New issue

Jump to bottom

Cross Site Script Vulnerability on "Pages" in Codoforum feature V.5.0.2 #3

Closed r0ck3t1973 opened this issue on Sep 14, 2020 · 1 comment

r0ck3t1973 commented on Sep 14, 2020 Owner

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

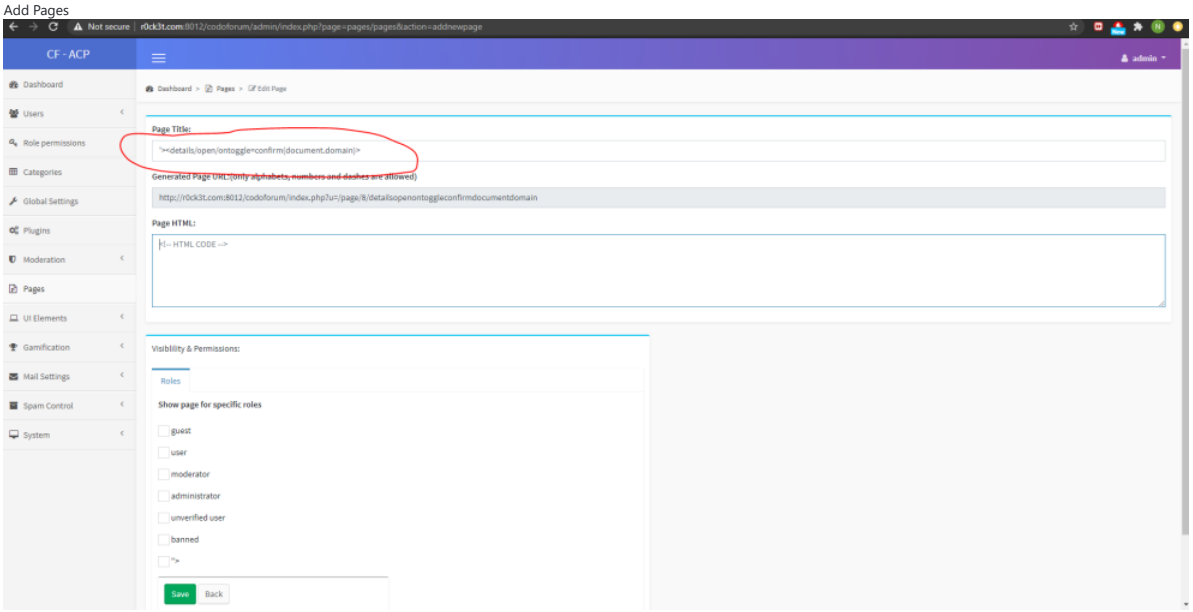
To Reproduce
Steps to reproduce the behavior:

1. Login into the Admin panel
2. Go to 'codoforum/admin/index.php?page=pages/pages'
3. Click Add Page
4. Insert Payload in 'Page Title':
   '><details/open/ontoggle=confirm(document.domain)>
5. Click Save
6. Go to Page 'codoforum/admin/index.php?page=pages/pages'
7. XSS Alert Message

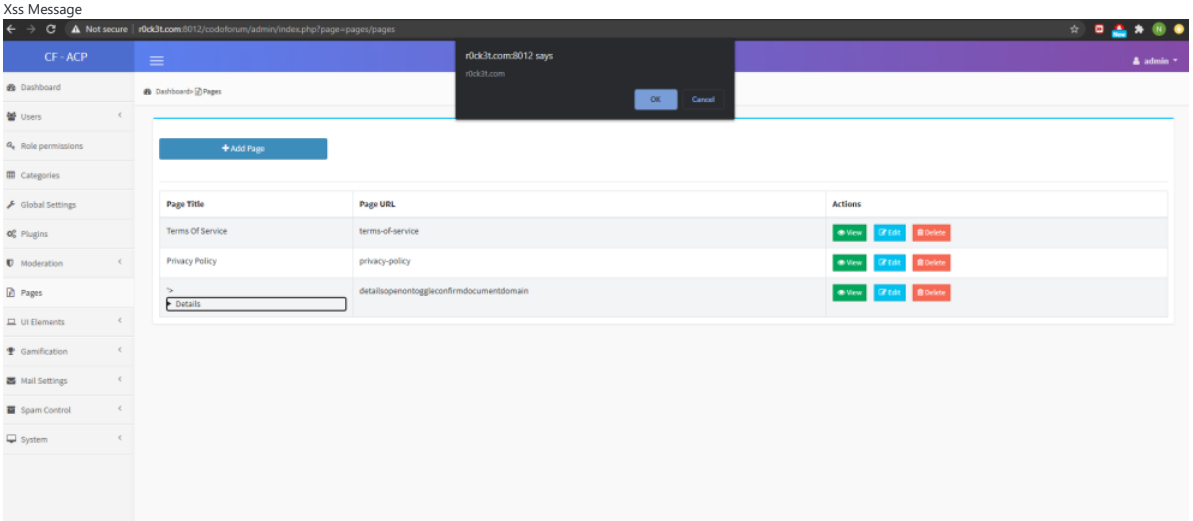
Expected behavior
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page

Screenshots

1. Add Pages



2. Xss Message



Desktop (please complete the following information):

OS: Windows
Browser: All
Version

r0ck3t1973 commented on Jul 10, 2021 Owner Author

CVE-2020-25876

r0ck3t1973 closed this as completed on Jul 10, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant