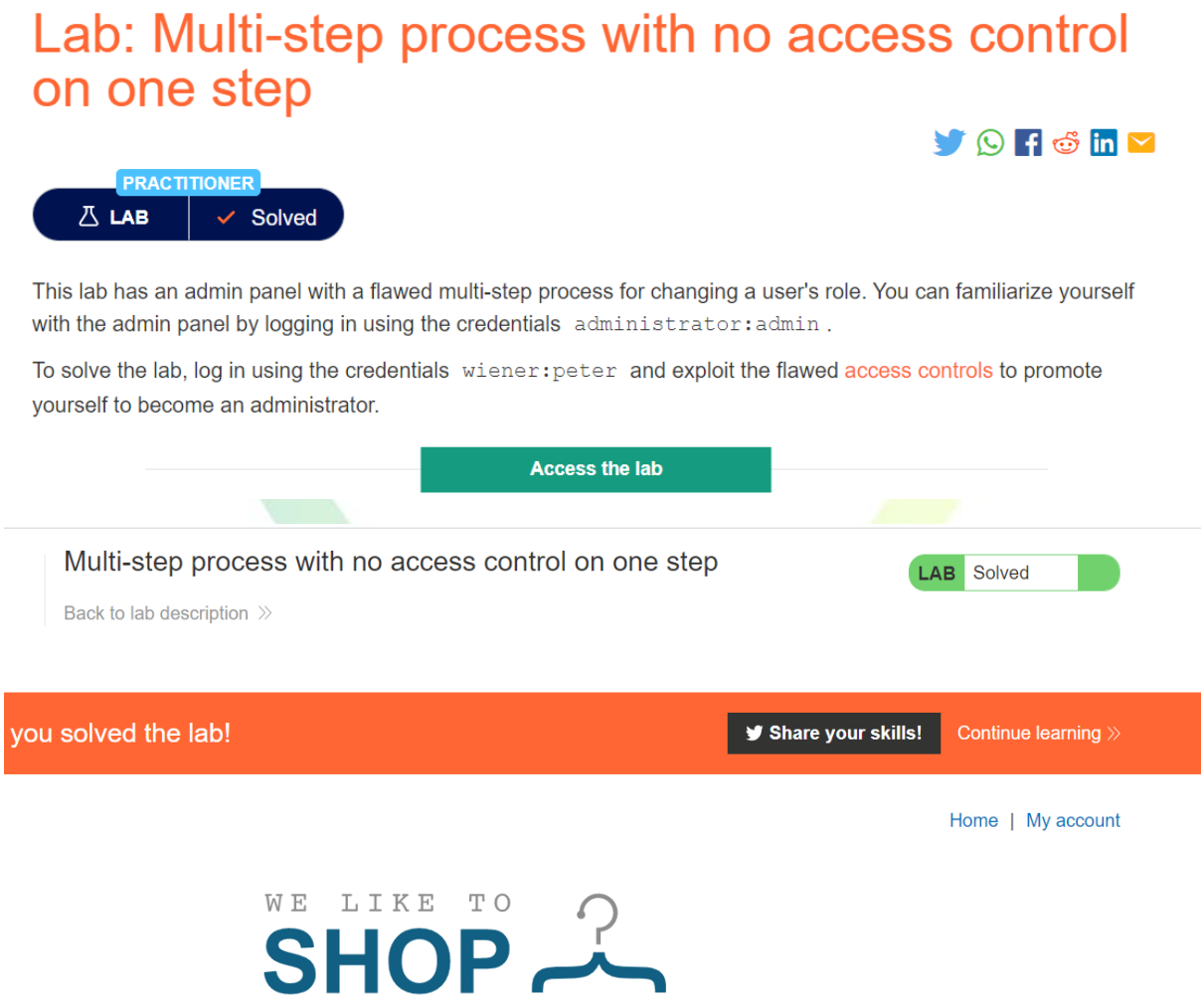
TASK REPORT - SAFE YOUR WEB

Name	Sadiq Sonalkar
Email	sadiqsonalkar21@gmail.com
Submission Date	01-05-2023

Task 5

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



TASK REPORT - SAFE YOUR WEB

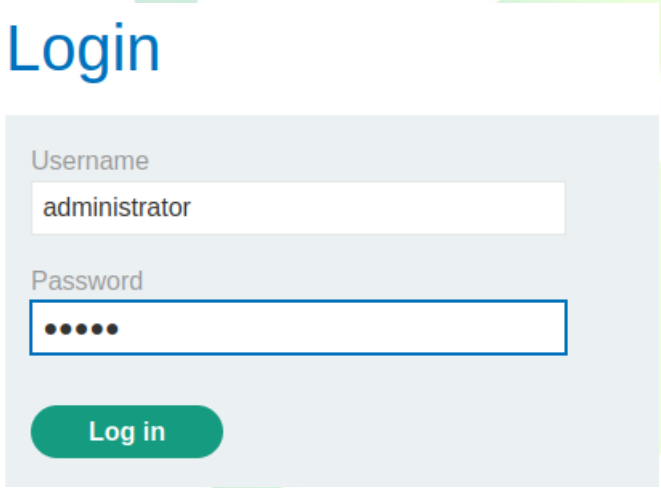
The goal is to exploit the multi-step process in a way so we can change a user's role and use is to promote ourself to become an administrator by exploiting the flawed access controls.

