy attack time).



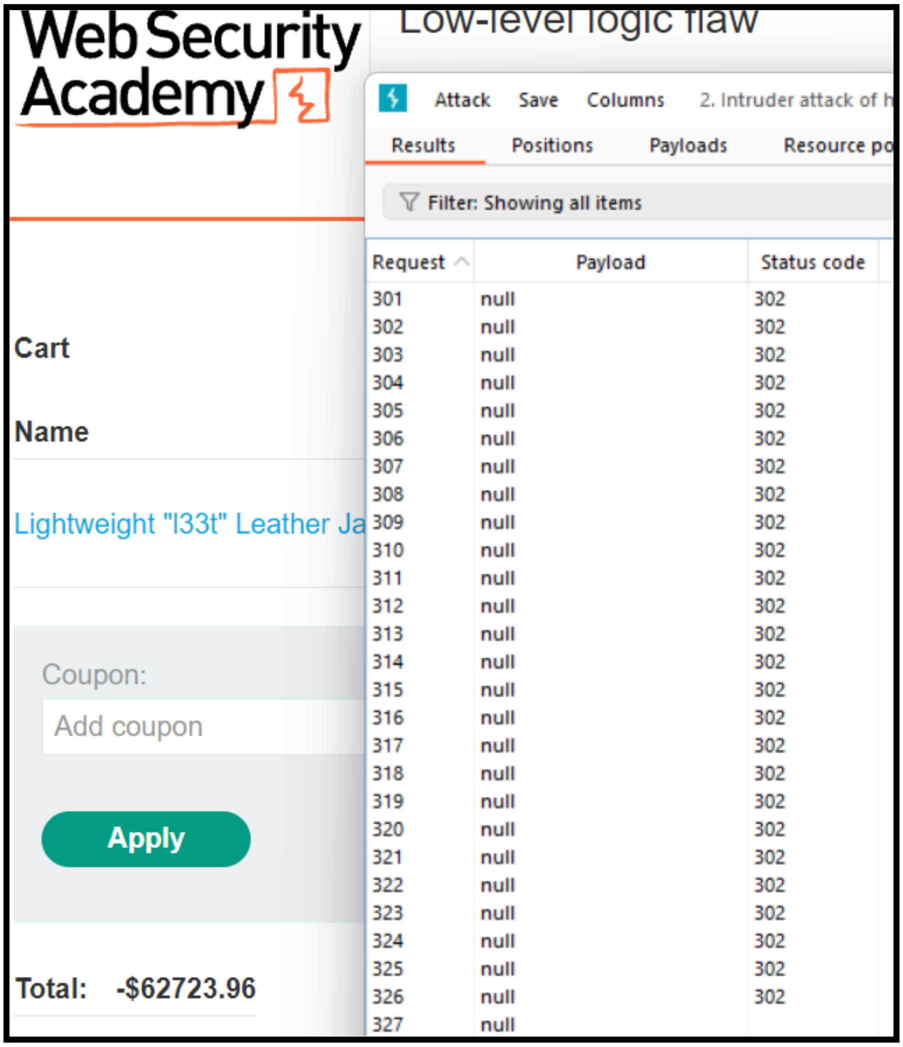
```
POST /cart HTTP/2
Host: 0ad60030033b723d8088c61300810007.web-security-academy.net
Cookie: session=x8b6kYtKtR2QTX0BjoxHgCC3iirApHIB
Content-Length: 36
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="117", "Not;A=Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0ad60030033b723d8088c61300810007.web-security-academy.ne
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ad60030033b723d8088c61300810007.web-security-academy.n
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

productId=1&redir=PRODUCT&quantity=99
```

- **b.** Click the payloads tab and underneath “Payload sets” change the “Payload type” from a “Simple list” to “Null Payloads.” Underneath the “Payload setting” click “Continue indefinitely.”
- **c.** Finally, start the attack.

6. Refresh the lab webpage and notice how the cart total is increasing. Eventually, the cart total will reach its maximum and spill into a negative number. Continue to monitor the price until it reaches -$62,723.96. (If you let the attack continue for too long, then the price will loop back around to a positive number.)

- If you've set up your attack according to this guide, then stop your attack at request 326.



