

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 in quokka/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.

The screenshot shows the CMS Administration page. At the top, there's a navigation bar with 'CMS', 'Home', 'Articles', 'Pages', and 'Administration'. A user 'ADMIN123' is logged in. Below the navigation bar, there's a 'List (4)' section with a 'Create' button and a '20 items' dropdown. A table lists users with columns: Username, Email, and Profile. The first row is 'admin' with email 'admin@qq.com'. The second row is '<script>alert(1)</script>' with email '<script>alert(1)</script>@qq.com'. The third row is '<script>alert(3)</script>' with email '<script>alert(4)</script>@qq.com'. The fourth row is 'admin123' with email 'admin123@qq.com'. A context menu is open over the third row, showing options: 'Create a copy', 'Create user profile block' (highlighted with a red box), 'Delete', and 'Publish/Unpublish'. The 'Create user profile block' option is also highlighted with a red box.

Username	Email	Profile
admin	admin@qq.com	
<script>alert(1)</script>	<script>alert(1)</script>@qq.com	Edit Profile View Profile
<script>alert(3)</script>	<script>alert(4)</script>@qq.com	Edit Profile View Profile
admin123	admin123@qq.com	Edit Profile View Profile

192.168.100.8:8000 显示

3

确定

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

