Title: Cross site scripting

Domain: Vulnweb.com

Subdomain: testasp.vulnweb.com

Step to reproduce:

Step 1) Visit <http://testasp.vulnweb.com/>

Step 2) On the top menu you will find a search option.

Step 3) Click on it and you will be prompted with the search box.

Step 4) Code <img src=x onerror="alert(1)"> . You can intercept the request in Burp suite

Step 5) Now you can find different payloads for XSS.

Step 6) Send the request to intruder and paste all the payloads.

Step 7: Try to find a successful payload for XSS.

Step 8: Prepare a report for it.

Impact: Cross site scripting can lead to stealing of your user data and it can be harmful for your website.

Mitigation: If you want to prevent your website to be vulnerable of cross site scripting then you can just enable noscript on browser.

POC including screenshort is included in the report which is attached below

