**Title:** Cross site scripting.

**Domain:** Vulnweb.com .

**Sub-domain:** <http://testasp.vulnweb.com/>

**Steps to Reproduce:**

1)Visit http://testasp.vulnweb.com/.

2)On the top menu, locate the search option.

3) Click on the search box and input the following JavaScript payloads one by one:

4)Click on the search option to be prompted with a search box.

<script>alert(document.cookie)</script>

<script>prompt(8)</script>

>&#x000003c<script>alert(2)</script>

5)Observe the resulting behavior where the payloads trigger alerts and prompts in the browser, indicating successful execution of the scripts.

**Impact:**

Cross Site Scripting (XSS) vulnerabilities can have severe consequences, including:

Data Theft: Malicious scripts can steal user data, such as cookies, session tokens, and personal information.

User Impersonation: Attackers can hijack user sessions, leading to unauthorized actions on behalf of the user.

Phishing Attacks: XSS can be used to redirect users to malicious websites, potentially capturing sensitive information.

Loss of User Trust: Repeated XSS attacks can damage the reputation of a web application and reduce user trust.

**Mitigation:** Mitigating XSS requires a combination of strategies tailored to the web application. The following measures are recommended:

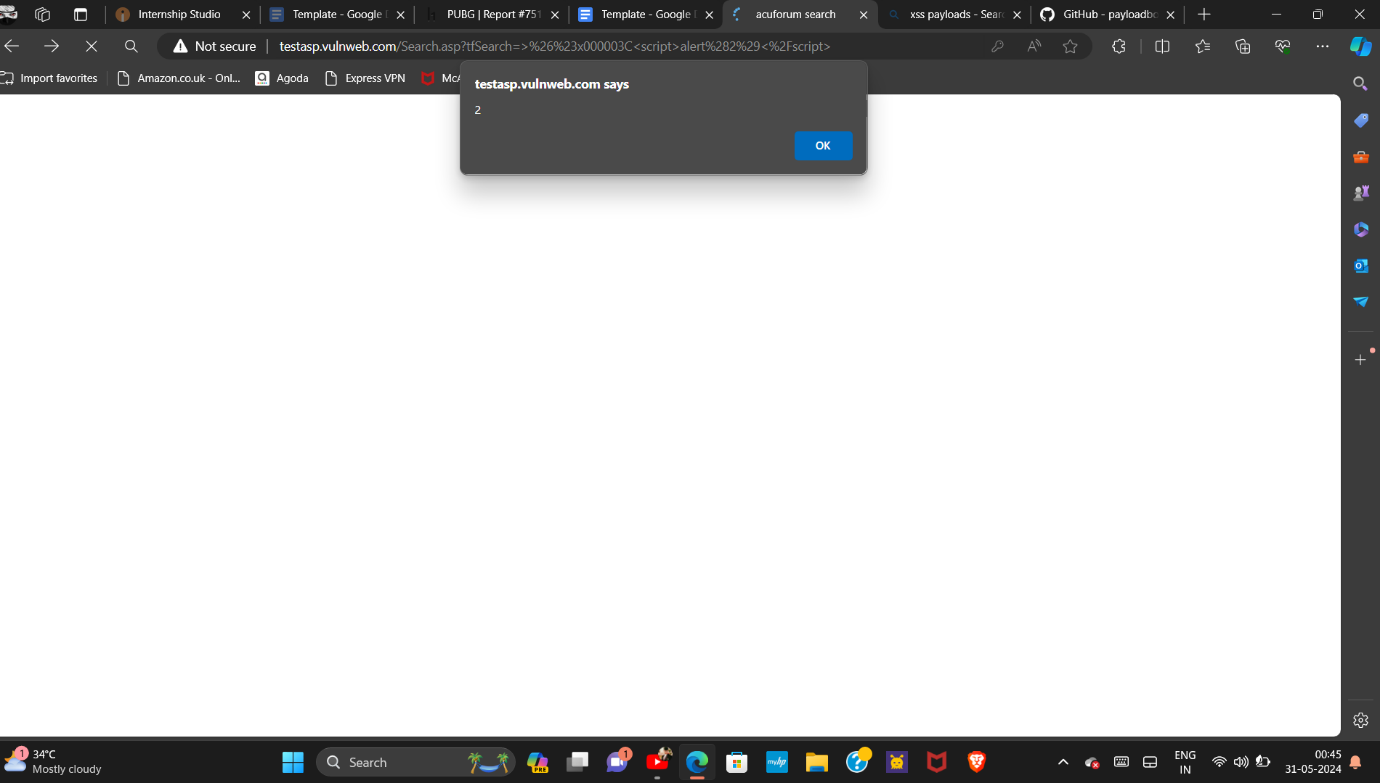
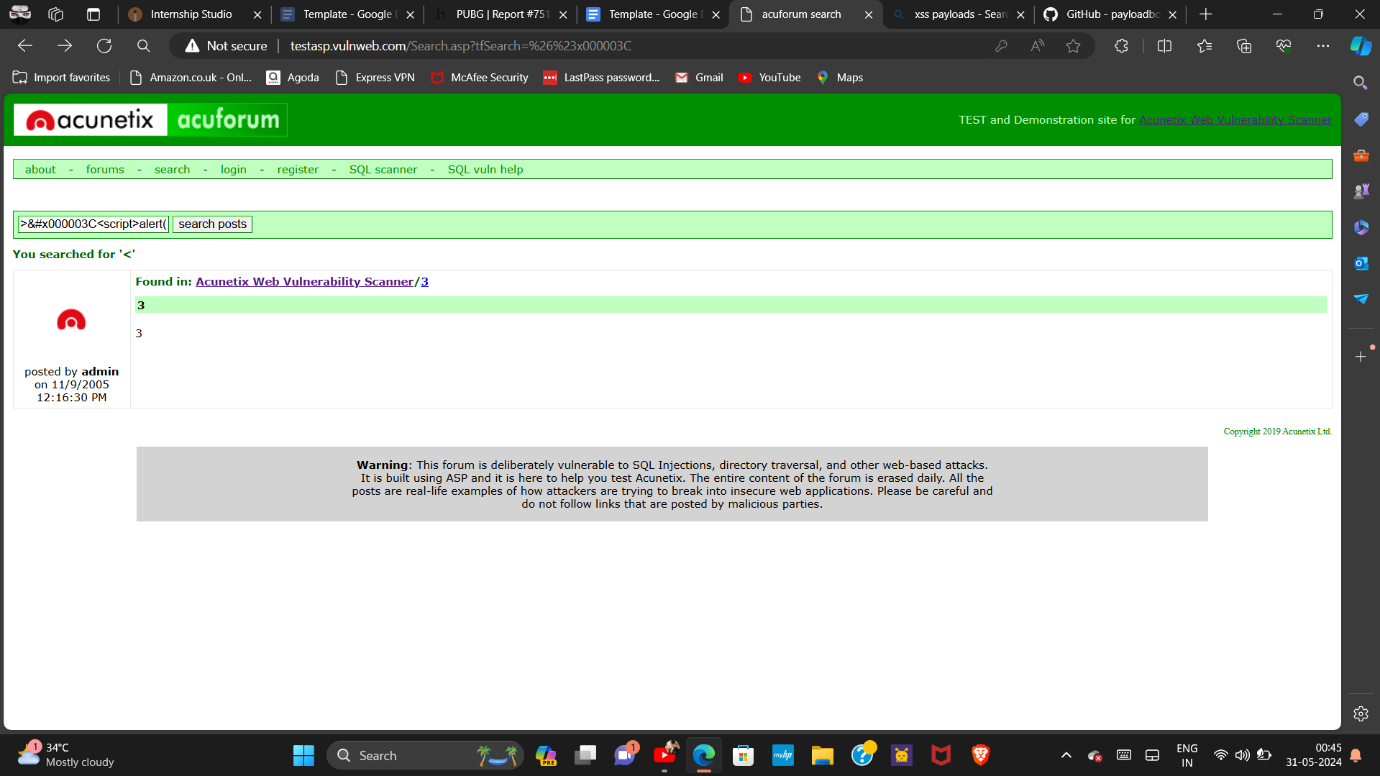
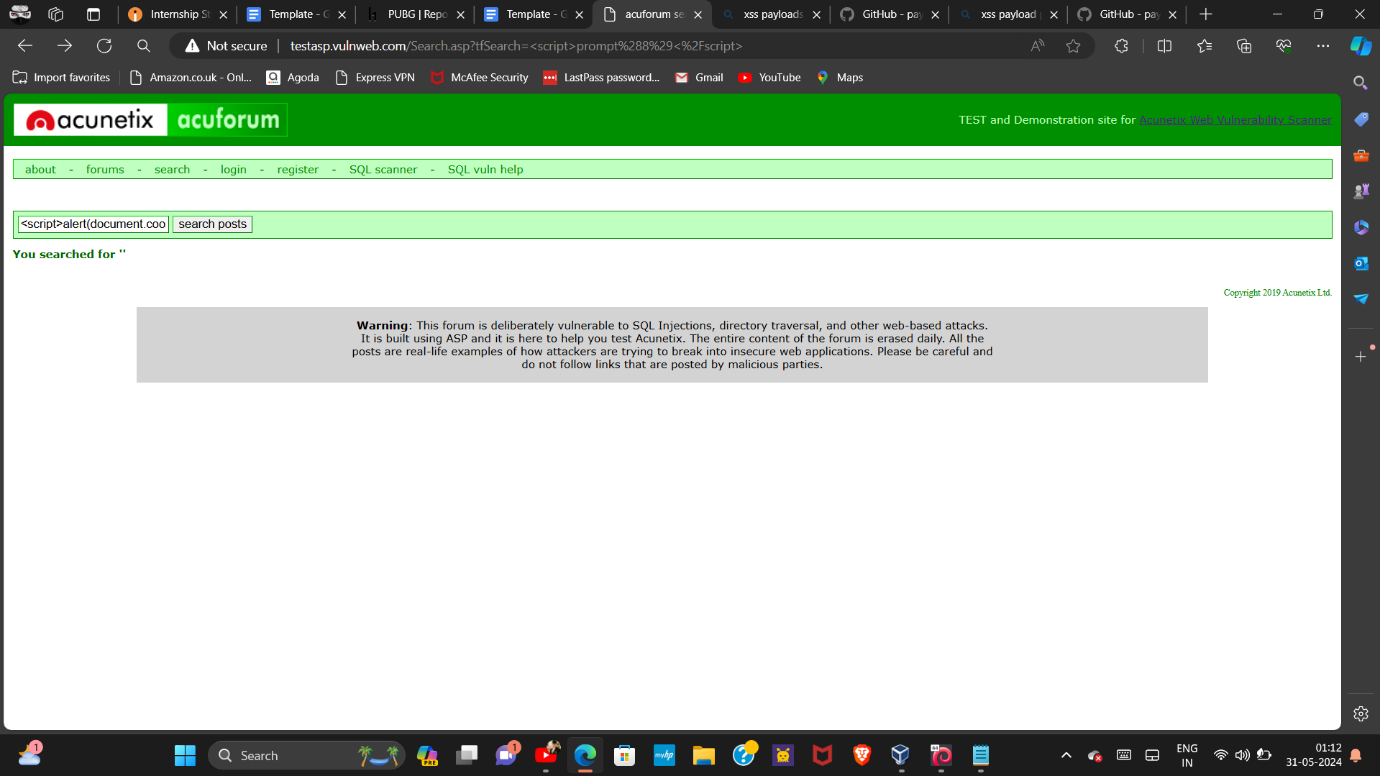
