



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

Лабораторна робота №3

Безпека ПЗ

Тема: Протокол OAuth2

Виконав

студент групи ІП-11:

Панченко С. В.

Перевірив:

Курченко О. А.

Київ 2024

ЗМІСТ

1 Мета лабораторної роботи.....6

2 Завдання.....7

3 Виконання.....8

 3.1 Основне завдання.....8

 3.2 Отримання з refresh-токен нового токена.....10

 3.3 Додаткове завдання.....11

Висновок.....18

1 МЕТА ЛАБОРАТОРНОЇ РОБОТИ

Засвоїти базові навички OAuth2 авторизаційного протоколу.

2 ЗАВДАННЯ

1) Використовуючи наведені налаштування з лабораторної роботи 2 зробити запит на отримання user token (попередньо створеного в лабораторній роботі POST https://YOUR_DOMAIN/oauth/token

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

audience=API_IDENTIFIER&grant_type=client_credentials&client_id=YO

UR_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.

3) 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

3.1 Основне завдання

Налаштуємо додаток для використання grant type password на рисунку 3.1.

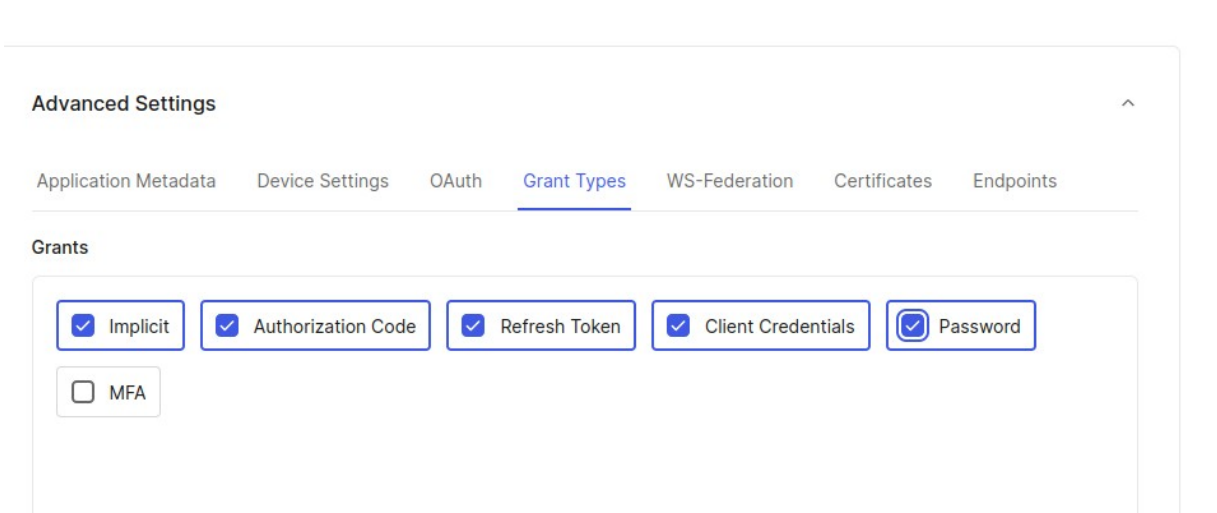


Рисунок 3.1 — Налаштування grants

Зробимо стандартні налаштування запитів на рисунку 3.2.

