# A stored XSS vulnerability in the feedback function module of jfinal_cms V5.1.0 #32

Open **SomUrim** opened this issue on Mar 10 · 1 comment

**SomUrim** commented on Mar 10

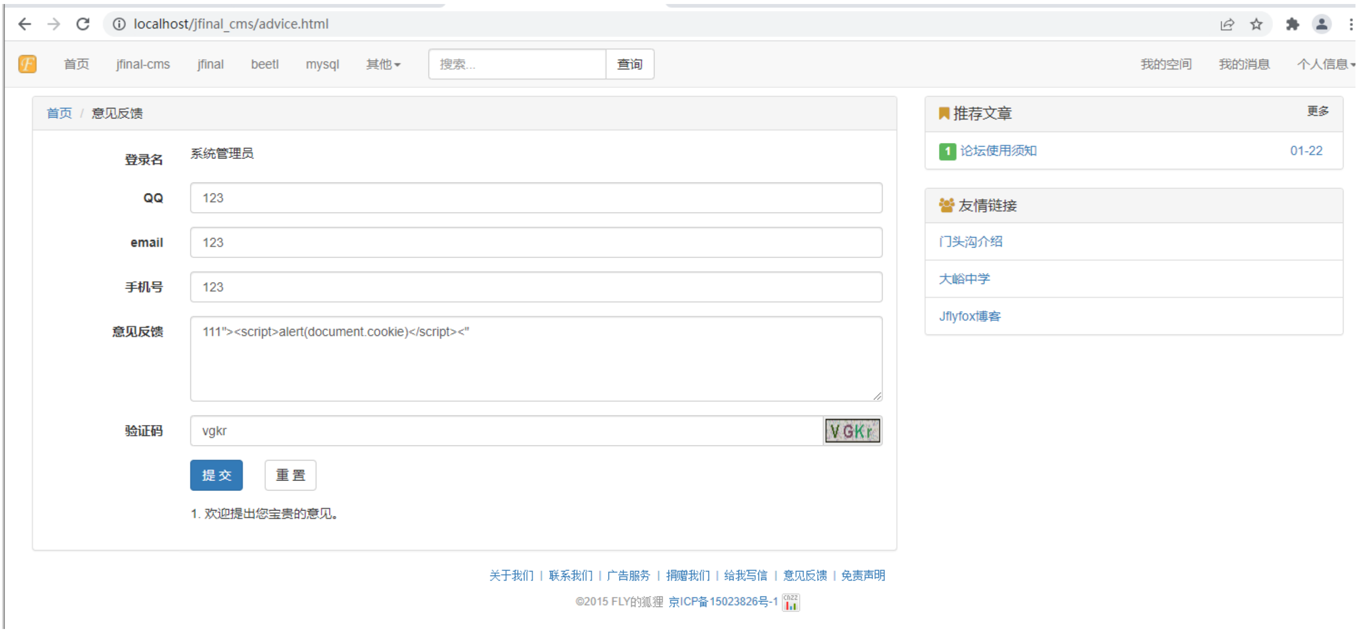
# There is a stored XSS vulnerability in the feedback function module of jfinal_cms V5.1.0

There is a stored XSS vulnerability in the feedback of jfinal_cms. An attacker can insert malicious XSS code into the feedback content. When the administrator views the feedback list in the background, the malicious XSS code is successfully triggered.

First register for a user test, then enter the feedback page, insert malicious XSS attack code in the feedback content:

Payload : **111"><script>alert(document.cookie)</script>**

Then, when the administrator views the feedback in the background, the malicious XSS code is successfully triggered, and there is no need to click on the corresponding feedback, it can be triggered only on the list page.



localhost/jfinal_cms/advice.html

首页 / 意见反馈

登录名 系统管理员

QQ 123

email 123

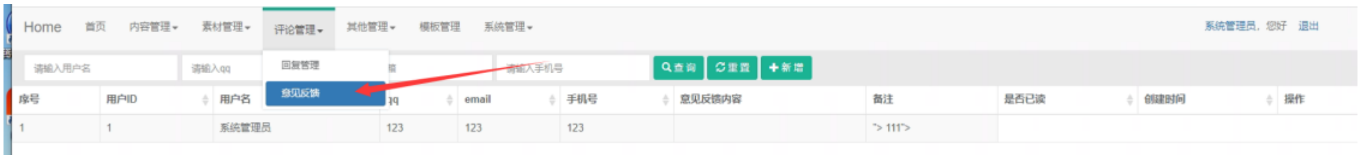
手机号 123

意见反馈 111"><script>alert(document.cookie)</script><"

验证码 vgkr

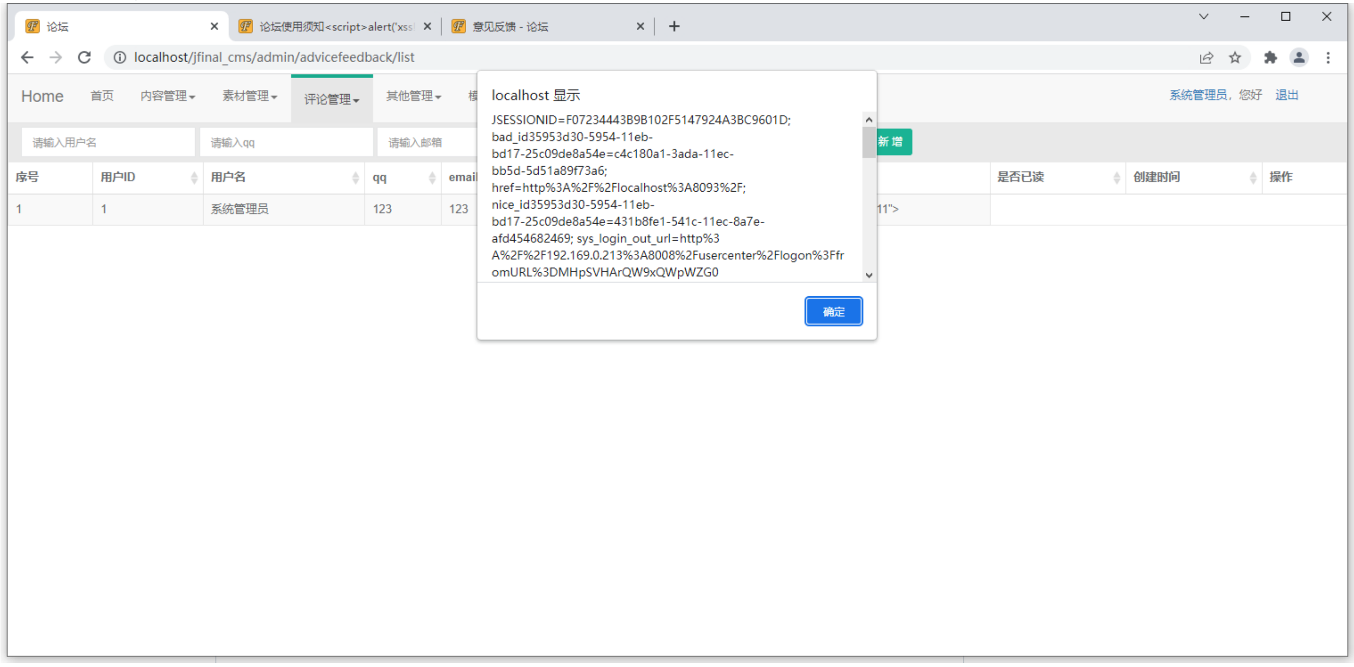
1. 欢迎提出您宝贵的意见。

Administrators view the feedback list:



| 序号 | 用户ID | 用户名 | qq | email | 手机号 | 意见反馈内容 | 备注 | 是否已读 | 创建时间 | 操作 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 系统管理员 | 123 | 123 | 123 |  | "> 111"> |  |  |  |

Successfully executed malicious XSS code:



localhost/jfinal_cms/admin/advicefeedback/list

localhost 显示

```
JSESSIONID=F07234443B9B102F5147924A3BC9601D;
bad_id35953d30-5954-11eb-
bd17-25c09de8a54e=c4c180a1-3ada-11ec-
bb5d-5d51a89f73a6;
href=http%3A%2F%2Flocalhost%3A8093%2F;
nice_id35953d30-5954-11eb-
bd17-25c09de8a54e=431b8fe1-541c-11ec-8a7e-
afd454682469; sys_login_out_url=http%3
A%2F%2F192.169.0.213%3A8008%2Fusercenter%2Flogon%3Ffr
omURL%3DMHpSVHArQW9xQWpWZG0
```

Safety advice:

- Strictly filter the user's input
- Strict control of page rendering content

**ElevenKong** commented on Mar 10

您好，您的来信我已收到！谢谢！
Best  Wishes!
——孔祥亮

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants