Title: XSS Vulnerability in your website

Domain: Vulweb.com

Subdomain: <http://testasp.vulnweb.com/>

Summary:

<http://testasp.vulnweb.com/> has an endpoint that is vulnerable to an injection vulnerability - namely a reflected injection of JavaScript, also known as Cross Site Scripting (XSS). As per OWASP's definition: "Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. "

Steps to reproduce:

To reproduce this, an attacker must:

1. Visit <http://testasp.vulnweb.com/>
2. On the top of the website, you will find a search option
3. Click on it and you will prompt with the search box
4. You can intercept the request in the burpsuite or in direct inject the Payload injection XSS in search box [<svg onload=alert(1)>].
5. Send the request to intruder and paste all the payloads.
6. When you will insert the payload in search box click on search button an popup will appear testasp.vulnweb.com says 1
7. It means website is vulnerable with XSS vulnerability

Proof of Concept:

Screenshots:

A screenshot of a computer

Description automatically generatedA computer screen shot of a white screen

Description automatically generatedA screenshot of a computer

Description automatically generated

Video:

<https://github.com/Mallickwasim2001/INternstuDioProject/blob/main/XSS%20vulnerability.mp4>

Impact:

Cross site scripting is very dangerous and can be lead to stealing data of your user and also can harmful your website/company

Mitigation:

If you want to prevent this Cross Site Scripting attack from any cracker so just do an simple jobs that just enable the noscript on browser