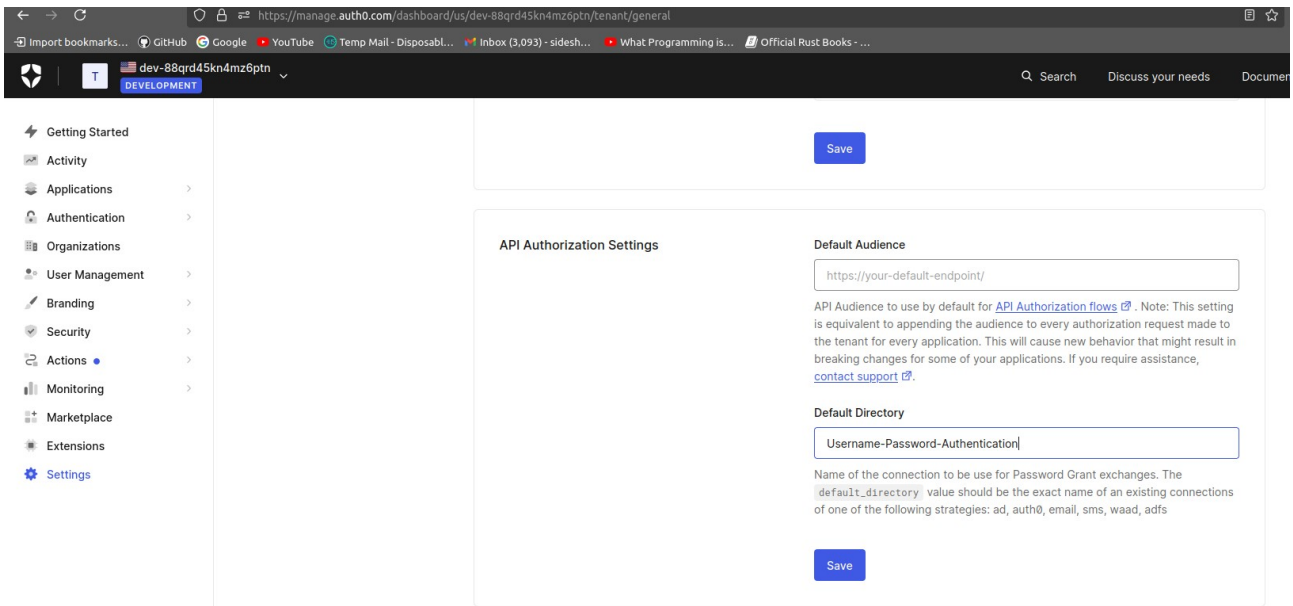


Рисунок 3.2 — Стандартні налаштування запитів

Створюємо запит та отримаємо відповідь на рисунку 3.3.

```
curl --request POST \
  --url https://dev-88qrd45kn4mz6ptn.us.auth0.com/oauth/token \
  --header 'content-type: application/json' \
  --data '{
    "client_id": "zdzhN4dIDmIuptnArPhrZ4TEQakQNGDH",
```


3.2 Отримання з refresh-токен нового токenu

Увімкнемо Refresh Token Rotation, щоб токен можна було використати лише один раз на рисунку 3.4.

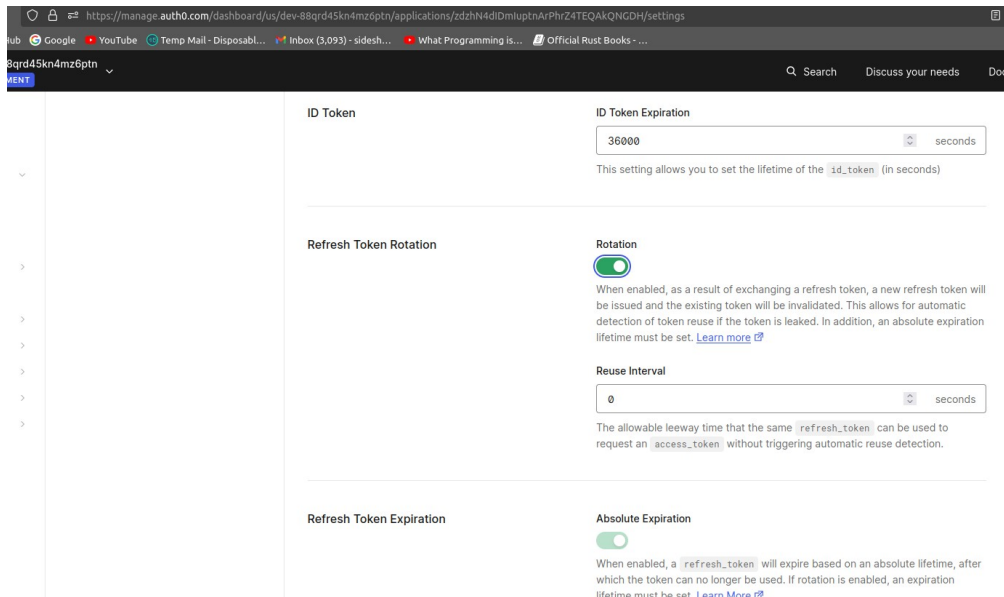


Рисунок 3.4 — Refresh Token Rotation

Побудуємо новий запит та отримаємо новий токену на рисунку 3.5.

```
curl --request POST \
  --url https://dev-88qrd45kn4mz6ptn.us.auth0.com/oauth/token \
  --header 'content-type: application/json' \
  --data
'{"client_id":"zdzhN4dIDmIuptnArPhrZ4TEQAKQNGDH","client_secret":"3e54llBevPi1cN
u22Yr7ggExIntYXkJs7_BZ50TleTF1GFnt3ei0TrSlPkTLK4a","audience":"https://dev-
88qrd45kn4mz6ptn.us.auth0.com/api/
v2/","grant_type":"refresh_token","refresh_token":"oxDixhT-
rQSGTNq0ZdTo3DVdtU7XCU9kMRKLtA10p9RoM"}'
```

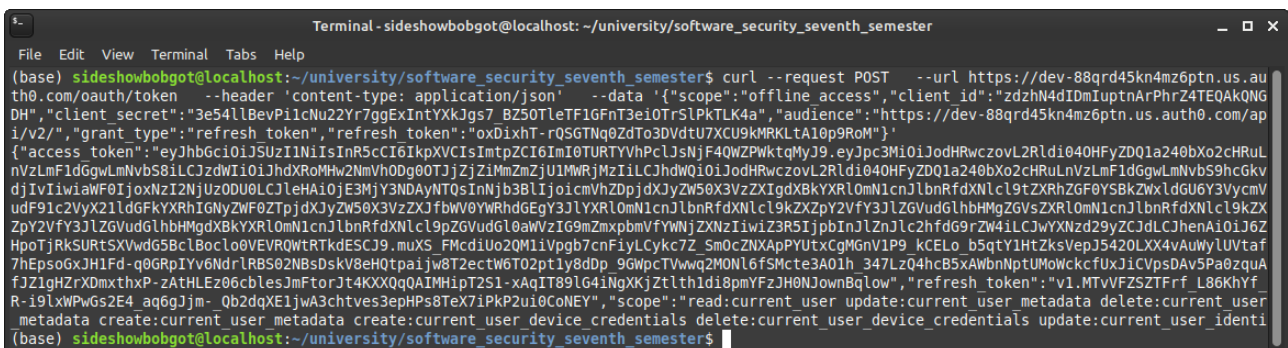


Рисунок 3.5 — Отримання нового токена з refresh токена

У результаті отримали новий access token та refresh token.

