МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ЗВІТ

Про виконання лабораторної роботи №3
З дисципліни “Безпека програмного забезпечення”
На тему “Засвоювання базових навичок OAuth2 авторизаційного протокола”

Виконали:
Студенти групи ІП-15
Мєшков А. І.

Перевірила:
пос. Соколовський В. В.

Київ 2024

ЛАБОРАТОРНА РОБОТА №3

Завдання:

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

https://auth0.com/docs/api/authentication?javascript#resource-owner-password

```
POST https://YOUR_DOMAIN/oauth/token
                application/x-www-form-urlencoded

audience=API_IDENTIFIER&grant_type=client_credentials&client_id=YOUR_C
LIENT_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.

ХІД РОБОТИ

1. Використовуючи наведені налаштування з лабораторної роботи 2 зробити запит на отримання user toke

```
curl --request POST \
--url 'https://kpi.eu.auth0.com/oauth/token' \
--header 'content-type: application/x-www-form-urlencoded' \
--data 'audience=https://kpi.eu.auth0.com/api/v2/' \
--data 'grant_type=client_credentials' \
--data 'client_id=JIvCO5c2IBHlAe2patn6l6q5H35qxti0' \
--data 'client_secret=ZRF8Op0tWM36p1_hxXTU-B0K_Gq_-
eAVtlrQpY24CasYiDmcXBhNS6IJMNcz1EgB'
```

Відповідь:

{"**access_token**":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjVCZTlBZFhrMERaUjhmR1dZYjdkViJ9.eyJpc3MiOiJodHRwczovL2twaS5ldS5hdXRoMC5jb20vIiwic3ViIjoiSkl2Q081YzJJQkhsQWUycGF0bjZsNnE1SDM1cXh0aTBAY2xpZW50cyIsImF1ZCI6Imh0dHBzOi8va3BpLmV1LmF1dGgwLmNvbS9hcGkvdjIvIiwiaWF0IjoxNzM0MjAxNjAzLCJleHAiOjE3MzQyODgwMDMsInNjb3BlIjoicmVhZDp1c2VycyBjcmVhdGU6dXNlcnMiLCJndHkiOiJjbGllbnQtY3JlZGVudGlhbHMiLCJhenAiOiJKSXZDTzVjMklCSGxBZTJwYXRuNmw2cTVIMzVxeHRpMCJ9.V0CRo5QMoAW_-jlXzG7zIUqXEzz0agrLwt2I-KbvQOHqbRlssHGycYntGtp-SXt0ITcyKR4MJa1jSEJNq9oztkwdbAIzqs31AgrUKI3Kxbwy7L2kRw0YjIDNwTpuAHHg1llutQvGEMvi0y74MSXgHTfHZ4xEJYWzCi3u7x05fgysTlLNTIXEWrUKyK32u58KX65kMpOJQXyP1xJmREq0hntAAKTCkMWQSin1K46AfKxunl4TznAaC4SZnbTvnBbPhD6mkeHxmykKckC4cNPOoHTIwAI7din9XOQCHEP5OFP27JIQBB8kNk7vtbntwJgTM60jqZPUuXsehJjy6rL0uQ",
"**scope**":"read:users create:users",
"**expires_in**":86400,
"**token_type**":"Bearer"}

2. Отримати оновлений токен використовуючи refresh-token grant type

Отримаємо code:
https://kpi.eu.auth0.com/authorize?response_type=code&client_id=JIvCO5c2IBHlAe2patn6l6q5H35qxti0&redirect_uri=http://localhost:3000&scope=openid

Отримаємо рефреш токен

```
curl --request POST \
  --url 'https://kpi.eu.auth0.com/oauth/token' \
  --header 'content-type: application/x-www-form-urlencoded' \
  --data 'grant_type=authorization_code' \
  --data 'code=rK7JVTSQtpTgymLewrWRLfTdt7iW2kFgUQZ1llPfNX2lW' \
  --data 'redirect_uri=http://localhost:3000' \
  --data 'client_id=JIvCO5c2IBHlAe2patn6l6q5H35qxti0' \
  --data 'client_secret=ZRF8Op0tWM36p1_hxXTU-B0K_Gq_-
eAVtlrQpY24CasYiDmcXBhNS6IJMNcz1EgB'
```

Відповідь:
{"**access_token**":"eyJhbGciOiJkaXIiLCJlbmMiOiJBMjU2R0NNIiwiaXNzIjoiaHR0cHM6Ly9rcGkuZXUuYXV0aDAuY29tLyJ9..Tc9GIHyqYCfH7jtx.oOS2OebIWFeEHBsgfzZcpNQ0qqj0jyL27iXNtcOKnFWkXgvdBBuJuQYJy5rEhs_-J8Rt0Hc0inIglmol0Rk6w5ZZj1UExUFXoPhEuikUo_0WKI7e1Yj8sdz90jX5Ityko5lqn2Qnn0nOoBasoymeRV3SUsRBCxbQqKY9GW14IefdD6PgUFT-YY7Zd-D5SZa42k5vRdcf0RVAQmfsCHNQauyrNuBep1zMYKK1k9nSFiSdPA9McwKYVkcWwg0Y_PMzIQg9WmN0lPWuVtDmOD4XwKJ3T5Tl_SDCK1ZoWx9Mzxoa.k7-uF_lhwPGkQ_6COfPJ9g",
"**refresh_token**":"NQHEBKI5NK9TGBrF7E6ZD8a1PwbH678MYt0JbHi9CmtGh",
"**id_token**":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjVCZTlBZFhrMERaUjhmR1dZYjdkViJ9.eyJpc3MiOiJodHRwczovL2twaS5ldS5hdXRoMC5jb20vIiwiYXVkIjoiSkl2Q081YzJJQkhsQWUycGF0bjZsNnE1SDM1cXh0aTAiLCJpYXQiOjE3MzQyMDQxOTMsImV4cCI6MTczNDI0MDE5Mywic3ViIjoiYXV0aDB8Njc1ZGM5NjA3OTdkY2Y0NmFhM2VlZDBjIiwic2lkIjoiNE1TSVFXbExib05FRllxZGJLTUZIcTFZR2piTnNTSl8ifQ.GhK2BRDRq06a-8VLqMFT5sdFpvximgE0GlzkEpebFvlz-coZYg6gnNnIyUOrHeq2R8_ShHB_D7TTH5fJQD0kNeZiGduZm_hFOymp0cvG6dGX20Vl24VAFsx7WUMovCNlnq_aCZY4iSi_tFv1mgUmnxFZNYI7qadU0FYtHD7tZ_gXIrR9RL6uR42F5AGtEMoFt5YGpsuTYoJ_qphFIMLoyJ7Wd-gYQaky8qrZgJ2Q5PNItLAp5mJfSbifZSssw7wDRLy-a9WBfMGOK5tWrqasInmoyyUTS08ldbNisnUVYoUn3Q4UBBw7KkDGFLBi8HHNHaiXfuhhe0nROs2MHcHxOg",
"**scope**":"openid offline_access",
"**expires_in**":86400,
"**token_type**":"Bearer"}

Тепер оновимо токен:

```
curl --request POST \
  --url 'https://kpi.eu.auth0.com/oauth/token' \
  --header 'content-type: application/x-www-form-urlencoded' \
  --data 'grant_type=refresh_token' \
  --data 'refresh_token=NQHEBKI5NK9TGBrF7E6ZD8a1PwbH678MYt0JbHi9CmtGh' \
  --data 'client_id=JIvCO5c2IBHlAe2patn6l6q5H35qxti0' \
  --data 'client_secret=ZRF8Op0tWM36p1_hxXTU-B0K_Gq_-
eAVtlrQpY24CasYiDmcXBhNS6IJMNcz1EgB'
```

Відповідь:

{"**access_token**":"eyJhbGciOiJkaXIiLCJlbmMiOiJBMjU2R0NNIiwiaXNzIjoiaHR0cHM6Ly9rcGkuZXUuYXV0aDAuY29tLyJ9..IUHQYPvIEqsrM5Cy.KRGC6qWriqzl-QCCtZDS8xl-W70bsXdsuEEHDbLq7geIVgDYufgqFJS-w2R_1PLYcDdHmum7llhbWxhB1lzLXIa-vrnuxpFiXQGmGoJfmHJ2QV16DZJVX_xks0ED1DhV6tDLTeBqTt0UIeJpl597Qd97LJwkD-LjE7wWuCctLNRYUBuM5hugElo78GwkRfi0XTKnt-SY-fGaSMHiUCBx1wsMyEYi8FR4W4orBBAiXj670n7UvKI6Onm5sQ8w1DWpDmhu_6Z-N2IB8sBADmYAZBW-ty0XH02IkS35vNL7L0ul.z3Ygp2aqg79MslglCl_AvQ",
"**id_token**":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjVCZTlBZFhrMERaUjhmR1dZYjdkViJ9.eyJpc3MiOiJodHRwczovL2twaS5ldS5hdXRoMC5jb20vIiwiYXVkIjoiSkl2Q081YzJJQkhsQWUycGF0bjZsNnE1SDM1cXh0aTAiLCJpYXQiOjE3MzQyMDQzNDMsImV4cCI6MTczNDI0MDM0Mywic3ViIjoiYXV0aDB8Njc1ZGM5NjA3OTdkY2Y0NmFhM2VlZDBjIiwic2lkIjoiNE1TSVFXbExib05FRllxZGJLTUZIcTFZR2piTnNTSl8ifQ.dnjcNJpiNWn9evXYkUF9sA6oPkVsPIOCmRaO51pdwAIkH549Nd3RrLv-Kk63DTlY1MlZivIkiqiH9Drpve-bVpHXI_9gpjDTS_PtC4kDKIMrOxEafmgH2MA6WnNCD8w1Ll9lGpLwe3w79bZoG0MVJVCQUZgEuve8dv9dfbjPh95jJZDG-i-4bPgKWTRMKFzKoJDEKL3RiGISxAumQ6U06fPxptQ7yNMtW_OM3efpozjRSIBK31urS5aqZvUByEQoV9YQnp1adaClPMnRi-x0QPSlQ6oQ-ZqMidMkdU65gZNdxWerst_s4BejBUo0JViuLHuvEWosdcSe_VQTxM_5HA",
"**scope**":"openid offline_access",
"**expires_in**":86400,
"**token_type**":"Bearer"}

ВИСНОВКИ

В результаті виконання лабораторної роботи було засвоєно основні принципи роботи з протоколом авторизації OAuth2, зокрема, отримання access токена за допомогою різних типів грантів, а також отримання оновленого токена за допомогою refresh token.

Отримання access токена: Перший етап роботи полягав у використанні протоколу OAuth2 для отримання доступу до API. Було успішно здійснено запит для отримання access токена. Цей токен надає можливість доступу до ресурсів API відповідно до наданих прав доступу (scope).

Отримання оновленого токена: Для отримання оновленого токена використано механізм refresh_token, що дозволяє отримати новий access токен, не запитуючи заново процес авторизації. Це є важливим аспектом для підтримки сесій без необхідності відновлювати авторизацію щоразу після закінчення терміну дії токена.

Технічний аспект: В ході роботи було виконано низку запитів, зокрема:

Отримання первісного токена за допомогою клієнтських облікових даних.

Отримання refresh токена за допомогою авторизаційного коду.

Використання refresh токена для отримання нового access токена.

Усі операції виконувались через інтерфейс curl для виконання HTTP запитів, що дозволяє зручніше взаємодіяти з API. Токени були отримані успішно, що підтверджує правильність налаштувань і реалізації протоколу OAuth2.

Отже, лабораторна робота дозволила набрати необхідні навички для роботи з OAuth2, що є важливою складовою безпеки програмного забезпечення та інтеграції з сучасними API.