Artem Volokyta

Software Security

Lab Work 4

OAuth2-ClientCredentialsFlow

kulubecioglu Mehmet

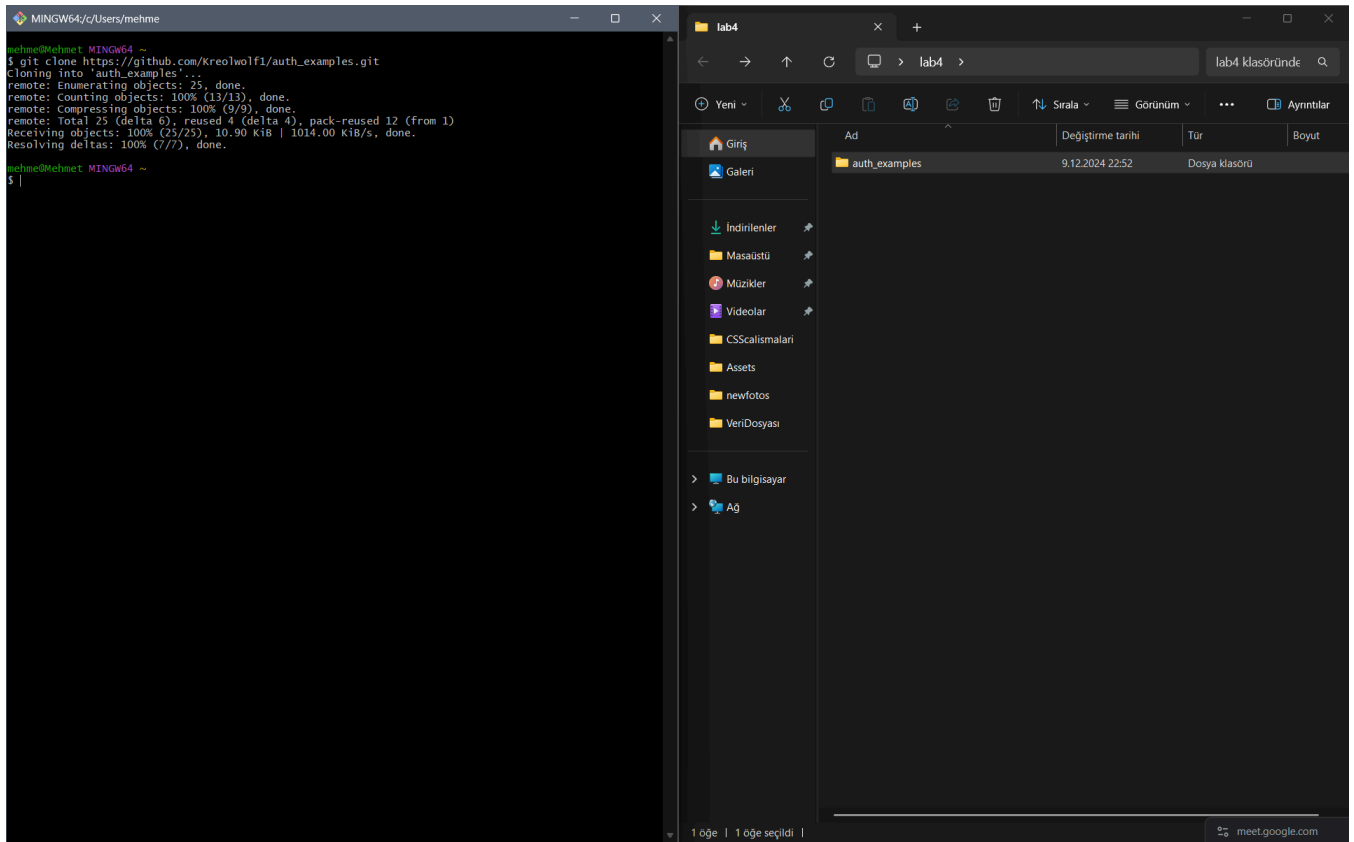**Class Number 12**

IM-14 FIOT

Kyiv

IHORY SIKORSKY KYIV POLYTECHNIC INSTITUTE

2024

LAB4.1

File cloning using MINGW

First, I downloaded the necessary files to my computer from github and created an empty folder and named it lab4. Then I pasted the "git clone - github link" on the right side to the computer and the folders in github were cloned to lab4.

Go to basic_auth and run index.js

Then I opened Windows cmd and installed express with "npm install express" to easily open "basic_auth > index.js."

```
Komut İstemi - node index.js   ×   +   ∨
Microsoft Windows [Version 10.0.26100.2454]
(c) Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\mehme>node index.js
node:internal/modules/cjs/loader:1252
  throw err;
  ^

Error: Cannot find module 'C:\Users\mehme\index.js'
    at Function._resolveFilename (node:internal/modules/cjs/loader:1249:15)
    at Function._load (node:internal/modules/cjs/loader:1075:27)
    at TracingChannel.traceSync (node:diagnostics_channel:322:14)
    at wrapModuleLoad (node:internal/modules/cjs/loader:219:24)
    at Function.executeUserEntryPoint [as runMain] (node:internal/modules/run_main:170:5)
    at node:internal/main/run_main_module:36:49 {
  code: 'MODULE_NOT_FOUND',
  requireStack: []
}

Node.js v22.12.0

C:\Users\mehme>npm install express

added 66 packages in 2s

13 packages are looking for funding
  run `npm fund` for details
npm notice
npm notice New patch version of npm available! 10.9.0 -> 10.9.2
npm notice Changelog: https://github.com/npm/cli/releases/tag/v10.9.2
npm notice To update run: npm install -g npm@10.9.2
npm notice
```

Then, I went to the file path of index.js with the cd command and got the port for the index.js file with the "basic_auth node index.js" command.

```
C:\Users\mehme\OneDrive\Masaüstü\lab4\auth_examples\basic_auth>node index.js
Example app listening on port 3000

========================================================

authorizationHeader undefined
```

We opened the localhost 3000 we received in the browser and saw a login panel.

Opening index.js in basic_auth on port 3000
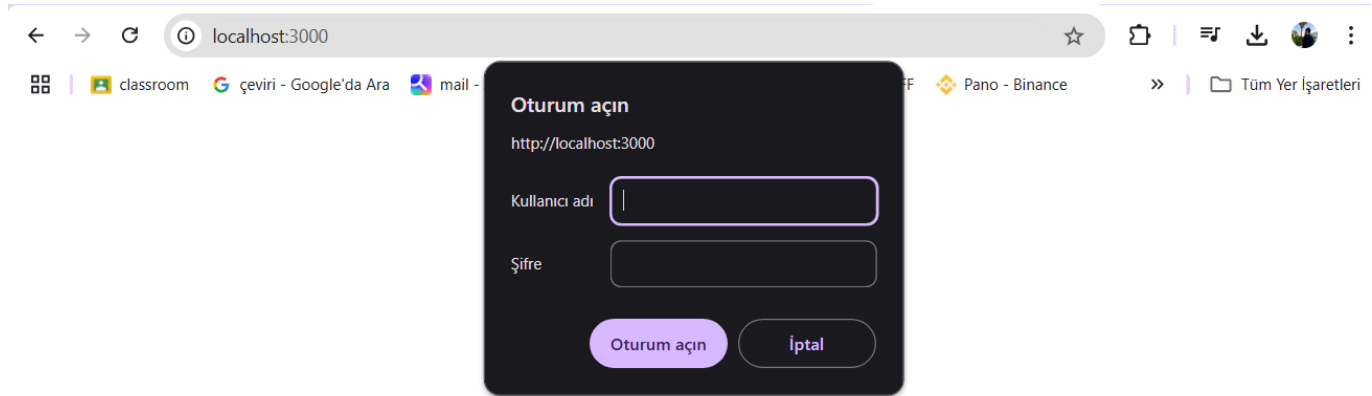
The index you go to after successful login

After logging in, an index with "Hello DateArt" opened.

Hello DateArt

Go to index.js for forms_auth

Then, I went to the file path containing "forms_auth" with the cd command and installed cokie-parser using the "npm install Cookie-parser" command and I used the node index.js command

```
C:\Users\mehme\OneDrive\Masaüstü\lab4\auth_examples\forms_auth>npm install cookie-parser

added 2 packages, and audited 70 packages in 957ms

14 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities

C:\Users\mehme\OneDrive\Masaüstü\lab4\auth_examples\forms_auth>node index.js
Example app listening on port 3000
```

Then a new login page opened

When I logged in incorrectly, it gave an incorrect login warning as follows.

Login

Invalid username
and/or password

haogerog

•••••••

Login

When I logged in correctly, an index page opened as follows.
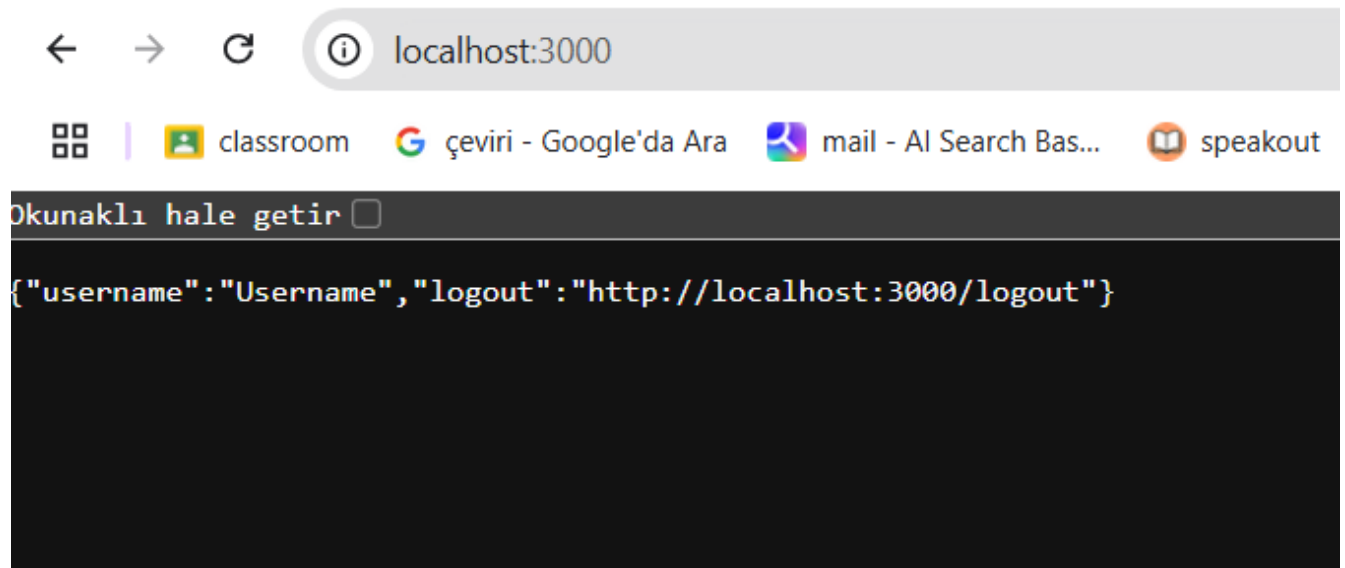
Go to index.js for token_auth

Then I entered token_auth with the "cd .. /token_auth" command and installed the uuid with the "npm install uuid" command and then I installed "express" again and finally I got the port again with the "node index.js" command.

```
C:\Users\mehme\OneDrive\Masaüstü\lab4\auth_examples\forms_auth>cd ../token_auth

C:\Users\mehme\OneDrive\Masaüstü\lab4\auth_examples\token_auth>npm install uuid

up to date, audited 70 packages in 848ms

14 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities

C:\Users\mehme\OneDrive\Masaüstü\lab4\auth_examples\token_auth>npm install express

up to date, audited 70 packages in 783ms

14 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities

C:\Users\mehme\OneDrive\Masaüstü\lab4\auth_examples\token_auth>node index.js
Example app listening on port 3000
```
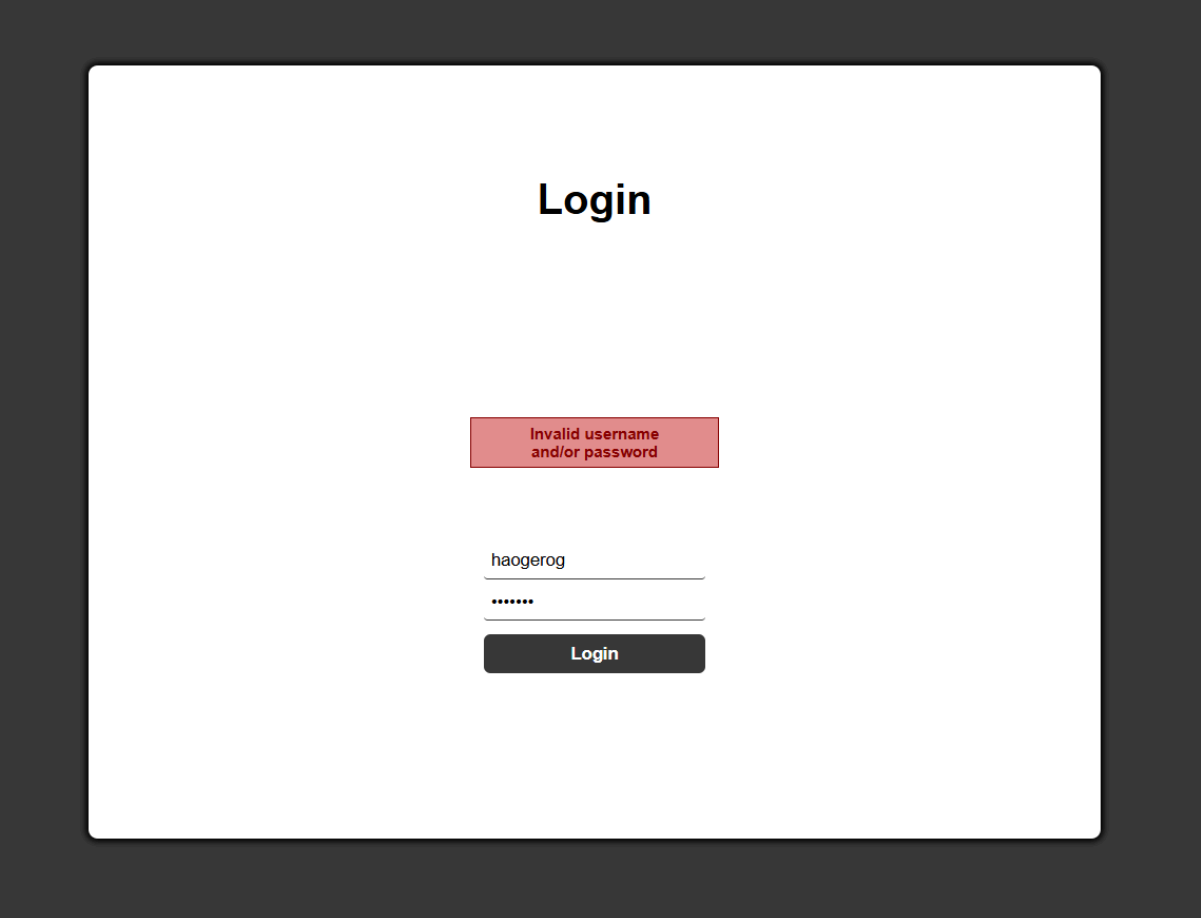
I went to port 3000 and opened the following index
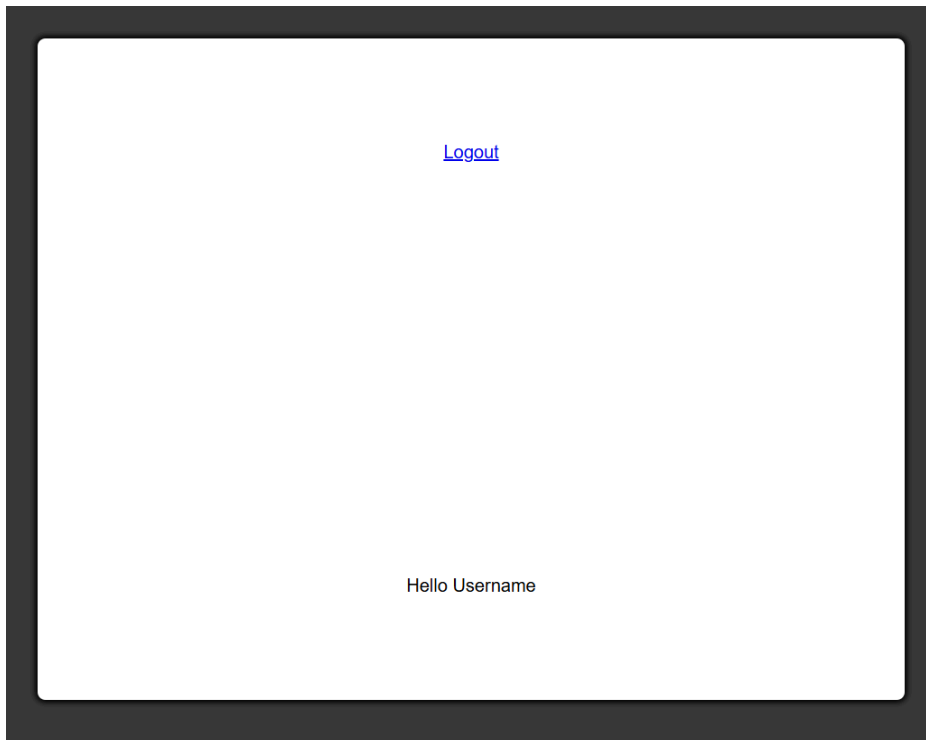
LAB4.2

I created an auth0 account and installed "default application" in it.

I added my own domain, client ID, client secret, etc. information to the necessary parts of the code and transferred a token.

```
13
14
15  curl -L 'https://kpi.eu.auth0.com/api/v2/users' \
16  -H 'Content-Type: application/json' \
17  -H 'Accept: application/json' \
18  -H 'Authorization: Bearer
19  --data-raw '{"email":"user@example.com","phone_n        _verified":false,"phone_verified":::
20
21
22
23
24
25  curl --request POST --url 'https://dev-002vckfqm                        application/x-www-form-urlencoded
26
27
28
29  yw1qtxk54FBPWM2Sjz1UOvDSRuBAioDb
30  https://dev-002vckfqm8dvka6d.us.auth0.com/api/v2
31
32
33
34  curl -L 'https://dev-002vckfqm8dvka6d.us.auth0.com/api/v2/client-grants' -H 'Content-Type: application/json' -H 'Accept: application/json'
35
36
37
38
39  curl --request POST --url 'https://dev-002vckfqm8dvka6d.us.auth0.com/oauth/token' --header 'content-type: application/x-www-form-urlencoded
40
```

Terminal output:
```
h0.com/api/v2/","organization_usage":"deny","allow_any_organization":false,"scop
e":["create:users"]}
$ curl --request POST --url 'https://dev-002vckfqm8dvka6d.us.auth0.com/oauth/tok
en' --header 'content-type: application/x-www-form-urlencoded' --data 'audience=
https://dev-002vckfqm8dvka6d.us.auth0.com/api/v2/&grant_type=client_credentials&
client_id=yPSnydnG99Xf6CO4NOwQXYFLjZIRCPwE&client_secret=kk0JSR6FTx3NQghSjMOiXLc
4jDD7bOb87WoEC4eDAvzpYspDreW5v7aTYquuDfMv'
{"statusCode":401,"error":"Unauthorized","message":"Missing authentication"}
{"access_token":"eyJhbGciOiJSUzIINiIsInR5cCI6IkpXVCIsImtpZCI6IkJkcVk4N3Z3SkprdTh
XcOpxYXdoaiJ9.eyJpc3MiOiJodHRwczovL2Rldi0wMDJ2V2tmcW04ZHZrYTZkLnVzLmF1dGgwLmNvbS
8iLCJzdWIiOiJ5UFNueWRuRzk5WGY2Q2AOTk93UVFZRkxqWk1SQ1B3RUBjbGllbnRzIiwiYXVkIjoiaH
ROcHM6Ly9kZXYtMDAydmNrZnFtOGR2a2E2ZC51cy5hdXRoMC5jb20vYXBpL3YyLyIsImlhdCI6MTczMz
g2MTYwO5w1ZXhwIjoxNzMzOTQ4MDA5LCJzY29wZSI6InJlYWQ6dXNlcnMgdXBkYXRlOnVzZXJzIGRlbG
VOZTp1c2Vycy8jcmVhdGU6dXNlcnMiLCJndHki0iJjbGllbnQtY3JlZGVudGlhbHMiLCJhenAi0iJ5UF
NueWRuRzk5WGY2QzAOTk93UVFZRkxqMklSQ1B3RSJ9.xBsOQaOQCUze5kp4Y2GqlcFSZOgcKI6Ul6wKh
XPVbSeLnLd8rEP_YQCn7lDmOf9o5YrCFDaVN_MKRp4bL2bkve56deU_TYG1yYnqabj9N7prIlI3ioWad
618AR8kSt3W-EeY8N8UO2dx_paA-zMCjAM_sjIoN-zkM2ZFJTsRdTGGBxJYblGp6a_dCm7bS8lYIXP8L
hMUiNPjyByamqqrlSNMghtxjx52cEujSzw8rwwuJYvWoo6Et6OqiGhqH_7QUxpJ7PRKGhJX3ByWQlAML
ZSlBxcPQjRPUku6CM8OjZ-uNJ2JWtluZYSioNCzbWDXYPr9SPdztRLznCrrgCUrHfQ","scope":"read
:users update:users delete:users create:users","expires_in":86400,"token_type":"
Bearer"}
mehme@Mehmet ~
```

Then I created a new user

← Back to Users

ME **memoklbc@icloud.com**
user_id: auth0|67588fe213106cf8e4b5b20e

Actions ⌄

Details   Devices   History   Raw JSON   Authorized Applications   Permissions   Roles

Name	Email	Signed Up
memoklbc@icloud.com	memoklbc@icloud.com VERIFIED	December 10th 2024, 10...
Edit	Edit	

Primary Identity Provider	Latest Login	Accounts Associated
Database	December 11th 2024, 12:...	None

Browser
curl 8.10.1 / Other 0.0.0

Passkeys

Then, I added my password and username, filled in the relevant parts of the code with my own information, and received a new token.

```
mehme@Mehmet ~
$ curl --request POST --url 'https://dev-002vckfqm8dvka6d.us.auth0.com/oauth/token' --header 'content-type: applicatio
n/x-www-form-urlencoded' --data 'grant_type=password&username=memoklbc@icloud.com&password=Mehmet123456789.&audience=h
ttps://dev-002vckfqm8dvka6d.us.auth0.com/api/v2/&scope=offline_access&client_id=yPSnydnG99Xf6CO4NOwQQYFLj2IRCPwE&clien
t_secret=kk0JSR6FTx3NQghSjMOiXLc4jDD7bOb87WoEC4eDAvzpYspDreW5v7aTYquuDfMv'
{"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IkJkcVk4N3Z3SkprdThXc0pxYXdoaiJ9.eyJpc3MiOiJodHRwczovL2Rl
diOwMDJ2Y2tmcW04ZHZrYTZkLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJhdXRoMHw2NzU4OGZlMjEzMTA2Y2Y4ZTRiNWIyMGUiLCJhdWQiOiJodHRwczovL2
Rldi0wMDJ2Y2tmcW04ZHZrYTZkLnVzLmF1dGgwLmNvbS9hcGkvdjIvIiwiaWF0IjoxNzMzODY2MzA3LCJleHAiOjE3MzM5NTI3MDcsInNjb3BlIjoicmVh
ZDpjdXJyZW50X3VzZXIgdXBkYXRlOmN1cnJlbnRfdXNlcl9tZXRhZGF0YSBkZWxldGU6Y3VycmVudF91c2VyX21ldGFkYXRhIGNyZWF0ZTpjdXJyZW50X3
VzZXJfbWV0YWRhdGEgY3JlYXRlOmN1cnJlbnRfdXNlcl9kZXZpY2VfY3JlZGVudGlhbHMgZGVsZXRlOmN1cnJlbnRfdXNlcl9kZXZpY2VfY3JlZGVudGlh
bHMgdXBkYXRlOmN1cnJlbnRfdXNlcl9pZGVudGl0aWVzIG9mZmxpbmVfYWNjZXNzIiwiZ3R5IjoicGFzc3dvcmQiLCJhenAiOiJ5UFNueWRuRzk5WGY2Qz
AOTk93UVFZRkxxqMklSQlB3RSJ9.YAjvVGbsuYBVdbbWHpgHYHOnJSQMYXAPNZcYnLHbO7mL3h76FoqygAvRrKVxlVFRF68Fn-UBEZEEEqdWllDDvDGG7WW
ApHrBVeih1YcNmjMr_il6Yq7s_ggJqr2wAv8F2eIi1gC3cXD37VoOnxl7FiX_i6kfcEiLCxX9sV-brmQjxGHuqRacoeaOJDQd31ojmFXJ7mL4Y7DjOuHtE
ioBvRNA8pNW2TzzPNM6NVSFw24k59hmwdVsDhceu-NIBQQXuRixFodEng4yg8sSzg6Ny-KY83X7d7MJDkSN7ov2sro7dUxEftvOY-mrTI-1doNmM1FQFpv
7TD1Nfgd4f-Y-kw","refresh_token":"c-tC7dDF7CyUYaFcYaXR_RNWPh1NtHSntdH3Co4QAR1nL","scope":"read:current_user update:cur
rent_user_metadata delete:current_user_metadata create:current_user_metadata create:current_user_device_credentials de
lete:current_user_device_credentials update:current_user_identities offline_access","expires_in":86400,"token_type":"B
earer"}
mehme@Mehmet ~
$
```

