12

# Conclusão

### Transcrição

Chegamos ao final da primeira parte do curso **Segurança web em Java: Evitando SQL Injection, força bruta e outros ataques**, que utiliza Spring MVC. Vamos recapitular o que aprendemos nessa primeira parte do curso?

Vimos inicialmente que a parte de *login* utilizava requisições **GET**, expondo na URL os valores de usuário e senha. Dessa forma mudamos para o tipo de requisição **POST**, onde os parâmetros são passados no corpo da requisição.

Mas isso não garante a segurança de aplicação pelo fato de que os dados ainda são passados pela requisição. Com o ***SQLMap*** conseguimos injetar códigos SQL e acessar diversas informações da aplicação.

Para corrigir, mudamos a implementação da classe `UsuarioDaoImpl`. Anteriormente os códigos de acesso aos dados eram concatenações entre código SQL e Java. Quando passamos para especificação da **JPA** utilizando `EntityManager` e *querys* com **JPQL**, a aplicação primeiro envia o comando e só depois pega os parâmetros de usuário e senha.

Outro detalhe é que as senhas dos usuários eram armazenadas em texto puro no banco de dados. Utilizamos a classe `BCrypt` para transformar essa senha em código *Hash*, armazenando no banco apenas esse código.

A aplicação ainda estava vulnerável a ataques de força bruta, para evitar o ataque nós implementamos o botão do *reCAPTCHA*. Para a comunicação ocorrer com o Google, usamos a classe `Retrofit` para criar o objeto e implementamos a interface `GoogleService` para enviar a requisição **POST**, passando os parâmetros `secret` e `response`.

Com o *reCAPTCHA*, nós modificamos o método `login()` de `UsuarioController` para verificar o clique, caso o Google tenha respondido que o clique foi válido, nós verificamos o usuário e senha.

Espero que você tenha gostado do curso. Te encontro na segunda parte [Segurança web em Java parte 2: XSS, Mass Assignment e Uploads de arquivos! (https://cursos.alura.com.br/course/seguranca-web-em-java-parte-2)](https://cursos.alura.com.br/course/seguranca-web-em-java-parte-2).