

[New issue](#)
[Jump to bottom](#)

## Cross Site Script Vulnerability on "content" in moziloCMS Admin 2.0 ("Amalia") #28

🔒 Closed

r0ck3t1973 opened this issue on Sep 8, 2020 · 1 comment

r0ck3t1973 commented on Sep 8, 2020

### Describe the bug

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

### To Reproduce

Steps to reproduce the behavior:

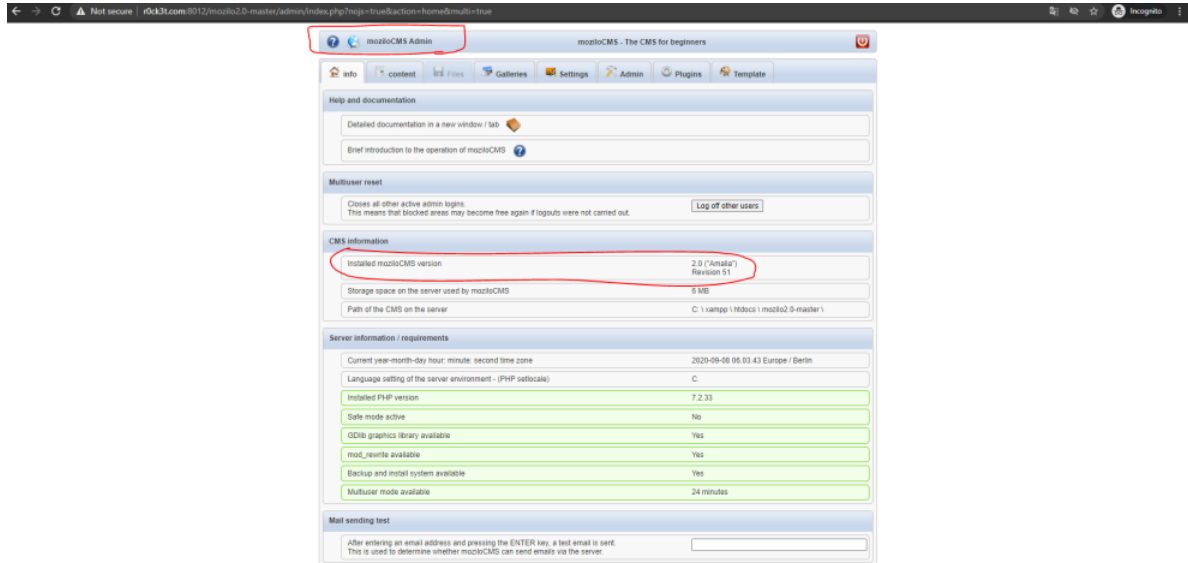
1. Login into the panel
2. Go to "mozilo2.0-master/admin/index.php?nojs=true&action=catpage&multi=true"
3. Click Edit "Content"
4. Insert Payload:  
'> <details/ open/ontoggle=confirm (document.domain)>
5. Save
6. Click Edit
7. XSS Alert Message

### Expected behavior

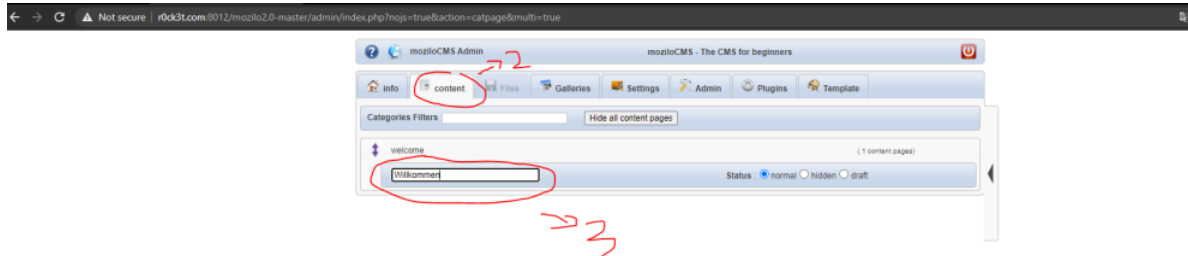
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page.

### Screenshots

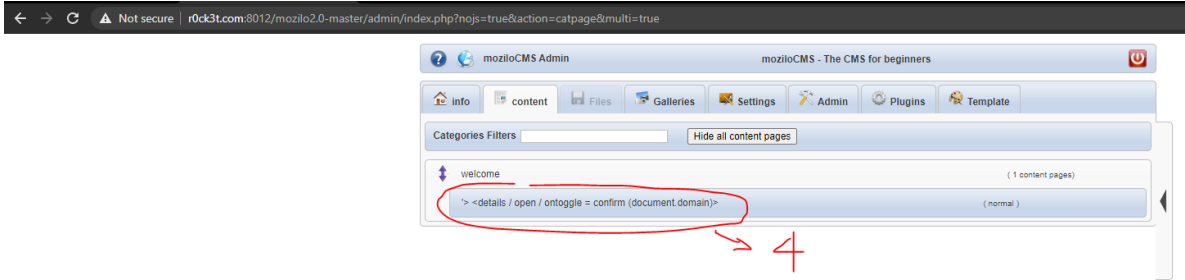
1. Infor moziloCMS Admin:



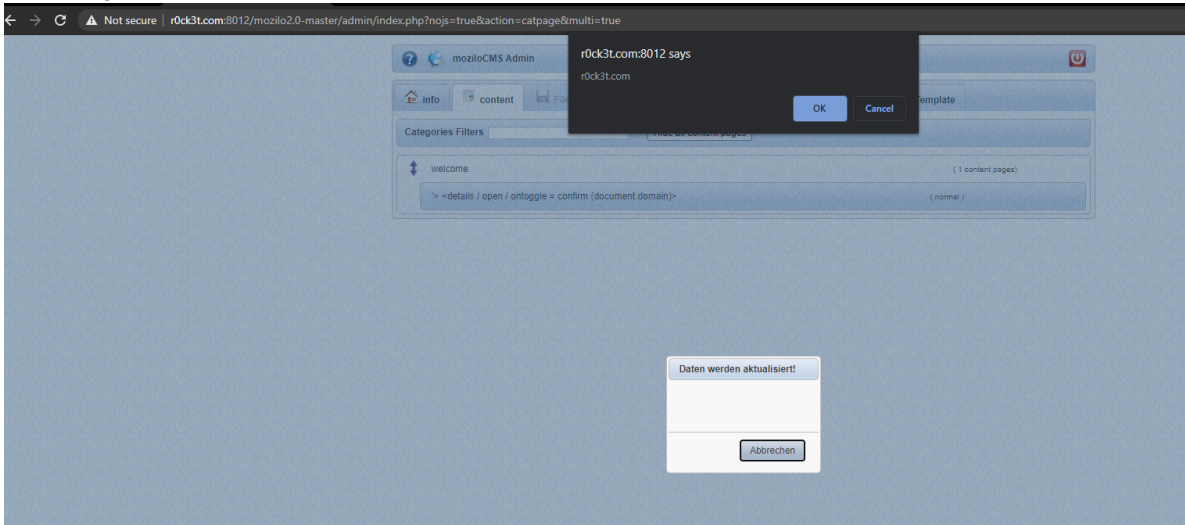
2. Go to "Content" and Edit:



### 3. Insert Payload XSS:



### 4. XSS Alert Message:



Desktop (please complete the following information):


OS: Windows  
Browser Chrome  
Version 85.0.4183.83 (Official Build) (64-bit)

 **r0ck3t1973** changed the title ~~Cross Site Script Vulnerability on "content" in moziloCMS Admin~~ Cross Site Script Vulnerability on "content" in moziloCMS Admin 2.0 ("Amalia") on Sep 8, 2020

**r0ck3t1973** commented on Jul 10, 2021

Author

[CVE-2020-25394](#)

 **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

