Solved Portswigger Labs

Submitted by: P. K. Amudhini

Ethical Hacking Internship -- Task-1



Lab: Reflected XSS into HTML context with nothing encoded















This lab contains a simple reflected cross-site scripting vulnerability in the search functionality.

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

Access the lab

https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded

Lab: Reflected XSS into HTML context with most tags and attributes blocked















Solved



This lab contains a reflected XSS vulnerability in the search functionality but uses a web application firewall (WAF) to protect against common XSS vectors.

To solve the lab, perform a cross-site scripting attack that bypasses the WAF and calls the print() function.



Your solution must not require any user interaction. Manually causing print () to be called in your own browser will not solve the lab.

Access the lab

Lab: Reflected XSS with event handlers and href attributes blocked





This lab contains a reflected XSS vulnerability with some whitelisted tags, but all events and anchor href attributes are blocked..

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

Note that you need to label your vector with the word "Click" in order to induce the simulated lab user to click your vector. For example: click me

Access the lab

Lab: Reflected XSS into attribute with angle brackets HTML-encoded



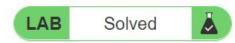












This lab contains a reflected cross-site scripting vulnerability in the search blog functionality where angle brackets are HTML-encoded. To solve this lab, perform a cross-site scripting attack that injects an attribute and calls the alert function.

Access the lab

Lab: Reflected XSS into a JavaScript string with single quote and backslash escaped















This lab contains a reflected cross-site scripting vulnerability in the search query tracking functionality. The reflection occurs inside a JavaScript string with single quotes and backslashes escaped.

To solve this lab, perform a cross-site scripting attack that breaks out of the JavaScript string and calls the alert function.



Thank You