

New issue

[Jump to bottom](#)

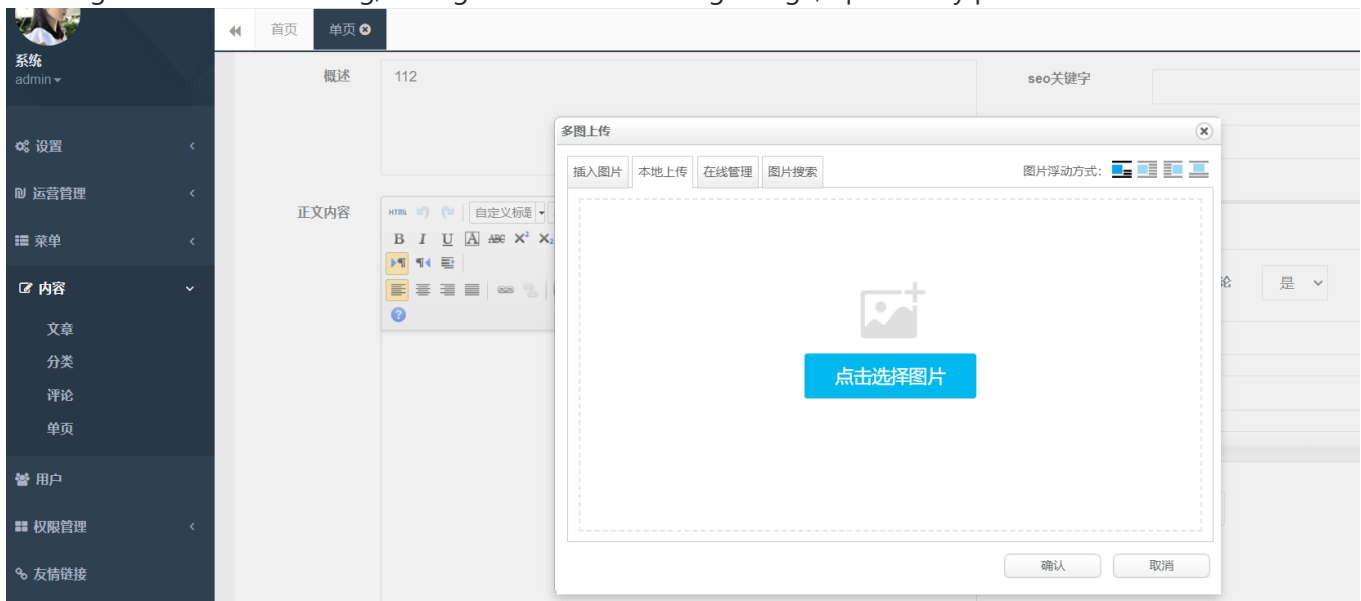
There are some XSS vulnerabilities in FeehiCMS-2.1.1 #3

Open Zzr7x opened this issue on Sep 7 · 0 comments

Zzr7x commented on Sep 7 • edited ▾

There is a stored XSS vulnerability in the background of FeehiCMS.

First register a user for testing, then go to Content -> Single Page, upload any picture in the comment box.

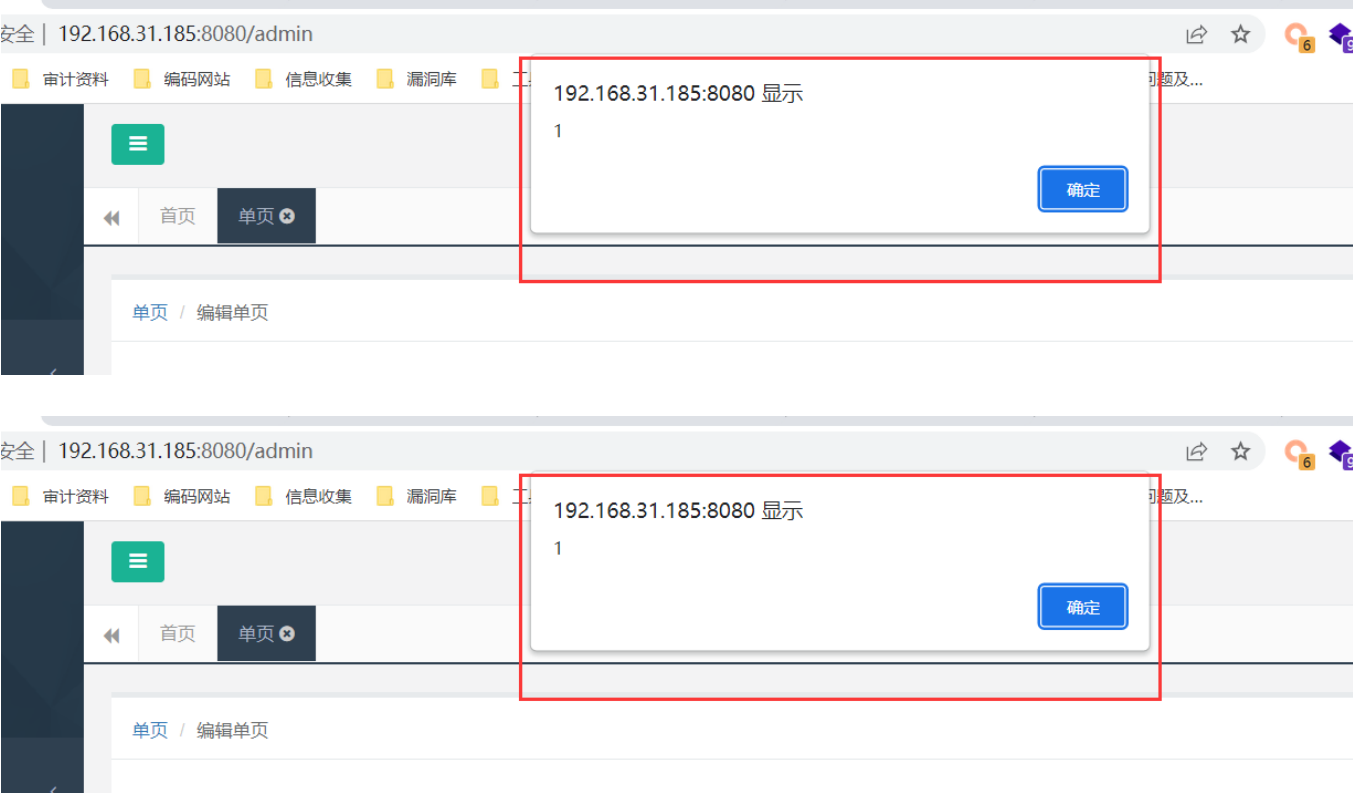



Then send a comment, capture the odd packet while sending the Forward, change the value of SRC under the tag in the packet to: 'x' [onerror='alert(1)', and send the message.

```
<p><img src='x' onerror='alert(1)' title='166254049415573380.jpg' alt='phpinfo.jpg' /></p>
-----WebKitFormBoundaryrJCE3vLoZsgjDXU7
Content-Disposition: form-data; name="Article[seo_title]"

-----WebKitFormBoundaryrJCE3vLoZsgjDXU7
Content-Disposition: form-data; name="Article[seo_keywords]"
```

Refresh the page, and pop-up windows will appear on the current page and the home page.



 **Zzr7x** changed the title **FeehiCMS-2.1.1中存在一些XSS漏洞** There are some XSS vulnerabilities in FeehiCMS-2.1.1 on Sep 7

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