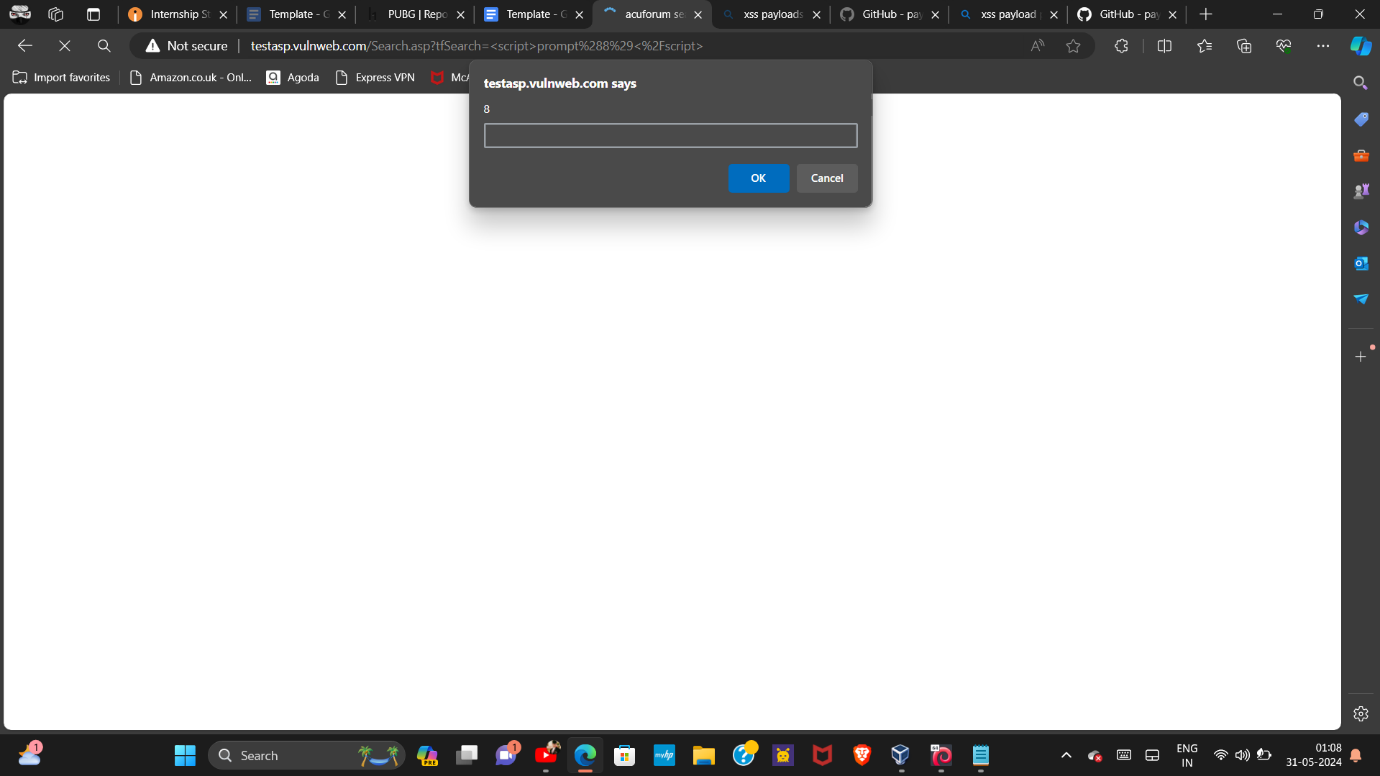
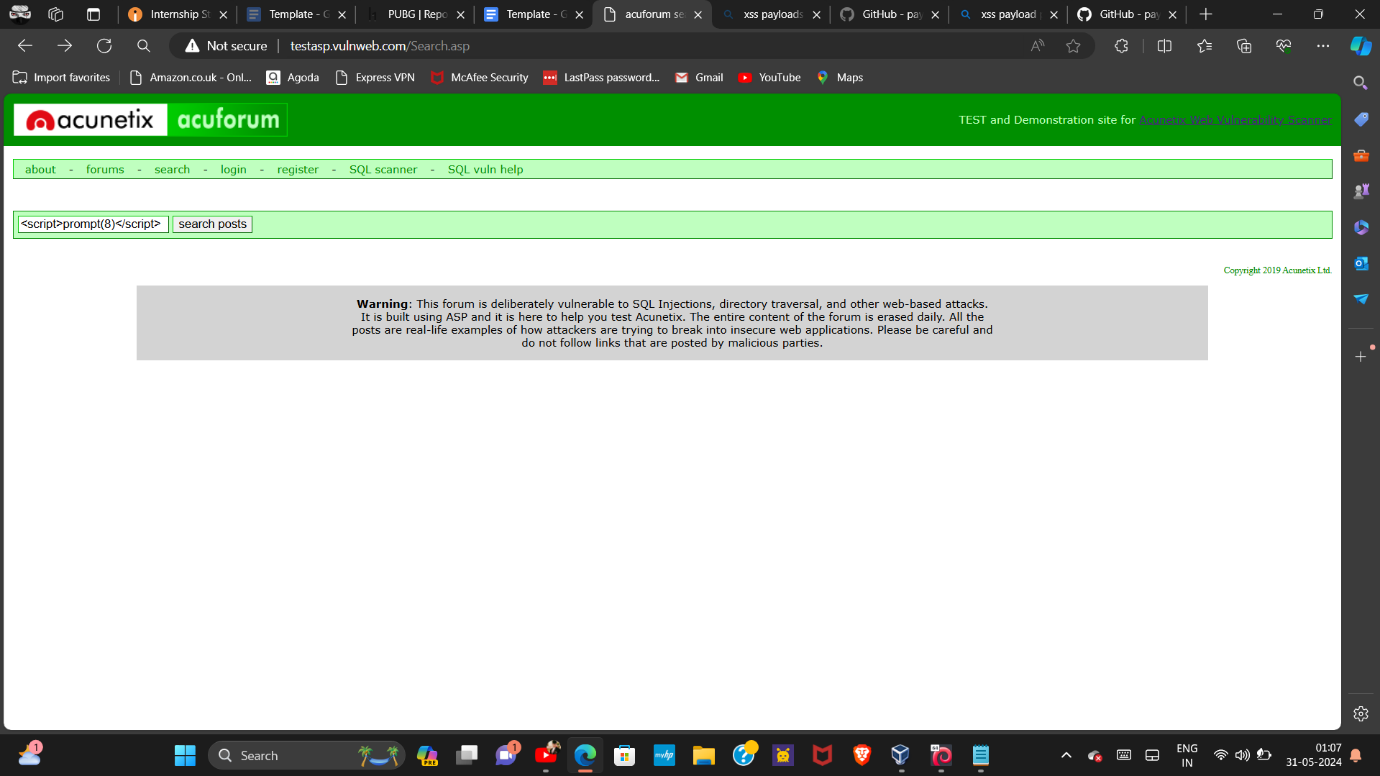
Validate Inputs: Implement strict validation to ensure form inputs meet specific criteria and reject any potentially harmful data.

Web Application Firewall (WAF): Deploy a WAF to detect and block abnormal server requests that may indicate an XSS attack. A WAF can also protect against other threats like SQL injection and DDoS attacks.

Prohibit HTML Code in Inputs: Prevent users from entering HTML code into form inputs to reduce the risk of XSS attacks.

Secure Your Cookies: Set secure attributes for cookies to prevent access through JavaScript. Use flags such as HttpOnly, Secure, and SameSite.

Sanitize Data: Sanitize all user inputs and outputs to remove or escape any harmful content. Utilize libraries like DOMPurify for sanitizing HTML.

**POC :**POC including screenshot and screen recording is included in report which is given below: 

By- Achisman Basu