New issue

Jump to bottom

NoneCMS V1.3.0 has a XSS vulnerability in admin/article/add.html #32

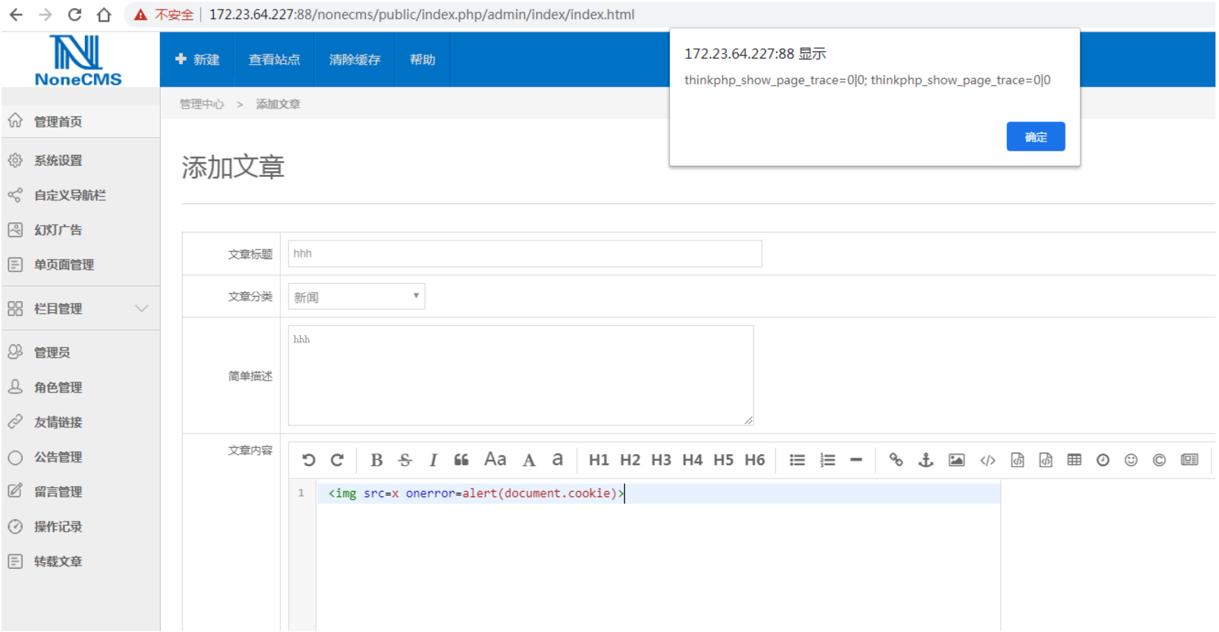
Open **ghost** opened this issue on Jun 2, 2020 · 0 comments

ghost commented on Jun 2, 2020 • edited by ghost

Cross-site scripting (XSS) vulnerability in admin/article/add.html in noneCMS v1.3.0 allows remote authenticated attackers to inject arbitrary web script or HTML via the name parameter.

By default, noneCMS uses Editor.md for users to edit their articles. However, Editor.md has a XSS vulnerability. A remote user who has the right to edit articles can inject arbitrary web script or HTML in admin/article/add.html.

PoC: `<img src=x onerror=alert(document.cookie)>`



不安全 | 172.23.64.227:88/nonecms/public/index.php/admin/index/index.html

172.23.64.227:88 显示

thinkphp_show_page_trace=0|0; thinkphp_show_page_trace=0|0

确定

添加文章

文章标题: hhh

文章分类: 新闻

简单描述: hhh

文章内容:

```
<img src=x onerror=alert(document.cookie)>
```

ghost changed the title ~~NoneCMS V1.3.0 has a XSS vulnerability~~ NoneCMS V1.3.0 has a XSS vulnerability in admin/article/add.html on Jun 2, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

0 participants