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 № 4 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 4**

**Тема:** Засвоювання базових навичок OAuth2 авторизаційного протокола.

**Завдання:** Використовуючи наведені налаштування з лабораторної роботи 2-3 та приведених запитів модифікувати аплікейшен <https://github.com/Kreolwolf1/auth_examples/tree/main/token_auth>. Використовую-чи перевірку юзера та отримання токена з auth0 (password grant type) Надати код модифікованного аплікейшена.

**Для отримання додаткового балу:** додатково розшири аплікайшен створенням юзера та перевіркою життя токена (у разі близького завершення – оновити токен використовуючи refresh-token grant type).

**Хід роботи**

Код даного застосунку можна переглянути на гітхабі за посиланням

<https://github.com/muzy4ukV/softwareSecurityLabsKPI/tree/main/%D0%9B%D0%B0%D0%B1%D0%B0%204>

Змінимо виконання запиту для логінації користувача так, щоб додаток на основі username та password отримував user\_access\_token.

Код буде виглядати наступним чином

**Висновок**

У межах лабораторної роботи було успішно реалізовано аутентифікацію користувачів і управління токенами за допомогою API Auth0. Для отримання access token через Password Grant було здійснено POST-запит до API Auth0 на адресу https://kpi.eu.auth0.com/oauth/token, який повернув access token із доступом до захищених ресурсів API і HTTP статусом 200 OK, що підтвердило правильність налаштувань і переданих параметрів, як-от grant\_type, audience, client\_id, client\_secret, username, password, scope та realm. Далі, для оновлення access token, був використаний refresh token, що дало змогу отримати новий access token із аналогічним статусом 200 OK. Також у додатковому завданні, за допомогою access token із певним скоупом, було виконано PATCH-запит для зміни пароля користувача, що продемонструвало можливість управління обліковими записами через API.