

# Solved Cross-site scripting Labs

## Cross-site scripting

 LAB

APPRENTICE

Reflected XSS into HTML context with nothing encoded →


✓ Solved

 LAB

APPRENTICE

Stored XSS into HTML context with nothing encoded →


✓ Solved

 LAB

APPRENTICE

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

✓ Solved

 LAB

APPRENTICE

DOM XSS in `innerHTML` sink using source `location.search` →

✓ Solved

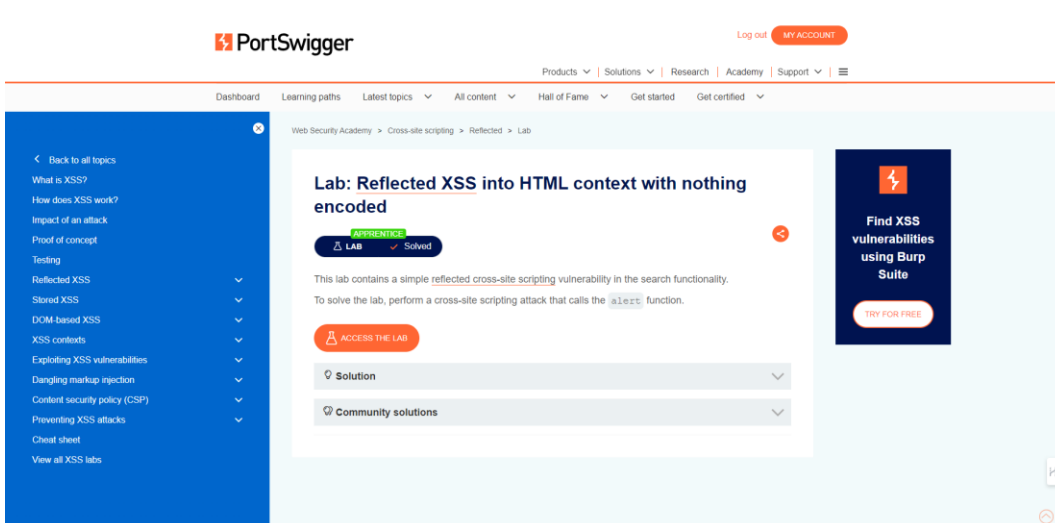
 LAB

EXPERT

Reflected XSS in a JavaScript URL with some characters blocked →

✓ Solved

### 1. Lab: Reflected XSS into HTML context with nothing encoded



PortSwigger

Log out MY ACCOUNT

Products | Solutions | Research | Academy | Support

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

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

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

APPRENTICE ✓ 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

Solution

Community solutions

Find XSS vulnerabilities using Burp Suite

TRY FOR FREE

## 2. Lab: Stored XSS into HTML context with nothing encode

The screenshot shows the PortSwigger Web Security Academy interface. The top navigation bar includes 'Log out' and 'MY ACCOUNT'. Below it, a secondary navigation bar lists 'Products', 'Solutions', 'Research', 'Academy', and 'Support'. The main header area contains 'Dashboard', 'Learning paths', 'Latest topics', 'All content', 'Hall of Fame', 'Get started', and 'Get certified'. The left sidebar is a blue menu with a close button, listing various topics under 'Back to all topics', including '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', and 'View all XSS labs'. The main content area displays the lab title 'Lab: Stored XSS into HTML context with nothing encoded' with a difficulty level of 'APPRENTICE' and a 'Solved' status. It describes a 'stored cross-site scripting vulnerability' in the comment functionality, requiring a comment that calls the `alert` function. An 'ACCESS THE LAB' button is present. Below the description are sections for 'Solution' and 'Community solutions'. A right sidebar promotes 'Find XSS vulnerabilities using Burp Suite' with a 'TRY FOR FREE' button. The URL at the bottom left is <https://portswigger.net/web-security/index.html>.

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

The screenshot shows the PortSwigger Web Security Academy interface for a different lab. The top navigation bar includes 'Log out' and 'MY ACCOUNT'. Below it, a secondary navigation bar lists 'Products', 'Solutions', 'Research', 'Academy', and 'Support'. The main header area contains 'Dashboard', 'Learning paths', 'Latest topics', 'All content', 'Hall of Fame', 'Get started', and 'Get certified'. The left sidebar is a blue menu with a close button, listing various topics under 'Back to all topics', including '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', and 'View all XSS labs'. The main content area displays the lab title 'Lab: DOM XSS in `document.write` sink using `source location.search`' with a difficulty level of 'APPRENTICE' and a 'Solved' status. It describes a 'DOM-based cross-site scripting vulnerability' in the search query tracking functionality, mentioning the use of the JavaScript `document.write` function and the `location.search` property. An 'ACCESS THE LAB' button is present. Below the description are sections for 'Solution' and 'Community solutions'. A right sidebar promotes 'Find XSS vulnerabilities using Burp Suite' with a 'TRY FOR FREE' button. The URL at the bottom left is <https://portswigger.net/web-security/index.html>.

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

The screenshot shows the PortSwigger Web Security Academy interface. The left sidebar contains a navigation menu with categories like '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', and 'View all XSS labs'. The main content area displays the lab title 'Lab: DOM XSS in innerHTML sink using source location.search' with a difficulty level of 'APPRENTICE' and a status of 'Solved'. The lab description states: '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.' Below the description are buttons for 'ACCESS THE LAB', 'Solution', and 'Community solutions'. A right sidebar promotes 'Find XSS vulnerabilities using Burp Suite' with a 'TRY FOR FREE' button.

#### 5. Lab: Reflected XSS in a JavaScript URL with some characters blocked

The screenshot shows the PortSwigger Web Security Academy interface for a different lab. The left sidebar is the same as in the previous image. The main content area displays the lab title 'Lab: Reflected XSS in a JavaScript URL with some characters blocked' with a difficulty level of 'EXPERT' and a status of 'Solved'. The lab description states: 'This lab reflects your input in a JavaScript URL, but all is not as it seems. This initially seems like a trivial challenge; however, the application is blocking some characters in an attempt to prevent XSS attacks. To solve the lab, perform a cross-site scripting attack that calls the alert function with the string 1337 contained somewhere in the alert message.' Below the description are buttons for 'ACCESS THE LAB', 'Solution', and 'Community solutions'. A right sidebar promotes 'Find XSS vulnerabilities using Burp Suite' with a 'TRY FOR FREE' button.