REPORT

Summary :

During testing on testasp.vulnweb.com, a Cross-Site Scripting (XSS) vulnerability was identified in an input field. When injecting the payload "<scrip</script>t><img src =q onerror=prompt(8)>" into the input box, the website reflects this input back to the user without proper sanitization or encoding.

Steps to Reproduce :

- Navigate to the Website:
  Open a web browser and go to the URL: testasp.vulnweb.com.

- Locate the Input Field:
  Identify an input field or form on the website where user input is reflected back tothe page without proper sanitization.

- Inject Payload:
  Enter the following payload into the identified input field:

  " <scrip</script>t><img src =q onerror=prompt(8)> "

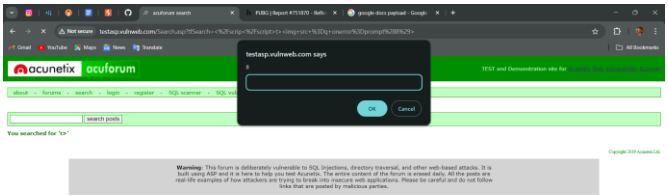
- Submit or Process the Input:
Submit or process the input field to trigger the server's response.

- Observe the Result:
After submitting the input, observe the webpage for any unexpected behavior or pop-up dialogs.

- Verification of XSS:
  If a pop-up dialog box appears displaying the number "8", it confirms the presence of a Cross-Site Scripting (XSS) vulnerability. This indicates that the injected JavaScript (prompt(8)) executed successfully in the context of the web page.

POC :

image :



Video :

Impact :

Client-Side Execution: Allows arbitrary JavaScript (prompt(8)) execution in users' browsers.

Malicious Actions: Potential for session hijacking, data theft, and content manipulation.

User Trust: Risks user trust and website reputation.

Legal Consequences: Non-compliance with data protection regulations.

Operational Impact: Requires urgent mitigation and security measures.