Spring Security

Um dos pontos mais importantes durante a implementação de uma aplicação web é a sua segurança. É de suma importância manter-se atualizado sobre todas as novas técnicas e formas de proteger o seu sistema, pois existem muitos conceitos que envolvem o processo de manter uma aplicação web segura. O **Spring Security** tem recursos avançados e de simples configuração para lhe ajudar com a segurança da sua aplicação.

O Spring Security é um framework do projeto Spring que possui um sistema de autenticação e autorização de alto nível e altamente customizável para aplicações Java. A framework inclusive é a solução oficial para implementação de recursos de segurança em aplicações Spring Boot que tem o foco em tornar a parte de autenticação e autorização uma coisa simples de fazer. Ele tem uma variedade muito grande de opções e ainda é bastante extensível.

Autenticação

Podemos dizer que a autenticação é o login na nossa aplicação. Trata-se da etapa de verificação se um determinado usuário possui credenciais (geralmente, combinação de login e senha) válidas para acessar a nossa aplicação. O sistema de autenticação do Spring Security pode ser configurado para que utilize diferentes mecanismos de autenticação, pois o mesmo trabalha com o conceito de providers de autenticação.

Os providers de autenticação são as estruturas responsáveis por efetivar as informações sobre os usuários que acessam a aplicação. Dessa maneira, você pode ter uma série de providers diferentes para utilizar nas aplicações.

Autorização

A autorização é um processo que acontece depois da autenticação. É o momento onde a aplicação verifica se o usuário atualmente autenticado tem permissão de acesso a um determinado recurso. O sistema de autorização do Spring Security também é bastante flexível, pois nos permite definir com facilidade quais são os possíveis tipos de usuários da nossa aplicação, como o sistema relaciona cada usuário com o seu determinado tipo e quais rotas de nossa aplicação cada tipo de usuário terá acesso. Tudo isso só é possível por que o Spring Security disponibiliza algumas

interfaces que devem ser implementadas e assim informamos qual será a regra de negócio de nossa aplicação para a realização dos processos de autenticação e autorização.

Armazenamento de Senha

Além dos sistemas de autenticação, autorização e proteção contra diferentes tipos de vulnerabilidades de aplicações web, o Spring Security também disponibiliza algoritmos de criptografias que evitam que sua aplicação guarde as senhas de seus usuários em texto puro no banco de dados.

Instalação do Spring Security

O processo de instalação do Spring Security dentro de uma aplicação Spring Boot é muito simples, já que o próprio Spring Boot possui um starter para instalar e pré-configurar o Spring Security. No caso de uma aplicação Spring Boot que utilize o Maven basta adicionar o código abaixo dentro da tag de dependências no arquivo pom.xml do seu projeto.

```
<dependency>
  <groupId>org.springframework.boot</groupId>
  <artifactId>spring-boot-starter-security</artifactId>
</dependency>
```

Depois de adicionado a dependência do spring security podemos realizar:

Configurar autenticação em memória

- Como fazer autenticação via JDBC
- Como fazer autenticação via JPA utilizando a interface `UserDetailsService`
- Criar uma página de login customizada
- A função “lembrar-me”
- Criar a funcionalidade de *logout*
- Como adicionar permissões (autorização) em nossas páginas

Com algumas poucas configurações já podemos ter uma autenticação via banco de dados, LDAP ou mesmo por memória. Sem falar nas várias integrações que ele já suporta e na possibilidade de criar as suas próprias.

Quanto a autorização, ele é bem flexível também. Através das permissões que atribuímos aos usuários autenticados, podemos proteger as requisições web (como as telas do nosso sistema, por exemplo), a simples invocação de um método e até a instância de um objeto.