

Przepraszam, czy można?

Autoryzacja w ASP.NET Core

@marcin_hoppe



auth0.com

Przepraszam, czy można?

Game of Reviews



Sansa Stark, Pracownik



Jon Snow, Użytkownik



Arya Stark, Anonim

Przepraszam, czy można?

Garść wymagań biznesowych

Przeglądanie recenzji:

- Każdy może przeglądać dowolne produkty i ich recenzje

Zarządzanie produktami:

- Jedynie pracownicy mogą dodawać produkty
 - Oczywiście, pracownicy muszą być zalogowani



Przepraszam, czy można?

Wymagań biznesowych ciąg dalszy

Dodawanie recenzji:

- Jedynie zalogowani użytkownicy mogą dodawać recenzje do produktów
- Użytkownicy mogą usuwać jedynie swoje recenzje

Moderowanie recenzji:

- Pracownicy mogą usuwać dowolne recenzje
 - Czy oznacza to, że pracownicy mogą usuwać swoje recenzje?



Przepraszam, czy można?

Często mylone pojęcia

Uwierzytelnianie	Autoryzacja
Czy użytkownik jest tym, za kogo się podaje?	Czy użytkownik może wykonać daną akcję?
System prosi użytkownika o poświadczenie swojej tożsamości	System udziela dostępu na podstawie reguł i polityk
Musi nastąpić przed autoryzacją	Przeprowadzana dopiero po pomyślnym uwierzytelnieniu
Wiem / Mam / Jestem	Aktor / Akcja / Zasób



Przepraszam, czy można?

Uwierzytelnianie

Skorzystamy z gotowca!



Przepraszam, czy można?

Name

Role

Claims

ClaimsIdentity



Przepraszam, czy można?

Garść wymagań biznesowych

Przeglądanie recenzji:

- Każdy może przeglądać dowolne produkty i ich recenzje

Zarządzanie produktami:

- Jedynie pracownicy mogą dodawać produkty
 - Oczywiście, pracownicy muszą być zalogowani



Przepraszam, czy można?

Garść wymagań biznesowych

Przeglądanie recenzji:

- Każdy może przeglądać dowolne produkty i ich recenzje

Zarządzanie produktami:

- Jedynie pracownicy mogą dodawać produkty
 - Oczywiście, pracownicy muszą być zalogowani



Przepraszam, czy można?

Wymagań biznesowych ciąg dalszy

Dodawanie recenzji:

- Jedynie zalogowani użytkownicy i pracownicy mogą dodawać recenzje do produktów
- Użytkownicy mogą usuwać jedynie swoje recenzje

Moderowanie recenzji:

- Pracownicy mogą usuwać dowolne recenzje
 - Czy oznacza to, że pracownicy mogą usuwać swoje recenzje?



Przepraszam, czy można?

Role Based Access Control

czy

Claims?



Przepraszam, czy można?

Wymagań biznesowych ciąg dalszy

Dodawanie recenzji:

- Jedynie zalogowani użytkownicy i pracownicy mogą dodawać recenzje do produktów
- Użytkownicy mogą usuwać jedynie swoje recenzje

Moderowanie recenzji:

- Pracownicy mogą usuwać dowolne recenzje
 - Czy oznacza to, że pracownicy mogą usuwać swoje recenzje?



Przepraszam, czy można?

Wymagań biznesowych ciąg dalszy

Dodawanie recenzji:

- Jedynie zalogowani użytkownicy i pracownicy mogą dodawać recenzje do produktów
- Użytkownicy mogą usuwać jedynie swoje recenzje

Moderowanie recenzji:

- Pracownicy mogą usuwać dowolne recenzje
 - Czy oznacza to, że pracownicy mogą usuwać swoje recenzje?



Przepraszam, czy można?

Polityki kontroli dostępu



Przepraszam, czy można?

Aktor

ClaimsIdentity

Akcja

IAuthorizationRequirement

Zasób

AuthorizationHandlerContext

AuthorizationHandler<IAuthorizationRequirement>



Przepraszam, czy można?

A co z warstwą widoku?



Przepraszam, czy można?

Wymaganie dodatkowe

Przeglądanie recenzji:

- Każdy może przeglądać dowolne produkty i ich recenzje

Zarządzanie produktami:

- Jedynie pracownicy mogą dodawać produkty
 - Oczywiście, pracownicy muszą być zalogowani
- Pracownicy mogą usuwać jedynie produkty, które sami dodali



Przepraszam, czy można?

Do zapamiętania

1. Uwierzytelnianie \neq Autoryzacja
2. RBAC \approx *claims*
3. Polityki kontroli dostępu
 - a. Deklaratywne
 - b. Imperatywne
4. Warstwa widoku \neq pełna ochrona
5. Podatności: IDOR i BOLA

Kod znajdziecie na GitHubie



Przepraszam, czy można?

Marcin Hoppe



Senior Manager, Product
Security

[@marcin_hoppe](#)



Node.js Foundation
Ecosystem Security
Working Group



OWASP Serverless Top 10
Project Leader



Do zobaczenia!



auth0.com