Cart

Name

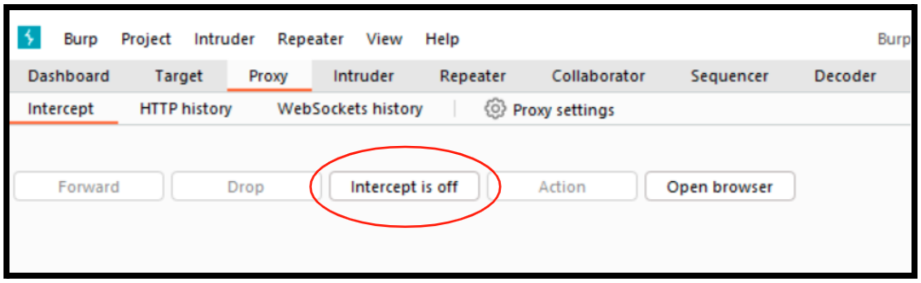
Lightweight "l33t" Leather Ja

Coupon: Add coupon

Total: -$62723.96

Request	Payload	Status code
301	null	302
302	null	302
303	null	302
304	null	302
305	null	302
306	null	302
307	null	302
308	null	302
309	null	302
310	null	302
311	null	302
312	null	302
313	null	302
314	null	302
315	null	302
316	null	302
317	null	302
318	null	302
319	null	302
320	null	302
321	null	302
322	null	302
323	null	302
324	null	302
325	null	302
326	null	302
327	null	

7. In Burp Suite go to the Proxy tab, then select "Intercept." In the lab, click on the link to the "Lightweight 'l33t' Leather Jacket."
   a. Turn on Intercept by clicking the "Intercept is off" button.

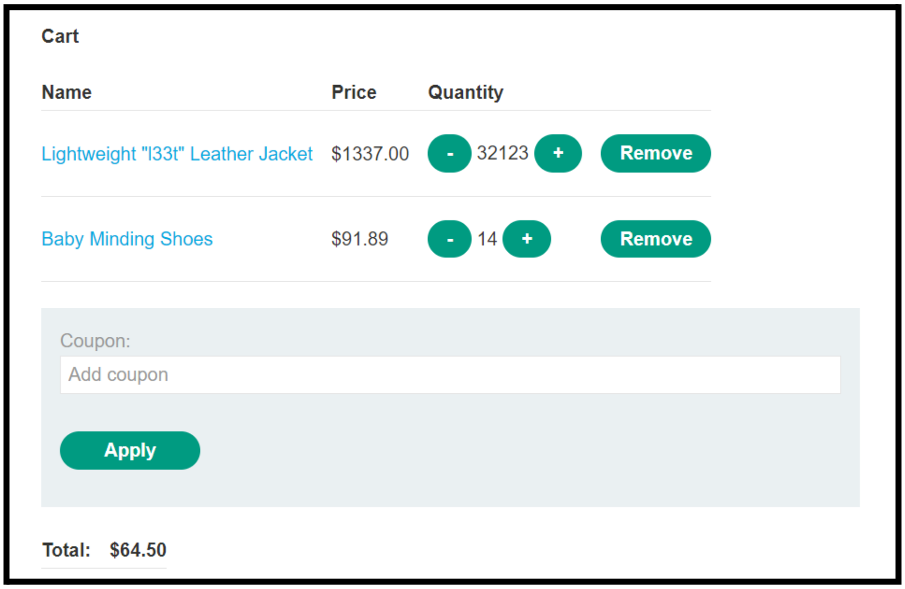


   b. In the lab, add another jacket to your cart.

c. When Burp Suite intercepts the request, change the quantity to 46. This number of jackets gets the value as close to zero as possible without exceeding zero.

d. The value of your cart should be -$1221.96.

8. Now add enough of any item that will get the value of your cart above $0 but below $100, then place your order to complete the lab.



Cart

Name	Price	Quantity	
Lightweight "l33t" Leather Jacket	$1337.00	- 32123 +	Remove
Baby Minding Shoes	$91.89	- 14 +	Remove

Coupon:

Add coupon

Total: $64.50

- The shop changes every time you open the lab, so the product you pick may be different.

Division of Labor

All of the members collaborated to figure out and complete this lab. Documentation and the Preface were finished by Isaac Falero. Isaac Vaillancourt and Casen Woody assisted with documentation and screenshots. Patrick Doolin, Josh Catt, and Aaron Thammavongsa helped with documentation and tested completing the lab using the guide.