New issue

Jump to bottom

XSS vulnerability1 in jfinal_cms 5.1.0 #45

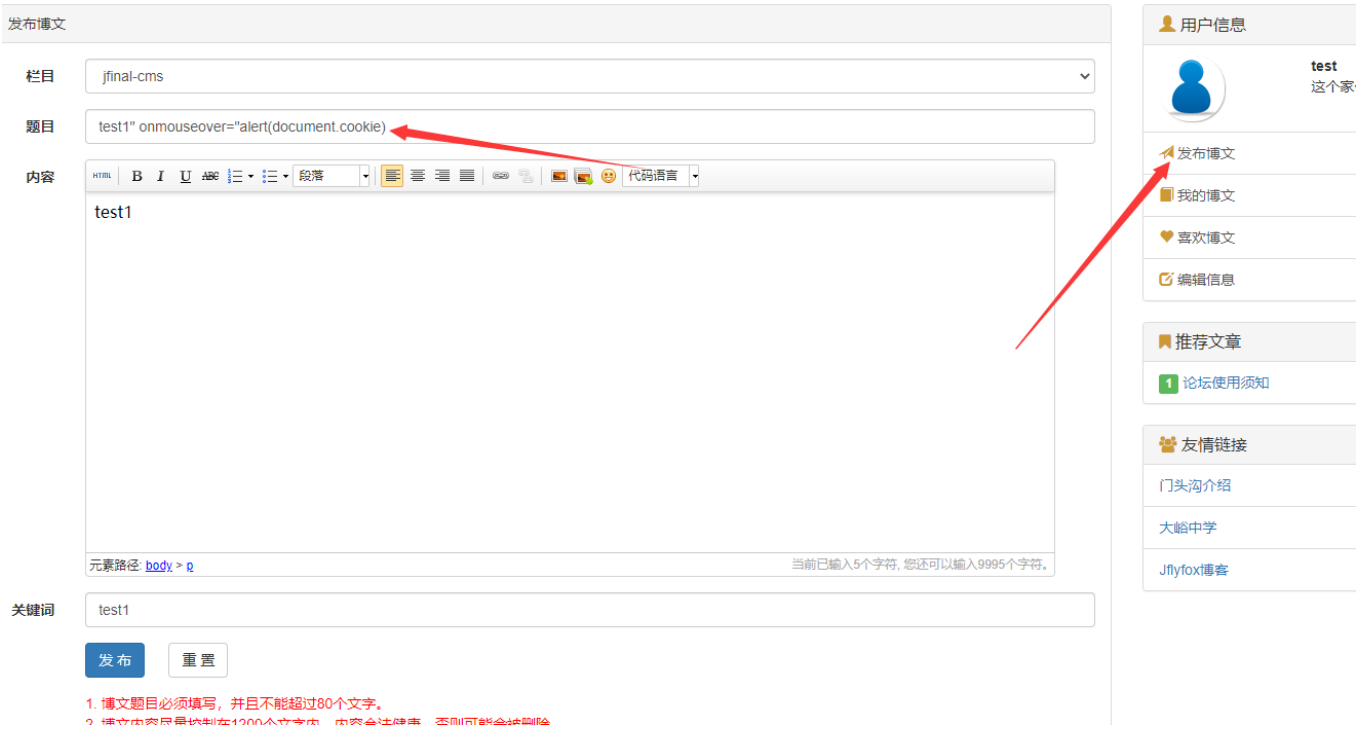
Open **Townmacro** opened this issue on Jul 18 · 0 comments

Townmacro commented on Jul 18

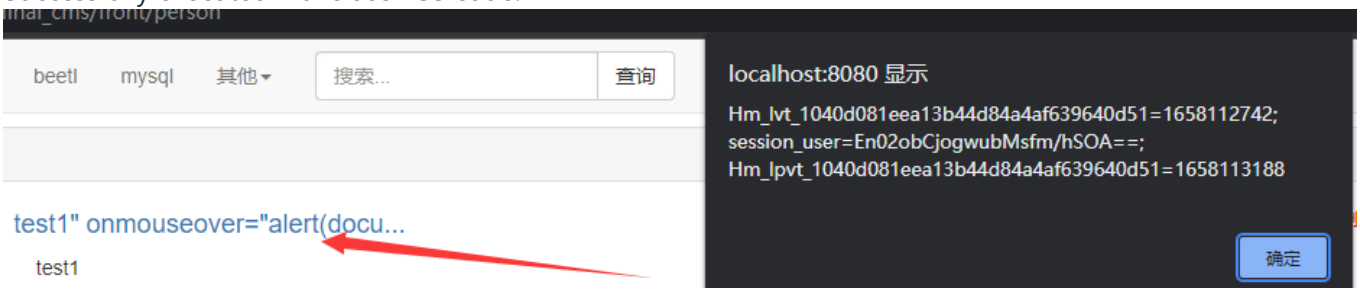
There is a stored XSS vulnerability in JFinal_cms 's publish blog module. An attacker could insert malicious XSS code into the post title. When users and administrators view the blog post, the malicious XSS code is triggered successfully.

First register a user to test it, then go to the submit blog post page and insert the malicious XSS code in the subject field

Payload： `test1" onmouseover="alert(document.cookie)`



Successfully executed malicious XSS code:



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant