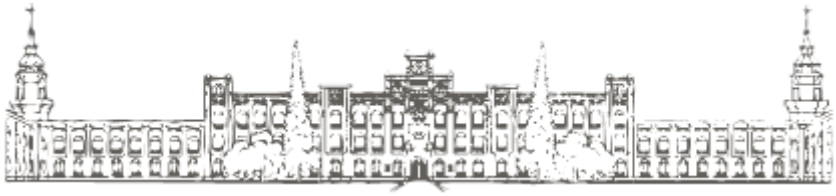


Міністерство освіти і науки України

Національний технічний університет України «КПІ

імені Ігоря Сікорського»

Факультет інформатики та обчислювальної техніки

Кафедра інформатики та програмної інженерії

# ЗВІТ

лабораторної роботи №6

з курсу «Безпека програмного забезпечення»

Перевірив:

Курченко О. А.

Виконав:

Студент Гр. ІП-01

Пашковський Є. С.

Київ 2023

Завдання

**Лабораторна робота 6**
Засвоювання базових навичок роботи з OAuth2 протоколом
Завдання:
Розширити **Лабораторну роботу 4**, змінивши логін сторінку на стандартну від SSO провайдера, для цього, треба зробити редіректна 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=JlvCO5c2IBHlAe2patn6l6q5H35qxti0&redirect_uri=http%3A%2F%2Flocalhost%3A3000&response_type=code&response_mode=query
Надати код рішення.
**Для отримання додаткового балу:** додатково розшири аплікайшен обробкою редіректа та отриманням юзер токена за допомогою **code grant type**.
https://auth0.com/docs/get-started/authentication-and-authorization-flow/authorization-code-flow

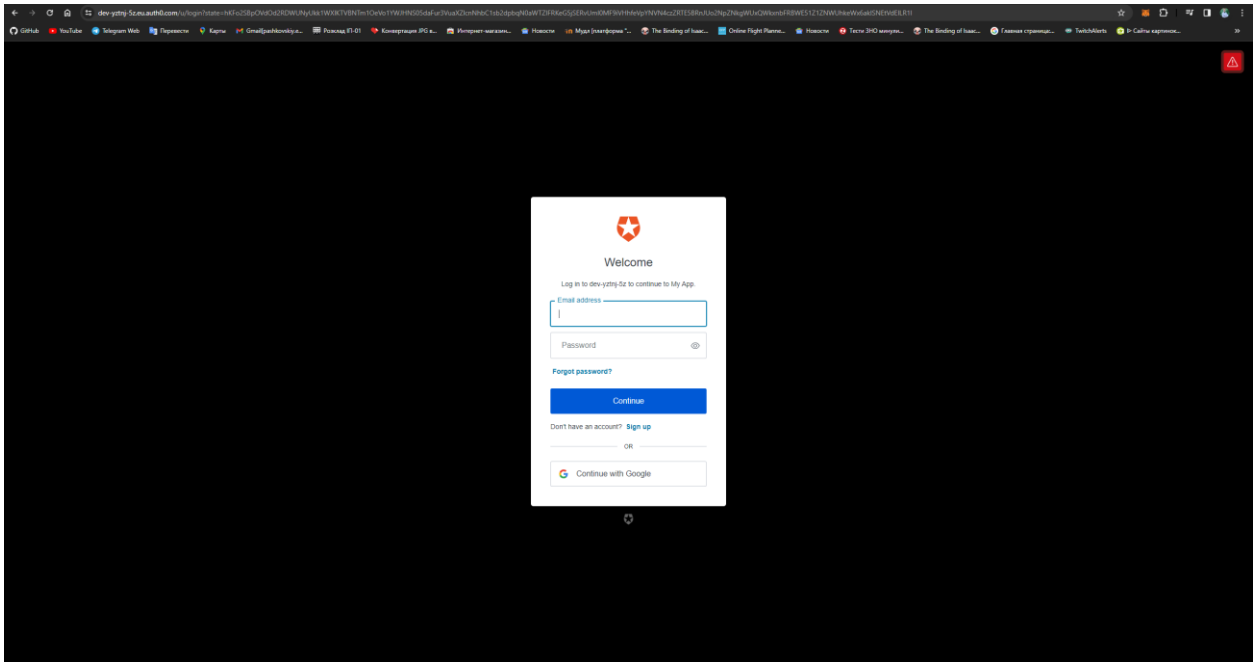
Хід роботи

Повний код:

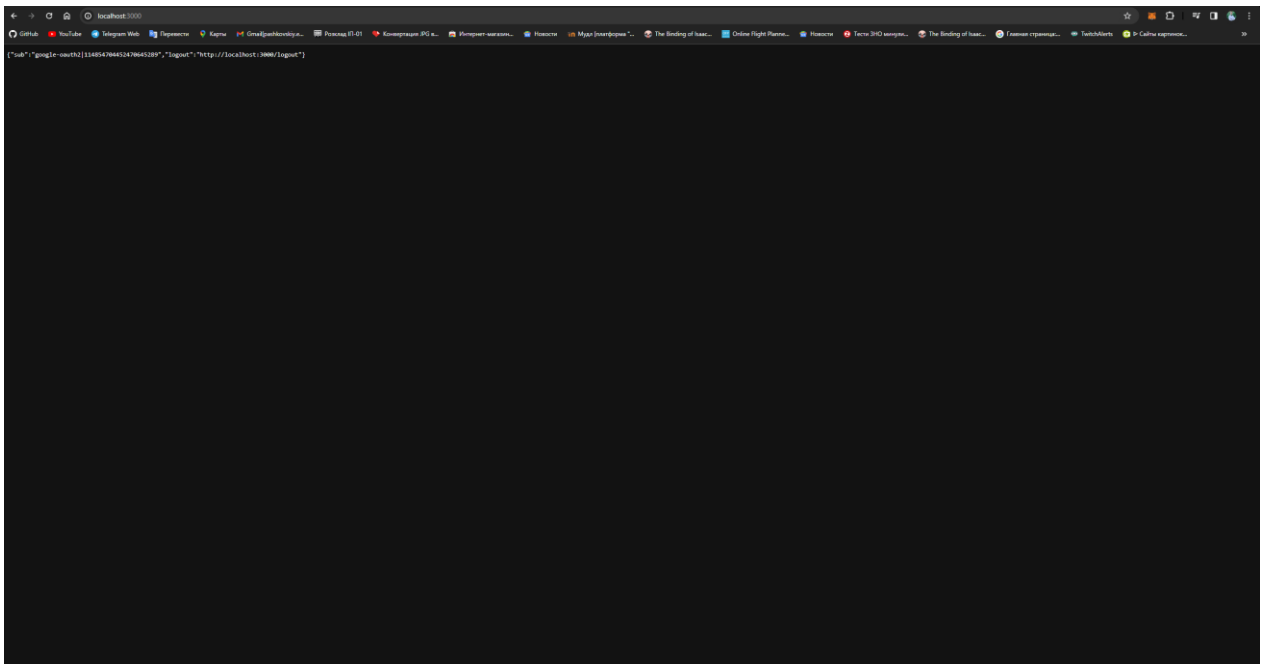
```
const express = require("express");
const bodyParser = require("body-parser");
const path = require("path");
const port = 3000;
const { auth } = require("express-openid-connect");
require("dotenv").config();

const app = express();
app.use(bodyParser.json());
app.use(bodyParser.urlencoded({ extended: true }));

app.use(
  auth({
    clientID: "YLPZLglTAXNugVMYHdylzjIR4KUtIKGR",
    clientSecret:
      "PPy_eRcX9BqP5dx3tqRB9jMcewyhJcCFwsAN3TAKfK7_Ssh1qkAbr0ntz5S5LUZx",
    baseURL: "http://localhost:3000",
    issuerBaseURL: "https://dev-yztnj-5z.eu.auth0.com/",
    secret: "asfasfas",
    idpLogout: true,
    authorizationParams: {
      response_type: "code", // This requires you to provide a client secret
      audience: "https://dev-yztnj-5z.eu.auth0.com/api/v2/",
      scope: "openid offline_access",
    },
  })
);
```

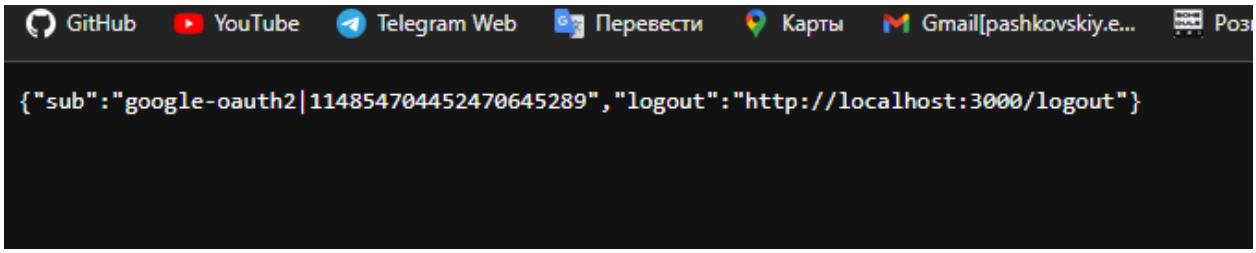
```
app.get("/", async (req, res) => {
  let { token_type, access_token, isExpired, refresh } = req.oidc.accessToken;

  if (isExpired()) {
    ({ access_token } = await refresh());
  }

  if (req.oidc?.user?.sub) {
    return res.json({
      sub: req.oidc.user.sub,
      logout: "http://localhost:3000/logout",
    });
  }
  res.sendFile(path.join(__dirname + "/index.html"));
});

app.listen(port, () => {
  console.log(`Example app listening on port ${port}`);
});
```

Сторінка логіну у додатку перенаправляється на сторінку від SSO провайдера:




У випадку успішного логіну маємо наступне:






На додатковий бал:

Обробка редіректу та отримання токена відбувається всередині middleware “auth”, що надається бібліотекою “express-openid-connect”.