

PORT SWIGGER

Solved Labs:

- **Reflected XSS into HTML context with nothing encoded**
- **Reflected XSS with event handlers and attributes blocked**
- **Stored XSS into HTML context with nothing encoded**
- **Stored DOM XSS**
- **Exploiting XSS to perform CSRF**

The screenshot displays the PortSwigger Web Security Academy interface. At the top, the PortSwigger logo is on the left, and 'Log out' and 'MY ACCOUNT' are on the right. A navigation bar includes links for Products, Solutions, Research, Academy, Daily Swig, and Support. Below this, a secondary navigation bar lists Academy Home, Learning Path, Latest Topics, All Labs, Hall of Fame, Getting Started Guide, and Get Certified. The main content area shows a breadcrumb trail: 'Web Security Academy » Cross-site scripting » Reflected » Lab'. The lab title is 'Lab: Reflected XSS into HTML context with nothing encoded'. Below the title are social media sharing icons. A progress indicator shows 'APPRENTICE' and 'LAB Solved'. The lab description states: '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.' A green button labeled 'Access the lab' is visible. On the right, a 'Track your progress' sidebar shows progress for Learning materials (0%), Vulnerability labs (2%), and Level progress (Level 2).

Lab: Reflected XSS with event handlers and `href` attributes blocked



EXPERT

LAB Solved

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`

Track your progress

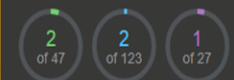
Learning materials: [View all](#)

0%

Vulnerability labs: [View all](#)

2%

Level progress:



Lab: Stored XSS into HTML context with nothing encoded



APPRENTICE

LAB 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](#)

[Solution](#)

Track your progress

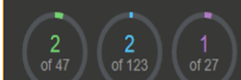
Learning materials: [View all](#)

0%

Vulnerability labs: [View all](#)

2%

Level progress:



Lab: Stored DOM XSS



PRACTITIONER

LAB Solved

This lab demonstrates a stored DOM vulnerability in the blog comment functionality. To solve this lab, exploit this vulnerability to call the `alert()` function.

[Access the lab](#)

Solution

Community solutions

Track your progress

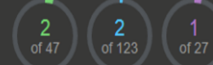
Learning materials: [View all](#)

0%

Vulnerability labs: [View all](#)

2%

Level progress:



Lab: Exploiting XSS to perform CSRF



PRACTITIONER

LAB Solved

This lab contains a **stored XSS** vulnerability in the blog comments function. To solve the lab, exploit the vulnerability to perform a **CSRF attack** and change the email address of someone who views the blog post comments.

You can log in to your own account using the following credentials: `wiener:peter`

Learning path

If you're following our suggested [learning path](#), please note that this lab requires some understanding of topics that we haven't covered yet. Don't worry if you get stuck; try coming back later once you've developed your knowledge further.

Track your progress

Learning materials: [View all](#)

0%

Vulnerability labs: [View all](#)

2%

Level progress:

