

Task-1:screenshot of solved Portswigger labs

The screenshot shows a web browser window with the URL `https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-document-write-sink`. The page title is "Lab: DOM XSS in `document.write` sink using source `location.search`". The lab is marked as "APPRENTICE" and "Solved". The description states: "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." Below the description is an "ACCESS THE LAB" button and two expandable sections: "Solution" and "Community solutions". A left sidebar contains a navigation menu with various XSS topics.

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
- Dangling markup injection
- Content security policy (CSP)
- Preventing XSS attacks
- Cheat sheet
- View all XSS labs

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

APPRENTICE LAB 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.

ACCESS THE LAB

Solution

Community solutions

The screenshot shows a web browser window with the URL `https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-jquery-href-attribute-sink`. The page title is "Lab: DOM XSS in jQuery anchor href attribute sink using source `location.search`". The lab is marked as "APPRENTICE" and "Solved". The description states: "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`." Below the description is an "ACCESS THE LAB" button and two expandable sections: "Solution" and "Community solutions". A left sidebar contains a navigation menu with various XSS topics.

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
- Dangling markup injection
- Content security policy (CSP)
- Preventing XSS attacks
- Cheat sheet
- View all XSS labs

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

APPRENTICE LAB Solved

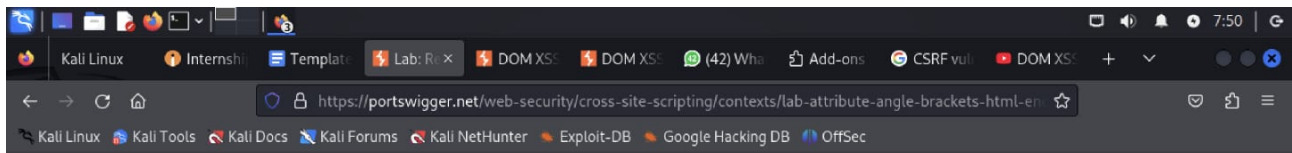
This lab contains a DOM-based cross-site scripting vulnerability in the submit feedback page. It uses the jQuery library's `$` selector function to find an anchor element, and changes its `href` attribute using data from `location.search`.


To solve this lab, make the "back" link alert `document.cookie`.

ACCESS THE LAB

Solution

Community solutions





Log outMY ACCOUNT

Products | Solutions | Research | Academy | Support

Dashboard | Learning paths | Latest topics | All content | Hall of Fame | Get started | Get certified

Back to all topics

What is XSS?

How does XSS work?

Impact of an attack


Proof of concept

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

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

APPRENTICE

LAB Solved



Log outMY ACCOUNT

Products | Solutions | Research | Academy | Support

Dashboard | Learning paths | Latest topics | All content | Hall of Fame | Get started | Get 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


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

Lab: Reflected XSS into a JavaScript string with angle brackets HTML encoded

APPRENTICE

LAB Solved

This lab contains a reflected cross-site scripting vulnerability in the search query tracking functionality where angle brackets are encoded. The reflection occurs inside a JavaScript string. To solve this lab, perform a cross-site scripting attack that breaks out of the JavaScript string and calls the `alert` function.



Log outMY ACCOUNT

Products | Solutions | Research | Academy | Support

Dashboard | Learning paths | Latest topics | All content | Hall of Fame | Get started | Get 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: Reflected DOM XSS

PRACTITIONER

LAB Solved

This lab demonstrates a reflected DOM vulnerability. Reflected DOM vulnerabilities occur when the server-side application processes data from a request and echoes the data in the response. A script on the page then processes the reflected data in an unsafe way, ultimately writing it to a dangerous sink.

To solve this lab, create an injection that calls the `alert()` function.

ACCESS THE LAB