New issue

Jump to bottom

Cross Site Scripting Vulnerability on "Roles & Permissions" feature in Lavelite. #322

Open **Songohan22** opened this issue on May 25, 2020 · 6 comments

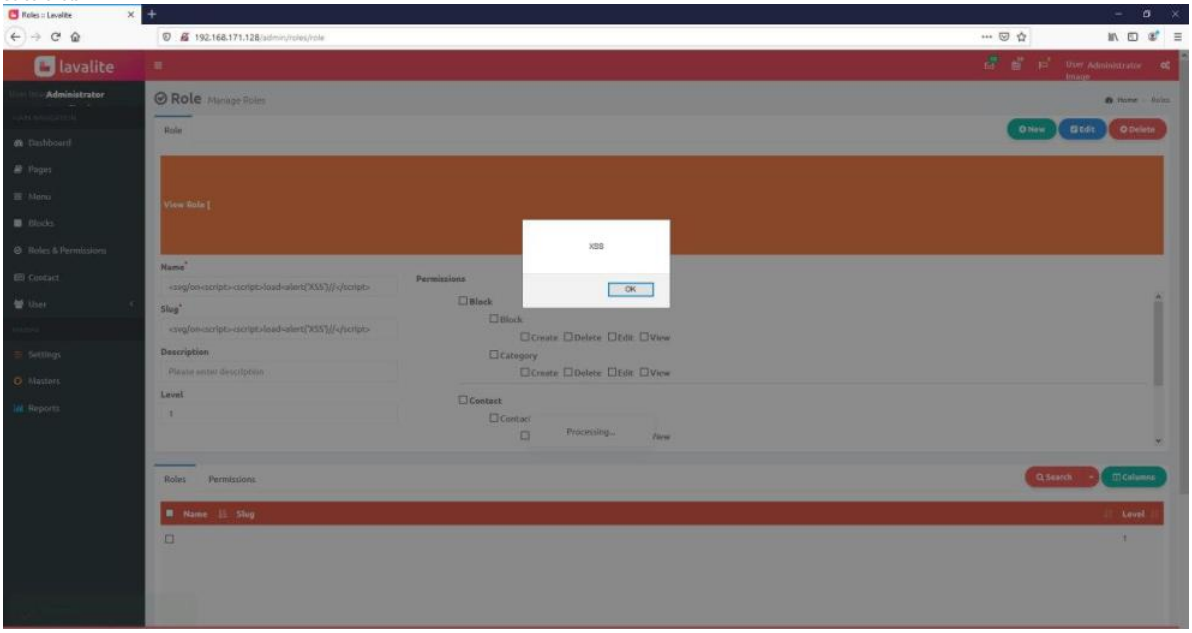
Songohan22 commented on May 25, 2020 • edited

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

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

   <svg/on<script><script>load=alert('XSS')//</script>
   // # "><svg/onload=prompt('XSS')>
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



Desktop (please complete the following information):

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

lavie3k commented on Jul 4, 2021

How to request CVE ID ?

Songohan22 commented on Jul 4, 2021 Author

@lavie3k

Submit https://cveform.mitre.org/

nivos888 commented on Jul 5, 2021

> **@lavie3k**
>
> Submit https://cveform.mitre.org/

CVE-2020-36396 was assign for it.

❤️ 1

lavie3k commented on Jul 5, 2021

How long did you have to wait for the vendor to respond? **@nivos888 @Songohan22**

Songohan22 commented on Jul 5, 2021 Author

Mine is 2 years :D

faisalfs10x commented on Feb 1

this issue is not even fix yet

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants