New issue

Jump to bottom

"Nickname" has a stored XSS vulnerability #52

Open xfiftyone opened this issue on Jul 6, 2021 · 2 comments

Labels bug

xfiftyone commented on Jul 6, 2021

Description

There is no escaping in the nickname field on the user list page，When viewing this page, the JavaScript code will be executed in the user's browser.

Impact Version

v1.03

Steps to Reproduce

1、Visit the profile page after logging in， `http://xxx/user`
2、Click on the nickname and insert the javascript code， `test<img/src=x onerror=alert(1)>`
3、Click save, the payload has been executed

The original request is as follows:

```
POST /admin/user/updateuser
name=Nickname&value=test%3Cimg%2Fsrc%3Dx+onerror%3Dalert(1)%3E&pk=300
```

3xxx commented on Jul 9, 2021 Owner

thank you,I will fix it.

3xxx commented on Jul 9, 2021 Owner

```
value := c.Input().Get("value")
value = template.HTMLEscapeString(value) //过滤xss攻击
err = m.UpdateUser(id, name, value)
```

3xxx added the bug label on Jul 10, 2021

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants