Cross Site Scripting Vulnerability in Latest Release #675

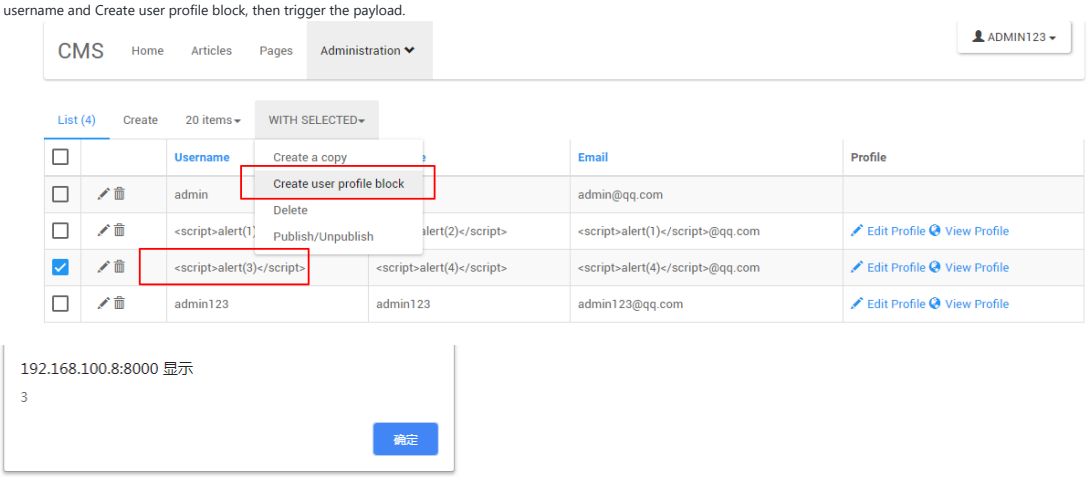
Open **HatBoy** opened this issue on Mar 21, 2019 · 1 comment

HatBoy commented on Mar 21, 2019

Hi, I would like to report Cross Site Scripting vulnerability in latest release.
Description:
Cross-site scripting (XSS) vulnerability inquokka/admin/actions.py 90, 151 line, Because there is no filter username.
The vulnerability code is:

```
flash(Markup( f'Profile block for {user["username"]} ' f'Created at: ' f'<a href="{newlink}">{new.inserted_id}</a>' ))
```

Steps To Reproduce:
1.Create a user, username is xss payload, like: <script>alert(3)</script>
2.Select the username and Create user profile block, then trigger the payload.



author by jin.dong@dbappsecurity.com.cn

3

marcosptf mentioned this issue on May 19, 2019

fixing XSS vulnerability #678

Open

marcosptf commented on Jun 7, 2019 Collaborator

this issue fixed on pr #678

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants