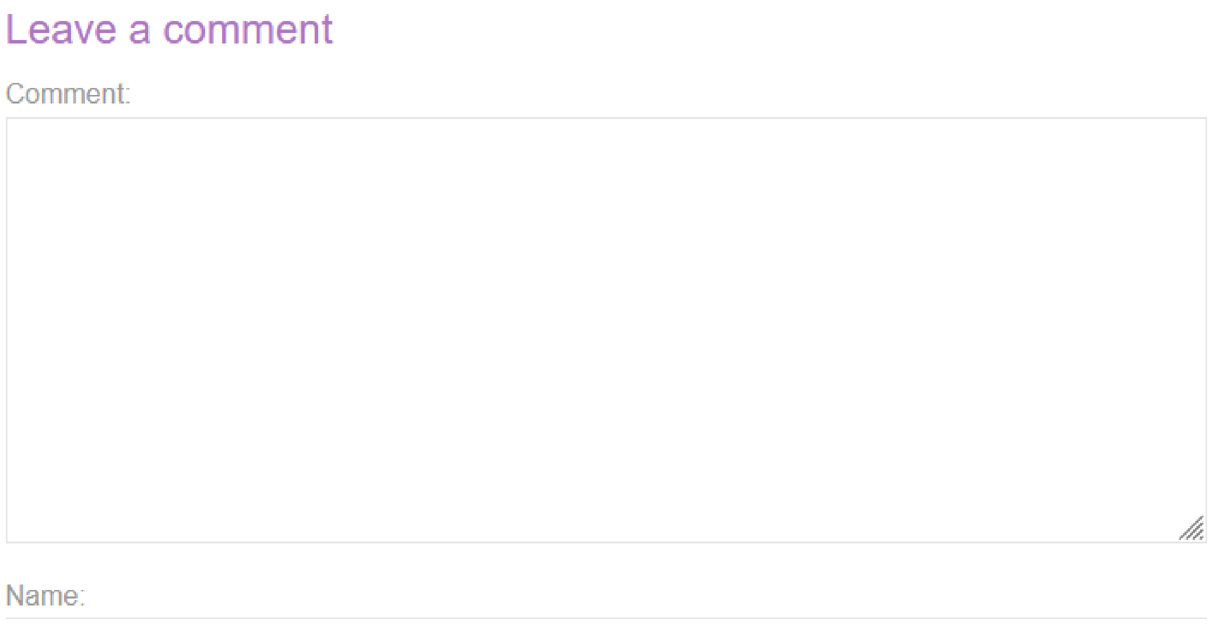
Lab: Stored XSS into HTML context with nothing encoded

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.

The outcome of this lab is to submit and alert script in the comments. When the comment is posted it is baked into the html. When a user then visits the page the "alert" pops up as a webpage pop up box displaying the message articulated in the script.

Find Injection Point

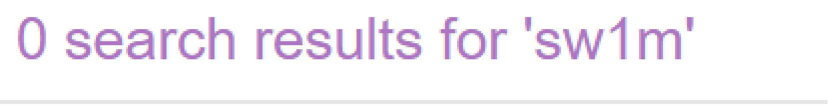


Leave a comment

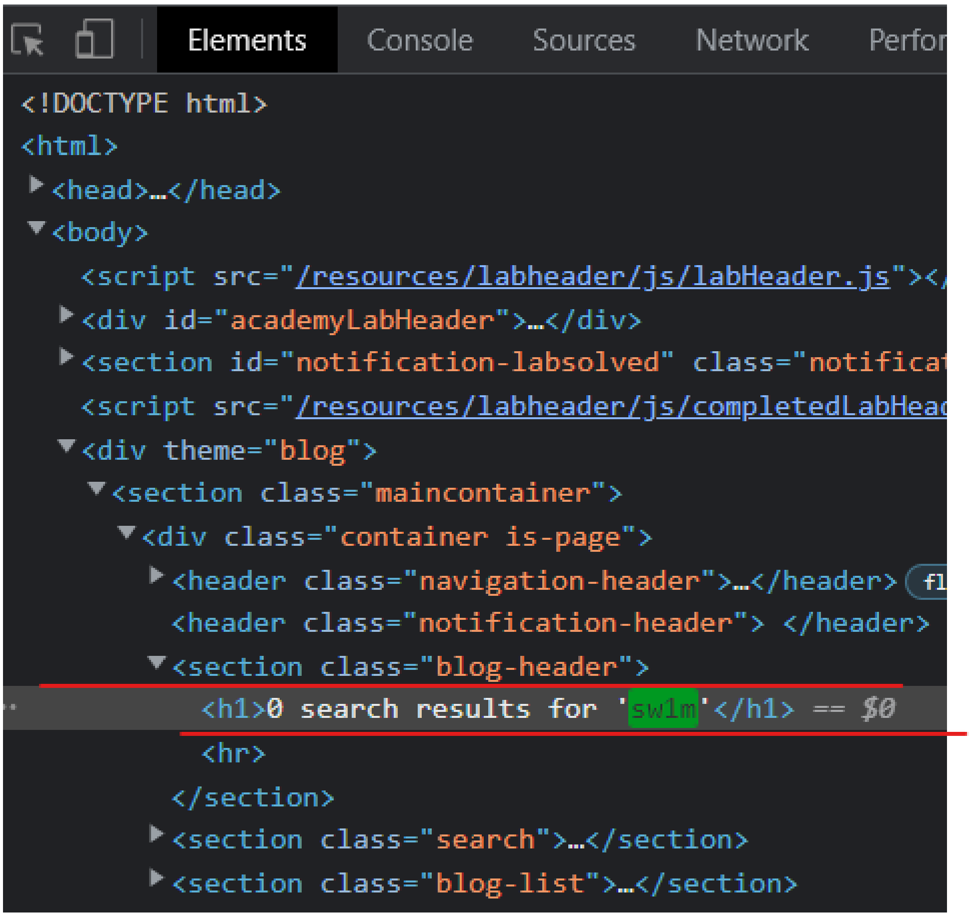
Comment:

Name:

Check where the results appear in Elements

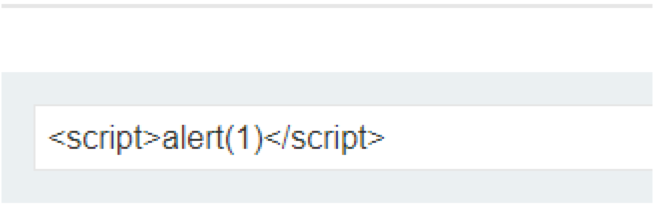


0 search results for 'sw1m'



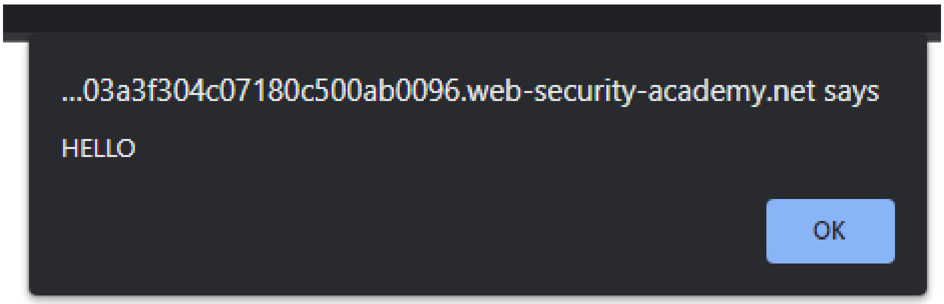
```
<!DOCTYPE html>
<html>
 <head>…</head>
 <body>
    <script src="/resources/labheader/js/labHeader.js"></
   <div id="academyLabHeader">…</div>
   <section id="notification-labsolved" class="notificat
    <script src="/resources/labheader/js/completedLabHead
   <div theme="blog">
     <section class="maincontainer">
       <div class="container is-page">
         <header class="navigation-header">…</header> fl
          <header class="notification-header"> </header>
         <section class="blog-header">
            <h1>0 search results for 'sw1m'</h1> == $0
            <hr>
          </section>
         <section class="search">…</section>
         <section class="blog-list">…</section>
```

Use injectable script



<script>alert(1)</script>

Profit with pop ups



...03a3f304c07180c500ab0096.web-security-academy.net says

HELLO