11

O que aprendemos?

Nesta aula, aprendemos:

- O que é ***SQL Injection*** e como realizar esse ataque em nossa aplicação
- Que adicionar parâmetros na *string* SQL é perigoso
- A resolver esse problema, utilizando ***Prepared Statements***
- Que *prepared statements* podem inclusive ajudar na performance da aplicação
- As diferenças entre `bindValue` e `bindParam` para vincular parâmetros aos *prepared statements*
- Que podemos informar o tipo de dado que estamos passando através do `PDO`, utilizando o terceiro parâmetro de `bindValue` e `bindParam`