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

Звіт

З комп’ютерного практикуму № 6 з дисципліни

**«Безпека програмного забезпечення»**

Виконав студент ІП-13 Музичук Віталій Андрійович

(шифр, прізвище, ім'я, по батькові)

Перевірив Соколовський Владислав Володимирович

(прізвище, ім'я, по батькові)

Дата оцінювання \_\_\_\_\_\_\_\_\_\_\_\_\_

Київ 2024

**Лабораторна робота 6**

**Тема:** Засвоювання базових навичок роботи з OAuth2 протоколом

**Завдання:** 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 аплікейшена client\_id, redirect\_uri, response\_type=code, response\_mode=query https://kpi.eu.auth0.com/authorize?client\_id=JIvCO5c2IBHlAe2patn6l6q5H35qxti0&redirect\_uri=http%3A%2F%2Flocalhost%3A3000&response\_type=code&response\_mo de=query Надати код рішення.

**Для отримання додаткового балу:** додатково розшири аплікайшен обробкою редіректа та отриманням юзер токена за допомогою **code grant type**.

[Authorization Code Flow (auth0.com)](https://auth0.com/docs/get-started/authentication-and-authorization-flow/authorization-code-flow)

**Хід роботи**

Репозиторій: <https://github.com/muzy4ukV/softwareSecurityLabsKPI/tree/main/%D0%9B%D0%B0%D0%B1%D0%B0%206>

Додамо нескладний редірект на стандартну сторінку від провайдера

app.get('/', (req, res) => {

    return res.redirect(

        `https://${domain}/authorize?client\_id=cAY5VTOGPxBlTJPgLyDCMWl9jaDR50BP`+

        "&scope=offline\_access"+

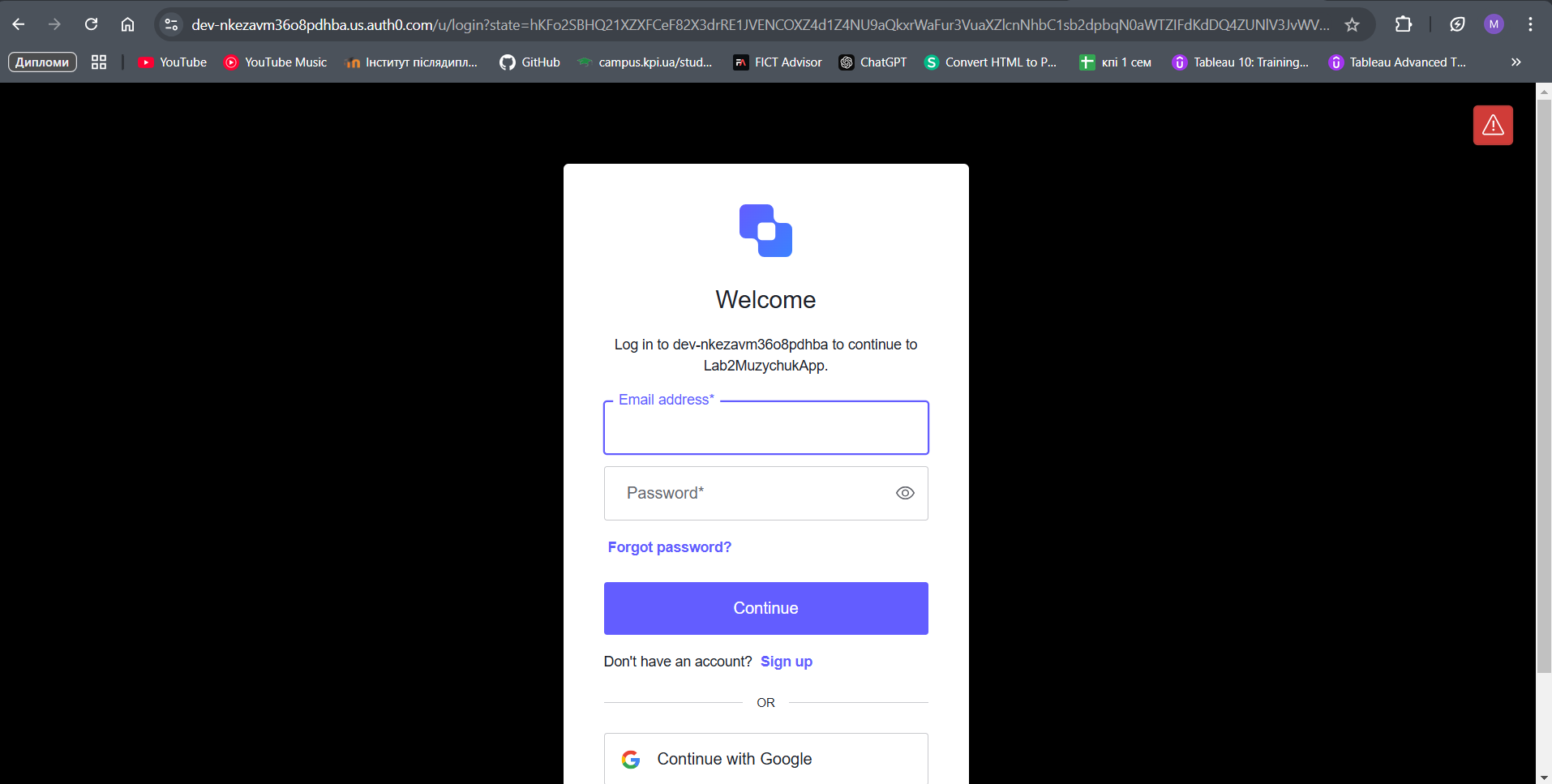
        "&redirect\_uri=http%3A%2F%2Flocalhost%3A3000%2Flogin"+

        "&response\_type=code"+

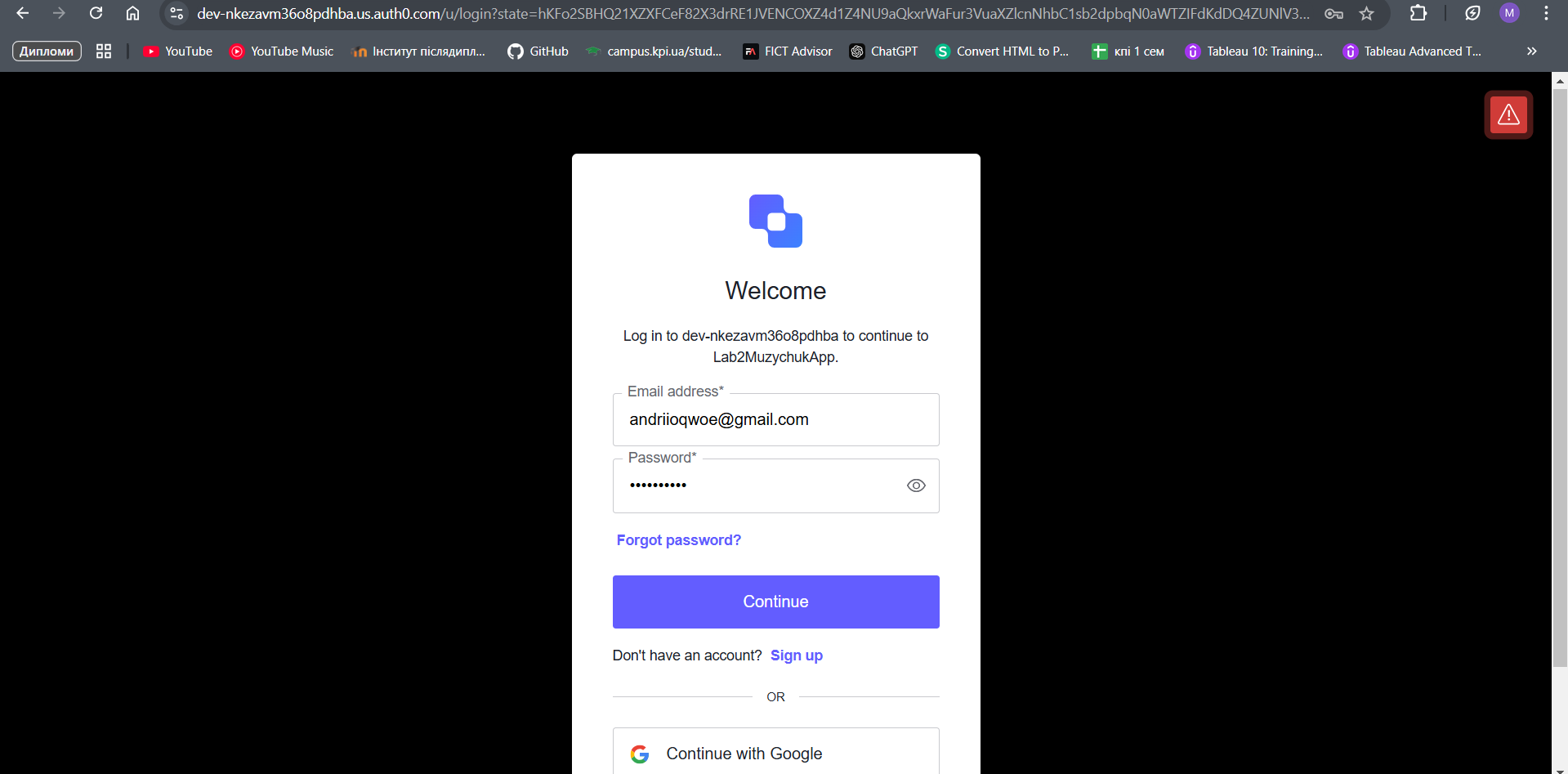
        "&response\_mode=query");

});

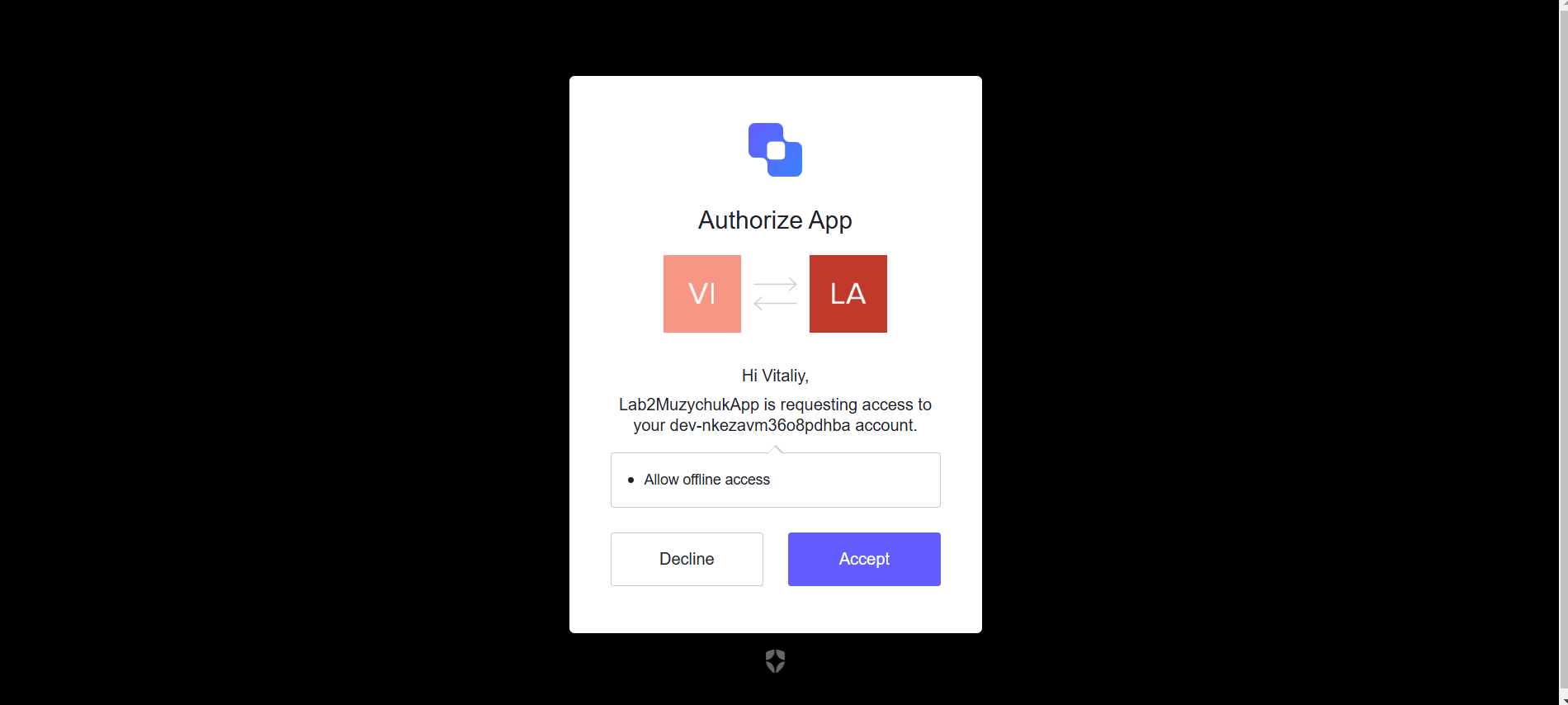
Відкриємо додаток на localhost:3000. Бачимо, що відбувається редірект на API\_DOMAIN.



Виконаємо логін як один з юзерів



Підтверджуємо надання доступів для додатку



**Додаткове завдання**

Наступний код отримуватиме user\_access\_token використовуючи наданий у запиті тимчасовий **code**

app.get('/private', async (req, res) => {

    const { code } = req.query;

    if (!code) {

        return res.status(400).json({ error: 'Authorization code is missing' });

    }

    try {

        const tokenResponse = await axios.post(

            `https://${domain}/oauth/token`,

            querystring.stringify({

                grant\_type: 'authorization\_code',

                client\_id: clientId,

                client\_secret: clientSecret,

                code,

                redirect\_uri: redirectUri,

            }),

            {

                headers: {

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

                },

            }

        );

        const accessToken = tokenResponse.data.access\_token;

        // Отримання інформації про користувача

        const userInfoResponse = await axios.get(`https://${domain}/userinfo`, {

            headers: {

                Authorization: `Bearer ${accessToken}`,

            },

        });

        const userInfo = userInfoResponse.data;

        // Відповідь із даними користувача

        res.json({

            message: 'Your token is valid and you have private access!',

            user: userInfo,

        });

    } catch (error) {

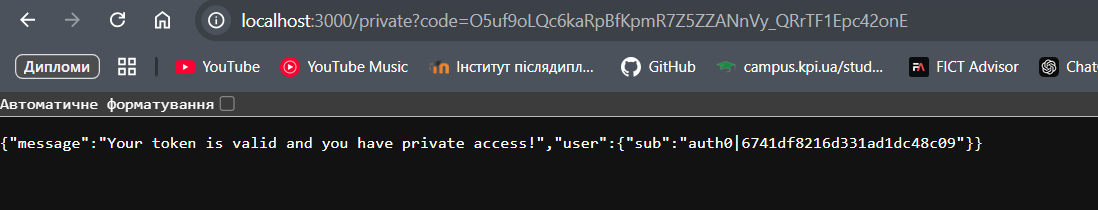
        console.error('Error:', error.response ? error.response.data : error.message);

        res.status(500).json({ error: 'Failed to fetch access token or user info' });

    }

});

Доступ через access\_token до даних користувача ми отримали



**Висновок**

В ході виконання лабораторної роботи були засвоєні базові навички роботи з протоколом авторизації **OAuth2**, зокрема реалізація процесу авторизації через SSO провайдера (Auth0) із використанням **Authorization Code Flow**.

1. **Обробка редіректа з отриманням Authorization Code**: Реалізовано маршрут для обробки редіректа, який приймає код авторизації (code) у параметрах запиту.
2. **Обмін Authorization Code на Access Token**: За допомогою API /oauth/token виконано запит на отримання Access Token із використанням **grant type: authorization\_code**.
3. **Запит до /userinfo**: Використовуючи отриманий Access Token, реалізовано запит до Auth0 /userinfo для отримання інформації про користувача.

Успішно реалізовано аутентифікацію користувача з використанням стороннього SSO провайдера, отримано Access Token та базову інформацію про користувача.

Таким чином, виконані завдання демонструють інтеграцію стандартного логіну з OAuth2 провайдером та дозволяють зрозуміти принципи роботи з Authorization Code Flow.