

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 №4 з

курсу «Безпека програмного забезпечення»

Тема: «Засвоювання базових навичок OAuth2 авторизаційного протокола»

Перевірів:

Виконав:

Група ІІІ-11 Головня Олександр

Київ 2024

Завдання:

Використовуючи наведені налаштування з лабораторної роботи 2 - 3 та приведених запитів модифікувати аплікейшен

https://github.com/Kreolwolf1/auth_examples/tree/main/token_auth

Використовуючи 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)

З попередніх лаб:

```
client_id: 'JIvC05c2IBH1Ae2patn6l6q5H35qxti0'  
client_secret: 'ZRF80p0tWM36p1_hxXTU-B0K_Gq_-eAVt1rQpY24CasYiDmcXBhNS6IJMNcz1EgB'
```

Login: dsrnjhszz@gmail.com | password: IP11Holovnia

Повний лістинг файлів можна знайти тут:

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

Результат виконання:

Файл Session.js:

Цей файл реалізує клас Session для керування сесіями користувачів у Node.js додатку. Клас зберігає сесії у JSON-файлі (sessions.json) і надає методи для збереження (setSession), отримання (getSession) та видалення сесій (finish).

File Index.js

Цей файл створює сервер на Node.js з використанням Express, який керує аутентифікацією користувачів. Він обробляє запити на вхід (/api/login), надання інформації про сторінку для аутентифікованих користувачів (/page-

info) та вихід користувачів із сесії (/logout). Сесії зберігаються і керуються за допомогою класу Session.

File Utils.js

```
const generateLoginRequestOptions = (login, password) => ({
  method: "POST",
  url: "https://kpi.eu.auth0.com/oauth/token",
  headers: { 'content-type': 'application/x-www-form-urlencoded' },
  form: {
    client_id: 'JIvC05c2IBH1Ae2patn6l6q5H35qxti0',
    audience: 'https://kpi.eu.auth0.com/api/v2/',
    realm: 'Username-Password-Authentication',
    scope: 'offline_access',
    client_secret: 'ZRF80p0tWM36p1_hxXTU-B0K_Gq_-eAVtlrQpY24CasYiDmcXBhNS6IJMNcz1EgB',
    username: login,
    password: password,
    grant_type: 'http://auth0.com/oauth/grant-type/password-realm',
  }
});

module.exports = {
  generateLoginRequestOptions
};
```

Цей файл експортує функцію **generateLoginRequestOptions**, яка генерує та повертає об'єкт конфігурації для запиту аутентифікації до Auth0. Цей об'єкт використовується для відправки POST-запиту на сервер Auth0 з метою отримання токена доступу за допомогою логіна і пароля користувача.

```
PS C:\Users\Саха Головна\Desktop\security\lab4> node index.js
(node:8708) [DEP0040] DeprecationWarning: The 'punycode' module is deprecated.
(Use 'node --trace-deprecation ...' to show where the warning was created)
Example app listening on port 3000
```

Welcome on page of IP11Holovnia!

dsrnjhszz@gmail.com

Login

Після авторизації нас перекине на сторінку:

[Logout](#)

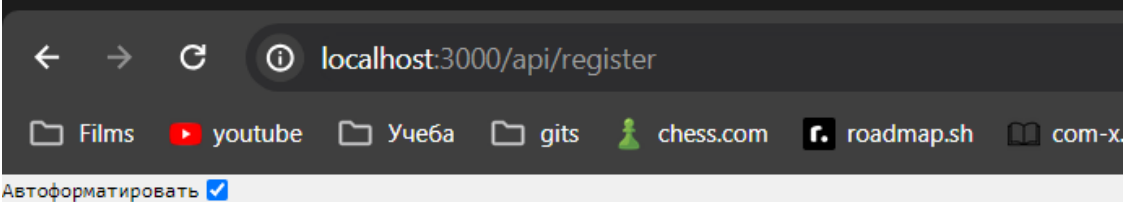
Username: dsrnjhszz@gmail.com

Додаткове завдання:

Насамперед, у файлі index.html було добавлено нову форму для реєстрації

А в index.js створено пост запит для реєстрації

Зареєструємо користувача:



```
{
  "success": true,
  "userId": {
    "created_at": "2024-09-06T19:43:33.149Z",
    "email": "b@gmail.com",
    "email_verified": false,
    "identities": [
      {
        "connection": "Username-Password-Authentication",
        "user_id": "66db5b65c4e1e9ea9ac1607d",
        "provider": "auth0",
        "isSocial": false
      }
    ]
  },
  "name": "Holovnia Oleksandr",
  "nickname": "Oleksandr",
  "picture": "https://i.pinimg.com/originals/e1/4c/ae/e14cae2f0f44121ab4e3506002b1a55.jpg",
  "updated_at": "2024-09-06T19:43:33.149Z",
  "user_id": "auth0|66db5b65c4e1e9ea9ac1607d"
},
  "login": "/"
}
```

Також додав додаткову функцію для перевірки дійсності токена і якщо до кінця дії токена менше 5 хвилин, то токен оновиться.

Висновки: У ході виконання лабораторної роботи було досліджено базові операції з системою авторизації Auth0. Створено авторизацію та виконане додаткове завдання з перевіркою дійсності токена.