

New issue

[Jump to bottom](#)

There is a Stored-XSS vulnerability in Dswjcms 1.6.4 #5

[Open](#) Shuai opened this issue on May 14, 2019 · 0 comments

Shuai commented on May 14, 2019

A Stored-XSS vulnerability exists in Dswjcms 1.6.4, allowing an attacker to execute HTML or JavaScript code via the `index.php/Dswjcms/Site/articleList.html`

PoC:

```
<img src=x onerror=alert(/xss/)>
```

Add an article

文章名称: test1

文章所属栏目: 新闻中心

关键词:

描述: test1

显示模板: 默认模板

排序: 1

Execute JavaScript code

JavaScript代码:

执行

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

