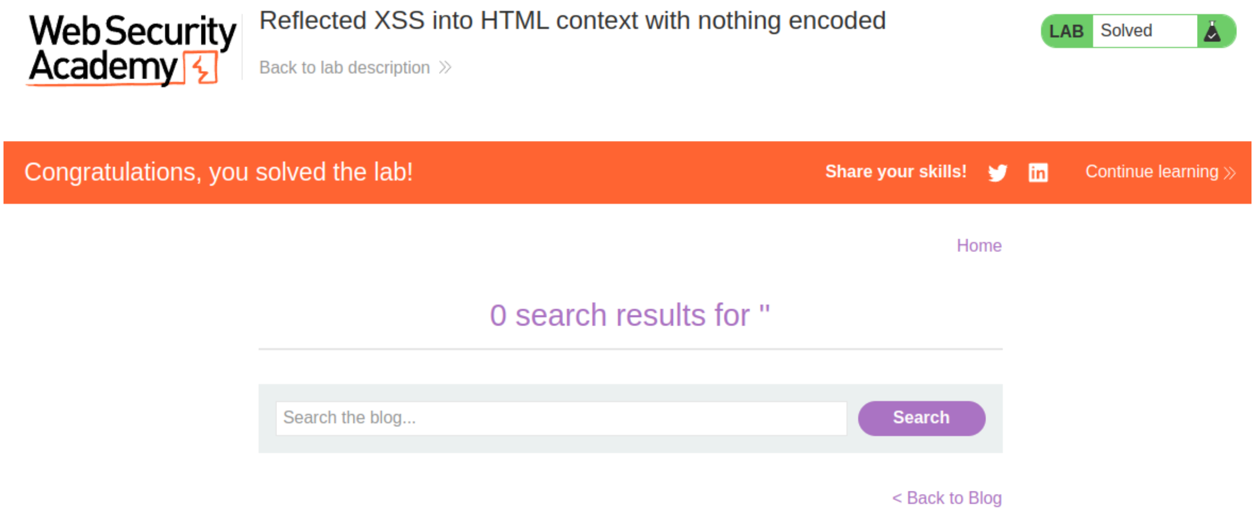
# TASK 1:

## 1. Reflected XSS into HTML context with nothing encoded:

Steps: - In the “search box” type: <script>alert(1)</script>
- Click Search.



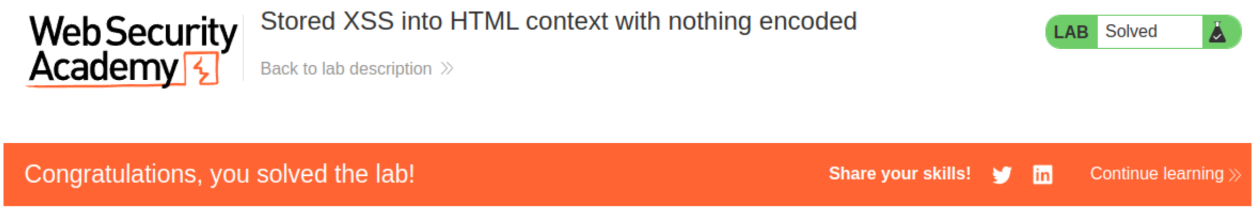
Reflected XSS into HTML context with nothing encoded

Congratulations, you solved the lab!

0 search results for ''

## 2. Stored XSS into HTML contest with nothing encoded:

Steps: In the comment box, type: <script>alert(1)</script>
Write Name, email and website
Click, post comment
Go back to the blog

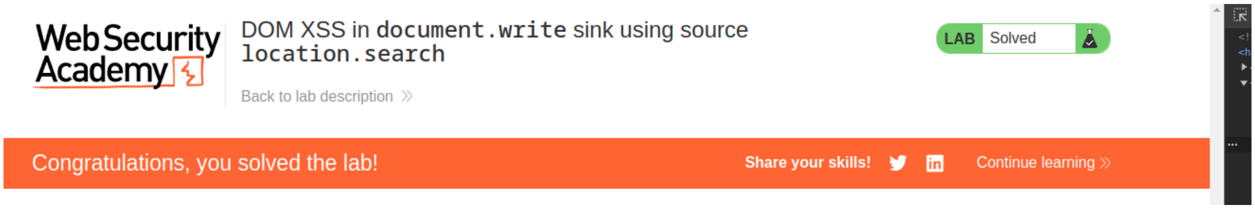


Stored XSS into HTML context with nothing encoded

Congratulations, you solved the lab!

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

Steps: Enter random alphanumeric string.
Now, random string has been placed inside the img tag.
Break out of the img attribute by searching for:
“><svg onload=alert(1)>

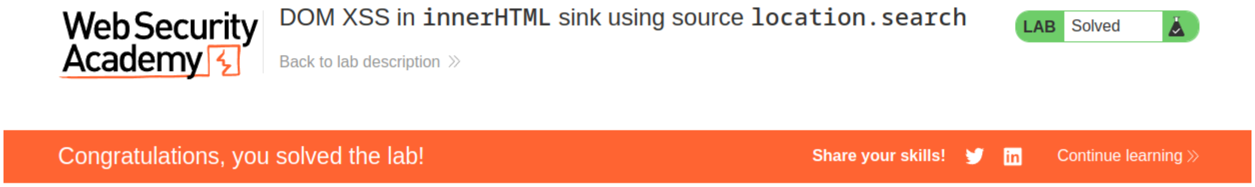


DOM XSS in `document.write` sink using source `location.search`

Congratulations, you solved the lab!

## 4. DOM XSS in innerHTML sink using source location.search:

Steps: In the search box, type: <img src=1 onerror=alert(1)>
Click search.

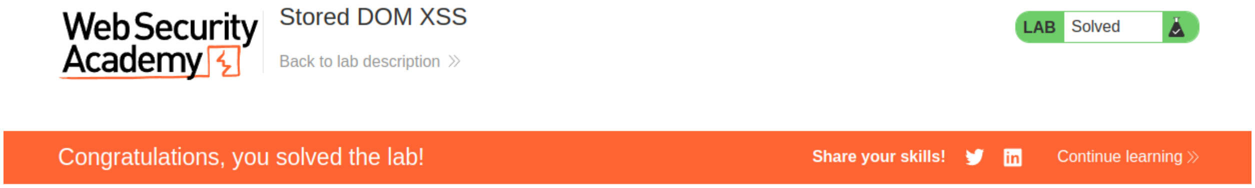


DOM XSS in `innerHTML` sink using source `location.search`

Congratulations, you solved the lab!

## 5. Stored DOM XSS:

Steps: Post comment with: <><img src=1 onerror=alert(1)>
Exploiting the vulnerability of replace() function by adding an extra pair of angular brackets.



Stored DOM XSS

Congratulations, you solved the lab!