



## O que aprendemos?

Nesta aula, aprendemos que:

- Ao executar SQL como `Statement`, temos um risco de segurança, chamado de ***SQL Injection***
  - *SQL Injection* nada mais é do que passar um novo comando SQL como parâmetro
- Para evitar *SQL Injection*, devemos usar a interface `PreparedStatement`
  - Diferentemente do `Statement`, o `PreparedStatement` trata (*sanatiza*) cada parâmetro do comando SQL