

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 :

The screenshot shows a web browser window with the address bar displaying a URL that includes a JavaScript payload: `<script>alert(1)</script>`. The page header identifies the site as 'acuforum' and 'TEST and Demonstration site for Acunetix Web Vulnerability Scanner'. A navigation bar contains links for 'about', 'forums', 'search', 'login', 'register', 'SQL scanner', and 'SQL vuln help'. Below this, a search bar contains the same JavaScript payload, and a 'search posts' button is visible. The search results section, titled 'You searched for "', displays two entries. Both entries show a post by 'admin' on 11/9/2005 at 12:16:25 PM. The first entry is titled 'Found in: Acunetix Web Vulnerability Scanner / 1' and the second is 'Found in: Weather / 1'. Both entries show a green bar with the number '1' and a small '1' below it. At the bottom of the page, a warning message states: 'Warning: This forum is deliberately vulnerable to SQL injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.' The footer indicates 'Copyright 2019 Acunetix Ltd.'