

New issue

[Jump to bottom](#)

Cross Site Scripting Vulnerability on "Menu Links" feature in LavaLite 5.8.0 #319

[Open](#) luuthehienhbit opened this issue on May 20, 2020 · 1 comment

luuthehienhbit commented on May 20, 2020 · edited

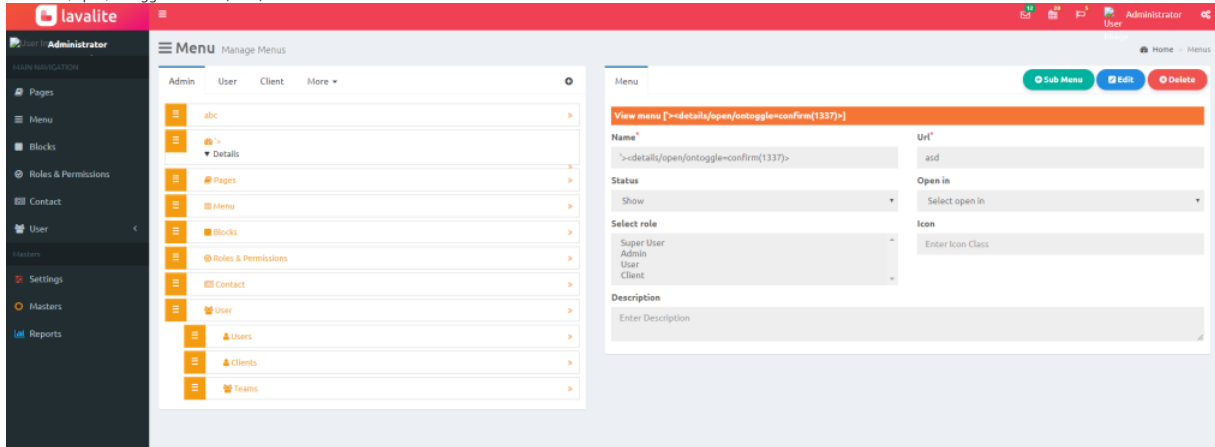
Describe the bug

An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Menu Links" feature. This can be bypassed by using HTML event handlers, such as "ontoggle".

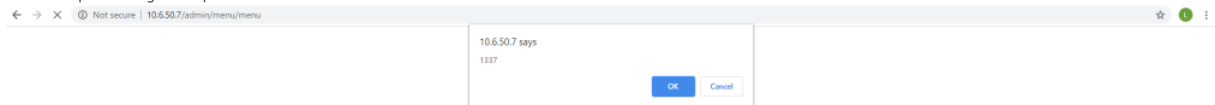
To Reproduce

Steps to reproduce the behavior:

1. Log into the /admin.
2. Go to "/admin/menu/menu"
3. Click "Admin/User/Client"
4. Select a function then press Edit
5. Insert payload to Name:
'> <details/open/ontoggle=confirm(1337)>



6. Click "Save"
7. View the preview to trigger XSS.
8. View the preview to get in request and such Stored XSS



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.

DEV696 commented on Oct 5, 2021

Did they resolved it ?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

