TASK - 3

Vulnerability- cross site scripting (XSS)

Severity-medium-low

high-0

medium-2

low-7

informational-1

Alert count by site and risk count: 10

Description- cross site scripting is atype of computer security vulnerability,

the attacker aims to execute malicious scripts in a web browser of the

victim by including malicious code in a legitimate web page of

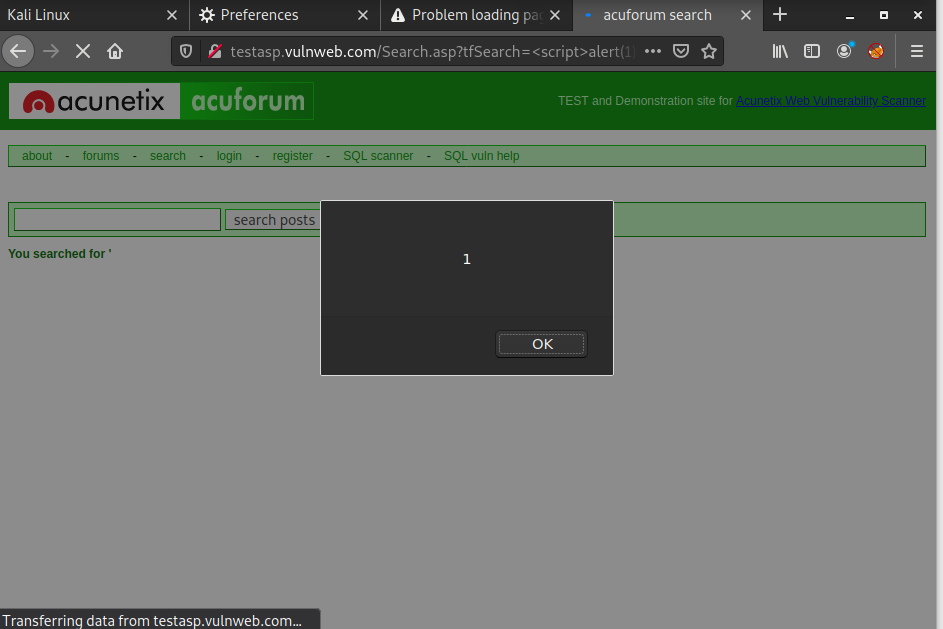
web application.

Instance:

Payload-

<script>alert(1);</script>

Proof of concept: screen shot of the browser page



Steps:

1. go to the website: http://testasp.vulnweb.com/

2. insert the payload in the search box.

<script>alert(1);</script>

3.wait for few seconds.

4.check the response

Impact:

open redirection: it arise when an application incorporates user-controllable data into the target of a redirection in an unsafe way.

session hijack: the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

phishing: its the practice of sending fraudulent communications that appear to come from a reputable source.

Cookie stealing: it occurs when a third party copies unencrypted session data and uses it to impersonate the real user.

Defacement: its the unauthorized modification of web pages, including the addition, removal, or alteration of existing content.

Mitigation: input valiadation:An input validation attack occurs when an attacker deliberately enters malicious input with the intention of confusing an application and causing it to carry out some unplanned action.

Encoding: Cross site scripting, or XSS, is a form of attack on a web application which involves executing code on a user's browser.

Reference: owasp