

Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”
Факультет інформатики та обчислювальної техніки
Кафедра автоматики та управління в технічних системах

Лабораторна робота №3
Системи безпеки програм і даних
*«Засвоювання базових навичок OAuth2 авторизаційного
протокола»*

Виконав:
студент групи ІА-12

Мельник М.С.

Київ 2024

Завдання на лабораторну роботу:

1) Використовуючи наведені налаштування з лабораторної роботи 2 зробити запит на отримання user token (попередньо створеного в л.р. 2)

2) Отримати оновлений токен використовуючи **refresh-token** grant type

<https://auth0.com/docs/api/authentication?javascript#refresh-token>

Надати скріншоти та отримані токени.

Для отримання додаткового балу: зробити запит до API для зміни пароля

<https://auth0.com/docs/authenticate/database-connections/password-change#directly-set-the-new-password>

Токен має бути використаний з прикладу client_credential grant прикладу.

Хід роботи

1. Робота була виконана за допомогою створення власного аккаунту в auth0.

2. В налаштуваннях обраного Application відкриваємо Advanced Settings, таб Grant Types, обираємо опцію Grant 'Password' – enabled.

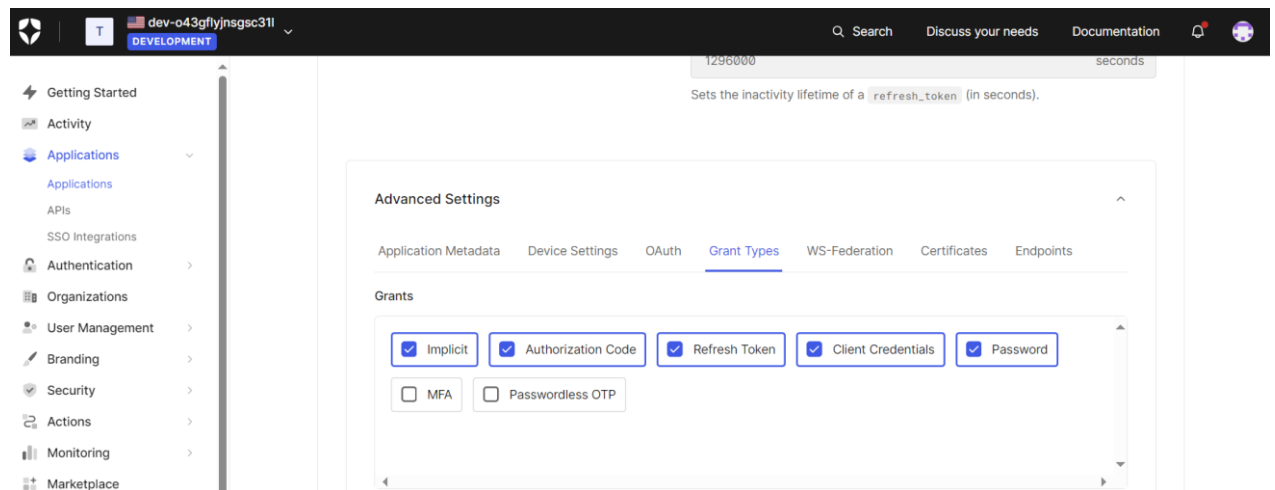


Рис 1 – Сторінка з користувацьким Default API application

3. Робимо запит на отримання user токена(access, refresh).

POST

https://dev-o43gflyjngsc31l.us.auth0.com/oauth/token

Send

Params

Authorization

Headers (10)

Body

Pre-request Script

Tests

Settings

Cookies

none

form-data

x-www-form-urlencoded

raw

binary

GraphQL

<input checked="" type="checkbox"/>	audience	https://dev-o43gflyjngsc31l.us.auth0.c...
<input checked="" type="checkbox"/>	client_id	2HRZLH0OWORpjTD0tf0uWjFc0xySsZaF
<input checked="" type="checkbox"/>	grant_type	http://auth0.com/oauth/grant-type/pass...
<input checked="" type="checkbox"/>	client_secret	HZ9HTTXanJgvmfjRgf5zavMKk8L33deV...
<input checked="" type="checkbox"/>	username	test3@test.com
<input checked="" type="checkbox"/>	password	TESTtest12345678
<input checked="" type="checkbox"/>	scope	offline_access
<input checked="" type="checkbox"/>	realm	Username-Password-Authentication

POST

https://dev-o43gflyjngsc31l.us.auth0.com/oauth/token

Send

Params

Authorization

Headers (10)

Body

Pre-request Script

Tests

Settings

Cookies

none

form-data

x-www-form-urlencoded

raw

binary

GraphQL

<input checked="" type="checkbox"/>	audience	https://dev-o43gflyjngsc31l.us.auth0.c...
-------------------------------------	----------	---

Body

Cookies (2)

Headers (18)

Test Results

200 OK 693 ms 1.94 KB Save as example

Pretty

Raw

Preview

Visualize

JSON

```

2  "access_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InZ4cVxYjFpbUZ0eHFwaFgyS2AyaS99.eyJpc3MiOiJodHRwczovL2Rldi1vNDNnZmx5am5zZ3NjMzFzLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJhdXR0MHw2NjAwNTliZGYyZTg2Njg0MTg4MDg5YWElLCJhdWQiOiJodHRwczovL2Rldi1vNDNnZmx5am5zZ3NjMzFzLnVzLmF1dGgwLmNvbS9hcGkvdjIvIiwiaWF0IjoxNzExMzAwODk0LmF1dG8iLCJleHAiOiJlMTEzODcyOTQsInNjb3BlIjoicmVhZDpjZDh0ZjZw50X3VzZXIgdXBkYXRlOmN1cnJlbnRfdXNlc19tZXRhZGF0YSBkZWxldGU6Y3VycmVudF91c2VY21ldGFKYXRhIGNyZWZ0ZTpjdXJyZW50X3VzZXJfbWV0YWRhdGEgY3JlYXRlOmN1cnJlbnRfdXNlc19kZXZpY2VfY3JlZGVudG1hbmMgZGVsZXRL0mN1cnJlbnRfdXNlc19kZXZpY2VfY3JlZGVudG1hbmMgdXBkYXRlOmN1cnJlbnRfdXNlc19pZGVudG10awVzIG9mZmxpbmVfYWNjZXNzIiwiaWF0Ij0iLCJhenAiOiIySFJaTEgtPUNBQVEQwdGYwdVdqRmMwH1Tc1phRiJ9.KtvZQEY3wx_nlhPERzxnp5Rh1u8n4g5R00C9MATRAOMWNUe7b_u04NyKkwuQfA0YYwhjs34nVTCsLRNEziupWUOUKSYyO_PaHCDFeb0iyT7807cSiSKsG5kYQQ6yAZzpYrKdZ5UdAQ2bXMyJfuttDEZtTP-qQZf5nQiddLfsiwsn41hqCi4tnWfdpEzwUCwkbcbesApkQnshQg-RKtBnSR44Q9tddqh_1UUGa1xJ77x0tIGfM26xLVU0Dvp0yJzArHv7XGSLJxMpHe0iF04-Q102nk1FdY9jzm7TcqU8p0NRN3twvvu-LG2iGyIDG3gskITIDmmVA3jM6fFC6Gg",
3  "refresh_token": "1ax-UNAgj8dnMGYDPkz9bgaIu-8UfxmneHNs0UL-3X0PZ",
4  "scope": "read:current_user update:current_user_metadata delete:current_user_metadata create:current_user_metadata create:current_user_device_credentials delete:current_user_device_credentials update:current_user_identities offline_access",
5  "expires_in": 86400,
6  "token_type": "Bearer"
7  }

```

Рис 2 – Refresh та access токен

4. Вказуємо grant_type: refresh_token і сам токен, та отримуємо оновлений access_token.