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

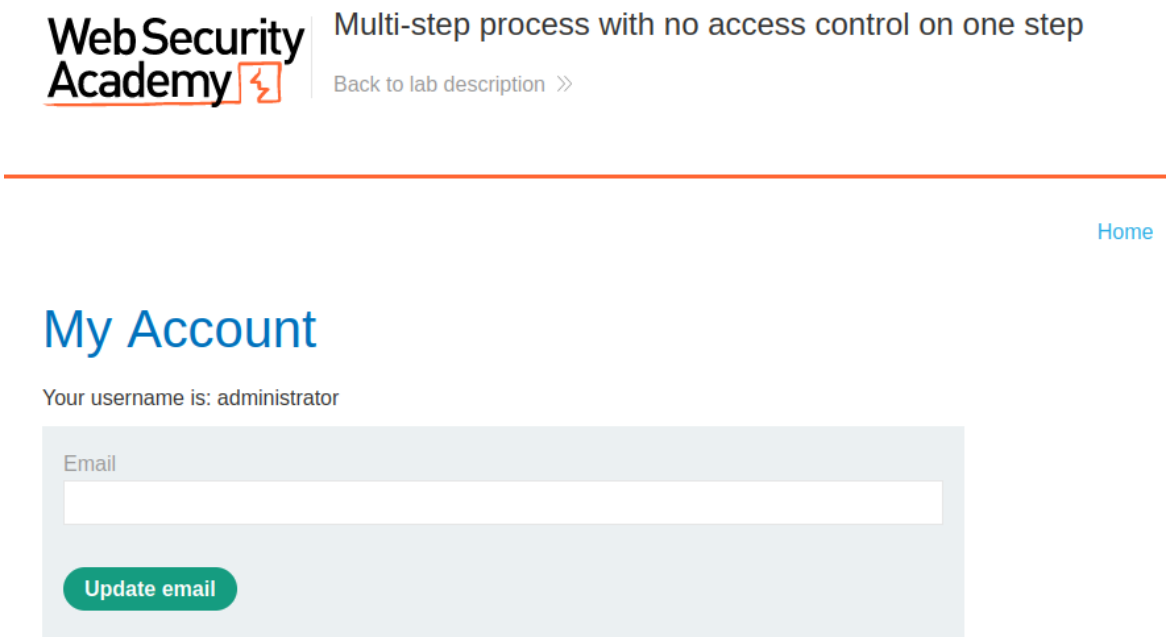
To solve the lab, we will be using the credentials wiener: peter

Make sure the interceptor and the BURP proxy is on.

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



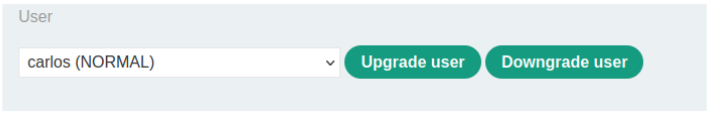
We will land on this page:



TASK REPORT - SAFE YOUR WEB

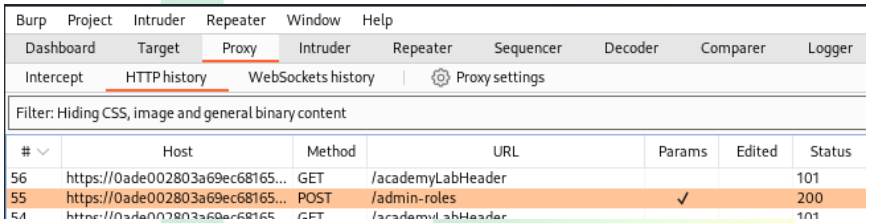
Then we will check admin panel.

