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 № 5 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 5**

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

**Завдання:** Розширити Лабораторну работу 4 перевіркой сігнатури JWT токена. Приклади SDK https://auth0.com/docs/quickstart/backend. У випадку асиметричного ключа, public є можливість отримати за посиланням https://kpi.eu.auth0.com/pem, aбо за формулою https://[API\_DOMAIN]/pem Надати код рішення.

**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%205>

Реалізуємо перевірку сигнатури JWT токена через express-oauth2-jwt-bearer

const { auth } = require('express-oauth2-jwt-bearer');

const app = express();

app.use(bodyParser.json());

app.use(bodyParser.urlencoded({ extended: true }));

const SESSION\_KEY = 'Authorization';

const domain = "dev-nkezavm36o8pdhba.us.auth0.com"

const checkJwt = auth({

    audience: `https://${domain}/api/v2/`,

    issuerBaseURL: `https://${domain}`,

});

Виділимо спеціальний маршрут та встановимо для нього перевірку JWT токена

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

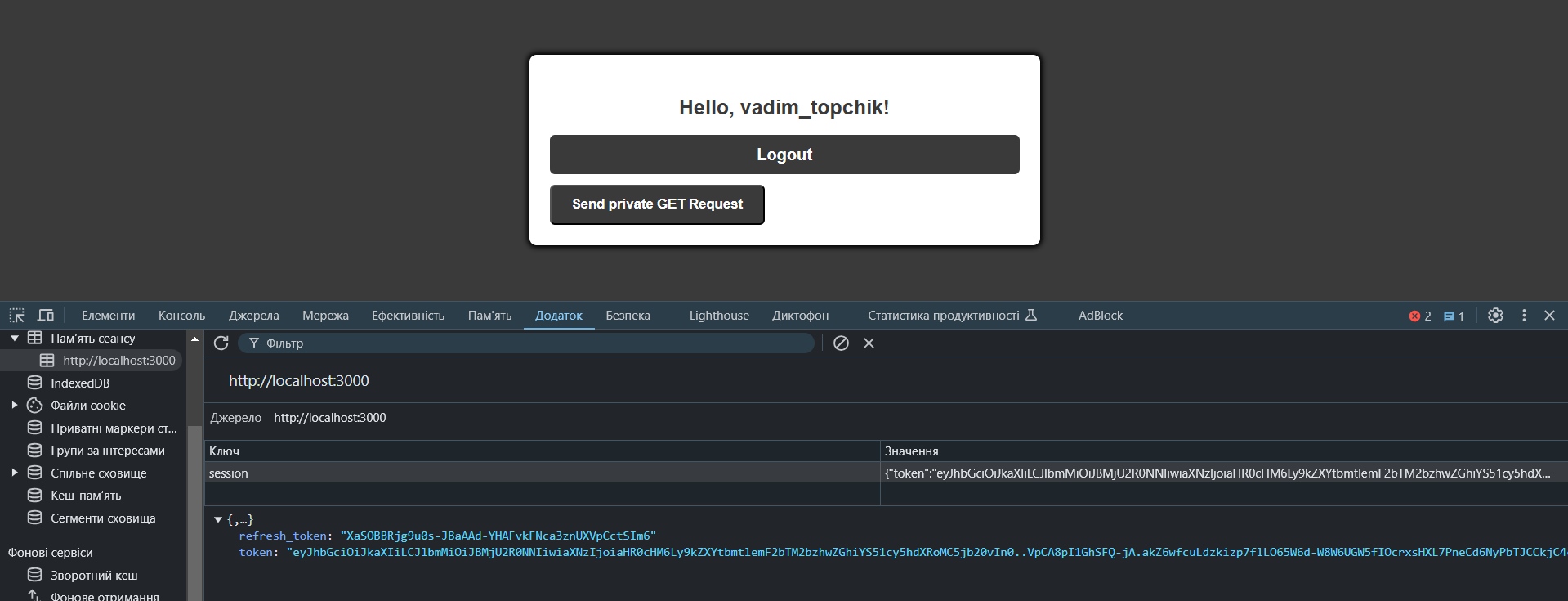
    res.json({

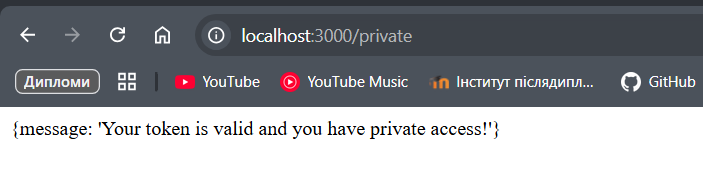
        message: 'Your token is valid and you have private access!'

    })

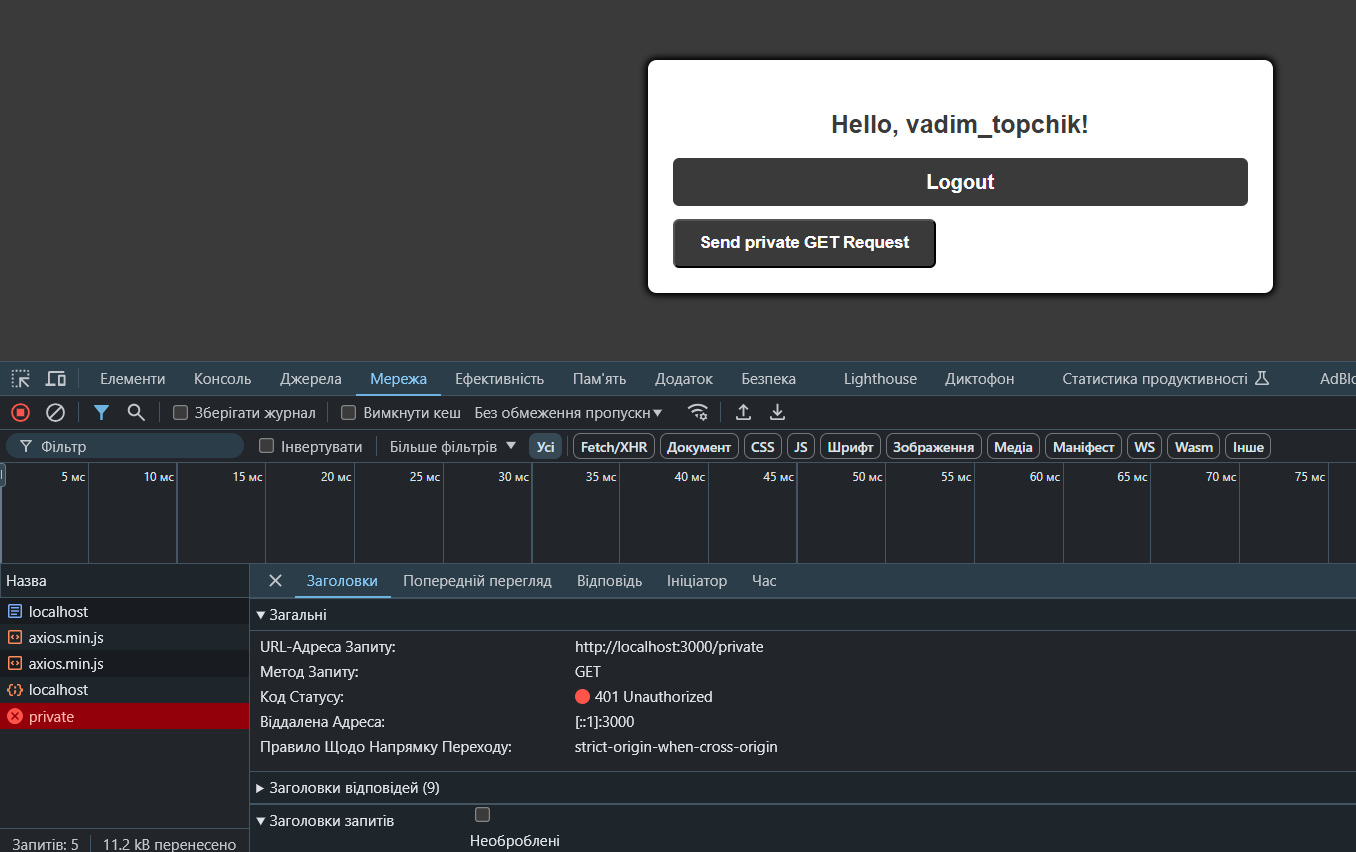
});

Перевіримо реалізацію

Попередньо ми залогінилися як користувач і маємо збережений access\_token  
  
Кнопка «Send private GET request» надсилає запит із токеном на маршрут з перевіркою JWT.



Перевірка пройшла валідно, тепер зламаємо JWT ключ.

При надсиланні запиту зі зламаним ключем, отримуємо 401 помилку, що свідчить про невалідність ключа.

**Висновок**

Засвоєння базових навичок OAuth2 авторизаційного протоколу включає розуміння роботи з JWT токенами, перевірку їх підпису та налаштування безпечного доступу до ресурсів. Використовуючи SDK, наприклад, від Auth0, можна ефективно впроваджувати аутентифікацію та авторизацію за допомогою JWT. При використанні асиметричного шифрування публічний ключ для перевірки сигнатури токена можна отримати за допомогою API або за наданим посиланням. Код для перевірки JWT токенів на сервері можна побудувати, використовуючи відповідні бібліотеки для Node.js чи іншого серверного середовища.