

Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»  
Факультет інформатики та обчислювальної техніки  
Кафедра Обчислювальної Техніки

Лабораторна робота №3

з дисципліни "Безпека програмного забезпечення"

Тема: "Засвоювання базових навичок OAuth0 авторизаційного протокола"

Виконав:

студент групи ІП-93

Домінський В.О.

Київ 2022

## Зміст

Виконання: .....	3
1. Базовий варіант .....	3
1.1 Отримати user token.....	3
1.2 Отримати оновлений токен .....	4
2. Зміна паролю .....	5
Висновок: .....	8
Посилання: .....	9

## Виконання:

### 1. Базовий варіант

#### 1.1 Отримати user token

Для початку Нам треба отримати токен користувача з такими параметрами:

- Grant\_type – повинно стояти значення «password», проте даний варіант працює лише для баз даних за замовчуванням, тому для того, аби все запрацювало Ми поставимо «http://auth0.com/oauth/grant-type/password-realm»
- Scope - offline\_access – для отримання refresh token
- Realm – назва з’днання (Username-Password-Authentication)
- Усі інші параметри – з минулої ЛР

The screenshot shows a REST client interface with the following details:

- Method:** POST
- URL:** https://{{Domain}}/oauth/token
- Body Type:** x-www-form-urlencoded (selected)
- Parameters:**

KEY	VALUE
grant_type	http://auth0.com/oauth/grant-type/pass...
scope	offline_access
username	{{email}}
password	{{password}}
realm	Username-Password-Authentication
client_id	JlvCO5c2IBHIAe2patn6l6q5H35qxti0
client_secret	ZRF8Op0tWM36p1_hxXTU-B0K_Gq_-eA...
audience	https://kpi.eu.auth0.com/api/v2/



eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjVCZTlBZFhrMERaUjhmR1dZyjdkViJ9.eyJpc3MiOiJodHRweZovL2twaS5ldS5hdXRoMC5jb20vIiwic3ViIjoieYXV0aDB8NjNhOGFiYzlkNTNiYTMTOTZlYjM4ZDdkIiwieYXVkJjoiaHR0cHM6Ly9rcGkuZXUuYXV0aDAuY29tL2FwaS92Mi8iLCJpYXQiOiE2NzIyMTMyNDYsImV4cCI6MTY3MjI5OTY0NiwiYXpwIjoiaSk12Q081YzJJQkhsQWUycGF0bjZsNnE1SDM1cXh0aTAiLCJzY29wZSI6InJlYWQ6Y3VycmVudF91c2VyIHVwZGF0ZTpdXJyZW50X3VzZXJfbWV0YWRhdGEgZGVsZXRIOmN1cnJlbnRfdXNlcl9tZXRhZGF0YSBjemVhdGU6Y3VycmVudF91c2VyX21ldGFkYXRhIGNyZWV0ZTpdXJyZW50X3VzZXJfZGV2aWNlX2NyZWRIbnRpYWxzIHVwZGF0ZTpdXJyZW50X3VzZXJfaWRlbnRpdGlleYBvZmZsaW5lX2FjY2VzcyIsImd0eSI6WjYyZWZyZXNoX3Rva2VuIiwicGFzc3dvcmQiOiXX0.G\_BtHybmKtGvFpbhe7Ze4HO7I49qpDW3szf-

XXIUiyngGDle6shDIeMvdA9VUvos\_n3DFR3P84V0tVHuVFJUSWWyKqpmLo3\_oe7brjkrVl\_THdkTPG10uix-

R5KfYMry7cEhtfly0HqmuGR9VyPM6ylGAMUH0VbBhfrAytgHno1EzIIYgUQaXVPb0f\_n5FahNxpJwkGBoHj\_C6YZaMnLhVTJRMsp6WYolsHaWApHtkncJ\_wT7QW\_HsyxRRtr8hMCMTFd8fbH9eRsUEG6j64dQ0dVRoXJpqKfzw-PC5palHTBrS0598w5bSrHv2EqwkTSL\_Zvx1uBtRivsIC8P1IYg

Тепер проглянемо усіх користувачів, аби зрозуміти, чи був проведений логін:

