Przepraszam, czy można?

Autoryzacja w ASP.NET Core

@marcin_hoppe

auth0.com

Game of Reviews

Sansa Stark, Pracownik

Jon Snow, Użytkownik

Arya Stark, Anonim

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

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?

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 po pomyślnym uwierzytelnieniu
Wiem / Mam / Jestem	Aktor / Akcja / Zasób

Przepraszam, czy można?

Uwierzytelnianie

Skorzystamy z gotowca!

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

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?

Role Based Access Control

czy

Claims?

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?

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?

Polityki kontroli dostępu

Aktor

ClaimsIdentity

Akcja

IAuthorizationRequirement

Zasób

AuthorizationHandlerContext

AuthorizationHandler<IAuthorizationRequirement>

A co z warstwą widoku?

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

Wnioski

1. Uwierzytelnianie !== Autoryzacja
2. RBAC ~== *claims*
3. Polityki kontroli dostępu
   a. Deklaratywne
   b. Imperatywne
4. Warstwa widoku !== pełna ochrona
5. Podatności: IDOR i BOLA

Kod znajdziecie na GitHubie

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