VULNERABILITY REPORT (BUG BOUNTY REPORT)

Vulnerability Name : Reflected XSS

Vulnerability Description : Reflected XSS attacks, also known as non-persistent attacks, occur when a malicious script is reflected off of a web application to the victim's browser. The script is activated through a link, which sends a request to a website with a vulnerability that enables execution of malicious scripts.

Vulnerable URL: http://testasp.vulnweb.com/search.php?test=query

Participants : Prathmesh Bharti

Reported on : 18/8/21

Reported to : internshipstudio.com

Payload : <script>alert(1)</script>

Steps of Reproduce :

1)http://testasp.vulnweb.com/search.php?test= open this url into the firefox

2)capture this request into the burpsuite.

3)send this request to the repeater.

4)put this payload after test = <Script>alert(1)</script>

5)right click and select show response in browser copy this into firefox and u will get the xss popup.

Impact : User can redirected into the malicious website and also can steal the cookie. An attacker can use reflected XSS vulnerabilities to inject content to pages served from http://testasp.vulnweb.com. This can be used e.g. for phishing purposes or to e.g. steal cookies from user's browser.

Mitigation : To keep yourself safe from XSS, you must sanitize your input. Your application code should never output data received as input directly to the browser without checking it for malicious code.

Supporting Material :