06

Autenticação real

Transcrição

[00:00] Na aula anterior aprendemos a fazer log out e a tratar acessos não autenticados, agora vamos aprofundar um pouco mais na autenticação para aumentar a segurança do nosso sistema. Vamos no autenticador e vamos confirmar que o usuário que está na sessão existe mesmo, então ao em vez de pegar esse valor aqui e passar direto como retorno, vamos guardar ele em uma variável chamada email e vamos perguntar para o nosso usuário DAO se esse usuário existe mesmo.

[00:40] Import UsuarioDAO usuarioDAO, então usuarioDAO.comEmail(email), se esse usuário existe, possível usuário, if(possivelUsuario isPresent()), se esse existe retornamos um valor, no caso eu vou retornar o nome dele, return possivelUsuario.get().getNome(), então aqui retornamos o nome do usuário, se ele não existir retornamos vazio, null.

[01:19] É isso então, isso protege contra injeção de valores na session, então agora a nossa autenticação está um pouco mais segura, pois conferimos se o valor que está na sessão é valido, impedindo que alguém insira algum valor aleatório ali, ou algum email que ele esteja tentando dar um take over. Mais para frente vamos ver uma melhoria ainda maior na segurança, utilizando um tipo de token ao em vez do email do usuário, um token criptografado.

[01:50] No próximo email vamos finalmente atrelar o cliente a um token para autenticar a API, para autenticar as requisições que vão retornar os nossos objetos, os nossos produtos em JSON e finalmente permitindo que só que usuários autorizados utilizem a nossa API.