transforme-se

serasa experian

WISEHANDS
Tecnologia e Acessibilidade

Bem-vindos ao curso de Java

Revisão Aula 37

Sumário

- Spring Security
  - Autenticação
  - Autorização
- OAUTH2
  - Papéis

Spring Security

Autenticação e Autorização

- Autenticação - Quem é usuário
- Autorização - O que o usuário pode fazer

Spring Security

Autenticação

Autenticação é o processo de verificação das credenciais que um usuário fornece com aquelas armazenadas em um sistema para provar que o usuário é quem diz ser. Se as credenciais corresponderem, você concederá acesso. Se não, você nega.

Spring Security

Autenticação

- Senha
- Token
- JWT
- Autenticação de chave pública e privada
- Autenticação de chave simétrica
- Autenticação de identidade digital
- Autenticação contextual
- Geolocalização
- Certificado digital
- Autenticação por SMS
- Autenticação centralizada

Spring Security

Autorização

Autorização é o processo de verificar se você tem permissão para acessar uma área de uma aplicação ou executar ações específicas, com base em determinados critérios e condições estabelecidos pela aplicação. Você também pode ouvi-lo ser chamado de controle de acesso ou controle de privilégio.

Geralmente para autenticação são distribuídos papéis para usuários, onde cada um desses papéis contêm um conjunto de permissões.

OAUTH2

OAUTH2

O OAuth 2.0 é um protocolo de autorização e NÃO um protocolo de autenticação. Como tal, ele foi projetado principalmente como um meio de conceder acesso a um conjunto de recursos, por exemplo, APIs remotas ou dados do usuário.

O Oauth 2.0 usa tokens de acesso. Um token de acesso é um dado que representa a autorização para acessar recursos em nome do usuário final. O OAuth 2.0 não define um formato específico para tokens de acesso. No entanto, em alguns contextos, o formato JSON Web Token (JWT) é frequentemente usado. Isso permite que os emissores de token incluam dados no próprio token. Além disso, por razões de segurança, os tokens de acesso podem ter uma data de validade.

OAUTH2

Papéis no OAUTH2

A ideia de papéis é parte da especificação central do framework de autorização do OAuth2.0, esses papéis definem os componentes essenciais de um sistema OAuth 2.0 e são:

- Resource Owner - Proprietário do Recurso
- Client - Cliente
- Resource Server - Servidor de Recurso
- Authorization Server - Servidor de Autorização

OAUTH2

Proprietário do Recurso: Usuário

O proprietário do recurso é o usuário que autoriza uma aplicação a acessar sua conta. O acesso da aplicação à conta do usuário é limitado ao “escopo” da autorização concedida (por exemplo: acesso para leitura ou escrita).

OAUTH2

Cliente: Aplicação

É a aplicação que interage com o Resource Owner, como por exemplo o browser, falando no caso de uma aplicação web.

OAUTH2

Servidor de Recursos: API

É o servidor com a API que está exposta na internet e precisa de proteção dos dados. Para conseguir acesso ao seu conteúdo é necessário um token que é emitido pelo authorization server.

OAUTH2

Servidor de Autorização: API

É o servidor responsável por autenticar o usuário e emitir os tokens de acesso. É ele que possui as informações do resource owner (o usuário), autentica e interage com o usuário após a identificação do client.

OAUTH2

Fluxo do OAUTH2

- A aplicação solicita autorização para acessar recursos do serviço do usuário
- Se o usuário autorizar a solicitação, a aplicação recebe uma concessão de autorização
- A aplicação solicita um token de acesso ao servidor de autorização (API) através da autenticação de sua própria identidade, e da concessão de autorização
- Se a identidade da aplicação está autenticada e a concessão de autorização for válida, o servidor de autorização (API) emite um token de acesso para a aplicação. A autorização está completa.
- A aplicação solicita o recurso ao servidor de recursos (API) e apresenta o token de acesso para autenticação
- Se o token de acesso é válido, o servidor de recurso (API) fornece o recurso para a aplicação

MUITO OBRIGADO PELA ATENÇÃO

Até a próxima aula!

transforme-se

O conhecimento é o poder
de transformar o seu futuro.