

Task 1

PortSwigger

Log outMY ACCOUNT

ProductsSolutionsResearchAcademySupport

DashboardLearning pathsLatest topicsAll contentHall of FameGet startedGet certified

Web Security Academy > Cross-site scripting > Reflected > Lab

Lab: Reflected XSS into HTML context with nothing encoded

APPRENTICELAB Solved

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

PortSwigger

Log outMY ACCOUNT

ProductsSolutionsResearchAcademySupport

DashboardLearning pathsLatest topicsAll contentHall of FameGet startedGet certified

Web Security Academy > Cross-site scripting > Stored > Lab

Lab: Stored XSS into HTML context with nothing encoded

APPRENTICELAB Solved

This lab contains a stored cross-site scripting vulnerability in the comment functionality.

To solve this lab, submit a comment that calls the `alert` function when the blog post is viewed.

ACCESS THE LAB

Back to all topics

What is XSS?

How does XSS work?

Impact of an attack

Proof of concept

Testing

Reflected XSS

Stored XSS

DOM-based XSS

XSS contexts

Exploiting XSS vulnerabilities

PortSwigger

Log outMY ACCOUNT

ProductsSolutionsResearchAcademySupport

DashboardLearning pathsLatest topicsAll contentHall of FameGet startedGet certified

Web Security Academy > Cross-site scripting > DOM-based > Lab

Lab: DOM XSS in `document.write` sink using source `location.search`

APPRENTICELAB Solved

This lab contains a DOM-based cross-site scripting vulnerability in the search query tracking functionality. It uses the JavaScript `document.write` function, which writes data out to the page. The `document.write` function is called with data from `location.search`, which you can control using the website URL.

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

Back to all topics

What is XSS?

How does XSS work?

Impact of an attack

Proof of concept

Testing

Reflected XSS

Stored XSS

DOM-based XSS

XSS contexts

Exploiting XSS vulnerabilities

PortSwigger

Log outMY ACCOUNT

ProductsSolutionsResearchAcademySupport

DashboardLearning pathsLatest topicsAll contentHall of FameGet startedGet certified

< Back to all topics

What is XSS?

How does XSS work?

Impact of an attack

Proof of concept

Testing

Reflected XSS

Stored XSS

DOM-based XSS

XSS contexts

Exploiting XSS vulnerabilities

Web Security Academy > Cross-site scripting > DOM-based > Lab

Lab: DOM XSS in innerHTML sink using source location.search

APPRENTICELAB Solved

This lab contains a DOM-based cross-site scripting vulnerability in the search blog functionality. It uses an innerHTML assignment, which changes the HTML contents of a div element, using data from location.search.
To solve this lab, perform a cross-site scripting attack that calls the alert function.

Upcoming Earnings

Search

ENG IN16:1516-07-2024

PortSwigger

Log outMY ACCOUNT

ProductsSolutionsResearchAcademySupport

DashboardLearning pathsLatest topicsAll contentHall of FameGet startedGet certified

< Back to all topics

What is XSS?

How does XSS work?

Impact of an attack

Proof of concept

Testing

Reflected XSS

Stored XSS

DOM-based XSS

XSS contexts

Exploiting XSS vulnerabilities

Web Security Academy > Cross-site scripting > DOM-based > Lab

Lab: DOM XSS in jQuery anchor href attribute sink using location.search source

APPRENTICELAB Solved

This lab contains a DOM-based cross-site scripting vulnerability in the submit feedback page. It uses the jQuery library's \$ selector function to find an anchor element, and changes its href attribute using data from location.search.
To solve this lab, make the "back" link alert document.cookie.

Upcoming Earnings

Search

ENG IN16:1716-07-2024