AKADEMIA HANDLOWA NAUK STOSOWANYCH W RADOMIU

RADOM ACADEMY OF ECONOMICS

INSTRUKCJA LABORATORYJNA NUMER 1	
Przedmiot: Zagrożenia bezpieczeństwa systemów	Tok: 2024/2025
Cel praktyczny projekt: Stworzenie aplikacji Web API, która rozwiązuje problemy bezpieczeństwa poznane na zajęciach.	

1. Stwórz domyślną aplikację Web API w technologii .NET, która udostępnia domyślny kontroler WeatherForecastController.
2. Utwórz i zaimplementuj bazę danych (In memory lub MSSQL), a w niej tabelę do przechowywania użytkowników o nazwie zawierającą odpowiednie kolumny. Alternatywą bazy danych może być zastosowanie pliku lub statycznej listy.
3. Utwórz serwis oraz metodę w kontrolerze do rejestrowania użytkowników, zadbaj o sprawdzenie czy użytkownik z danym emailem już istnieje oraz dodaj hashowanie hasła. Metoda musi przyjmować email oraz hasło wraz z jego potwierdzeniem. Rezultatem działania powinno być dodanie użytkownika do tabeli użytkowników z hashem hasła.
4. Utwórz serwis oraz metodę w kontrolerze do logowania użytkowników, w pierwszej kolejności sprawdź czy użytkownik o danym emailu już istnieje i czy podał poprawne hasło. Następnie wygeneruj i zwróć token, który pozwoli mu na autoryzację do pozostałych metod API.
5. Wymuś konieczność autoryzacji do metod z WeatherControllera.
6. Zabezpiecz metody API przed atakami DoS, w tym celu stwórz filtr lub middleware, który sprawdzi czy adres ip, z którego pochodzi wywołanie API nie wywołuje tej samej metody więcej niż 10 razy w ciągu 30sekund, jeśli tak będzie zablokuj kolejne wywołanie na 30sekund i zwróć odpowiednią informację konsumentowi API.
7. Stwórz mechanizm logowania dwuetapowego.
8. Jeśli 5 razy zostanie podane złe hasło, zablokuj możliwości kolejnych logowań na 10minut.
9. Jeśli 100 razy w ciągu jednego dnia będzie 100 nieudanych prób logowania z tego samego IP zablokuj konto na godzinę i nie pozwalaj więcej logować się z tego IP.
10. Sprawdzaj czy request nie jest atakiem typu SQL Injection, wykrywaj i odrzucaj takie żądania.
11. Dodaj mechanizm logowania przychodzących żądań, loguj informacje o requeście: typ metody, godzinę wykonania, zawartość, IP oraz Email użytkownika, który je wywołał.
12. *Dodaj role użytkowników oraz polityki CORS.
13. Zadbaj o czytelność kodu.