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 №2

Безпека ПЗ

Тема: Протокол OAuth2

Виконав
студент групи ІП-11:
Панченко С. В.

Перевірив:
Курченко О. А.

Київ 2024

ЗМІСТ

1 МЕТА ЛАБОРАТОРНОЇ РОБОТИ

Засвоїти базові навички OAuth2 авторизаційного протоколу.

2 ЗАВДАННЯ

1) Використовуючи наведені налаштування, створити запит на отримання токену через client_credential grant

https://auth0.com/docs/api/authentication#client-credentials-flow

curl --request POST --url 'https://YOUR_DOMAIN/oauth/token' --header 'content-type: application/x-www-form-urlencoded'--data 'audience=API_IDENTIFIER&grant_type=client_credentials&client_id=YOUR_CLIENT_ID&cient_secret=YOUR_CLIENT_SECRET'

Domain: kpi.eu.auth0.com

ClientID: JIvCO5c2IBHlAe2patn6l6q5H35qxti0

Client Secret: ZRF8Op0tWM36p1_hxXTU-B0K_Gq_eAVtlrQpY24CasYiDmcXBhNS6IJMNcz1EgB

Audience: https://kpi.eu.auth0.com/api/v2

2) Створити юзера з власним email в системі використовуючи метод https://auth0.com/docs/api/management/v2#!/Users/post_users та отриманий токен.

Для отримання додаткового балу – зробити власний акаунт в auth0 https://auth0.com/.Створити application та запити описані вище вже використовуючи власні налаштування. Детальну інформацію розбирали на практичному завданні.

3 ВИКОНАННЯ

3.1 Створення запиту на отримання токену

На рисунку 3.1 створюємо запит на отримання токену та отримуємо його. Його дія закінчується через 86400 секунд.

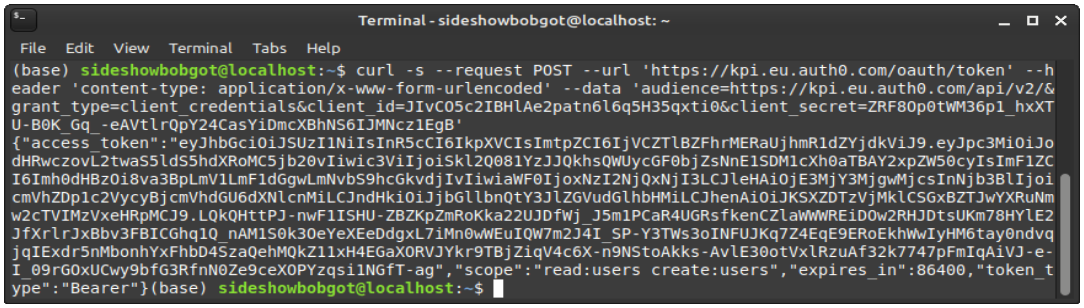

Рисунок 3.1 — Отримання токену

У результаті отримали токен:

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjVCZTlBZFhrMERaUjhmR1dZYjdkViJ9.eyJpc3MiOiJodHRwczovL2twaS5ldS5hdXRoMC5jb20vIiwic3ViIjoiSkl2Q081YzJJQkhsQWUycGF0bjZsNnE1SDM1cXh0aTBAY2xpZW50cyIsImF1ZCI6Imh0dHBzOi8va3BpLmV1LmF1dGgwLmNvbS9hcGkvdjIvIiwiaWF0IjoxNzI2NjQxNjI3LCJleHAiOjE3MjY3MjgwMjcsInNjb3BlIjoicmVhZDp1c2VycyBjcmVhdGU6dXNlcnMiLCJndHkiOiJjbGllbnQtY3JlZGVudGlhbHMiLCJhenAiOiJKSXZDTzVjMklCSGxBZTJwYXRuNmw2cTVIMzVxeHRpMCJ9.LQkQHttPJ-nwF1ISHU-ZBZKpZmRoKka22UJDfWj_J5m1PCaR4UGRsfkenCZlaWWWREiDOw2RHJDtsUKm78HYlE2JfXrlrJxBbv3FBICGhq1Q_nAM1S0k3OeYeXEeDdgxL7iMn0wWEuIQW7m2J4I_SP-Y3TWs3oINFUJKq7Z4EqE9ERoEkhWwIyHM6tay0ndvqjqIExdr5nMbonhYxFhbD4SzaQehMQkZ11xH4EGaXORVJYkr9TBjZiqV4c6X-n9NStoAkks-AvlE30otVxlRzuAf32k7747pFmIqAiVJ-e-I_09rGOxUCwy9bfG3RfnN0Ze9ceXOPYzqsi1NGfT-ag

3.2 Створення користувача

Будуємо запит на рисунку 3.2.

Рисунок 3.2 — Запит з мобільним телефоном

З рисунку 3.2 бачимо, що мобільний телефон не підтримується. Перебудуємо запит на рисунку 3.3. Бачимо, що користувач був зареєстрований у результаті запиту.

Рисунок 3.3 — Запит та відповідь, що користувач зареєстрований

3.3 Додаткове завдання

Для початку створимо тестовий додаток на рисунку 3.4.

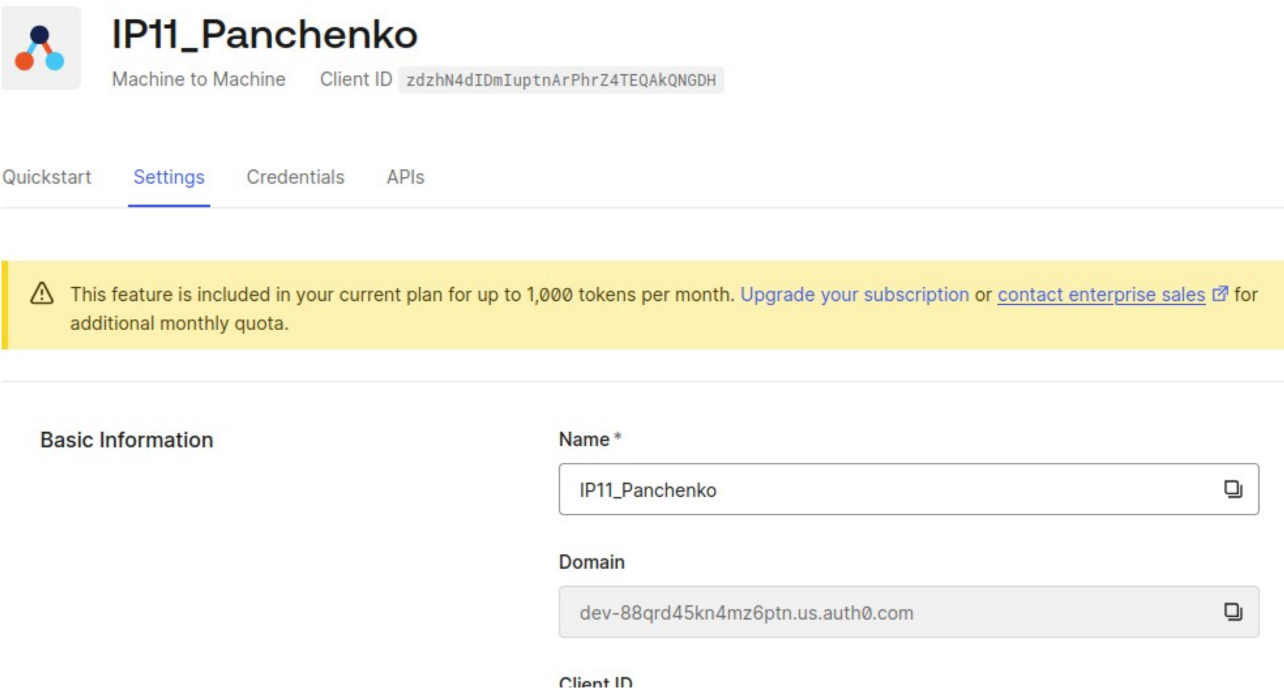

Рисунок 3.4 — Тестовий додаток

Надамо додатку необхідні дозволи на рисунку 3.5.

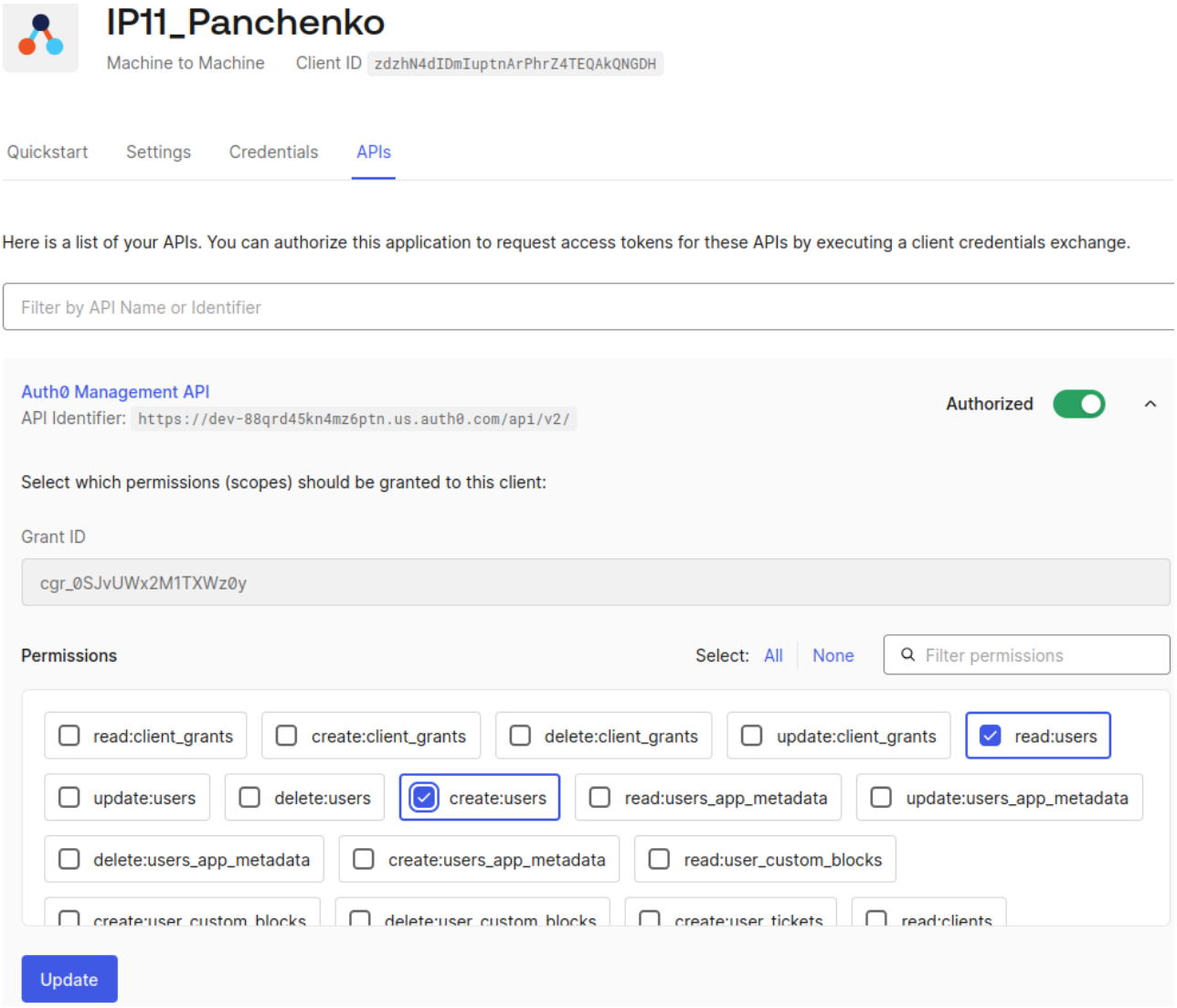

Рисунок 3.5 — Надання дозволів додатку

Спробуємо отримати токен на рисунку 3.6.

```
curl --request POST \
        --url https://dev-88qrd45kn4mz6ptn.us.auth0.com/oauth/token \
        --header 'content-type: application/json' \
        --data
'{"client_id":"zdzhN4dIDmIuptnArPhrZ4TEQAkQNGDH","client_secret":"3e54llBevPi1cN
u22Yr7ggExIntYXkJgs7_BZ5OTleTF1GFnT3eiOTrSlPkTLK4a","audience":"https://dev-
88qrd45kn4mz6ptn.us.auth0.com/api/v2/","grant_type":"client_credentials"}'
```

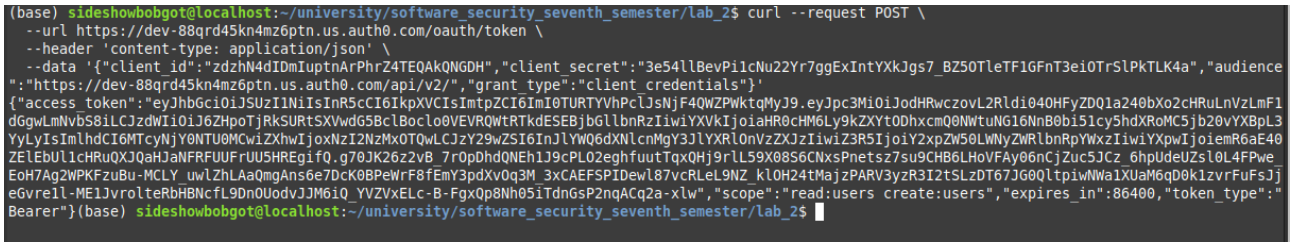

Рисунок 3.6 — Отримання токену

Отримали токен:

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImI0TURTYVhPclJsNjF4QWZPWktqMy
J9.eyJpc3MiOiJodHRwczovL2Rldi04OHFyZDQ1a240bXo2cHRuLnVzLmF1dGgwLmNvbS8iLCJzdWIiO
iJ6ZHpoTjRkSURtSXVwdG5BclBoclo0VEVRQWtRTkdESEBjbGllbnRzIiwiYXVkIjoiaHR0cHM6Ly9kZ
XYtODhxcmQ0NWtuNG16NnB0bi51cy5hdXRoMC5jb20vYXBpL3YyLyIsImlhdCI6MTcyNjY0NTU0MCwiZ
XhwIjoxNzI2NzMxOTQwLCJzY29wZSI6InJlYWQ6dXNlcnMgY3JlYXRlOnVzZXJzIiwiZ3R5IjoiY2xpZ
W50LWNyZWRlbnRpYWxzIiwiYXpwIjoiemR6aE40ZElEbUl1cHRuQXJQaHJaNFRFUUFrUU5HREgifQ.g7
0JK26z2vB_7rOpDhdQNEh1J9cPLO2eghfuutTqxQHj9rlL59X08S6CNxsPnetsz7su9CHB6LHoVFAy06
nCjZuc5JCz_6hpUdeUZsl0L4FPwe_EoH7Ag2WPKFzuBu-
MCLY_uwlZhLAaQmgAns6e7DcK0BPeWrF8fEmY3pdXvOq3M_3xCAEFSPIDewl87vcRLeL9NZ_klOH24tM
ajzPARV3yzR3I2tSLzDT67JG0QltpiwNWa1XUaM6qD0k1zvrFuFsJjeGvre1l-
ME1JvrolteRbHBNcfL9DnOUodvJJM6iQ_YVZVxELc-B-FgxQp8Nh05iTdnGsP2nqACq2a-xlw

Відправимо запит на створення користувача на рисунку 3.7.

```
curl -s -L 'https://dev-88qrd45kn4mz6ptn.us.auth0.com/api/v2/users' \
-H 'Content-Type: application/json' \
-H 'Accept: application/json' \
-H 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImI0TURTYVhPclJsNjF4QWZPWktqMyJ9.eyJ
pc3MiOiJodHRwczovL2Rldi04OHFyZDQ1a240bXo2cHRuLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJ6ZHp
oTjRkSURtSXVwdG5BclBoclo0VEVRQWtRTkdESEBjbGllbnRzIiwiYXVkIjoiaHR0cHM6Ly9kZXYtODh
xcmQ0NWtuNG16NnB0bi51cy5hdXRoMC5jb20vYXBpL3YyLyIsImlhdCI6MTcyNjY0NTU0MCwiZXhwIjo
xNzI2NzMxOTQwLCJzY29wZSI6InJlYWQ6dXNlcnMgY3JlYXRlOnVzZXJzIiwiZ3R5IjoiY2xpZW50LWN
yZWRlbnRpYWxzIiwiYXpwIjoiemR6aE40ZElEbUl1cHRuQXJQaHJaNFRFUUFrUU5HREgifQ.g70JK26z
2vB_7rOpDhdQNEh1J9cPLO2eghfuutTqxQHj9rlL59X08S6CNxsPnetsz7su9CHB6LHoVFAy06nCjZuc
5JCz_6hpUdeUZsl0L4FPwe_EoH7Ag2WPKFzuBu-
MCLY_uwlZhLAaQmgAns6e7DcK0BPeWrF8fEmY3pdXvOq3M_3xCAEFSPIDewl87vcRLeL9NZ_klOH24tM
ajzPARV3yzR3I2tSLzDT67JG0QltpiwNWa1XUaM6qD0k1zvrFuFsJjeGvre1l-
ME1JvrolteRbHBNcfL9DnOUodvJJM6iQ_YVZVxELc-B-FgxQp8Nh05iTdnGsP2nqACq2a-xlw' \
--data-raw '{
    "email":"panchenko.serhii@lll.kpi.ua",
    "user_metadata":{},
    "blocked":false,
    "email_verified":false,"app_metadata":{},
    "given_name":"Serhii",
    "family_name":"Panchenko",
    "name":"Serhii",
    "nickname":"Panchenko",
    "picture":"https://sonicsuperstars.com/img/characters/sonic.png",
    "connection":"Username-Password-Authentication",
    "password":"IP11Panchenko",
    "verify_email":false
}'
```

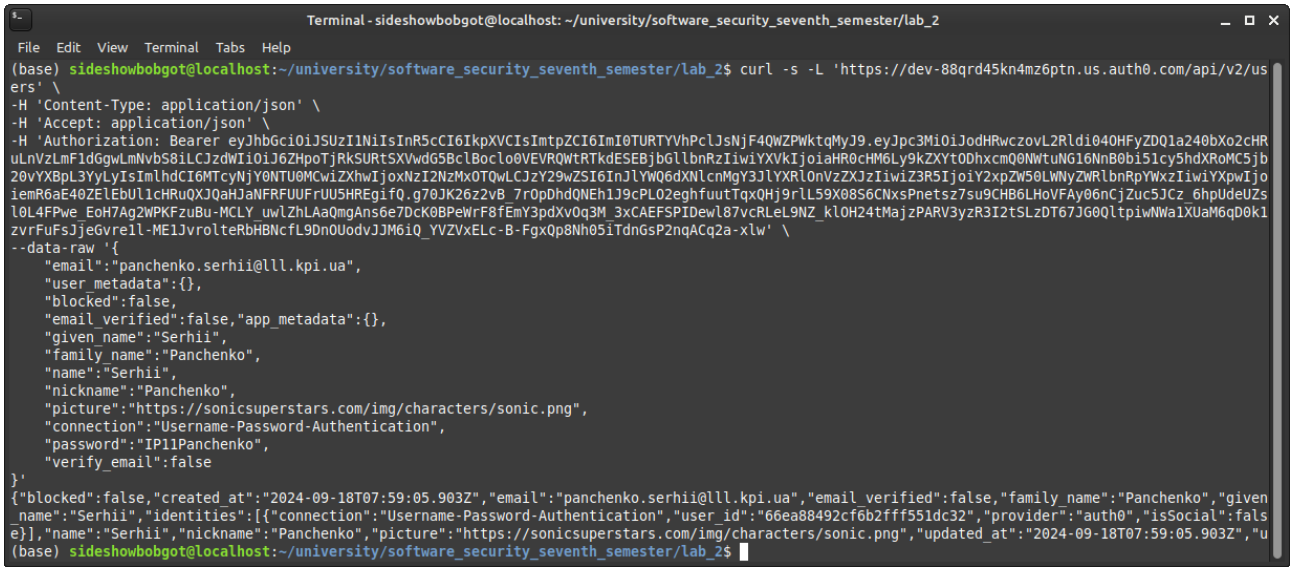

Рисунок 3.7 — Додавання нового користувача

Переглянемо доданого користувача на вкладці User Management/Users на рисунку 3.8.

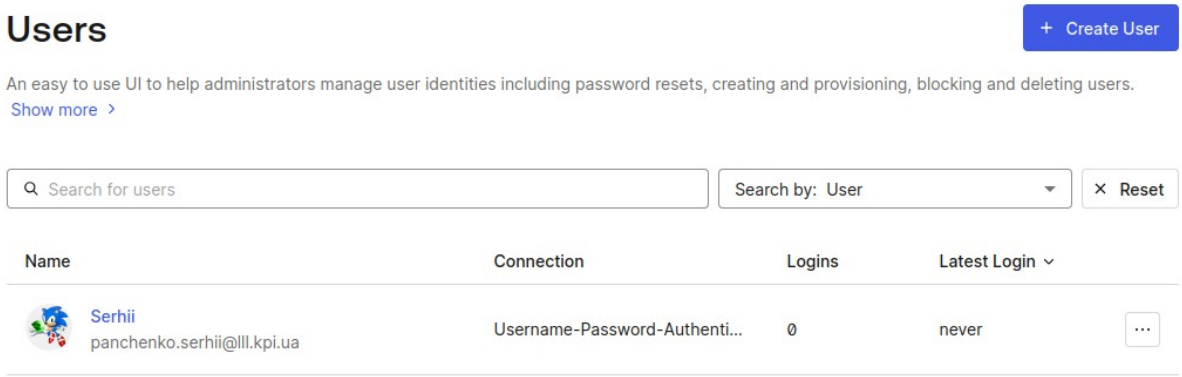

Рисунок 3.8 — Доданий користувач

ВИСНОВОК

У рамках цієї лабораторної роботи були успішно засвоєні основні принципи роботи з OAuth 2.0. Практична частина включала отримання токенів авторизації в системі КПІ та у власноруч створеному додатку, а також створення облікових записів користувачів з використанням єдиної електронної адреси. Робота з API управління Auth0 для створення користувачів надала цінний досвід у сфері програмного управління обліковими записами. Додатково, створення власного облікового запису в Auth0 та налаштування персонального додатку дозволило отримати практичний досвід роботи з реальною системою управління ідентифікацією та доступом. Загалом, ця лабораторна робота заклала міцний фундамент для подальшого вивчення та застосування сучасних протоколів безпеки в розробці веб-додатків.