**Lab: Reflected XSS into HTML context with nothing encoded**

This lab contains a simple [reflected cross-site scripting](https://portswigger.net/web-security/cross-site-scripting/reflected) vulnerability in the search functionality.

To solve the lab, perform a cross-site scripting attack that calls the alert function.

A la hora de ingresar sentencias en la barra de busqueda nos damos cuenta de que la aplicación tiene problemas con la lectura de los tags. Por lo que ese sencillo alterar el contenido de las pestañas con sentencias HTML.

La soluciòn sería ingresar esta sentencia en la barra de búsqueda.

***<script> alert() </script>***

