

Backend development

Laboratorium 3

Integracja protokołu OAuth2 w aplikacjach webowych

Mateusz Pawełkiewicz

Cel:

Rozszerzyć mechanizm logowania, umożliwiając użytkownikom uwierzytelnienie się za pomocą kont z zewnętrznych serwisów (np. Google, GitHub) poprzez OAuth2.

Wymagania:

- Integracja z wybranym dostawcą OAuth2 (np. Google lub GitHub).
- Implementacja logiki przekierowania użytkownika do dostawcy oraz odbiór tokenu autoryzacyjnego.
- Powiązanie danych zewnętrznego konta z kontem użytkownika w systemie.

Kroki do wykonania:

1. **Konfiguracja dostawcy OAuth2:**
 - Zarejestruj aplikację w wybranym serwisie (np. Google Developer Console lub GitHub Developer settings).
 - Uzyskaj klucz i sekret aplikacji oraz ustaw odpowiednie URI przekierowań.
2. **Implementacja endpointu logowania OAuth2:**
 - Utwórz endpoint (np. GET /auth/oauth2/redirect), który przekieruje użytkownika do strony logowania wybranego dostawcy.
 - Po autoryzacji, odbierz kod autoryzacyjny na skonfigurowane URI przekierowania.
3. **Wymiana kodu na token:**
 - Zaimplementuj mechanizm wymiany otrzymanego kodu na token dostępu (access token) przy użyciu odpowiednich endpointów dostawcy.
4. **Powiązanie kont:**
 - Jeśli użytkownik loguje się po raz pierwszy, utwórz konto w bazie danych.
 - Jeśli konto już istnieje, zaktualizuj dane lub po prostu zarejestruj sesję.
5. **Testowanie:**
 - Przetestuj cały proces logowania OAuth2: przekierowanie, autoryzację u dostawcy, odbiór tokenu oraz dostęp do chronionych zasobów w Twoim API.