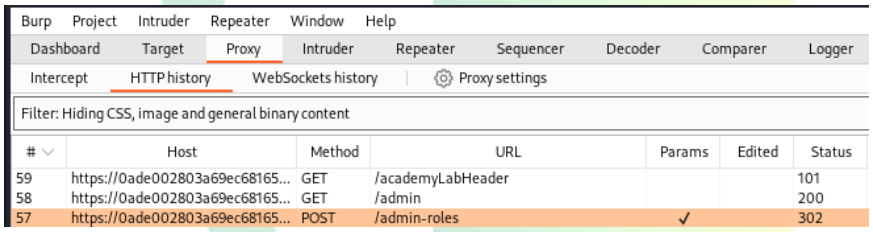
There is a functionality to upgrade or downgrade a user.



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.

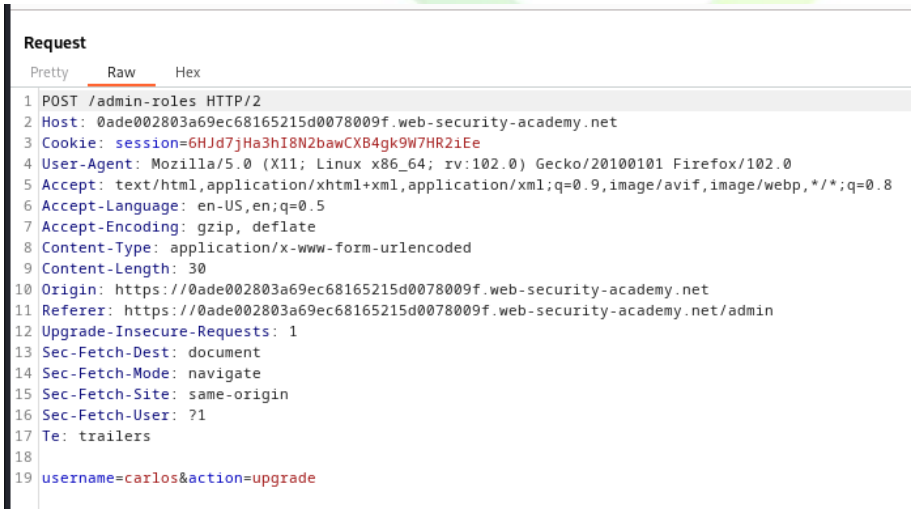




Send both to the repeater.

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:

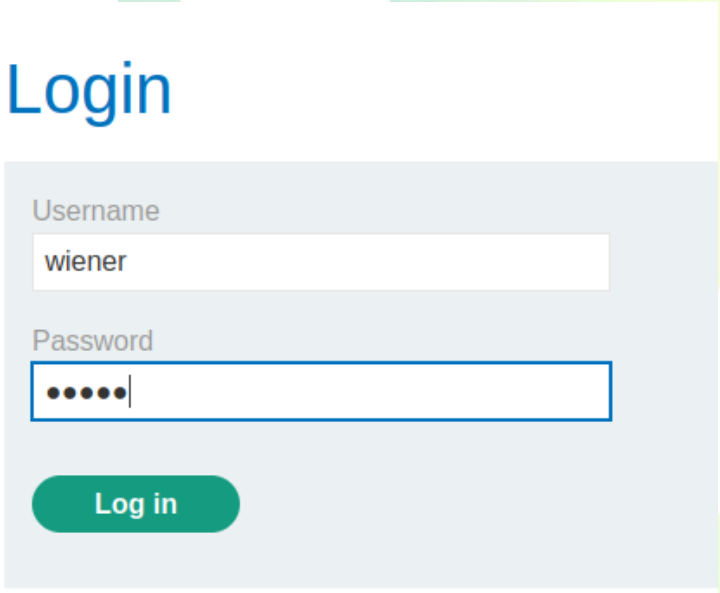


TASK REPORT – SAFE YOUR WEB

The second request is confirmation to upgrade:

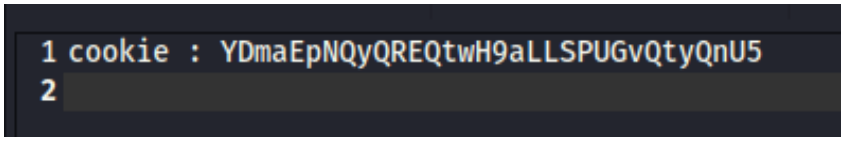
```
Request
Pretty  Raw  Hex
1  POST /admin-roles HTTP/2
2  Host: 0ade002803a69ec68165215d0078009f.web-security-academy.net
3  Cookie: session=6HJd7jHa3hI8N2bawCXB4gk9W7HR2iEe
4  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8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



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.



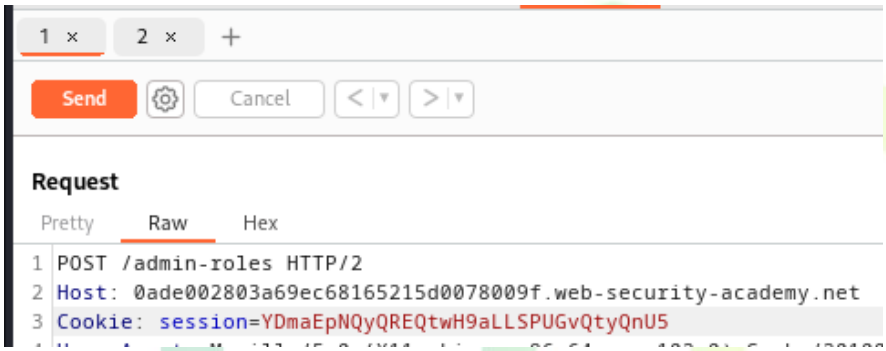
```
1 cookie : YDmaEpNQyQREQtwH9aLLSPUGvQtyQnU5
2
```

TASK REPORT - SAFE YOUR WEB

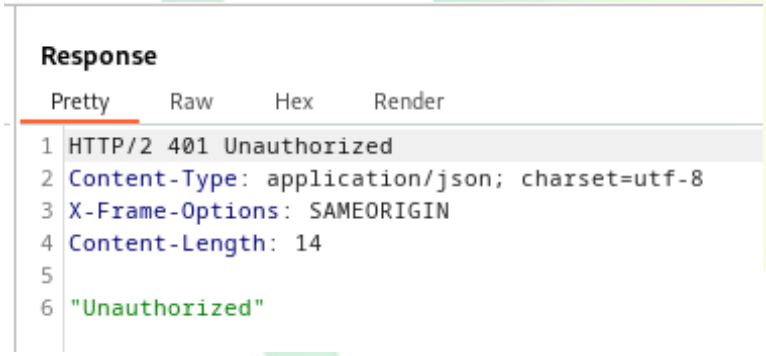
This is the cookie to identify the user wiener.

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:

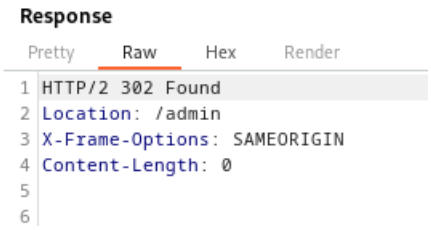


