New issue

Jump to bottom

XSS exists in YzmCMS V5.6 #46

Closed ghost opened this issue on May 22, 2020 · 1 comment

ghost commented on May 22, 2020 • edited by ghost

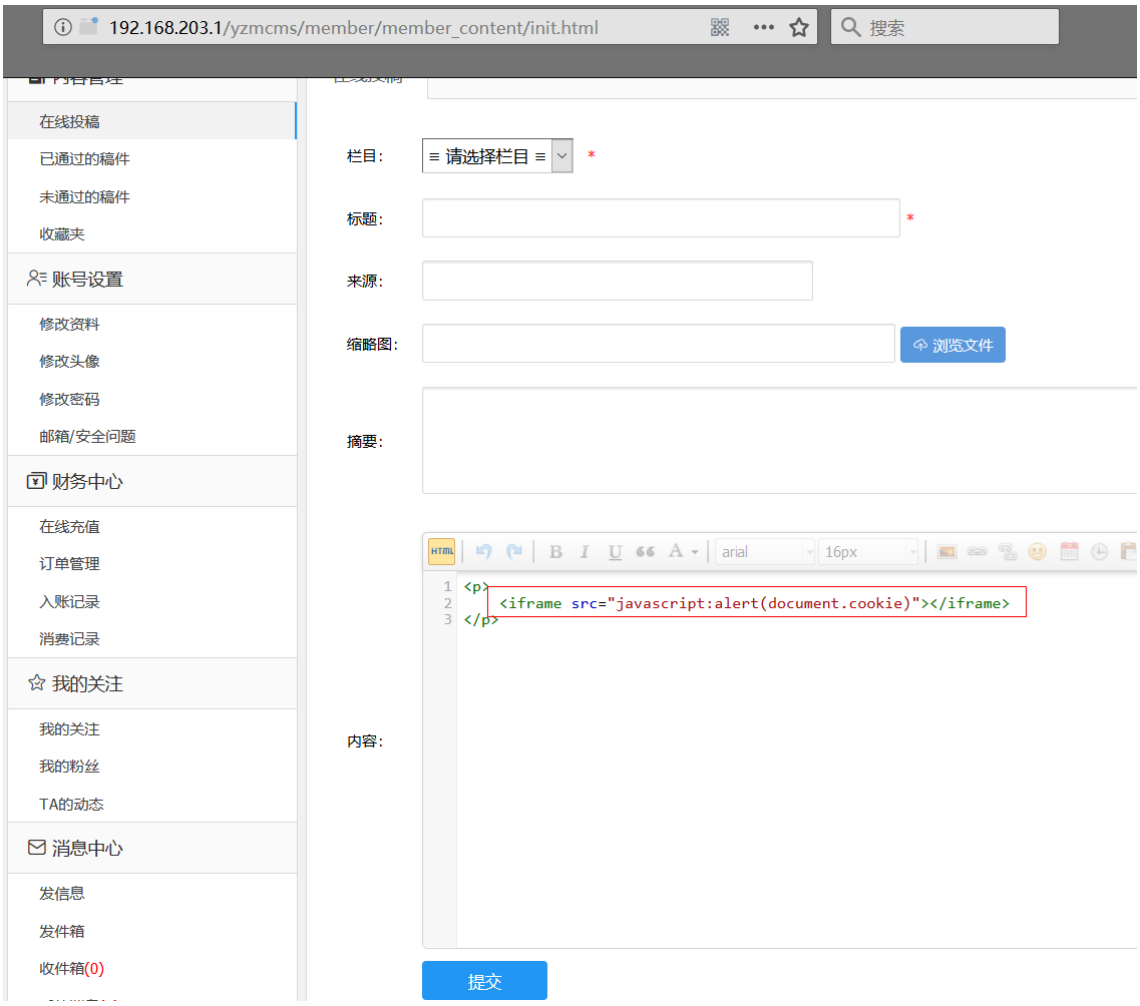
Description

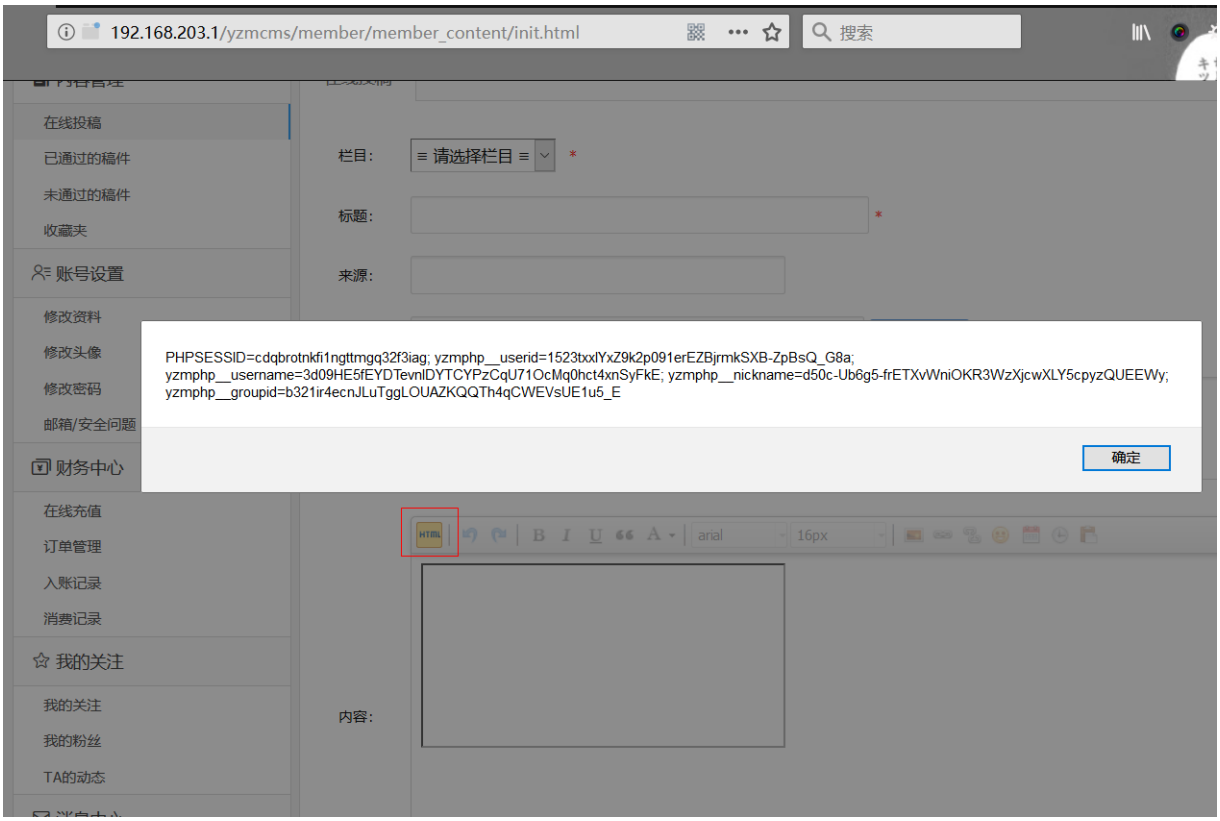
In YzmCMS 5.6, XSS in edit article page via the SRC attribute of an IFRAME element because of using UEditor 1.4.3.3.

PoC

```
<iframe src="javascript:alert(document.cookie)"></iframe>
```

Script tags are filtered, but iframe tags are not:





Refer to: http://www.51testing.com/html/17/n-3721417.html

ghost changed the title ~~XSS exists in YzmCMS 5.6~~ XSS exists in YzmCMS V5.6 on May 22, 2020

yzmcms commented on May 22, 2020 Owner

谢谢你的反馈，下一个版本修复。

yzmcms closed this as completed on May 22, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant