



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

Logar com usuário administrador sem saber a senha.

## Laboratório

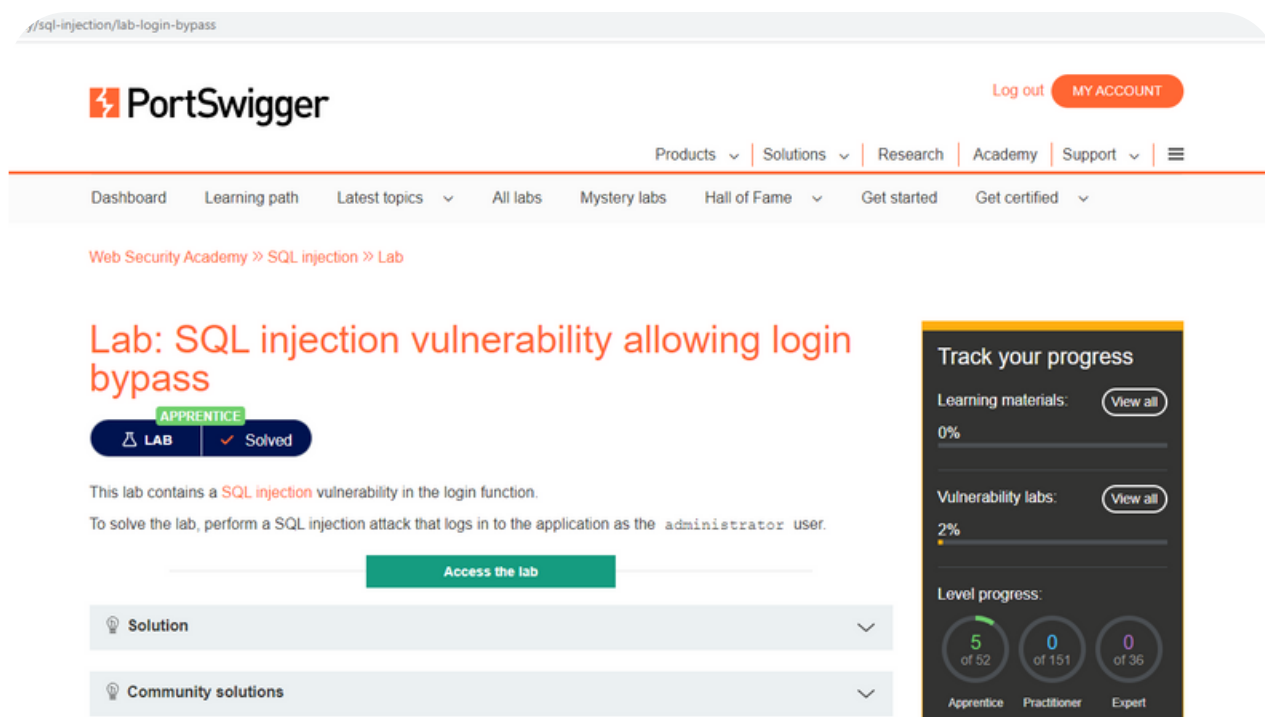
- SQL injection vulnerability allowing login bypass

## Pré-requisitos

- Navegador.

# 1.ACESSANDO O LABORATÓRIO

Clique na opção "**Access the lab**":



The screenshot displays the PortSwigger Web Security Academy interface. At the top, the URL is `/sql-injection/lab-login-bypass`. The PortSwigger logo is on the left, and 'Log out' and 'MY ACCOUNT' are on the right. A navigation bar includes links for Products, Solutions, Research, Academy, and Support. Below this, a secondary navigation bar lists Dashboard, Learning path, Latest topics, All labs, Mystery labs, Hall of Fame, Get started, and Get certified. The breadcrumb trail reads 'Web Security Academy » SQL injection » Lab'. The main heading is 'Lab: SQL injection vulnerability allowing login bypass', with a green 'APPRENTICE' tag. Below the heading are 'LAB' and 'Solved' buttons. The lab description states: 'This lab contains a SQL injection vulnerability in the login function. To solve the lab, perform a SQL injection attack that logs in to the application as the administrator user.' A green 'Access the lab' button is prominently displayed. Below this are sections for 'Solution' and 'Community solutions'. On the right, a 'Track your progress' sidebar shows 'Learning materials' at 0%, 'Vulnerability labs' at 2%, and 'Level progress' for Apprentice (5 of 52), Practitioner (0 of 151), and Expert (0 of 36).

**Observação:** É importante observar que a plataforma já nos fornece informações sobre o 'usuário', no entanto, a 'senha' não é disponibilizada.

## 2.LOGANDO NA PLATAFORMA

Ao seguir o exemplo abaixo, observa-se que apenas modificamos o final do nome de usuário. Isso é suficiente para explorar uma vulnerabilidade no banco de dados, permitindo o acesso sem a necessidade da senha.

dc07240fe009f00fd.web-security-academy.net/login



SQL injection vulnerability allowing login bypass

[Back to lab description >>](#)

Congratulations, you solved the lab!

[Share y](#)

Login

**administrador'--**

Username

administrator'--

Password

.....

Log in

Aqui você coloca qualquer senha, pois o que fizemos no usuário vai bugar o banco de dados, deixando agente entrar.

## 3. JÁ DENTRO DO SITE

Seguindo o exemplo fornecido, a plataforma deverá interpretar o código inserido no campo de pesquisa e fornecer o valor correspondente como resultado.

### RESULTADO

WebSecurity Academy

Reflected XSS into HTML context with nothing encoded

Back to lab description >>

LAB

Home

Só colocar esse código no campo de pesquisa, ele tem que abrir um modal, pronto é só isso

WE LIKE TO BLOG

<script>alert('xss 2023')</script>

Search