Then, after receiving the refresh_token, I added it to the relevant sections of the code.

```
mehme@Mehmet ~
$ curl --request POST --url 'https://dev-002vckfqm8dvka6d.us.auth0.com/oauth/token' --header 'content-type: application/x-www-
form-urlencoded' --data 'grant_type=refresh_token&client_id=yPSnydnG99Xf6CO4NOwQQYFLj2IRCPwE&client_secret=kk0JSR6FTx3NQghSjMO
iXLc4jDD7bOb87WoEC4eDAvzpYspDreW5v7aTYquuDfMv&refresh_token=c-tC7dDF7CyUYaFcYaXR_RNWPh1NtHSntdH3Co4QAR1nL'
{"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IkJkcVk4N3Z3SkprdThXc0pxYXdoaiJ9.eyJpc3MiOiJodHRwczovL2Rldi0wMDJ2
Y2tmcW04ZHZrYTZkLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJhdXRoMHw2NzU4OGZlMjEzMTA2Y2Y4ZTRiNWIyMGUiLCJhdWQiOiJodHRwczovL2Rldi0wMDJ2Y2tmcW
04ZHZrYTZkLnVzLmF1dGgwLmNvbS9hcGkvdjIvIiwiaWF0IjoxNzMzODY3MDk0LCJleHAiOjE3MzM5NTM0OTQsInNjb3BlIjoicmVhZDpjdXJyZW50X3VzZXIgdXBk
YXRlOmN1cnJlbnRfdXNlcl9tZXRhZGF0YSBkZWxldGU6Y3VycmVudF91c2VyX21ldGFkYXRhIGNyZWF0ZTpjdXJyZW50X3VzZXJfbWV0YWRhdGEgY3JlYXRlOmN1cn
JlbnRfdXNlcl9kZXZpY2VfY3JlZGVudGlhbHMgZGVsZXRlOmN1cnJlbnRfdXNlcl9kZXZpY2VfY3JlZGVudGlhbHMgdXBkYXRlOmN1cnJlbnRfdXNlcl9pZGVudGl0
aWVzIG9mZmxpbmVfYWNjZXNzIjpbInJlZnJlc2hfdG9rZW4iLCJwYXNzd29yZCJdLCJhenAiOiJ5UFNueWRuRzk5WGY2QzAOTk93UVFZRkxxqMklSQlB3RS
J9.j6poVzBAcTBcXWZOywq2DYZkk3GepIFQTdKdqoUfhEX_YEWkrM7yw6MMs64zrVprOuMv_h61iYwHoiLOufg8UuQ5KBVFd4y5-co8Sp_nzDi_aSBraRAErWqgxXr
E9CBQbgdJ7Rlu5HdVndJS5c4k5d8DoIVEEoWwxSyVQphZEa_29tuVNlWRrlKi4RtLE_bXQ-RQgl3pp7wY3euDtwFXuMoKIPZjtm6JI6mctSFyBcheXze5Ybb83Jn95
zTVx5GPR2zOV72c8Sr-B6ZxNpTdz6UrHgsgJYxScdtGJqRhTG_eDYrfTxd5Y103z5xK_yQWecmGG5GvFkbbqA8VkhVPfw","scope":"read:current_user upda
te:current_user_metadata delete:current_user_metadata create:current_user_metadata create:current_user_device_credentials dele
te:current_user_device_credentials update:current_user_identities offline_access","expires_in":86400,"token_type":"Bearer"}
mehme@Mehmet ~
$
```

Finally, I checked the account to check the accuracy of all transactions with user management > user.

Users

[+ Create User]

An easy to use UI to help administrators manage user identities including password resets, creating and provisioning, blocking and deleting users.
Show more ›

Q Search for users	Search by: User	× Reset

Name	Connection	Logins	Latest Login ˅	
ME memoklbc@icloud.com memoklbc@icloud.com	Username-Password-Authenti...	1	26 minutes ago	...