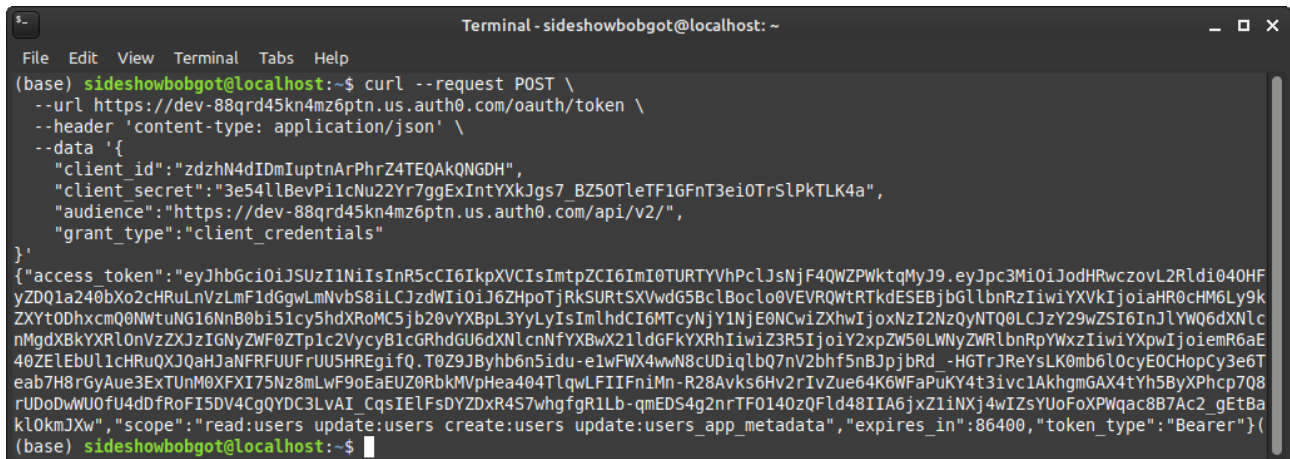
```
{"access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImI0TURTYVhPc  
lJsnJfF4QWZPWktqMyJ9.eyJpc3MiOiJodHRwczovL2Rldi04OHFyZDQ1a240bXo2cHRuLnVzLmF1dGgw  
LmNvbS8iLCJzZdWIiOiJhdXR0Mhw2NmVhODQ0OTJjZjZiMmZmZjU1MWRjZmZiLCJhdWQiOiJl  
siaHR0cHM6
```

Надамо дозволи на оновлення даних користувачів на рисунку 3.6.


```
--data '{
  "client_id":"zdzhN4dIDmIuptnArPhrZ4TEQAKQNGDH",

"client_secret":"3e54llBevPi1cNu22Yr7ggExIntYXkJgs7_BZ50TleTF1GFnt3ei0TrSlPkTLK4
a",

  "audience":"https://dev-88qrd45kn4mz6ptn.us.auth0.com/api/v2/",
  "grant_type":"client_credentials"
}'
```



```
Terminal - sideshowbobgot@localhost: ~
File Edit View Terminal Tabs Help
(base) sideshowbobgot@localhost:~$ curl --request POST \
--url https://dev-88qrd45kn4mz6ptn.us.auth0.com/oauth/token \
--header 'content-type: application/json' \
--data '{
  "client_id":"zdzhN4dIDmIuptnArPhrZ4TEQAKQNGDH",
  "client_secret":"3e54llBevPi1cNu22Yr7ggExIntYXkJgs7_BZ50TleTF1GFnt3ei0TrSlPkTLK4a",
  "audience":"https://dev-88qrd45kn4mz6ptn.us.auth0.com/api/v2/",
  "grant_type":"client_credentials"
}'
{"access_token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImI0TURTYVhPc
lJmNjF4QWZPWktqMyJ9.eyJpc3MiOiJodHRwczovL2Rldi04OHFyZDQ1a240bXo2CHRuLnVzLmF1dGgw
LmNvbS8iLCJzdWIiOiJ6ZHp0TjRkSURtSXVwdG5BclBoclo0VEVRQWtRTkdESEBjbGllbnRzIiwiaXVh
IjoiaHR0cHM6Ly9kZXltODhxcM0NWtuNG16NnB0bi51cy5hdXRoMC5jb20vYXBpL3YyLyIsImldh
dCI6MTcyNjY1NjE0NCwiZXhwIjozNzI2NzQyNTQ0LCJzY29wZSI6InJlYWQ6dXNlcnMgdXBkYXRl
OnVzZXJzIGNyZWZlZDp1c2VycyB1cGRhdGU6dXNlcnNfYXBwX21ldGFkYXRhIiwiaXNjZ3R5Ijo
iY2xpZW50LWVhZWRlbnRpbWxzIiwiaXpwIjoiemR6aE40ZELEbUl1cHRuQXJQaHJaNFRFUUFRU
U5HREg1fQ.T0Z9JBByhb6n5idu-elwFWX4wwN8cUDiqlbQ7nV2bhf5nBJpbRd_-HGTrJReYsLK0
mb6l0cyEOCHopCy3e6Teab7H8rGyAue3ExTUnM0XFXI75Nz8mLwF9oEaEUZ0RbkMVPHea404Tl
qwlFIIFniMn-R28Avks6Hv2rIvZue64K6WfAPuKY4t3ivc1AkhgmGAX4tYh5ByXPhcp7Q8rUD
oDwWU0fU4dDfRoFI5DV4CgQYDC3LVAI_CqsIElFsDYDZXR4S7whgfgR1Lb-qmEDS4g2nrTF014
0zQFl48IIA6jxZ1iNXj4wIZsYUoFoXPWqac8B7Ac2_gEtBakl0kmJXw","scope":"read:users
update:users create:users update:users_app_metadata","expires_in":86400,"token_type":
"Bearer"}
```

