Vulnerability Scan Report

- Kaushik Walwadkar

Title	: Cros Site Scripting
Domain	: Vulnweb.com
Subdomain	: http://testasp.vulnweb.com/
Parameter Name	: tfSearch

Summary :

We detected cross-site scripting, which allows an attacker to execute a dynamic script (JavaScript, VBScript) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Steps 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: You can intercept the request in Burp Suite

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

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

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

Step 8: Prepare a report for it.

Impact :

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

1) Hijacking user's active session.

2) Mounting phishing attacks.

3) Intercepting data and performing man-in-the-middle attacks.

Remedy :

The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex, therefore it's strongly recommended to use an encoding library such as OWASP ESAPI and Microsoft Anti-cross-site scripting.

Proof Of Concepts :

POC including screenshots and screen recording is included in the report which is attacked below.

1. Vulnerability screenshots 1.png
2. Vulnerability screenshots 2.png
3. Vulnerability screenshots 3.png
4. Vulnerability screenshots 4.png
5. Vulnerability screenshots 5.png
6. Vulnerability screenshots 6.png
7. Vulnerability screenshots 7.png
8. Vulnerability screenshots 8.png
9. Video.mp4