**Report**

**Steps to Reproduce:**

1. Navigate to: http://testasp.vulnweb.com/
2. Locate the **Search** option in the top menu.
3. Click on it to open the search input field.
4. Capture the request using **Burp Suite**.
5. Test the request with various **XSS payloads**.
6. Send the request to **Intruder** and inject multiple payloads.
7. Identify a payload that successfully triggers XSS.
8. Document the findings and prepare a detailed report.

**Impact:**  
Exploitation of this XSS vulnerability could allow an attacker to steal sensitive user data, compromise user sessions, and potentially damage the reputation of the affected website or company.

**Mitigation:**  
To prevent XSS vulnerabilities:

* Implement proper **input validation and output encoding**.
* Use **Content Security Policy (CSP)** to restrict script execution.
* Employ frameworks or libraries with built-in XSS protection.
* Avoid suggesting "NoScript" as the only solution—it’s not practical for end-users.

**Proof of Concept (POC):**  
Supporting evidence is included in the form of screenshots and a video:



 