06

# Para saber mais: PreparedStatement

No curso utilizamos a especificação da JPA para corrigirmos o problema de SQL Injection que estávamos tendo, essa é somente uma das alternativas disponíveis que decidimos adotar. Poderíamos também ter utilizado a interface `PreparedStatement`.

A ideia assim como na JPA seria realizar o isolamento da query com os parâmetros que serão passados pelo formulário. Para isso, teremos por exemplo:

```
String sql = "insert into USUARIO (email, senha, nome, nomeImagem) values (?,?,?,?)";
PreparedStatement stmt = connection.prepareStatement(sql);
```

Com isso, também estamos isolando a query dos parâmetros vindo do formulário, pois com o `?` estamos informando que não sabemos ainda que dado será passado. Logo em seguida, chamamos o método setString do PreparedStatement para preencher os valores juntamente com as suas respectivas posições que deverão ser colocados:

```
stmt.setString(1, usuario.getEmail());
stmt.setString(2, usuario.getSenha());
stmt.setString(3, usuario.getNome());
stmt.setString(3, usuario.getNomeImagem());
```

Caso deseje aprender mais a respeito, segue link com a apostila da Caelum explicando mais sobre o PreparedStatement: https://www.caelum.com.br/download/caelum-java-web-fj21.pdf (https://www.caelum.com.br/download/caelum-java-web-fj21.pdf)