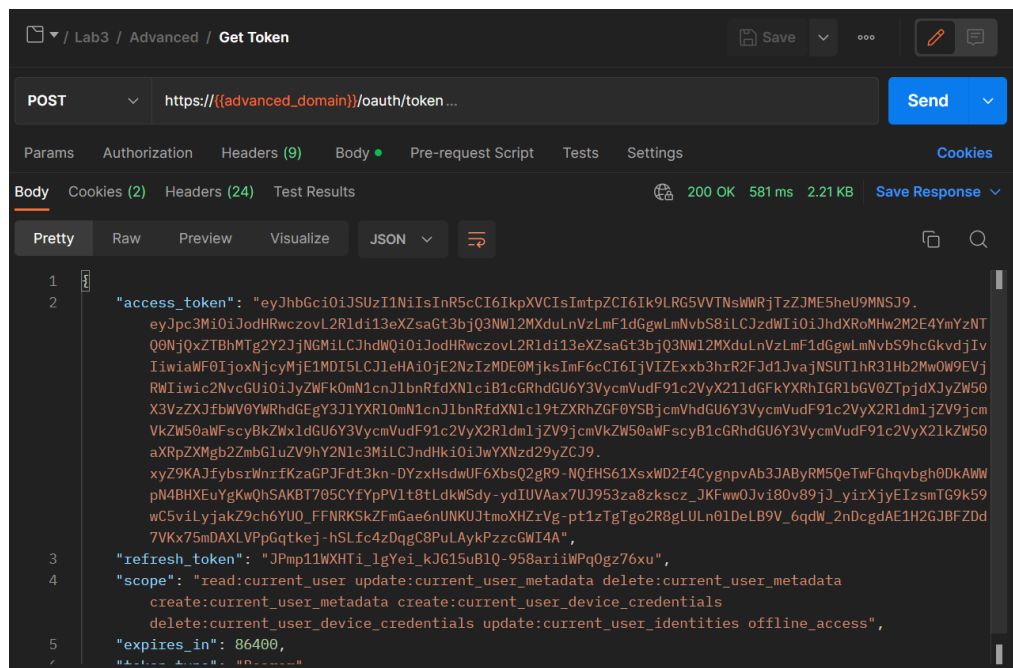
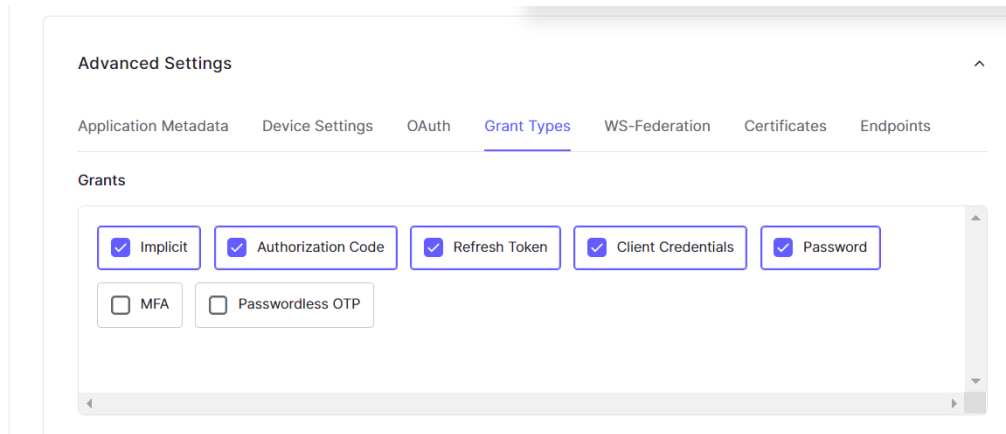
```
33         "provider": "auth0",
34         "connection": "Username-Password-Authent
35         "isSocial": false
36     },
37 ],
38     "name": "Valentyn Dominskyi",
39     "nickname": "vsig",
40     "picture": "config.picture",
41     "updated_at": "2022-12-28T07:35:00.199Z",
42     "user_id": "auth0|63a8abc9d53ea3596eb38d7d",
43     "user_metadata": {},
44     "last_login": "2022-12-28T07:35:00.198Z",
45     "last_ip": "94.158.88.251",
46     "logins_count": 2,
47     "app_metadata": {}
48 },
49 {
50     "created_at": "2022-12-08T15:04:12.349Z",
51     "email": "colleglion02@gmail.com"
```

## 2. Зміна паролю

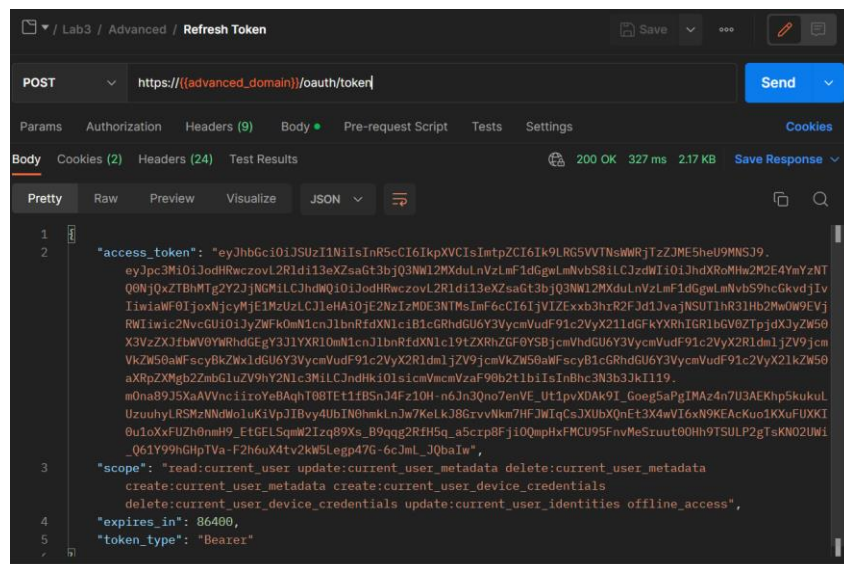
Якщо Ми відразу спробуємо зробити такі ж дії для Нашого застосунку, то отримаємо таку помилку:

```
1 {
2   "error": "unauthorized_client",
3   "error_description": "Grant type 'http://auth0.com/oauth/grant-type/password-realm' not allowed for
   the client.",
4   "error_uri": "https://auth0.com/docs/clients/client-grant-types"
5 }
```

Саме тому Нам треба зайти на сайт auth0 та змінити для Нашого Application Grant types:



Тепер отримаємо новий токен:



Щоб змінити пароль Нам треба дати доступ до такої можливості:

BPZ-Advanced

Client Id: 5HdLqoxkGaIwRoj3RQ9aGyGoc09oDV4V

Authorized ☒

Select which permissions (scopes) should be granted to this client:

Grant ID

cgr\_fn5bQswbPaho9hsT

Permissions

Select: All None

☐ read:client\_grants ☐ create:client\_grants ☐ delete:client\_grants ☐ update:client\_grants ☒ read:users

☒ update:users ☐ delete:users ☒ create:users ☐ read:users\_app\_metadata ☐ update:users\_app\_metadata

☐ delete:users\_app\_metadata ☐ create:users\_app\_metadata ☐ read:user\_custom\_blocks

Та отримати user ID (кому цей пароль змінити):

← Back to Users

VD **Valentyn Dominskyi**

user\_id: auth0|63a8bf3544641e0a186cbc4c

Details Devices History Raw JSON Authorized Applications Permissions

```
1 {
2   "blocked": false,
3   "created_at": "2022-12-25T21:23:01.823Z",
4   "email": "ronny_leuschke@gmail.com",
5   "email_verified": false,
6   "family_name": "Dominskyi",
7   "given_name": "Valentyn",
8   "identities": [
9     {
10      "user_id": "63a8bf3544641e0a186cbc4c",
11      "provider": "auth0",
12      "connection": "Username-Password-Authentication",
13      "isSocial": false
14    }
15  ]
16 }
```

Ось коли був оновлений користувач перед зміною паролю:

```
"nickname": "vsig",
"picture": "config.picture",
"updated_at": "2022-12-28T08:18:15.979Z",
"user_id": "auth0|63a8bf3544641e0a186cbc4c",
"user_metadata": {},
```

Міняємо пароль:

▼ / Lab3 / Advanced / Password Change

Save ▼

PATCH ▼

https://{{advanced\_domain}}/api/v2/users/auth0|63a8bf3544641e0a186cbc4c

Params

Authorization ●

Headers (10)

Body ●

Pre-request Script ●

Tests

Settings

● none

● form-data

● x-www-form-urlencoded

● raw

● binary

● GraphQL

JSON ▼

1 {

2   "connection": "Username-Password-Authentication",

3   "password": "{{\$advanced\_password\_3}}"

4 }

Body

Cookies (2)

Headers (23)

Test Results

🌐 200 OK 391 ms 1.39 KB

Pretty

Raw

Preview

Visualize

JSON ▼

↺

17   "nickname": "vsig",

18   "picture": "config.picture",

19   "updated\_at": "2022-12-28T08:28:52.117Z",

20   "user\_id": "auth0|63a8bf3544641e0a186cbc4c",

21   "user\_metadata": {},

22   "last\_ip": "94.158.88.251",

23   "last\_login": "2022-12-28T08:28:52.116Z",

24   "logins\_count": 5

25 }

← Back to Users



Valentyn Dominskyi

user\_id: auth0|63a8bf3544641e0a186cbc4c

Details    Devices    History    Raw JSON    Authorized Applications    Permissions    Roles

Max. Log Storage: 1 days

	Event	When	App	Identity Provider
✓	Success Change Password	a few seconds ago	N/A	Username-Pass...

### Висновок:

Під час виконання роботи я розібрався з різними запитами та зумів змінити пароль користувача



## Посилання:

- [Проект на GitHub](#)