New issue

Jump to bottom

Cross Site Scripting Vulnerability on "Team" feature in Lavelite #321

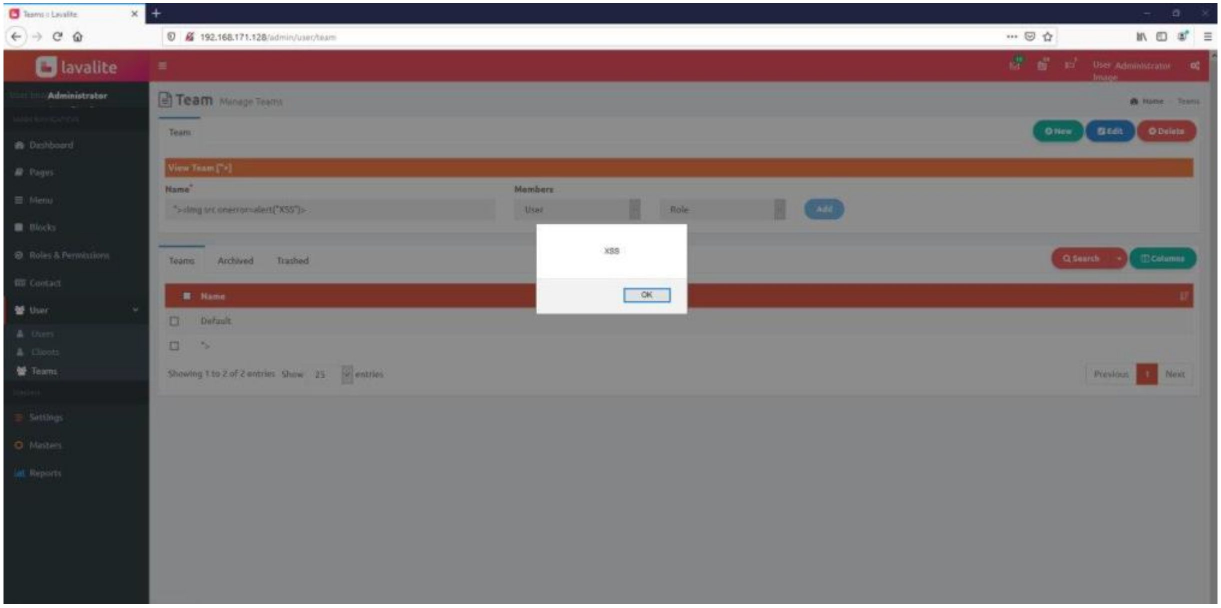
⊙ Open Songohan22 opened this issue on May 25, 2020 · 0 comments

Songohan22 commented on May 25, 2020 • edited

Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Teams" feature.
To Reproduce
Steps to reproduce the behavior:

1. Log into the panel.
2. Go to "/admin/user/team"
3. Click "New"
4. Insert payload:
   `"><img src onerror=alert(1)>`

<svg/on<script><script>load=alert(/XSS/)//</script>
// # "><svg/onload=prompt(1337)>
5. Click "Save "
6. View the preview to trigger XSS.
7. View the preview to get in request and such Stored XSS
Expected behavior
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is stored 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.
Screenshots



192.168.171.128/admin/user/team

Name*: "><img src onerror=alert("XSS")>

XSS

OK

Showing 1 to 2 of 2 entries Show 25 entries

Desktop (please complete the following information):

- OS: Windows
- Browser: Firefox
- Version: 76.0.1

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant