08

O que aprendemos?

Nesta aula 04, finalmente começamos a configurar nosso projeto IdentityServer 4.

Poderíamos falar de vários aspectos envolvendo segurança de aplicativos MVC e microsserviços, e este assunto poderia render facilmente vários cursos como este. Portanto, neste curso, nos limitamos à autenticação, autorização e segredos da aplicação.

Quando você desenvolve serviços Web API, os recursos que eles expõem não podem ficar abertos para qualquer um acessar. Eles precisam ser limitados a determinados usuários ou clientes (aplicativos) confiáveis. No caso do nosso serviço de Relatórios, queremos proteger as funcionalidades de gravar e ler dados do relatório contra acesso anônimo, e também queremos garantir que somente a aplicação MVC (cliente) possa acessá-lo. E tudo começa com a autenticação. Autenticação é o processo de confirmar a identidade do usuário de forma confiável.

No curso anterior, vimos como a autenticação pode ser feita pelo ASP.NET Core Identity. Ele funcionou bem para autenticarmos usuários numa aplicação única, isto é, monolítica. Porém, o ASP.NET Core Identity não é adequado para uma arquitetura de microsserviços. Para isso, vamos precisar de um serviço dedicado para autenticar os usuários e fornecer os tokens de segurança que serão compartilhados entre as aplicações e serviços da solução. É aí que entra o IdentityServer 4. O IdentityServer 4 em nossa solução funcionará como um microsserviço de autenticação central, dedicado agindo como um STS (serviço de token de segurança), e poderá ser usado para autenticar os usuários. A decisão de confiar ou não no usuário que está fazendo a requisição depende de tokens de segurança, que são armazenados na forma de cookies que são enviados e recebidos entre as requisições HTTP. Esses tokens serão compartilhados entre o aplicativo MVC e o serviço Relatório Web API.

- Configurando IdentityServer + Cliente MVC
  - Explicando o Identity Server 4
  - IdentityServer4, OAuth e OpenIdConnect
  - Configurando IdentityServer + Cliente MVC