Міністерство освіти і науки України
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського"
Факультет інформатики та обчислювальної техніки

Кафедра інформатики та програмної інженерії

Звіт

з лабораторної роботи №3 з дисципліни
«Системи безпеки програм і даних»

«Протокол OAuth2»

Виконав(ла) *ІП-11 Сідак Кирил Ігорович*
(шифр, прізвище, ім'я, по батькові)

Перевірив *Іваніщев Б. В.*
(прізвище, ім'я, по батькові)

Київ 2024

ЗМІСТ

1 МЕТА ЛАБОРАТОРНОЇ РОБОТИ

Мета роботи – засвоювання базових навичок OAuth2 авторизаційного протокола.

2 ЗАВДАННЯ

2.1 Основне завдання

1) Використовуючи наведені налаштування з лабораторної роботи 2 зробити запит на отримання user token (попередньо створенного в лабораторній роботі 2)

POST https://YOUR_DOMAIN/oauth/token

Content-Type: application/x-www-form-urlencoded

audience=API_IDENTIFIER&grant_type=client_credentials&client_id=YOUR_CLIENT_ID&client_secret=YOUR_CLIENT_SECRET

2) Отримати оновлений токен використовуючи refresh-token grant type https://auth0.com/docs/api/authentication?javascript#refresh-token

Надати скріншоти та отримані токени.

2.2 Додаткове завдання

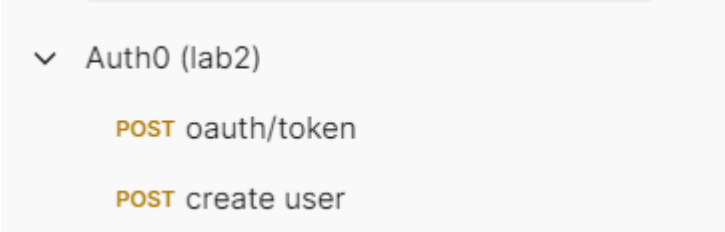
Зробити запит до API для зміни пароля https://auth0.com/docs/authenticate/database-connections/password-change#directly-set-the-new-password

Токен має бути використаний з прикладу client_credential grant прикладу

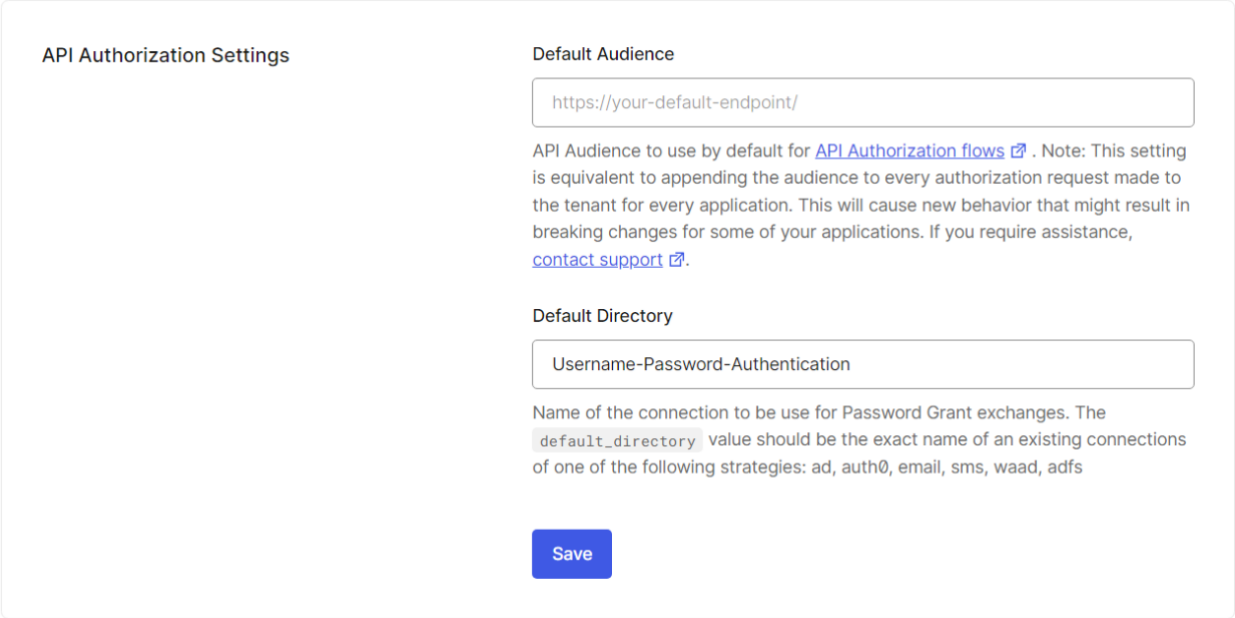
3 ВИКОНАННЯ ОСНОВНОГО ЗАВДАННЯ

3.1 Отримання User Token

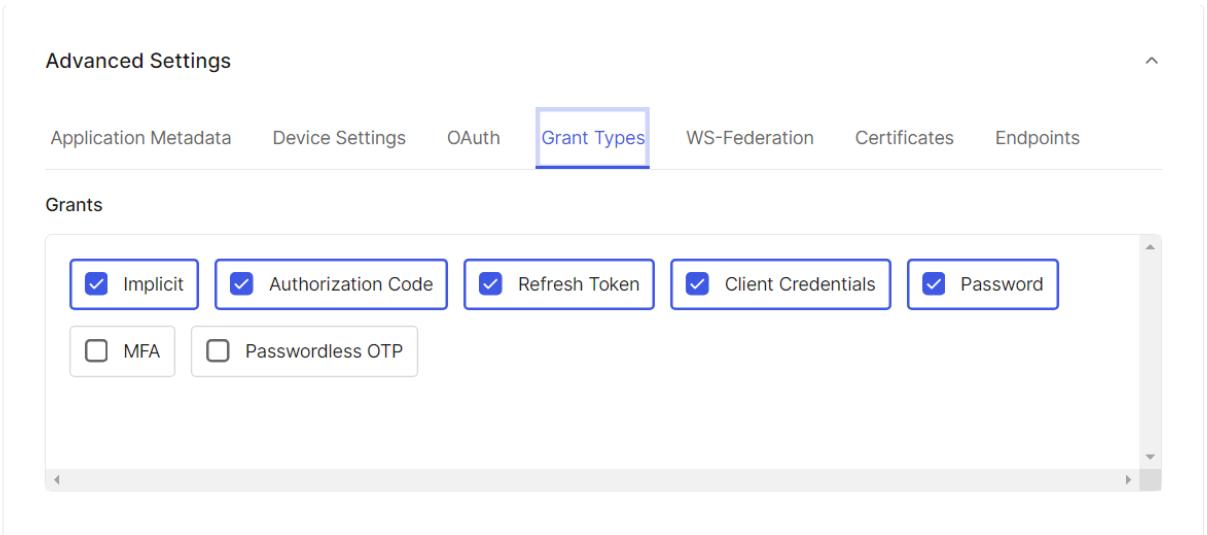
Для подальшої комфортної роботи, запити було перенесено в Postman:



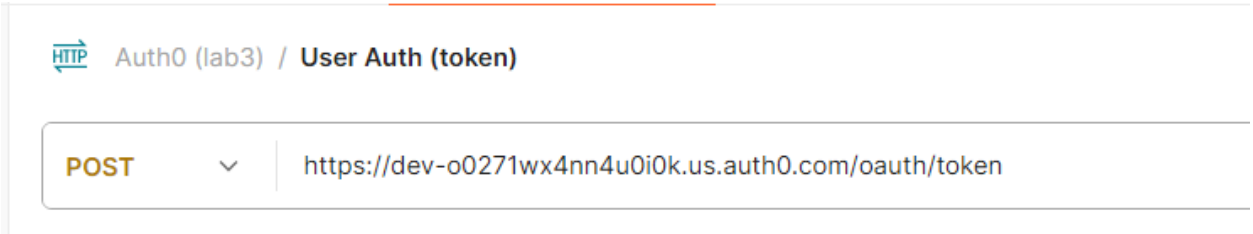
Наступним кроком, налаштовуємо стандартні налаштування для запитів:



Налаштовуємо аплікейшин, для використання grant type password:

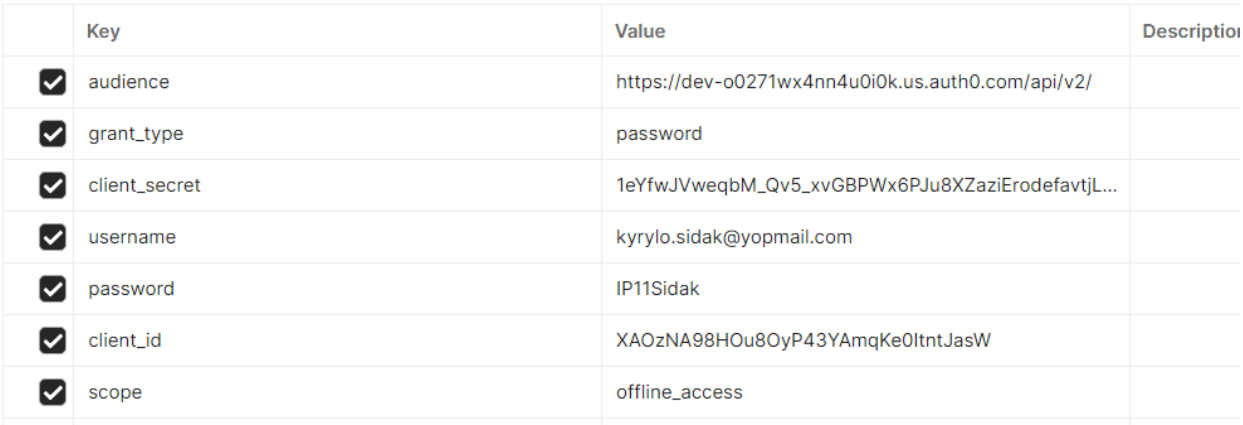


Створюємо новий запит в постман, та зазначаємо метод POST та посилання https://dev-o0271wx4nn4u0i0k.us.auth0.com/oauth/token:



Встановлюємо хедер з типом контенту:

Будуємо тіло запиту. В запиті вказуємо grant_type password, авторизаційні дані створеного користувача та параметр scope, для отримання refresh_token:



Key	Value	Description
audience	https://dev-o0271wx4nn4u0i0k.us.auth0.com/api/v2/	
grant_type	password	
client_secret	1eYfwJVweqbM_Qv5_xvGBPWx6PJu8XZaziErodefavtjL...	
username	kyrylo.sidak@yopmail.com	
password	IP11Sidak	
client_id	XAOzNA98HOu8OyP43YAmqKe0ltntJasW	
scope	offline_access	

Перевіряємо побудований запит:


```
{
    "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjNTTFRrW
        eyJpc3MiOiJodHRwczovL2Rldi1vMDI3MXd4NG5uNHUwaTBrLnVzLmF1dGgwLmNvbS
        HRwczovL2Rldi1vMDI3MXd4NG5uNHUwaTBrLnVzLmF1dGgwLmNvbS9hcGkvdjIvIiwi
        JyZW50X3VzZXIgdXBkYXRlOmN1cnJlbnRfdXNlcl9tZXRhZGF0YSBkZWxldGU6Y3Vy
        lYXRlOmN1cnJlbnRfdXNlcl9kZXZpY2VfY3JlZGVudGlhbHMgZGVsZXRlOmN1cnJlbi
        dGl0aWVzIG9mZmxpbmVfYWNjZXNzIiwiZ3R5IjoicGFzc3dvcmQiLCJhenAiOiJYQU
        mIcHgXHN15Ss7r9Vxj3gGlUgIEtFAmznnQdzlQ0wfmO2rBQ0FW3YZvYn5CuW1_kT6F8
        ZYMYU8oMxcW6YGqHQvfA17Rq47T_nvBn_aqvTNHOr4varHg3Tw-zkWmYbzxGhvv94LM
        gWvSYjmro5ZU_i0Rpoy0kg0Kqfb7QVjWDvO3ImsERMPVVk1en5cqrCnzVIb2q2O9Kbi
    "refresh_token": "v1.Ma8Wvbt_ZIDp6Ha-ZQ6vCY2JP2Ld1RDTmImiozHz8UyY9bWQSa
    "scope": "read:current_user update:current_user_metadata delete:current
        create:current_user_device_credentials delete:current_user_device_c
    "expires_in": 86400,
    "token_type": "Bearer"
}
```

У відповідь ми отримали user token:

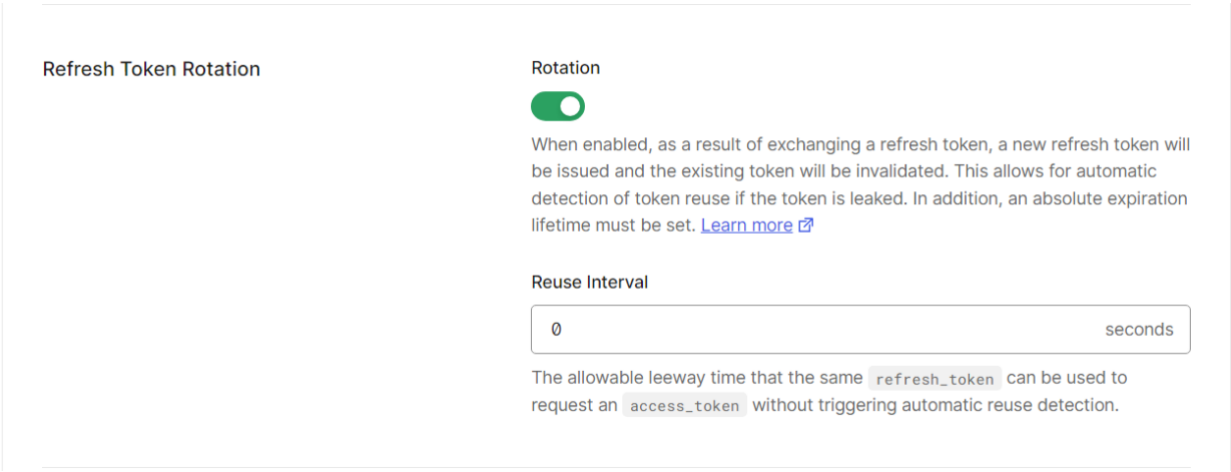
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjNTTFRrWGh0SllhS2pvSW55UnduWCJ
9.eyJpc3MiOiJodHRwczovL2Rldi1vMDI3MXd4NG5uNHUwaTBrLnVzLmF1dGgwLmNvbS8i
LCJzdWIiOiJhdXRoMHw2NjM0YWVmNzY3MWY5ZWViN2QwNGVkNzAiLCJhdWQiOiJo
dHRwczovL2Rldi1vMDI3MXd4NG5uNHUwaTBrLnVzLmF1dGgwLmNvbS9hcGkvdjIvIiwia
WF0IjoxNzE0ODExMDIwLCJleHAiOjE3MTQ4OTc0MjAsInNjb3BlIjoicmVhZDpjdXJyZW5
0X3VzZXIgdXBkYXRlOmN1cnJlbnRfdXNlcl9tZXRhZGF0YSBkZWxldGU6Y3VycmVudF91
c2VyX21ldGFkYXRhIGNyZWF0ZTpjdXJyZW50X3VzZXJfbWV0YWRhdGEgY3JlYXRlOm
N1cnJlbnRfdXNlcl9kZXZpY2VfY3JlZGVudGlhbHMgZGVsZXRlOmN1cnJlbnRfdXNlcl9kZX
ZpY2VfY3JlZGVudGlhbHMgdXBkYXRlOmN1cnJlbnRfdXNlcl9pZGVudGl0aWVzIG9mZmx
pbmVfYWNjZXNzIiwiZ3R5IjoicGFzc3dvcmQiLCJhenAiOiJYQU96TkE5OEhPdThPeVA0M1
lBbXFLZTBJdG50SmFzVyJ9.mIcHgXHN15Ss7r9Vxj3gGlUgIEtFAmznnQdzlQ0wfmO2rBQ0
FW3YZvYn5CuW1_kT6F8ytQ06Nm3bn-DVjpPxs6Ja3EMBhXQuoa-l7G-
QiyvZ01KSg6qLmXqCtl4DpE4-
qM26yZYMYU8oMxcW6YGqHQvfA17Rq47T_nvBn_aqvTNHOr4varHg3Tw-
zkWmYbzxGhvv94LNDeB3Bh4XmXV0XevYERQzwE4ZbNeEKM0awSvufeahyo1k-
gh903LeduyEOh51_5X_YGgWvSYjmro5ZU_i0Rpoy0kg0Kqfb7QVjWDvO3ImsERMPVVk1e
n5cqrCnzVIb2q2O9KbiY1YSWx9gw

Також збережемо отриманий refresh token, він нам потрібен буде в майбутньому:

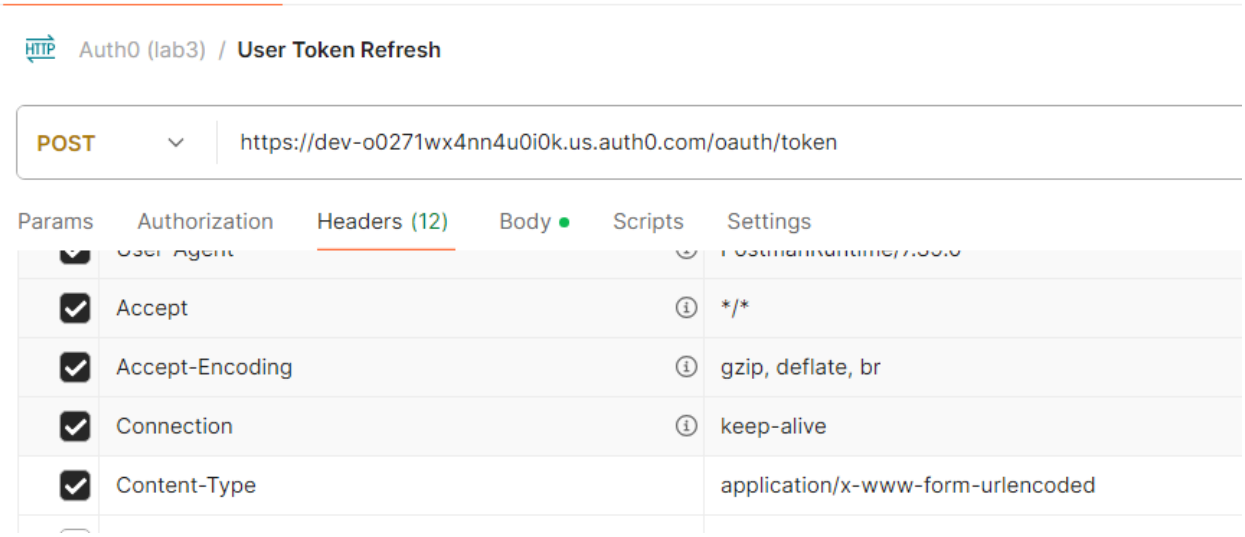
v1.Ma8Wvbt_ZIDp6Ha-
ZQ6vCY2JP2Ld1RDTmImiozHz8UyY9bWQSa2V61z8CBk2pmwP6xZkp-
XASa2FwOHzIauIq8o

3.2 Отримання нового токену, за допомогою refresh_token

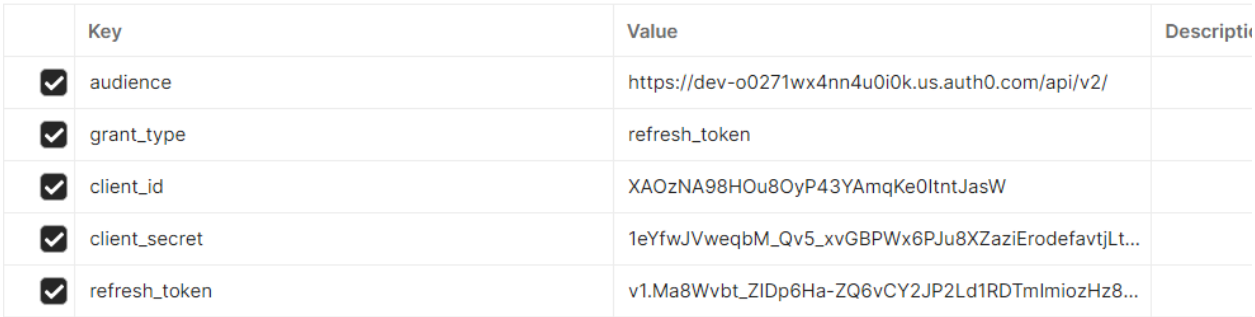
Для виконання цього завдання одразу налаштуємо Refresh Token Rotation в аплікейшині, для того щоб цей токен можна було використати одноразово:



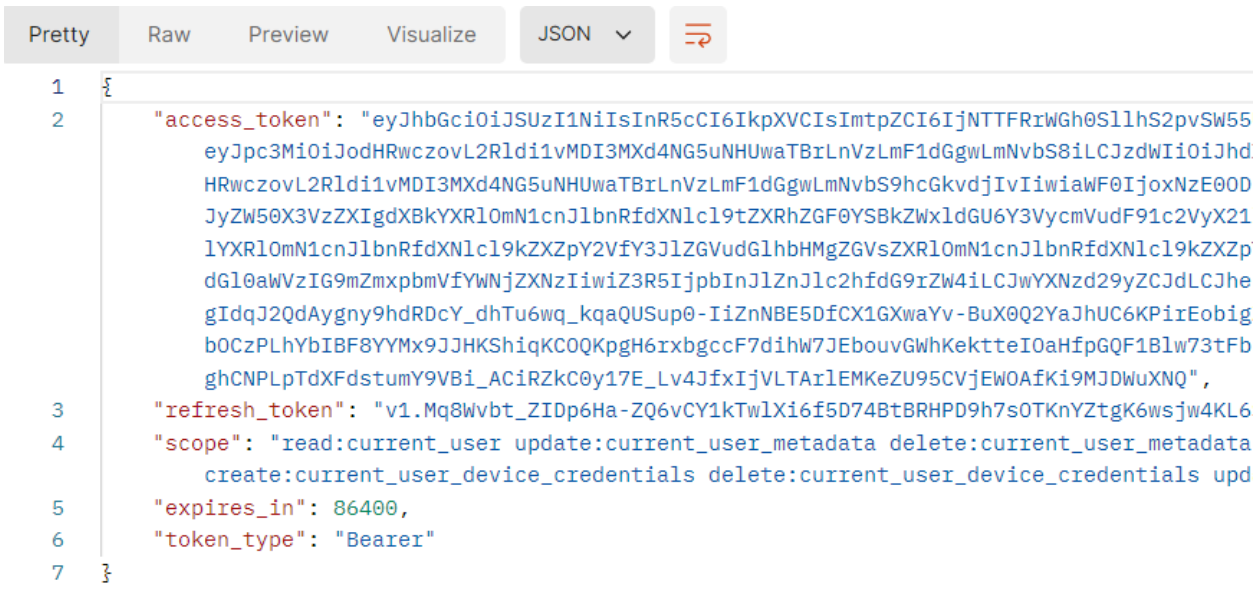
Тепер перейдемо в Postman для побудови нового запиту. Метод нового запиту Post, посилання https://dev-o0271wx4nn4u0i0k.us.auth0.com/oauth/token та content-type: application/x-www-form-urlencoded.



В тілі запиту вказуємо grant-type: refresh_token, налаштування та отриманий з попереднього завдання refresh_token:



Перевіряємо побудований запит в Postman:



В результаті ми отримали новий access_token:

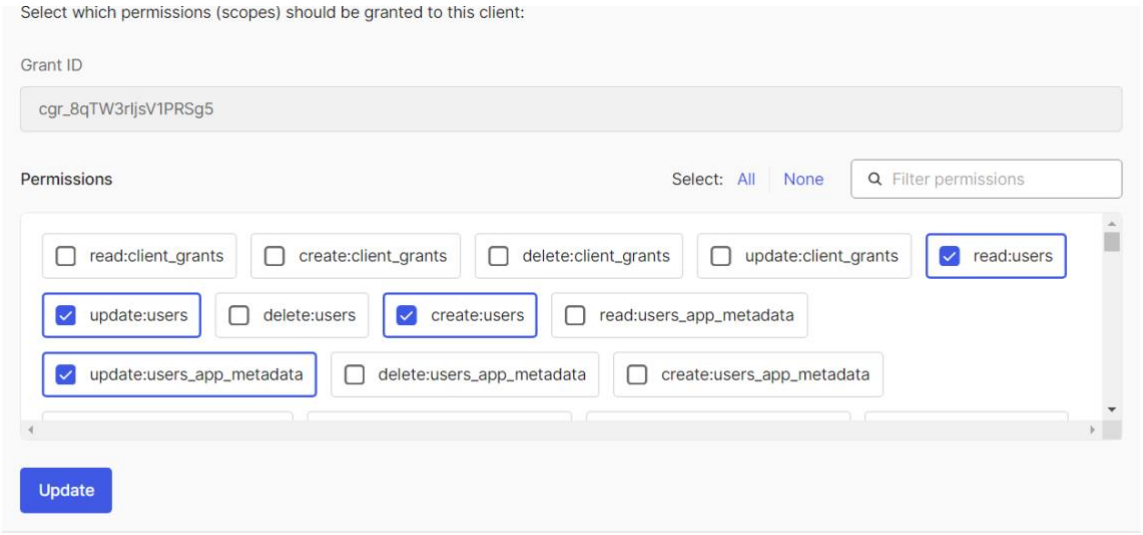
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjNTTFRrWGh0SllhS2pvSW55UnduWCJ9.eyJpc3MiOiJodHRwczovL2Rldi1vMDI3MXd4NG5uNHUwaTBrLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJhdXRoMHw2NjM0YWVmNzY3MWY5ZWViN2QwNGVkNzAiLCJhdWQiOiJodHRwczovL2Rldi1vMDI3MXd4NG5uNHUwaTBrLnVzLmF1dGgwLmNvbS9hcGkvdjIvIiwiaWF0IjoxNzE0ODEzMzE5LCJleHAiOjE3MTQ4OTk3MTksInNjb3BlIjoicmVhZDpjdXJyZW50X3VzZXIgdXBkYXRlOmN1cnJlbnRfdXNlcl9tZXRhZGF0YSBkZWxldGU6Y3VycmVudF91c2VyX21ldGFkYXRhIGNyZWF0ZTpjdXJyZW50X3VzZXJfbWV0YWRhdGEgY3JlYXRlOmN1cnJlbnRfdXNlcl9kZXZpY2VfY3JlZGVudGlhbHMgZGVsZXRlOmN1cnJlbnRfdXNlcl9kZXZpY2VfY3JlZGVudGlhbHMgdXBkYXRlOmN1cnJlbnRfdXNlcl9pZGVudGl0aWVzIG9mZmxpbmVfYWNjZXNzIiwiZ3R5IjpbInJlZnJlc2hfdG9rZW4iLCJwYXNzd29yZCJdLCJhenAiOiJYQU96TkE5OEhPdThPeVA0M1lBbXFLZTBJdG50SmFzVyJ9.gIdqJ2QdAygny9hdRDcY_dhTu6wq_kqaQUSup0-IiZnNBE5DfCX1GXwaYv-BuX0Q2YaJhUC6KPirEobigZKvX-OUMKEmtz5O1I0IHe_tjtlOTRSoHFqD69y8WOgVdFg_cVHBHbOCzPLhYbIBF8YYMx9JJHKShiqKCOQKpgH6rxbgccF7dihW7JEbouvGWhKektteIOaHfpGQF1Blw73tFbLOG-W8wf3m8kh9p2MiMyZSVa7_q-ziDa0N8W_3UJiFF_1WwECM2ighCNPLpTdXFdstumY9VBi_ACiRZkC0y17E_Lv4JfxIjVLTArlEMKeZU95CVjEWOAfKi9MJDWuXNQ

Також отримуємо новий рефреш токен:

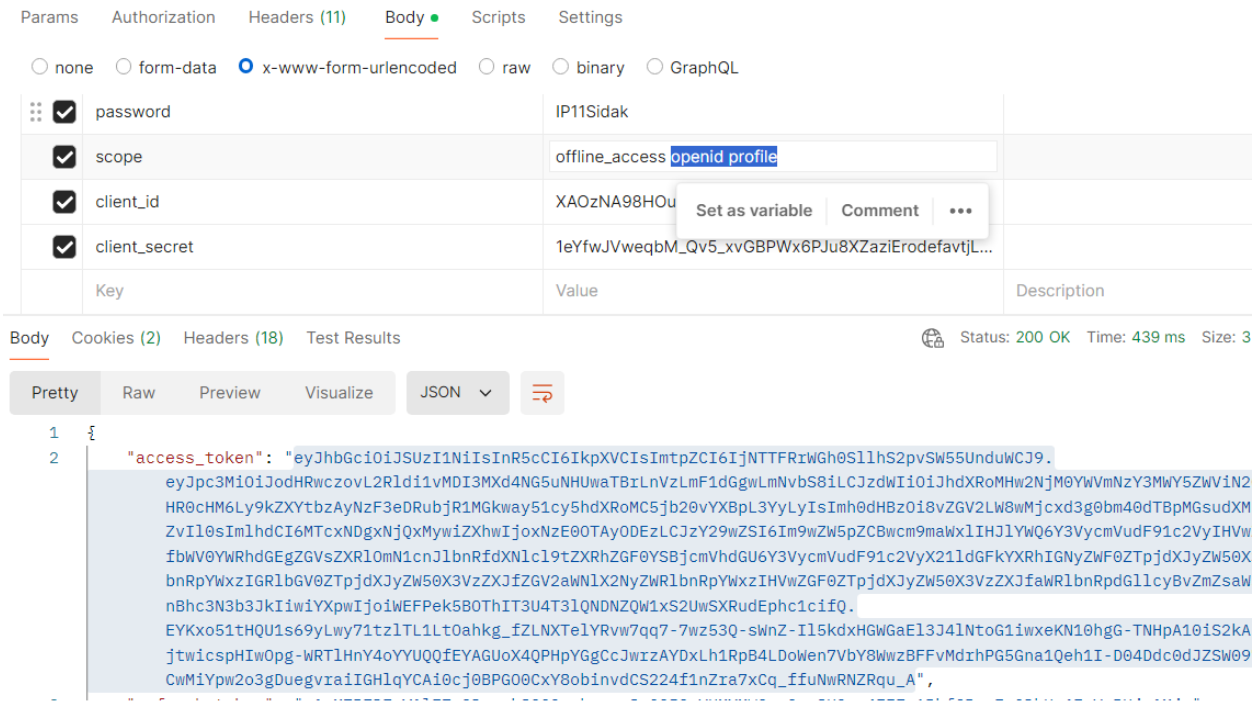
v1.Mq8Wvbt_ZIDp6Ha-ZQ6vCY1kTwlXi6f5D74BtBRHPD9h7sOTKnYZtgK6wsjw4KL6SVGOePr-RDArCEH_TbarzmY