Рисунок 3.9 — Отримання нового токenu

Відповідь на запит:

```
{"access_token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImI0TURTYVhPc
lJmNjF4QWZPWktqMyJ9.eyJpc3MiOiJodHRwczovL2Rldi04OHFyZDQ1a240bXo2CHRuLnVzLmF1dGgw
LmNvbS8iLCJzdWIiOiJ6ZHp0TjRkSURtSXVwdG5BclBoclo0VEVRQWtRTkdESEBjbGllbnRzIiwiaXVh
IjoiaHR0cHM6Ly9kZXltODhxcM0NWtuNG16NnB0bi51cy5hdXRoMC5jb20vYXBpL3YyLyIsImldh
dCI6MTcyNjY1NjE0NCwiZXhwIjozNzI2NzQyNTQ0LCJzY29wZSI6InJlYWQ6dXNlcnMgdXBkYXRl
OnVzZXJzIGNyZWZlZDp1c2VycyB1cGRhdGU6dXNlcnNfYXBwX21ldGFkYXRhIiwiaXNjZ3R5Ijo
iY2xpZW50LWVhZWRlbnRpbWxzIiwiaXpwIjoiemR6aE40ZELEbUl1cHRuQXJQaHJaNFRFUUFRU
U5HREg1fQ.T0Z9JBByhb6n5idu-elwFWX4wwN8cUDiqlbQ7nV2bhf5nBJpbRd_-
HGTrJReYsLK0mb6l0cyEOCHopCy3e6Teab7H8rGyAue3ExTUnM0XFXI75Nz8mLwF9oEaEUZ0RbkMVPHe
a404TlqwlFIIFniMn-
R28Avks6Hv2rIvZue64K6WfAPuKY4t3ivc1AkhgmGAX4tYh5ByXPhcp7Q8rUDoDwWU0fU4dDfRoFI5DV
4CgQYDC3LVAI_CqsIElFsDYDZXR4S7whgfgR1Lb-
qmEDS4g2nrTF0140zQFl48IIA6jxZ1iNXj4wIZsYUoFoXPWqac8B7Ac2_gEtBakl0kmJXw","scope"
:"read:users update:users create:users
update:users_app_metadata","expires_in":86400,"token_type":"Bearer"}
```

Будуємо запит для оновлення паролю на рисунку 3.10.

```
curl --request PATCH \
--url 'https://dev-88qrd45kn4mz6ptn.us.auth0.com/api/v2/users/auth0|
66ea88492cf6b2fff551dc32' \
--header 'content-type: application/json' \
```


Спробуємо увійти за старим паролем на рисунку 3.11. Бачимо, що вхід не є успішним.

```
curl --request POST \
  --url https://dev-88qrd45kn4mz6ptn.us.auth0.com/oauth/token \
  --header 'content-type: application/json' \
  --data '{
    "client_id":"zdzhN4dIDmIuptnArPhrZ4TEQAKQNGDH",
    "client_secret":"3e54llBevPi1cNu22Yr7ggExIntYXkJgs7_BZ50TleTF1GFnt3ei0TrSlPkTLK4
a",
    "audience":"https://dev-88qrd45kn4mz6ptn.us.auth0.com/api/v2/",
    "grant_type":"password",
    "username":"panchenko.serhii@lll.kpi.ua",
    "password":"IP11Panchenko",
    "scope":"offline_access openid profile"
  }'
```

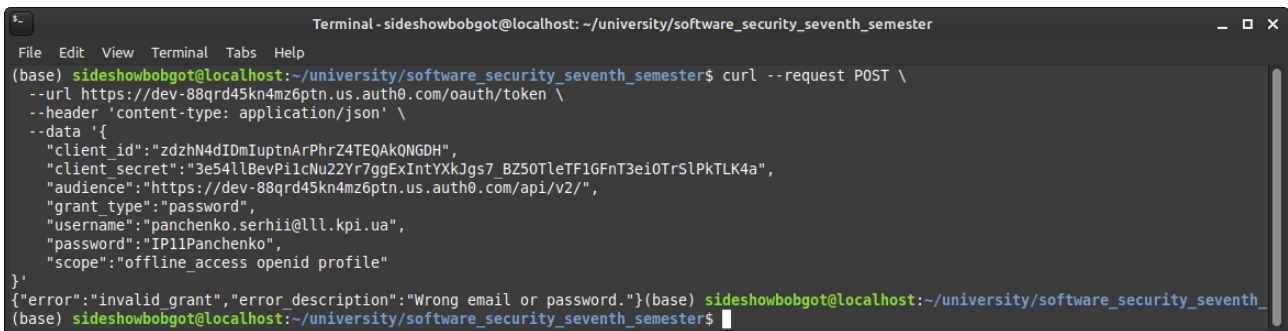


Рисунок 3.11 — Неуспішний вхід зі старим паролем

Спробуємо увійти за новим паролем на рисунку 3.12. Бачимо, що вхід є успішним.

```
curl --request POST \
  --url https://dev-88qrd45kn4mz6ptn.us.auth0.com/oauth/token \
  --header 'content-type: application/json' \
  --data '{
    "client_id":"zdzhN4dIDmIuptnArPhrZ4TEQAKQNGDH",
    "client_secret":"3e54llBevPi1cNu22Yr7ggExIntYXkJgs7_BZ50TleTF1GFnt3ei0TrSlPkTLK4
a",
    "audience":"https://dev-88qrd45kn4mz6ptn.us.auth0.com/api/v2/",
    "grant_type":"password",
    "username":"panchenko.serhii@lll.kpi.ua",
    "password":"IP11_NEW_Password",
    "scope":"offline_access openid profile"
  }'
```


[illegible]

Рисунок 3.12 — Успішний вхід з новим паролем

ВИСНОВОК

У ході виконання лабораторної роботи було поглиблено вивчення протоколу OAuth2, зосередившись на практичному застосуванні різних типів токенів та грантів. Основні завдання включали отримання user access token та оновлення access token за допомогою refresh token, що дозволило краще зрозуміти життєвий цикл токенів. Використання командного рядка та утиліти curl для взаємодії з API Auth0 сприяло глибшому розумінню структури HTTP-запитів та відповідей. Додаткове завдання з реалізації зміни пароля користувача через API розширило практичні навички роботи з Auth0. Успішне подолання технічних викликів, пов'язаних з формуванням запитів та обробкою токенів, дозволило вдосконалити навички управління налаштуваннями безпеки та поглибити розуміння механізмів аутентифікації та авторизації.