# Vulnerability Scan Report

- Ketan Urkudkar

**Domain:** www.vulnweb.com
**Subdomain:** http://testasp.vulnweb.com
**Type of Attack:** Cross Site Scripting
**Parameter Name:** tfSearch

## ■ Summary:

In our test, we discovered cross-site scripting, which allows an attacker to run a dynamic script (JavaScript, VBScript) in the context of the application.

This opens the door to a variety of attacks, the most common of which involve hijacking the user's current session or altering the appearance of the page by changing the HTML on the fly in order to steal the user's credentials. This occurs when a user's input has been processed by the browser as HTML/JavaScript/VBScript. Cross-site scripting attacks the application's users rather than the server. Although this is a flaw, because it allows attackers to hijack other users' sessions, an attacker may target an administrator in order to obtain complete control of the application.

## ■ Here are the steps to reproduce the issue:

Step 1: Go to https://testasp.vulnweb.com/
Step 2: Click on the Search option on the top menu.
Step 3: The Search box will appear.
Step 4: Using Burp Suite, intercept the request.
Step 5: Once you find XSS payloads, you can send them to the intruder.
Step 6: Paste all the payloads into a response to the intruder.
Step 7: Identify the successful payload for XSS.
Step 8: Create a report on it.

## ■ Impact:

Cross-site scripting can be used to carry out a variety of attacks, including:

- Hijacking the active session of a user.
- Carrying out phishing assaults.
- Using data interception and man-in-the-middle attacks.

## ■ Remedy:

Because the browser sees the input as active HTML, JavaScript, or VBScript, the problem occurs. To circumvent this, output should be encoded based on the location and context of the output. If the output is going inside a JavaScript block within an HTML document, for example, the output must be encoded appropriately. Because encoding can become somewhat complicated, it's highly advised that you utilize an encoding library like OWASP ESAPI or Microsoft Anti-cross-site scripting.

## ■ Proof of Concept:

POC including screenshot/screen recording is included in the report which is attached below.

- ✓ Vulnerability Snapshot 1.png
- ✓ Vulnerability Snapshot 2.png
- ✓ Vulnerability Snapshot 3.png
- ✓ Vulnerability Snapshot 4.png
- ✓ Vulnerability Snapshot 5.png
- ✓ Vulnerability Snapshot 6.png
- ✓ Vulnerability Snapshot 7.png
- ✓ Vulnerability Snapshot 8.png
- ✓ Vulnerability Video.mp4