It says its unauthorized which means proper access control rules were set in the first step (i.e., upgrade action).

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

TASK REPORT - SAFE YOUR WEB

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

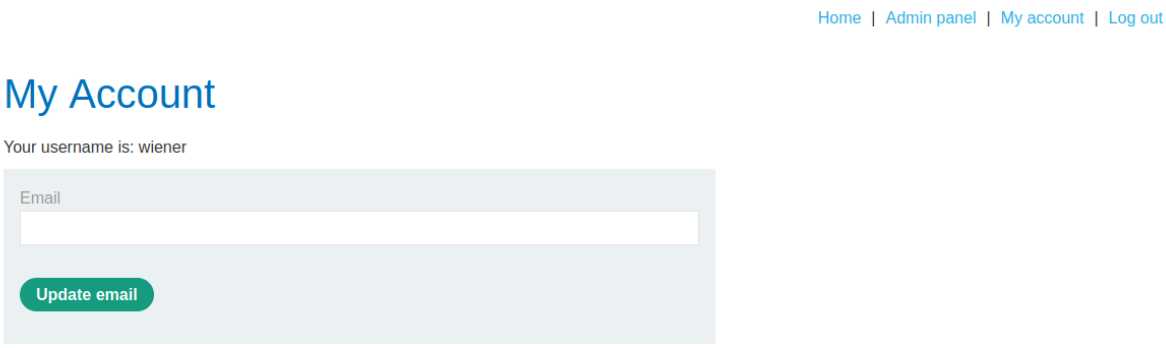


We got a 302 found message. So, which means no proper access control rules were set in the second step (i.e., confirmation to upgrade).

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

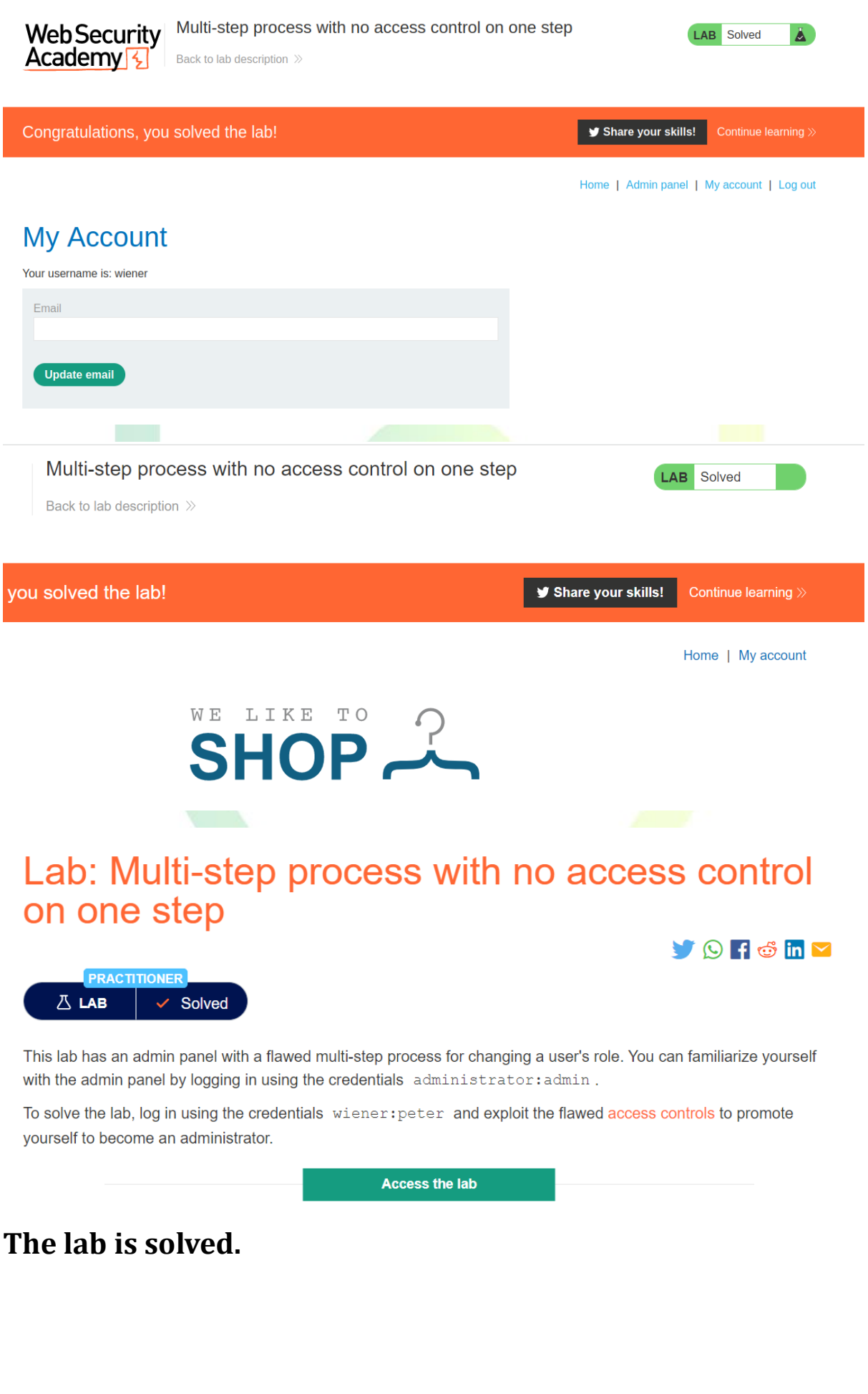
And we got the response, that means user wiener is upgrade to administrator.

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



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

TASK REPORT - SAFE YOUR WEB



The lab is solved.