



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

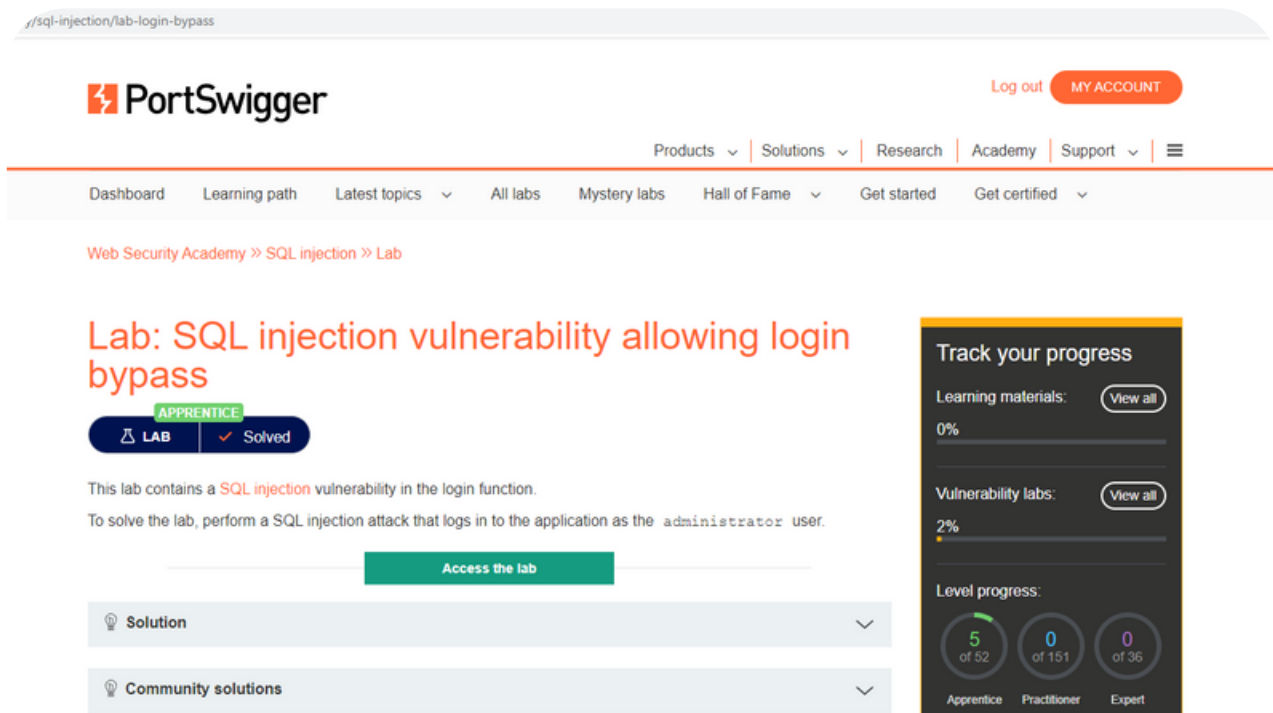
- [SQL injection vulnerability allowing login bypass](#)

Pré-requisitos

- Navegador.

1.ACESSANDO O LABORATÓRIO

Clique na opção "**Access the lab**":



The screenshot displays the PortSwigger Web Security Academy interface. The main content area shows the lab titled "Lab: SQL injection vulnerability allowing login bypass" with an "APPRENTICE" difficulty level. A "LAB" button and a "Solved" status are visible. 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." Below the description is a green "Access the lab" button. Underneath are sections for "Solution" and "Community solutions". On the right sidebar, the "Track your progress" section shows progress for learning materials (0%), vulnerability labs (2%), and level progress (5 of 52 for Apprentice, 0 of 151 for Practitioner, 0 of 36 for Expert).

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 do 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

The screenshot shows a web browser window with the URL `0a7d00db035a3ef281e7755900510020.web-security-academy.net`. The page title is "Reflected XSS into HTML context with nothing encoded". The Web Security Academy logo is visible on the left, and a "LAB" button is on the right. Below the header, there is a red horizontal line. On the right side, there is a "Home" link. On the left side, there is a red text box that says: "Só colocar esse código no campo de pesquisa, ele tem que abrir um modal, pronto é só isso". In the center, there is a "WE LIKE TO BLOG" section with a stylized face icon. Below this, there is a search bar with the text `<script>alert('xss 2023')</script>` entered. A red arrow points to the search bar. To the right of the search bar is a "Search" button. Below the search bar, there is a large image of a person's hair.