

Práctico 3 - Base de datos I

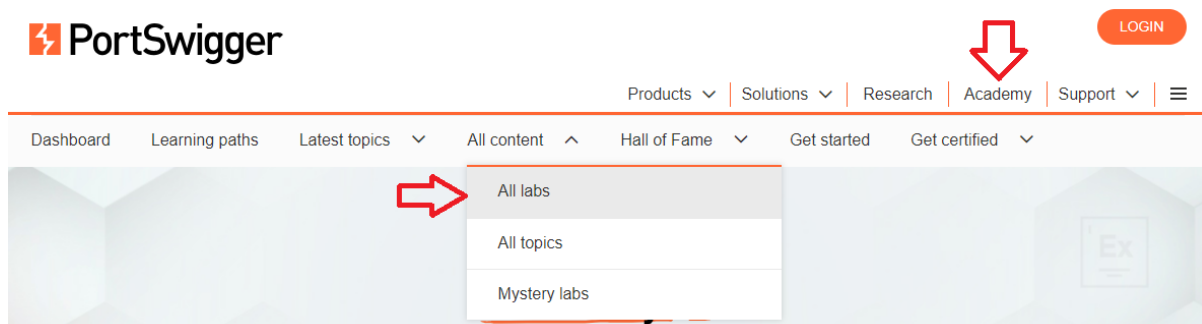
Injection

Introducción

Para este práctico deberás resolver al menos los primeros 10 laboratorios de Injection de la plataforma PortSwigger (<https://portswigger.net/>).

Para acceder a los laboratorios deberán registrarse en la plataforma:

- 1) Se registran <https://portswigger.net/users/register>
- 2) Les llega un correo con la contraseña
- 3) Se logean
- 4) Seleccionan Academy
- 5) Entrar a “All content” -> “All labs”



Laboratorios

Cada laboratorio tiene una introducción teórica y un link para acceder a la web del laboratorio particular.

Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

APPRENTICE

LAB ✓ Solved

This lab contains a SQL injection vulnerability in the product category filter. When the user selects a category, the application carries out a SQL query like the following:

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

To solve the lab, perform a SQL injection attack that causes the application to display one or more unreleased products.

ACCESS THE LAB

Solution

Community solutions

Cuando resuelven el laboratorio les notificará con un banner en la parte superior

WebSecurity Academy

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!

Continue learning >>

*como ven en la captura existe una parte de “Solución”, la idea es que hagan los ejercicios sin consultar esta sección ya que para las futuras evaluaciones se asumirá que ustedes saben los fundamentos de injection y realizar estos laboratorios.

Entregable

Deben entregar en un archivo de texto las soluciones para los laboratorios realizados, en los casos que manipularon la URL del laboratorio copian la URL que soluciona el problema, en los casos que utilizan un campo que debe rellenar el usuario indican el campo utilizado y el valor ingresado.