4 ВИКОНАННЯ ДОДАТКОВОГО ЗАВДАННЯ

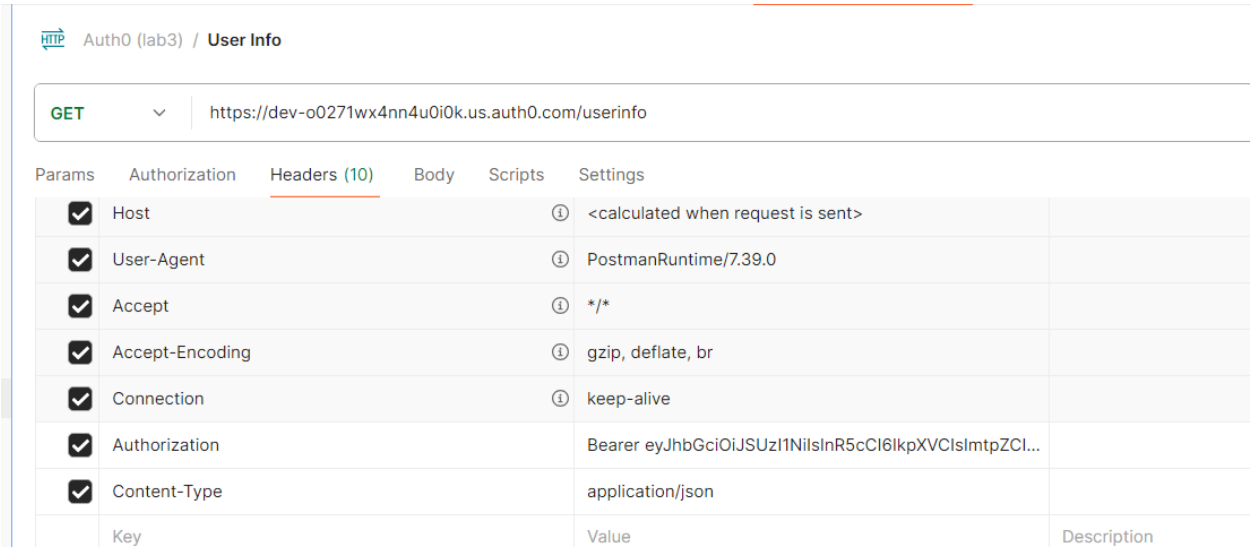
Перед виконанням додаткового завдання, одразу дамо дозвіл оновлення даних користувачів для аплікейшина в налаштуваннях API:



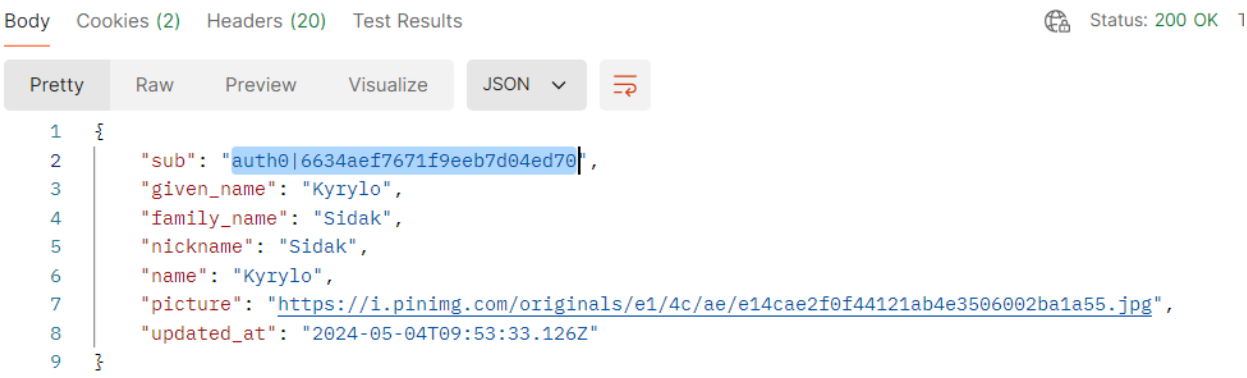
Для оновлення паролю нам потрібно знати userId, можна отримати відправивши запит user info. Але для цього оновимо наш запит авторизації, додавши в scope параметри openid та profile, та отримаємо новий токен:



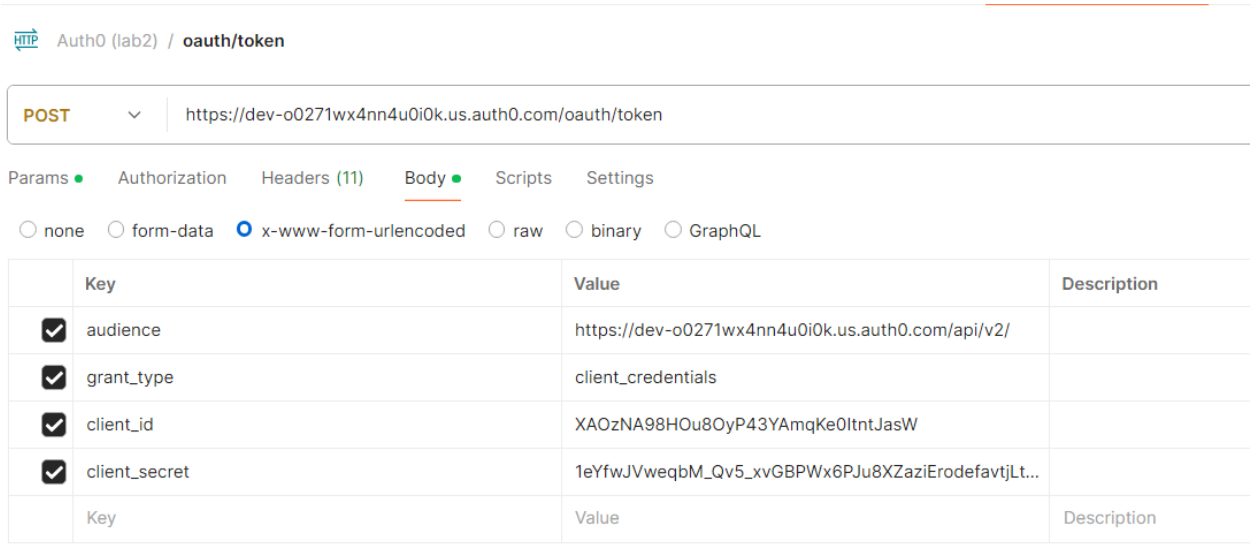
Тепер необхідно відправити GET запит на /userinfo з токеном, який ми тільки що отримали:



У відповідь ми отримали userId auth0|6634aef7671f9eeb7d04ed70:



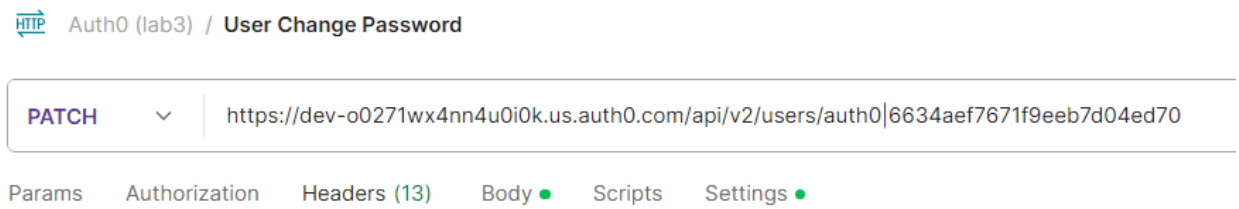
Повертаємось к запиту створеному в лабораторній 2 для отримання токену client_credentials:



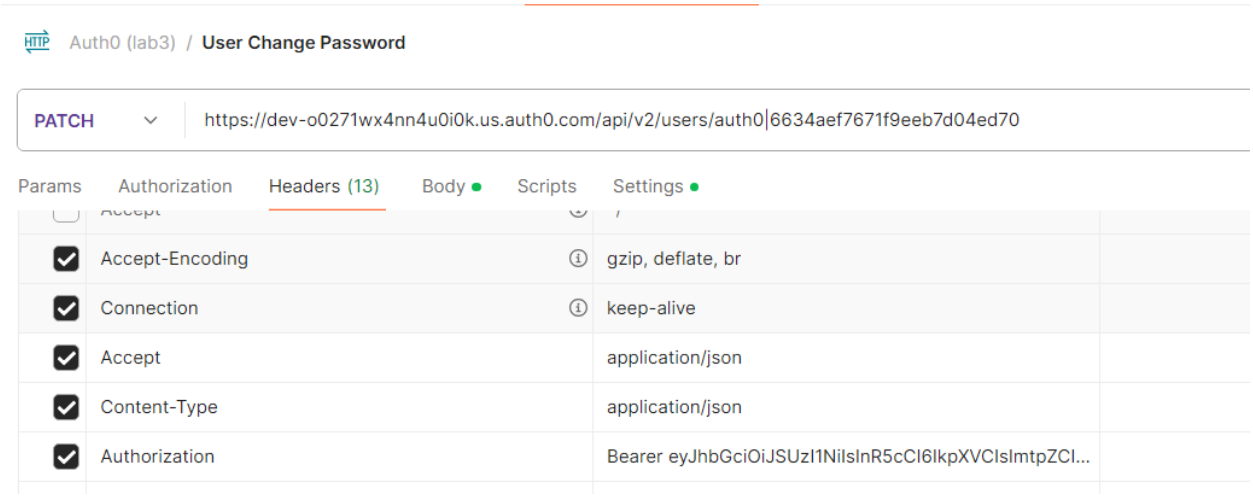
Та отримуємо новий токен:

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjNTTFRrWGh0SllhS2pvSW55UnduWCJ9.eyJpc3MiOiJodHRwczovL2Rldi1vMDI3MXd4NG5uNHUwaTBrLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJYQU96TkE5OEhPdThPeVA0M1lBbXFLZTBJdG50SmFzV0BjbGllbnRzIiwiYXVkIjoiaHR0cHM6Ly9kZXYtbzAyNzF3eDRubjR1MGkway51cy5hdXRoMC5jb20vYXBpL3YyLyIsImlhdCI6MTcxNDgxNjc2NCwiZXhwIjoxNzE0OTAzMTY0LCJzY29wZSI6InJlYWQ6dXNlcnMgdXBkYXRlOnVzZXJzIGNyZWF0ZTp1c2VycyB1cGRhdGU6dXNlcnNfYXBwX21ldGFkYXRhIHJlYWQ6cmVmcmVzaF90b2tlbnMgZGVsZXRlOnJlZnJlc2hfdG9rZW5zIiwiZ3R5IjoiY2xpZW50LWNyZWRlbnRpYWxzIiwiYXpwIjoiWEFPek5BOThIT3U4T3lQNDNZQW1xS2UwSXRudEphc1cifQ.NlC85g3kP9d1vY8sc1TqYdny5AYkbmqFrzUebIGM-O68COEBqnHqhavmHyUWF0WqO-_IUfSEDLBfRUVx0sgYkQouvlhNES67MdehoHoLwmC-2CA2aeZcDIKXQXzN75y5YNjLiqk1z4tyUKDKTE0fA5nh83vYHcfnqo3wuBMtQCY9uXgfLb3YqJ-l66dYM9L8Jx2-Iw2xyux9zke0mlRkMdLiz3jCmJ8xNGD51rWPyYsWvKNeovsAyPOvTmGEz9Iqy6va0qiU6oh-yWQqfxaOhC3AdTreAxcpvHb7_Y4X33XOP7MeLX0hYtI029MFlDPQv1a_ginzn1U4UOZbFjZKkw

Тепер будуємо запит для оновлення паролю. Метод запиту, як зазначено в технічній документації, повинен бути типу PATCH, посилання: https://dev-o0271wx4nn4u0i0k.us.auth0.com/api/v2/users/{Наш userId}:

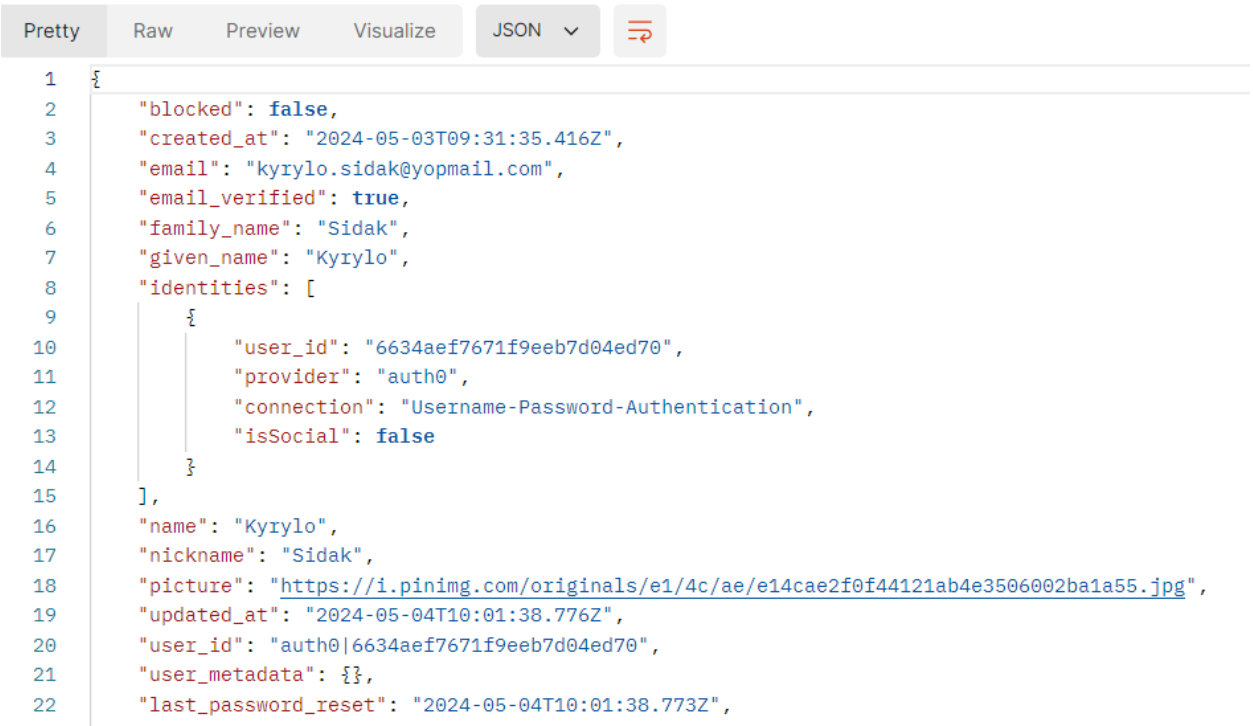


В заголовках запиту додаємо Accept та Content-Type типу application/json, а також додаємо Authorization: Bearer {Отриманий токен }:



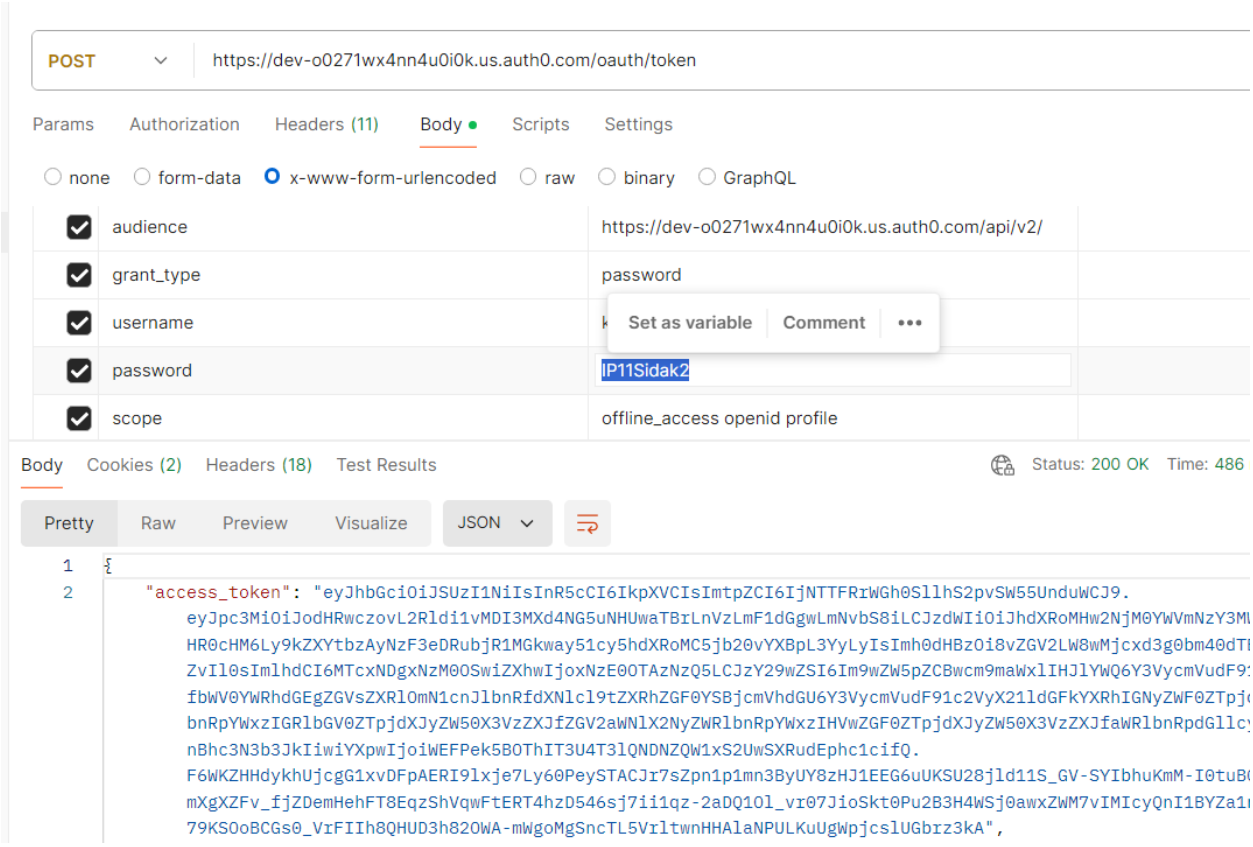
В тілі запиту додаємо новий пароль:

Перевіряємо побудований запит:



Успіх, тепер намагаємось авторизуватись за старим паролем:

Як ми бачимо авторизуватись за старим паролем не вдалось, намагаємось. Оновлюємо пароль в запиті, та перевіряємо:



Тепер користувача успішно авторизовано.

5 ВИСНОВОК

При виконанні лабораторної роботи №3 було продовжено розглядання протоколу OAuth2. Основне завдання полягало у отриманні user acces token та оновленому access token за допомогою refresh_token. Для полегшення роботи з аутентифікацією, всі запити було перенесено в Postman, що значно спростило процес налаштування,відправлення та тестування запитів.

Було також виконано додаткове завдання, пов'язане зі зміною пароля користувача через API. У ході виконання роботи було створено два нових запити та вирішено декілька технічних складнощів, пов'язаних з налаштуванням та отриманням токенів, а також практично застосовано навички роботи з auth0 налаштуваннями.