POST

https://dev-o43gflyjnsjsc31.us.auth0.com/oauth/token

Send

Params

Authorization

Headers (10)

Body

Pre-request Script

Tests

Settings

Cookies

☐ none

☐ form-data

☒ x-www-form-urlencoded

☐ raw

☐ binary

☐ GraphQL

Key	Value	Description	...	Bulk Edit
<input checked="" type="checkbox"/> audience	https://dev-o43gflyjnsjsc31.us.auth0.c...			


Рис 3 – Оновлення токєну

Рис 3 – Оновлення токєну

5. Виконуємо додаткове завдання, надсилаючи PATCH запит на зміну паролю, але нажаль його неможливо виконати через тип API, де також на рисунку попереднього пункту не вказано “scope”: update: current_user.

Available scopes and endpoints

With a Management API Token issued for a SPA, you can access the following scopes (and hence endpoints).

 Password changes through the [PATCH /api/v2/users/{id}](#) endpoint are **not possible** with a Management API Token issued for a SPA.

Scope for Current User	Endpoint
read:current_user	GET /api/v2/users/{id} GET /api/v2/users/{id}/enrollments
update:current_user_identities	POST /api/v2/users/{id}/identities DELETE /api/v2/users/{id}/identities/{provider}/{user_id}
update:current_user_metadata	PATCH /api/v2/users/{id}
create:current_user_metadata	PATCH /api/v2/users/{id}
create:current_user_device_credentials	POST /api/v2/device-credentials
delete:current_user_device_credentials	DELETE /api/v2/device-credentials/{id}

PATCH

https://dev-o43gflyjnsgsc31l.us.auth0.com/api/v2/users/auth0|660059bdf2e86684188089aa

Send

ParamsAuthorizationHeaders (11)BodyPre-request ScriptTestsSettingsCookies

none

form-data

x-www-form-urlencoded

raw

binary

GraphQL

JSON

Beautify

1 {

2 "password": "newPasswordTEST3",

3 "connection": "Username-Password-Authentication"

4 }

bodyCookies (2)Headers (14)Test Results403 Forbidden800 ms657 BSave as example

PrettyRawPreviewVisualizeJSON

1 {

2 "statusCode": 403,

3 "error": "Forbidden",

4 "message": "You cannot update the following fields: password, connection",

5 "errorCode": "insufficient_scope"

6 }

Рис 4 – Запит на зміну паролю

6. До речі, якщо вказати токен з прикладу `client_credential grant`, то нам з поточної помилки стане відомо, що “scope” немає запитаних значень.

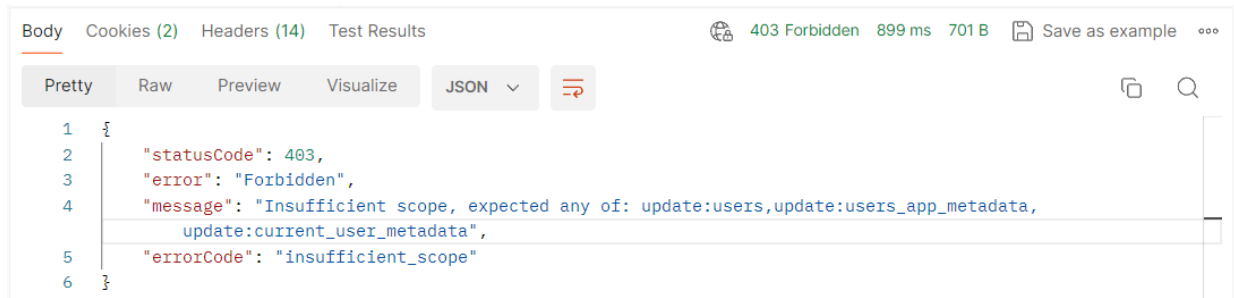


Рис 5 – Вказуємо токен з прикладу `client_credential grant`

Висновок: у даній лабораторній роботі було ознайомлено та засвоєно базові навички OAuth2 авторизаційного протокола.