webTareas Tickets

A WebBased Collaboration OpenSource Tool
Brought to you by: luiswang

#41 Cross Site Script Vulnerability on "Search" in webtareas feature v2.1

Milestone: 2.0 **Status:** closed **Owner:** Luis. Wang **Labels:** Bugs? (2)
Updated: 2020-09-03 **Created:** 2020-06-24 **Creator:** r0ck3t **Private:** No

Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Search" feature.

To Reproduce
Steps to reproduce the behavior:

1. Login into the panel
2. Go to '/webtareas/general/search.php?searchtype=simple'
3. Click Search
4. Insert Payload:
5. Payload XSS: "><script>alert('hello')</script>
6. Payload HTML: <marquee>R0ck3t!</marquee>
7. XSS and HTML: "><script>alert('hello')</script><marquee>R0ck3t!</marquee>
8. XSS Alert Message

Expected behavior
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page.
Impact
Commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.
Desktop (please complete the following information):

OS: Windows
Browser: ALL

5 Attachments

Capture.PNG


Capture1.PNG


Capture2.PNG


alert_mess.PNG


alert_mess1.PNG

Discussion

Luis. Wang - *2020-06-24*

Luis, Wang - *2020-06-24*

patch released : webTareas v2.1 p1

r0ck3t - *2020-06-24*

Hi, Luiz, Wang
I'm using webTareas v2.1 p1.

Luis, Wang - *2020-09-03*

- **status**: open --> closed

Luis, Wang - *2020-09-03*

webTareas v2.1 p3 released

Log in to post a comment.