

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 Перевірив:

студент групи ІП-11: Курченко О. А.

Панченко С. В.

3MICT

1 Мета лабораторної роботи	6
2 Завдання	
3 Виконання	8
3.1 Створення запиту на отримання токену	8
3.2 Створення користувача	8
3.3 Додаткове завдання	9
Висновок	13

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.

```
File Edit View Terminal Tabs Help

(base) sideshowbobgot@Localhost:-$ curl -s --request POST --url 'https://kpi.eu.auth0.com/oauth/token' --h eader 'content-type: application/x-www-form-urlencoded' --data 'audience=https://kpi.eu.auth0.com/api/v2/& grant_type=client_credentials&client_id=JIvCO5c2IBHlAe2patn6l6q5H35qxti0&client_secret=ZRF80p0tWM36p1_hxXT U-B0K_6q_-eAVtI-OpV24CasyIDmxCRNhS65JNMcz1EgB'

{"access_token":"eyJhbGci0iJSUzIINiIsInR5cC16IkpXVCIsImtpZC16IjVCZTlBZFhrMERaUjhmR1dZYjdkViJ9.eyJpc3M10iJodHRwczovL2twaS5ldS5hdXRoMC5jb20vIiwic3ViIjoiSkL2Q081IY2JJQkhSQWUycGF0bjZsNnE1SDM1cXh0aTBAY2xpZW95cyIsImF1ZC16Imh0dHBZ018va3BpLmV1LmF1dGgwLmwNb59hc6kvdjIvIiwiaWF0IjoxVZ12NjQxwJj3lLCJleHalt0jE3MjY3MjgwMjcSInNjb3BIJjoicmVhZDp1c2VycyBjcmVhdGU6dXNlcnMiLCJndHki0iJjbGllbnQtY3JlZGVudGlhbHMiLCJhenAi0iJKSXZDTzVjMklCSGxBZTJwYXRuNmw2cTVIMzVxeHRpMCJ9.LQkQHttPJ-nwF1ISHU-ZBZKpZmRoKka2ZUJDfwj_J5m1PcAR4UGRsfkenCzlaWwNREiD0w2RHJDtsUKm78HYlEzJfXrlrJxBbv3FBIGGhql0_nAM1Sok320eveXEeDdgxL7iMnowWeILIOW7m2J1S-Pv3TWs3oINFUJMG7Z4EqBeBoEkhwklyHM6tay0mdvqjqIExdr5nMbonhYxFhbD45zaQehMQkZ11xH4EGaXORVJYkr9TBjZiqV4c6X-n9NStoAkks-AvlE30otVxlRzuAf32k7747pFmIqAiVJ-e-I_09rG0xUCwy9bfG3RfnN0Ze9ceXOPYzqsi1NGfT-ag", "scope": "read:users create:users", "expires_in":86400, "token_t ype": "Bearer"}(base) sideshowbobgot@localhost:-$
```

Рисунок 3.1 — Отримання токену

У результаті отримали токен:

eyJhbGci0iJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjVCZTlBZFhrMERaUjhmR1dZYjdkViJ9.eyJpc3Mi0iJodHRwczovL2twaS5ldS5hdXRoMC5jb20vIiwic3ViIjoiSkl2Q081YzJJQkhsQWUycGF0bjZsNnE1SDM1cXh0aTBAY2xpZW50cyIsImF1ZCI6Imh0dHBz0i8va3BpLmV1LmF1dGgwLmNvbS9hcGkvdjIvIiwiaWF0IjoxNzI2NjQxNjI3LCJleHAi0jE3MjY3MjgwMjcsInNjb3BlIjoicmVhZDp1c2VycyBjcmVhdGU6dXNlcnMilCJndHki0iJjbGllbnQtY3JlZGVudGlhbHMilCJhenAi0iJKSXZDTzVjMklCSGxBZTJwYXRuNmw2cTVIMzVxeHRpMCJ9.LqkQHttPJ-nwF1ISHU-

ZBZKpZmRoKka22UJDfWj_J5m1PCaR4UGRsfkenCZlaWWWREiDOw2RHJDtsUKm78HYlE2JfXrlrJxBbv3FBICGhq1Q_nAM1S0k30eYeXEeDdgxL7iMn0wWEuIQW7m2J4I_SP-

Y3TWs3oINFUJKq7Z4EqE9ERoEkhWwIyHM6tay0ndvqjqIExdr5nMbonhYxFhbD4SzaQehMQkZ11xH4EGaX0RVJYkr9TBjZiqV4c6X-n9NStoAkks-AvlE30otVxlRzuAf32k7747pFmIqAiVJ-e-

I_09rG0xUCwy9bfG3RfnN0Ze9ceX0PYzqsi1NGfT-ag

3.2 Створення користувача

Будуємо запит на рисунку 3.2.

Рисунок 3.2 — Запит з мобільним телефоном

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

```
File Edit View Terminal Tabs Help

/software_security_seventh_semester/lab_25 curl -s -L 'https://kpi.eu.auth0.com/api/v2/users' \rs'\

H 'Content-Type: application/json' \
H 'Authorization: Bearer eylhbic101JSUZ1NiIsInR5cC16IkpXVCIsImtpZC16IjVCZTlBZPhrMERaUjhmR1dZYjdkVIJ9.eyJpc3Mi01JodHRwczovLztwaS5ldS5hdXRoMC5jb28vIiw
ic3VIIjoiskl2088IY2JOkhsQMUycGPbjzsNnelSDNlcXhbdaTBAYzayZxSbcytsImtpZC16ImbdHEX018va3BpLmVlLmF1dGgyLmNvbSshcGkvdjVIIiwlaWFbjjoxklzZNjOkhyNj3LCLleHAlD
jEMNjY3NjgwhjgisInNjy3BlIJjoicMN/DplzCytyyejBcmModdWdddWNlcMHLClmhc10JibjoilNopV3JZCVJWHHBHLCDhenholJSXCDIZVJMHKGXSOEZTJWXTMUMmeZCYVIPZVWHBHDCD
j.UQkOHttPJ-nnF1ISHU-ZBZXpZmMokkAz2UJDYmj J3m PCaR4UGR5fkenCZlaWNMEIDDVZHHJDTSWKn3PHYLEZJTXrTrJxBbV3FBICCNc10_nnMIS6k30eYeXEEDdgxL7JNhnOwMeIDWN7ZJ4I
FY-Y3TWS2DHVLMQ7Z4EdgeDEACHMWJYMHARAYAND4AVATAPFHTATAPT-nnF1ISHU-ZBZXpZmMokkAz2UJDYmj J3m PCaR4UGR5fkenCZlaWNMEIDWZPHZJYXFTTSXBbV3FBICCNc10_nnAMIS6k30eYeXEEDdgxL7JNhnOwMeIDWN7ZJ4I
FY-Y3TWS2DHVLMQ7Z4EdgeDeACHMWJYMHARAYAND4XPAYAPFHTATAPT-nnF1ISHU-ZBZXpZmMokkAs-AVLE30ctVxlRzuAf3zk7747pFmIqAiVJ-e
-I @97CbVUCky9bfCsAftNND2e9cxXDPYzqs11NGfT-ag' \
-data-raw '"user metadata*i':{},
    "blocked*:false,
    "app metadata*i:{},
    "app metadata*i:{},
    "aname*:"Serhii",
    "inckname*:Pannchenko*,
    "picture*:Phtps://www.google.com/url?sa=i&url=https%3A%2F%2Fsonicsuperstars.com%2F&psig=AOvVaw3NJGibaTL85ZL-7RBqVlgt&ust=1726728496180000&source=images&cd=vf&opj=88978449&ved=0E00jRxqFwoTfCKFc0znzy4gDFQAAAAAdAAAAAA*,
    "connection*:Username*-Password-Authentication*,
    "password*::FPIIPanchenko*,
    "verify_enall*:false,
    "dentities*:[{"connection*:"Username-Password-Authentication*, user id*:"66ea78a2180694c25ze69466*, "provider*:auth0**, isocial*:false
    "Norder*: Serhii*, "identities*:[{"connection*:"Username-Password-Authentication*, user id*:"66ea78a2180694c25ze69466*, "provider*:auth0**, isocial*:false
    "plocked*:false, "created at*:"2824-09-18706:52:18.746Z*, "email*:"panchenko, serhii*, "identities*:[{"connection*:"Username-Password-Authentication*, u
```

Рисунок 3.3 — Запит та відповідь, що користувач зареєстрований

3.3 Додаткове завдання

Для початку створимо тестовий додаток на рисунку 3.4.

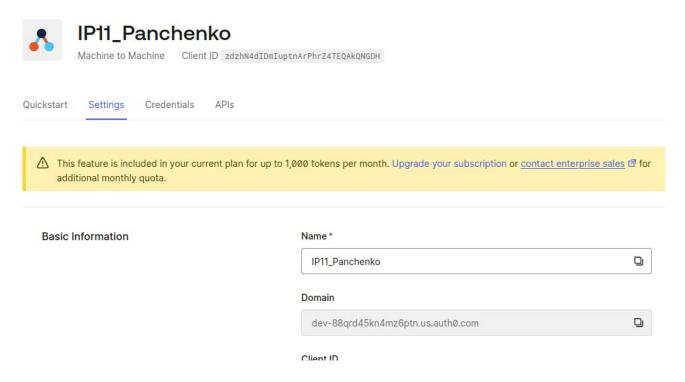


Рисунок 3.4 — Тестовий додаток

Надамо додатку необхідні дозволи на рисунку 3.5.

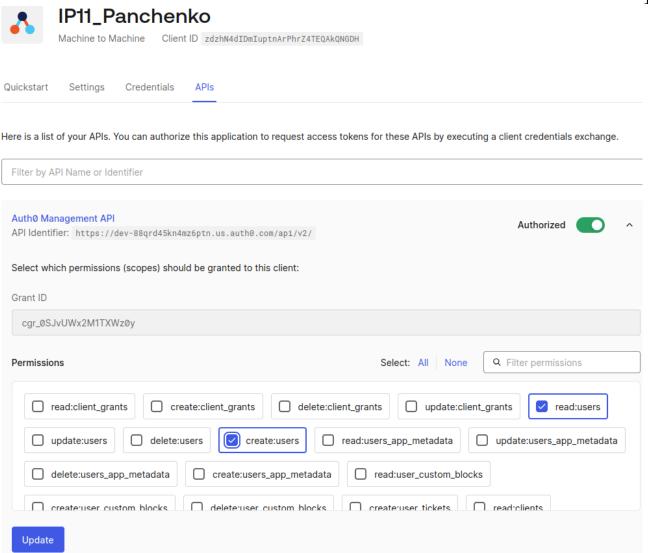


Рисунок 3.5 — Надання дозволів додатку

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":"3e54llBevPi1cNu22Yr7ggExIntYXkJgs7_BZ50TleTF1GFnT3ei0TrSlPkTLK4a","audience":"https://dev-88qrd45kn4mz6ptn.us.auth0.com/api/v2/","grant_type":"client_credentials"}'

```
(base) sideshowbobgot@localhost:-/university/software_security_seventh_semester/lab_2$ curl --request POST \
--url https://dev-88qrd45kn4mz6ptn.us.auth0.com/oauth/token \
--header 'content-type: application/json' \
--data '{"client_id":"zdzhNd4dIDmluptnArPhrZatEQAkONGDH","client_secret":"3e54llBevPilcNu22Yr7ggExIntYXkJgs7_BZ50TleTF1GFnT3ei0TrSlPkTLK4a","audience
":"https://dev-88qrd45kn4mz6ptn.us.auth0.com/api/v2/","grant_type":"client_credentials"}'
{"access token":"eyJhbGci0iJSUzIINisInR5cCI6IkpXvCIsImtpZCI6ImI0TURTYVhPciJsNjF4QWZPWktqMyJ9.eyJpc3Mi0iJodHRwczovL2Rldi040HFyZDQ1a240bXo2cHRuLnVzLmF1
dGgwLmNvbSsiLCJzdWIJi0iJ6ZHpoTjRkSURTSXXWdG5BclBoclo0VEVRQWHTRtdESEBjBollbnRzIiwiyXVKJjoiaHR0cHM6Ly9kZXYtODDhxcmQONWtuNG16NnB0bi5lcy5hdXR0MC5jb20vYXBpL3
YYLyIsImlhdCI6MTcyNjY0NTU0MCwiZXhwIjoxNzI2NzMxoTQwLCJzY29wZ5I6InJlYW06dXNlcnMgY3J\YXRl0nVzZXJzIiwiZ3R5IjoiY2xpZW50LWNyZWRlbnRpYWxzIiwiYXpwIjoiemR6aE40
ZELEbUllcHRuQXJQaHJaNFRFUUFrUU5HREgifQ.g70JKZ62z9B 7r0pDhdQNEh1J9cPL02eghfuutTqxQHj9rLL59X0856CNxsPnetsz7su9CHB6LHoVFAy06nCjZuc5JCz 6hpUdeUZsl0L4FPwe
E0H7Ag2MPKFzUBU-MCLY uwlZhLAadmgAns6e5TORCK0BPewrrRsfEmY3pdXvQ3M 3xcAEFSPIDewlRsfvcRLeyNZ_klOH24tHajzPaRAVJyzR3IZtSLzDf67J300QltjbiuMWalJXJM6QD0H3JVFFUESJjf
eGvrell-MElJvrolteRbHBNcfL9Dn0UodvJJM6iQ_YVZVxELc-B-FgxQp8Nh05iTdnGsP2nqACq2a-xlw", "scope":"read:users create:users", "expires_in":86400, "token_type":"
Bearer"}(base) sideshowbobgot@localhost:-/university/software_security_seventh_semester/lab_2$

■
```

Рисунок 3.6 — Отримання токену

Отримали токен:

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImIOTURTYVhPclJsNjF4QWZPWktqMy
J9.eyJpc3MiOiJodHRwczovL2Rldi04OHFyZDQ1a240bXo2cHRuLnVzLmF1dGgwLmNvbS8iLCJzdWIiO
iJ6ZHpoTjRkSURtSXVwdG5BclBoclo0VEVRQWtRTkdESEBjbGllbnRzIiwiYXVkIjoiaHR0cHM6Ly9kZ
XYtODhxcmQ0NWtuNG16NnB0bi51cy5hdXRoMC5jb20vYXBpL3YyLyIsImlhdCI6MTcyNjY0NTU0MCwiZ
XhwIjoxNzI2NzMxOTQwLCJzY29wZSI6InJlYWQ6dXNlcnMgY3JlYXRl0nVzZXJzIiwiZ3R5IjoiY2xpZ
W50LWNyZWRlbnRpYWxzIiwiYXpwIjoiemR6aE40ZElEbUl1cHRuQXJQaHJaNFRFUUFrUU5HREgifQ.g7
0JK26z2vB_7r0pDhdQNEh1J9cPL02eghfuutTqxQHj9rlL59X08S6CNxsPnetsz7su9CHB6LHoVFAy06
nCjZuc5JCz_6hpUdeUZsl0L4FPwe_EoH7Ag2WPKFzuBu-

 $\label{lem:mcly_uwlzhlaaQmgAns6e7DcK0BPeWrF8fEmY3pdXv0q3M_3xCAEFSPIDewl87vcRLeL9NZ_kl0H24tMajzPARV3yzR3I2tSLzDT67JG0QltpiwNWa1XUaM6qD0k1zvrFuFsJjeGvre1l-$

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
```

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImIOTURTYVhPclJsNjF4QWZPWktqMyJ9.eyJpc3MiOiJodHRwczovL2RldiO4OHFyZDQ1a240bXo2cHRuLnVzLmF1dGgwLmNvbS8iLCJzdWIiOiJ6ZHpoTjRkSURtSXVwdG5BclBocloOVEVRQWtRTkdESEBjbGllbnRzIiwiYXVkIjoiaHROcHM6Ly9kZXYtODhxcmQONWtuNG16NnBObi51cy5hdXRoMC5jb2OvYXBpL3YyLyIsImlhdCI6MTcyNjYONTUOMCwiZXhwIjoxNzI2NzMxOTQwLCJzY29wZSI6InJlYWQ6dXNlcnMgY3JlYXRlOnVzZXJzIiwiZ3R5IjoiY2xpZW50LWNyZWRlbnRpYWxzIiwiYXpwIjoiemR6aE40ZElEbUl1cHRuQXJQaHJaNFRFUUFrUU5HREgifQ.g70JK26z2vB_7rOpDhdQNEh1J9cPLO2eghfuutTqxQHj9rlL59X08S6CNxsPnetsz7su9CHB6LHoVFAyO6nCjZuc5JCz_6hpUdeUZslOL4FPwe_EOH7Ag2WPKFzuBu-

 $\label{lem:mcly_uwlzhlaaQmgAns6e7DcK0BPeWrF8fEmY3pdXv0q3M_3xCAEFSPIDewl87vcRLeL9NZ_kl0H24tMajzPARV3yzR3I2tSLzDT67JG0QltpiwNWa1XUaM6qD0k1zvrFuFsJjeGvre1l-$

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.

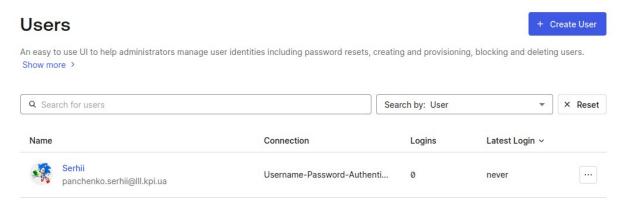


Рисунок 3.8 — Доданий користувач

ВИСНОВОК

У рамках цієї лабораторної роботи були успішно засвоєні основні принципи роботи з ОАuth 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 АРІ управління AuthO для створення користувачів надала цінний досвід у сфері програмного управління обліковими записами. Додатково, створення власного облікового запису в AuthO 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.