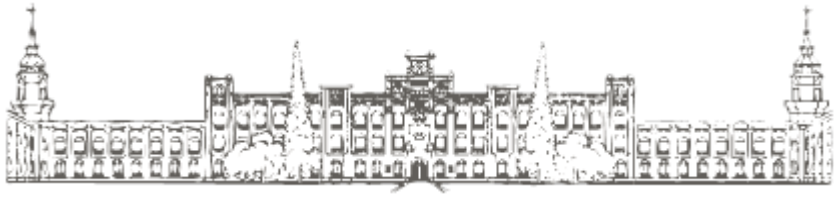


Міністерство освіти і науки України

Національний технічний університет України

„КПІ імені Ігоря Сікорського ”

Факультет інформатики та обчислювальної техніки

Кафедра інформаційних систем та технологій

ЗВІТ

лабораторна робота №6 з

курсу «Безпека програмного забезпечення»

Тема: «Засвоювання базових навичок OAuth2 авторизаційного протокола»

Перевірив:

Виконав:

Група ІП-11 Головня Олександр

Київ 2024

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&r

edirect_uri=http%3A%2F%2Flocalhost%3A3000&response_type=code&response_mo de=query

Надати код рішення.

Додаткове завдання:

Додатково розширити аплікайшен обробкою редіректа та отриманням юзер токена за допомогою code grant type. https://auth0.com/docs/getstarted/authentication-and-authorization-flow/authorization-code-flow

Повний лістинг файлів можна знайти тут:

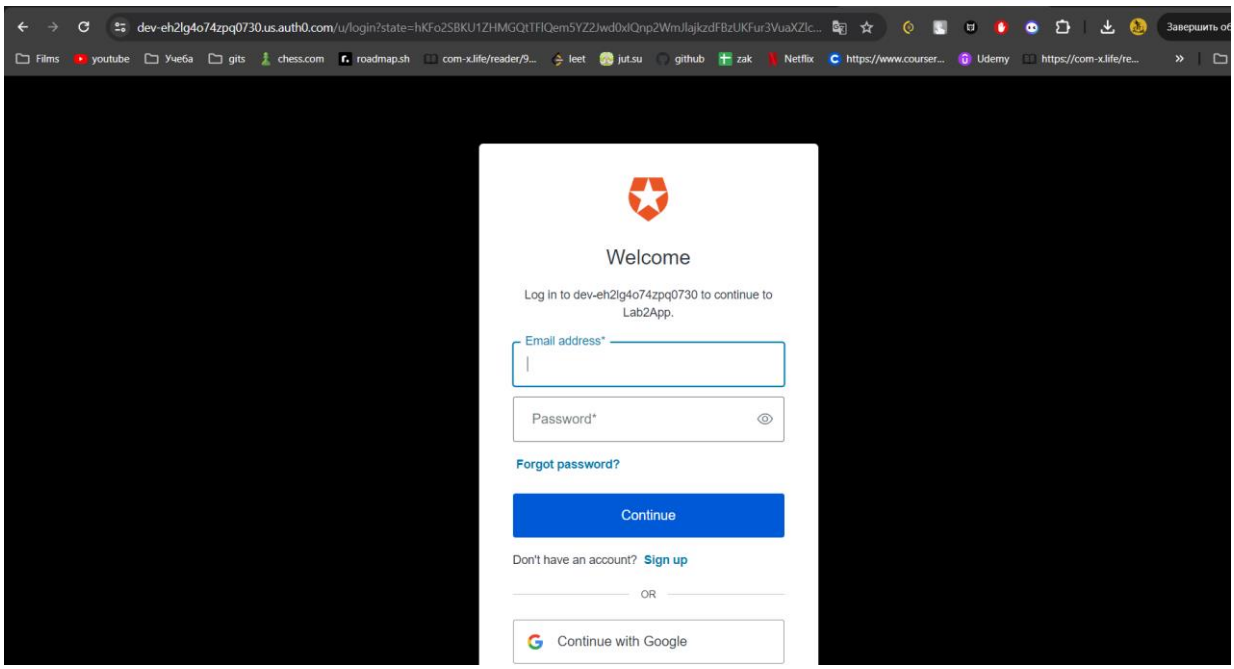
https://github.com/YeaLowww/KPI-ALL/tree/main/Fourth%20year/Software%20security

Результат виконання:

Щоб змінити логін сторінку на стандартну від SSO провайдера я додав endpoint, який відповідає за перехід на сторінку авторизації.

```
app.get('/login', (req, res) => {
  const authUrl =
    `https://${process.env.AUTH0_DOMAIN}/authorize?` +
    `client_id=${encodeURIComponent(process.env.AUTH0_CLIENT_ID)}&` +
    `redirect_uri=${encodeURIComponent('http://localhost:3000/callback')}&` +
    `response_type=code&` +
    `response_mode=query&` +
    `scope=openid profile email`
  res.redirect(authUrl)
})
```

Якщо запустимо код, побачимо сторінку авторизації від провайдера:



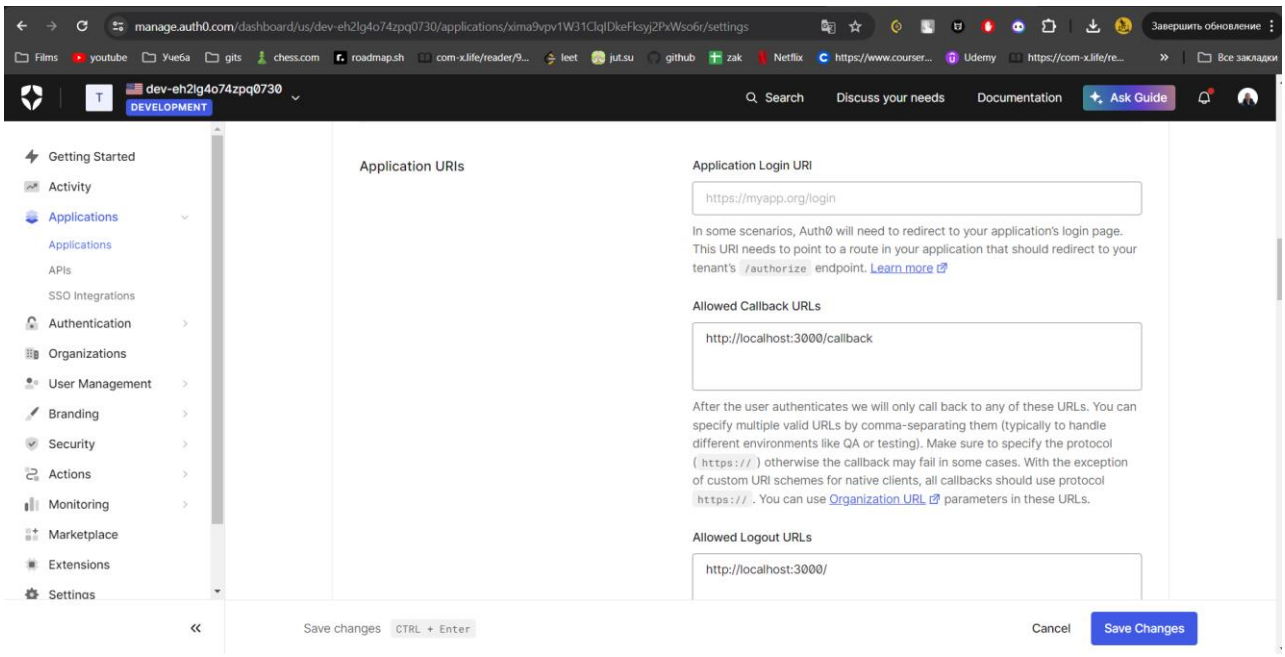
Додаткове завдання:

Для додаткового завдання створимо endpoint callback, при успішній авторизацій він надсилає наш токен на головну сторінку

```
app.get('/callback', async (req, res) => {
  const { code } = req.query
  try {
    const response = await axios.post(
      `https://${process.env.AUTH0_DOMAIN}/oauth/token`,
      new URLSearchParams({
        grant_type: 'authorization_code',
        client_id: process.env.AUTH0_CLIENT_ID,
        client_secret: process.env.AUTH0_CLIENT_SECRET,
        code,
        redirect_uri: 'http://localhost:3000/callback',
      }),
      {
        headers: { 'Content-Type': 'application/x-www-form-urlencoded' },
      }
    )

    const { access_token } = response.data
    res.redirect(`/?token=${access_token}`)
  } catch (error) {
    console.error('Error exchanging code for tokens:', error)
    res.status(500).send('Internal Server Error')
  }
})
```

Не забути додати callback в Auth0



В результаті побачимо ту ж інформацію про користувача:

Висновки: У ході виконання лабораторної роботи було досліджено базові операції з системою авторизації Auth0. Було змінено авторизаційну сторінку на сторінку авторизації провайдеру за допомогою редіректу. Також виконане додаткове завдання для обробки callback, тепер після авторизації та перезавантаження відображається інформація про користувача.