**REPORT-TASK3**

Domain: http://testasp.vulnweb.com/

Linux 7.1, Wifi

Title: Cross Site Scripting Found

Description : When i entered a payload in the search post option on your site i got alert meassage proving the site is vulnerable to cross site scripting.

Payload used: <script src=1 href=1 onerror="javascript:alert(1)"></script>

Steps to reproduce:

1) I visited http://testasp.vulnweb.com/

2) Then i clicked on search and in search post field i searched for the payload.

3)I received alert message 1.

Impact:

This can have a severe impact on the website.

With user interaction, an attacker could execute arbitrary Javascript code in a victim's browser.

This would allow an attacker to unwillingly make a victim:

Perform any action in the identified endpoint

View any information that the user is able to view

Modify any information that the user is able to modify (not sure if applicable in this case)

Interact with other application users as if it were him - impersonation (not sure if applicable in this case)

Mitigation:

You can remove coding present in input to avoid this attack.

POC:

Below I have attached the screenshots of the code and alert message for your reference.



