Bezpieczeństwo aplikacji internetowych

Laboratorium 3

Token, CORS

Mateusz Pawełkiewicz

Cel ćwiczenia:

Nauczyć się implementacji mechanizmów autoryzacji opartej na tokenach oraz zarządzania uprawnieniami Cross-Origin Resource Sharing (CORS) w aplikacjach internetowych.

Zadania

1: Utworzenie projektu

a) Utwórz nowy projekt w wybranym języku programowania.

b) Zainstaluj potrzebne pakiety do obsługi serwera, autoryzacji JWT, haszowania haseł oraz obsługi zmiennych środowiskowych.

c) Utwórz plik konfiguracyjny do przechowywania sekretów JWT (access token i refresh token).

2: Rejestracja użytkownika

a) Dodaj endpoint do rejestracji użytkownika.

b) Zaimplementuj mechanizm haszowania hasła przed zapisaniem w bazie danych.

c) Przetestuj endpoint rejestracji użytkownika, wysyłając odpowiednie dane i sprawdzając, czy użytkownik został poprawnie zarejestrowany.

3: Logowanie i generowanie tokenów

a) Dodaj endpoint do logowania użytkownika.

b) Zaimplementuj weryfikację hasła użytkownika.

c) Po poprawnej weryfikacji, wygeneruj i zwróć access token oraz refresh token.

d) Przetestuj endpoint logowania, wysyłając odpowiednie dane i sprawdzając, czy tokeny są poprawnie generowane.

4: Odświeżanie tokenu

a) Dodaj endpoint do odświeżania tokenu.

b) Zaimplementuj weryfikację refresh tokenu i wygeneruj nowy access token.

c) Przetestuj endpoint odświeżania tokenu, wysyłając refresh token i sprawdzając, czy nowy access token jest poprawnie generowany.

5: Zabezpieczenie endpointów

a) Zaimplementuj middleware do weryfikacji access tokenu.

b) Dodaj zabezpieczenie do wybranego endpointu, tak aby był dostępny tylko dla zalogowanych użytkowników.

c) Przetestuj zabezpieczony endpoint, sprawdzając dostęp z poprawnym i niepoprawnym tokenem.

6: Konfiguracja CORS

a) Zainstaluj i skonfiguruj obsługę CORS w projekcie.

b) Ustaw odpowiednie reguły CORS, pozwalając na dostęp tylko z określonych domen.

c) Przetestuj działanie CORS, wysyłając żądania z różnych domen i sprawdzając, czy tylko wybrane domeny mają dostęp do API.