10

O que aprendemos?

Nesta aula, aprendemos que:

- Em uma API Rest, não é uma boa prática utilizar autenticação com o uso de *session*;
- Uma das maneiras de fazer autenticação *stateless* é utilizando *tokens* **JWT** (*Json Web Token*);
- Para utilizar JWT na API, devemos adicionar a dependência da biblioteca **jjwt** no arquivo **pom.xml** do projeto;
- Para configurar a autenticação *stateless* no Spring Security, devemos utilizar o método `sessionManagement().sessionCreationPolicy(SessionCreationPolicy.STATELESS)`;
- Para disparar manualmente o processo de autenticação no Spring Security, devemos utilizar a classe `AuthenticationManager`;
- Para poder injetar o `AuthenticationManager` no *controller*, devemos criar um método anotado com `@Bean`, na classe `SecurityConfigurations`, que retorna uma chamada ao método `super.authenticationManager()`;
- Para criar o *token* JWT, devemos utilizar a classe `Jwts`;
- O *token* tem um período de expiração, que pode ser definida no arquivo **application.properties**;
- Para injetar uma propriedade do arquivo **application.properties**, devemos utilizar a anotação `@Value`.