

Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”
Факультет інформатики та обчислювальної техніки
Кафедра автоматики та управління в технічних системах

Лабораторна робота №6
Системи безпеки програм і даних
*«Засвоювання базових навичок OAuth2 авторизаційного
протокола»*

Виконав:
студент групи ІА-12

Мельник М.С.

Київ 2024

Завдання на лабораторну роботу:

Розширити Лабораторну роботу 4, змінивши логін сторінку на стандартну від SSO провайдера, для цього, треба зробити редірект на API_DOMAIN

<https://kpi.eu.auth0.com/authorize>

та додатково додати параметри Вашого апікейшена

client_id, redirect_uri, response_type=code, response_mode=query

https://kpi.eu.auth0.com/authorize?client_id=JlvCO5c2IBHlAe2patn6l6q5H35qxti0&redirect_uri=http%3A%2F%2Flocalhost%3A3000&response_type=code&response_mode=query

Надати код рішення.

Для отримання додаткового балу:

додатково розшири апікейшен обробкою редіректа та отриманням юзер токена за допомогою code grant type.

<https://auth0.com/docs/get-started/authentication-and-authorization-flow/authorization-code-flow>

Хід роботи

1. Робота була виконана за допомогою створення власного аккаунту в auth0.
2. Використовуючи енд-поінт `api/login` формуємо запит на апікейшен та редіректимо користувача по цьому шляху

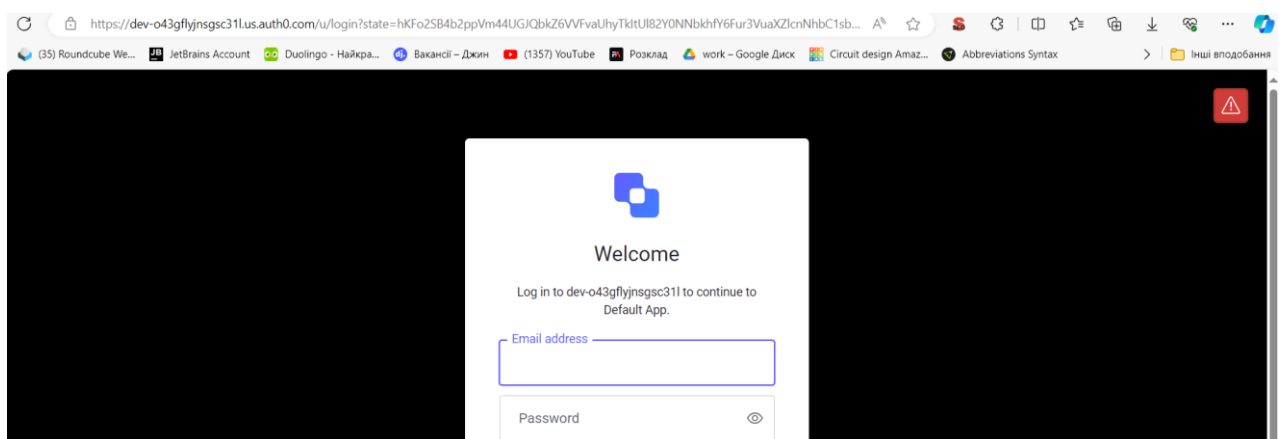


Рис 1 – Сторінка login

Нажаль, незважаючи на налаштовані CORS, власне застосунок не може
напрямую зробити редірект та перейти на дану сторінку login, але при цьому
посилання абсолютно валідне

Cross-Origin Authentication

Allow Cross-Origin Authentication



When allowed, [cross-origin authentication](#) allows applications to make authentication requests when the Lock widget or custom HTML is used.

Allowed Origins (CORS)

http://localhost:3000, http://localhost:3000/api/login

List additional origins allowed to make [cross-origin resource sharing \(CORS\)](#) requests. Allowed callback URLs are already included in this list.

- URLs can be comma-separated or added line-by-line
- Use wildcards (*) at the subdomain level (e.g. https://*.contoso.com)
- Query strings and hash information are ignored
- [Organization URL](#) placeholders are supported

Cross-Origin Verification Fallback URL

https://domain.tld/path

Рис 2 – Налаштування CORS для API

Висновок: у даній лабораторній роботі було ознайомлено та засвоєно базові навички OAuth2 авторизаційного протокола.