Title: Cross-Site Scripting (XSS)

Domain: vulnweb.com

Sub-Domain: <http://testphp.vulnweb.com/>

Payload: <image src/onerror=promt(8)>

Severity: Medium

Summary:

The website sub-domain "http://testphp.vulnweb.com/" of the "vulnweb.com" domain is vulnerable to cross-site scripting (XSS) attacks. The XSS vulnerability is in the checkbox, allowing attackers to inject malicious JavaScript code. The proof-of-concept payload `<image src/onerror=prompt(8)>` successfully triggers a JavaScript message, confirming the vulnerability. Appropriate input validation and output encoding must be used to overcome this issue. This report provides steps to confirm the vulnerability and outlines actions to address the XSS vulnerability.

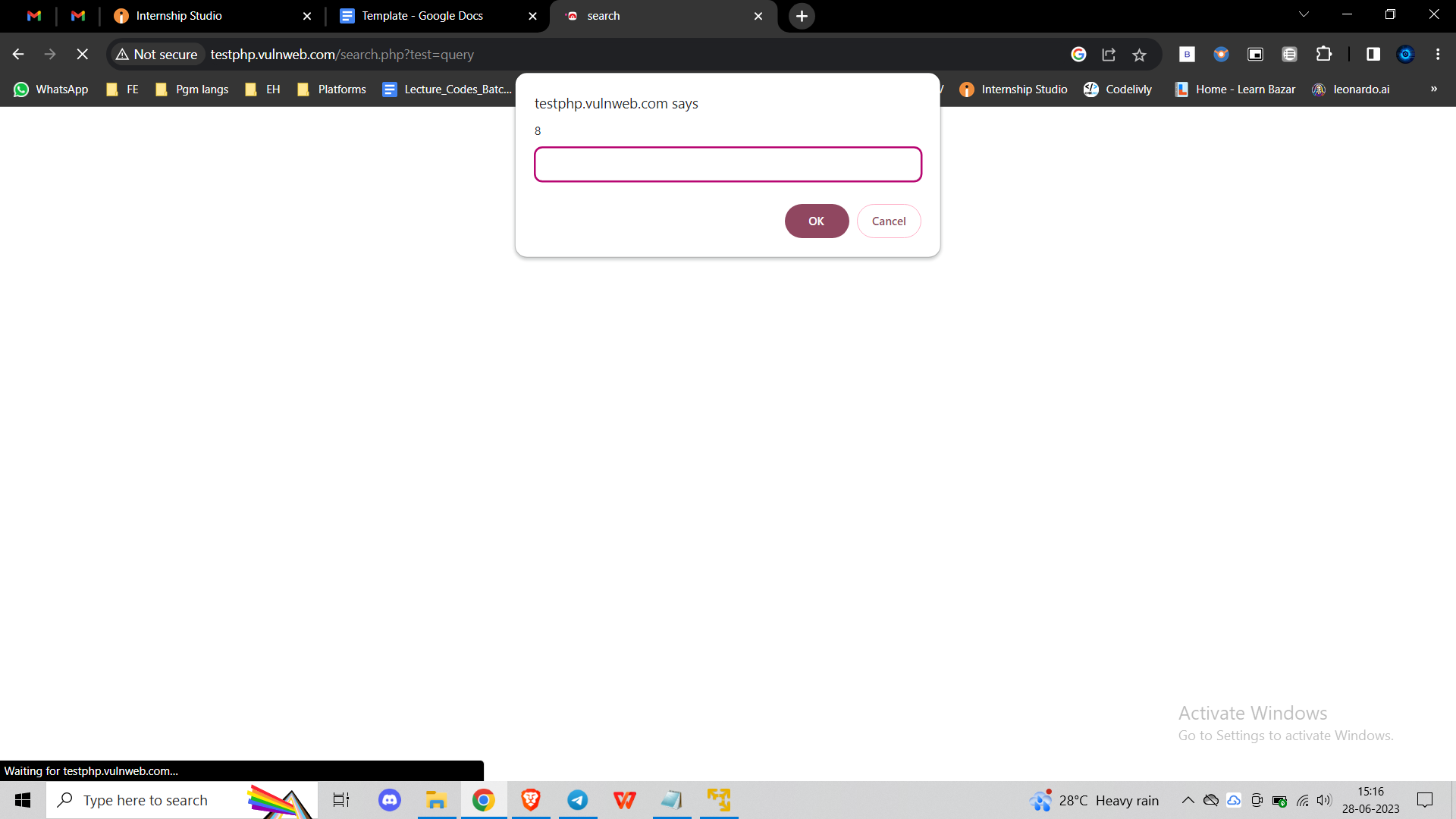
Steps in reproduction:

Step 1: See the sub-website: http://testphp.vulnweb.com/ .

Step 2: Look for the search box on the web page.

Step 3: Enter the following payload in the search box: <image src/onerror=prompt(8)>

Step 4: Submit the search query.



Step 5: Check out the answers on the website. When a JavaScript statement with the number 8 appears, it confirms that the Cross-Site Scripting (XSS) vulnerability in the checkbox has been successfully exploited.

Impact:

The check box on a web page is vulnerable to Cross-Site Scripting (XSS) attacks. This vulnerability allows an attacker to inject arbitrary JavaScript code into the site, potentially leading to session hijacking, phishing attacks, or unauthorized access to user data.

Recommendation:

Applying appropriate input validation and output encoding is suggested to mitigate this vulnerability. All user resources, including search queries, must be properly cleaned to prevent the execution of malicious scripts. Please let me know if you need any additional information or help to resolve this issue.