

# Cross-Site Scripting Lab-03

M.Gobi Shankar

CB.SC.P2CYS23019

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

Enter a random alphanumeric string into the search box. Right-click and inspect the element, and observe that your random string has been placed inside an `img src` attribute.

[Home](#)

0 search results for 'xavda134'

Search

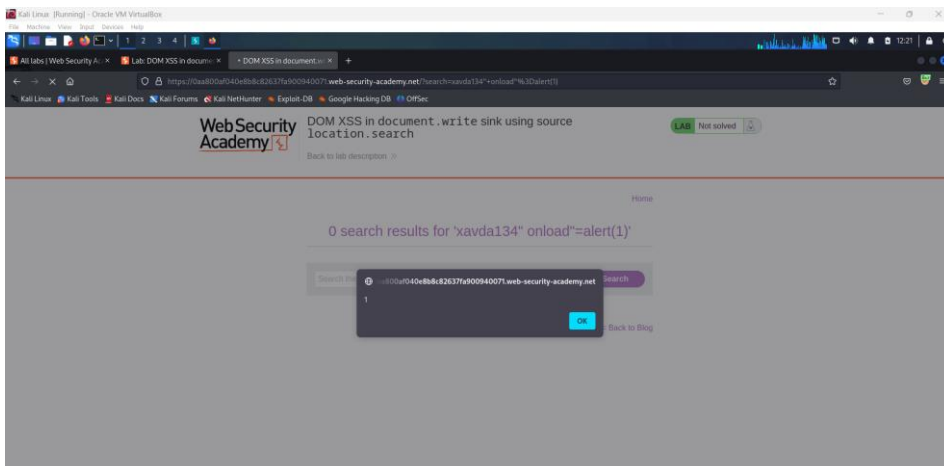
[< Back to Blog](#)

```
Inspector Console Debugger Network Style Editor Performance Memory Storage Acc
Search HTML
<!DOCTYPE html>
<html> scroll
  <head> </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js"></script>
    <div id="academyLabHeader"> </div> overflow
    <div theme="blog">
      <section class="maincontainer">
        <div class="container is-page"> overflow
          <header class="navigation-header"> </header> flex
          <header class="notification-header"> </header>
          <section class="blog-header"> </section>
          <section class="search">
            <form action="/" method="GET"> flex
              <input type="text" placeholder="Search the blog..." name="search">
              <button class="button" type="submit">Search</button>
            </form>
          </section>
          <script> </script>
          
          <section class="blog-list no-results"> </section>
        </div>
      </section>
    <div class="footer-wrapper"> </div> overflow
  </div>
</body>
</html>
```

Break out of the `img` attribute by searching for:

```
onload="alert(1)"
```

```
<!DOCTYPE html>
<html> <scroll>
<head> <img> </head>
<body>
  <script src="/resources/labheader/js/labHeader.js"></script>
  <div id="academyLabHeader"> <img> <div> <overflow>
  <div theme="blog">
    <div class="maincontainer">
      <div class="container is-page"> <overflow>
        <header class="navigation-header"> <img> </header> <flex>
        <header class="notification-header"> <img> </header>
        <section class="blog-header"> <img> </section>
        <section class="search">
          <form action="/" method="GET"> <flex>
            <input type="text" placeholder="Search the blog..." name="search">
            <button class="button" type="submit">Search</button>
          </form>
        </section>
        <script> <img> </script>
         <event>
        <section class="blog-list no-results"> <img> </section>
      </div>
    </section>
  <div class="footer-wrapper"> <img> </div> <overflow>
</div>
</body>
</html>
```



Lab Completed Successfully.

WebSecurity Academy

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 'xavda134" onload="alert(1)'"

Search the blog...

Search

< Back to Blog