Zajęcia 7

Prace implementacyjne.

Temat: Budżet

Kurs:
Integracja Systemów Informatycznych

Grupa:
Poniedziałek
15:15 - 16:55

Członkowie grupy:
Setlak Justyna
Kurpiński Michał
Drapała Jakub

W ramach pierwszego etapu prac nad aplikacją zostały stworzone funkcjonalności związane z autoryzacją użytkowników. Udostępniona jest możliwość stworzenia konta bezpośrednio w tworzonym systemie, ale również za pośrednictwem portali społecznościowych takich jak Facebook oraz Google. Umożliwione jest logowanie do aplikacji poprzez tradycyjne wpisanie loginu oraz hasła, a także za pomocą zewnętrznym portali, poprzez które można zarejestrować się w systemie.

Aplikacja jest tworzona w architekturze klient-serwer. REST API jest implementowane w oparciu o platformę .NET Core oraz Framework ASP.NET Core. Do połączenia z relacyjną bazą danych wykorzystano narzędzie typu ORM - Entity Framework Core. Jako kontener zależności wykorzystano narzędzie Autofac, które umożliwia realizację wzorca Inversion Of Control.

Do zarządzania kontem użytkownika wykorzystany został mechanizm dostarczony przez firmę Microsoft - ASP.NET Identity. ASP.NET Identity dostarcza nam klas odpowiadających za tworzenie konta użytkownika, porównywania haseł oraz przygotowywania hasła do przechowywania w bezpieczny sposób tzn. W postaci za haszowanej z losowo dodanym ciągiem zaburzającym tzw. solą. Podczas logowania do aplikacji użytkownika za pomocą lokalnego konta sprawdzana jest poprawność jego danych – adresu email oraz loginu.

Jako metoda uwierzytelnienia oraz autoryzacji użyty został standard RFC 7519 czyli Json Web Token, w skrócie JWT. Mechanizm logowania polega na wygenerowaniu niepowtarzalnego tokena, na podstawie którego użytkownik może zostać zidentyfikowany. Następnie, przy innych wykonywanych requestach do API jest weryfikowana poprawność tokena, który otwiera dostęp do pozostałych funkcjonalności danego systemu.

Schemat tokenu JWT:

Header.Payload.Signature

Header zawiera informację, w jaki sposób podpis tokenu powinien być szyfrowany oraz deklaracje typu JWT.
Payload - zawiera informację odnośnie danych, które są przekazywane w tokenie
signature, czyli podpis.

Wygenerowany token zostaje następnie zwrócony i wysyłany z każdym kolejnym zapytaniem w nagłówku pod kluczem Authorization z prefiksem „Bearer ”.

Logowanie za pomocą mediów społecznościowych

Rozpoczynając logowanie za pomocą mediów społecznościowych Google lub Facebook został wykorzystany tzw. Authorization Code Flow znany ze specyfikacji OpenId Connect.

Aplikacja serwerowa waliduje otrzymany parametr state oraz wymienia parametr code na access token, potwierdzający poprawne logowanie użytkownika, bezpośrednio komunikując się z API zewnętrznego systemu.

Po otrzymaniu access tokenu, aplikacja serwerowa pobiera dane użytkownika z zewnętrznego systemu, w razie potrzeby tworzy użytkownika w bazie danych, i odpowiada klientowi wygenerowanym tokenem. Proces generowania tokena przez aplikację serwerową jest dokładnie taki sam jak w przypadku logowania lokalnym kontem.