New issue

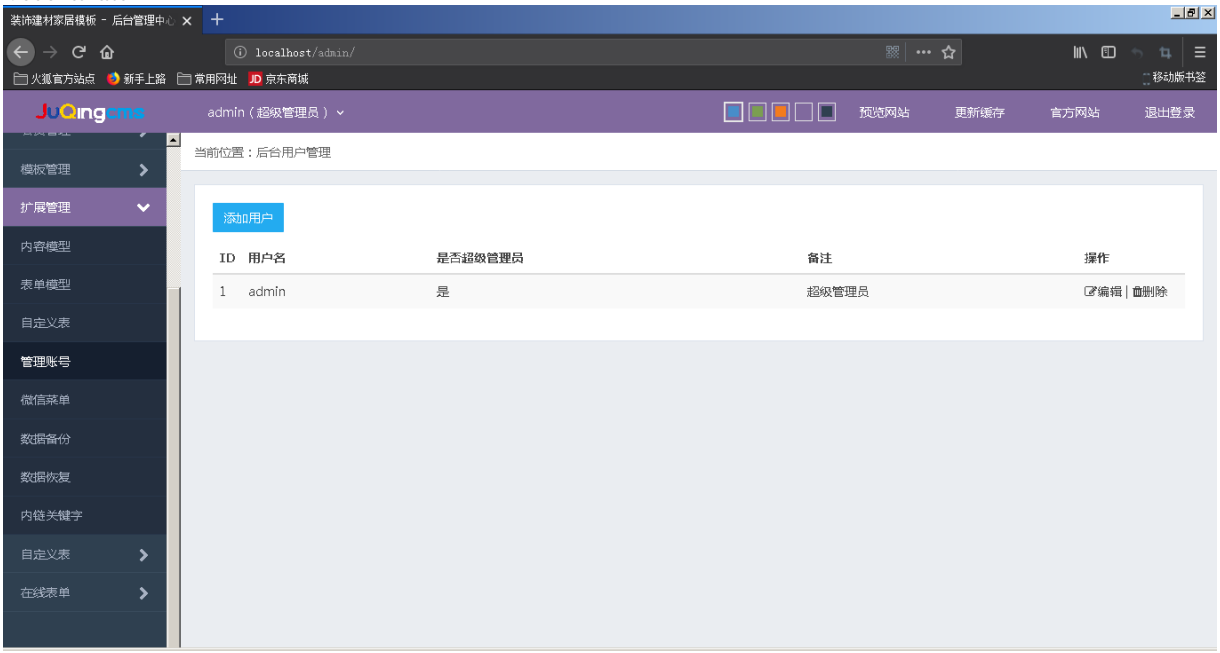
Jump to bottom

Bug: JuQingCMS V1.0 CSRF #1 #1

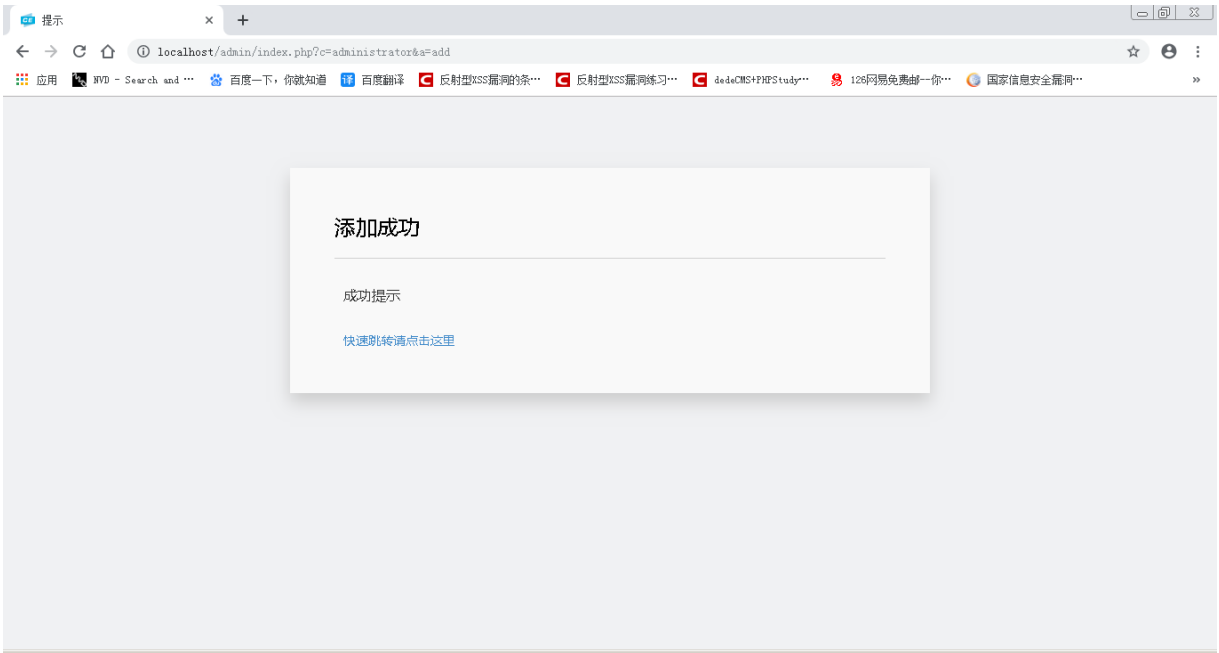
Open **GodEpic** opened this issue on Mar 14, 2019 · 0 comments

GodEpic commented on Mar 14, 2019 Owner

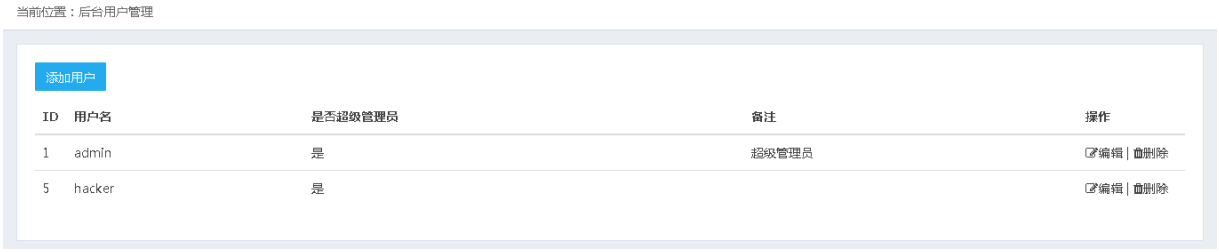
Hi, I would like to report CSRF vulnerability in JuQingCMS V1.0.
There is a CSRF vulnerability that can be added to modify administrator accounts.
POC:
1.Login to administrator panel.
2.Open below URL in browser which supports flash.
url:http://localhost/admin/index.php?c=administrator&a=add
http://localhost/admin/index.php?c=administrator&a=edit
eg:
1.Before modification



2.CSRF POC
csrf1.txt



3.After modification



fix:
Sensitive operations require validation codes, and changing passwords requires validation of old passwords.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant