

New issue

[Jump to bottom](#)

XSS exists in the information,can get cookie #69

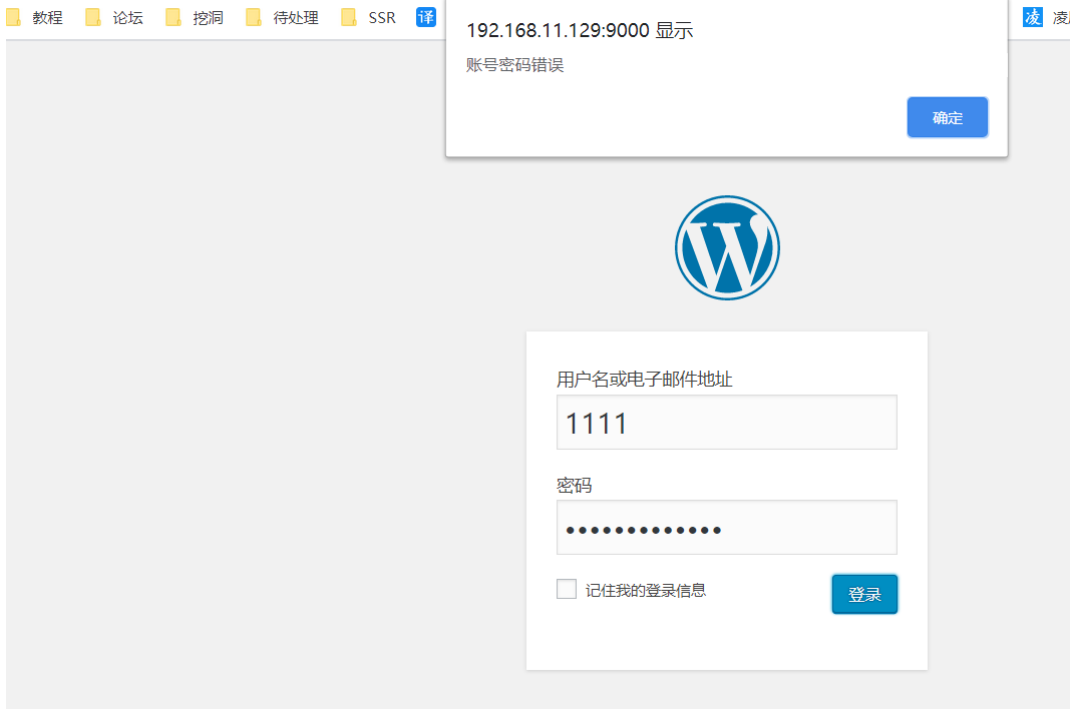
🔒 Closed Assassins-white opened this issue on Mar 15, 2020 · 1 comment

Assassins-white commented on Mar 15, 2020 • edited

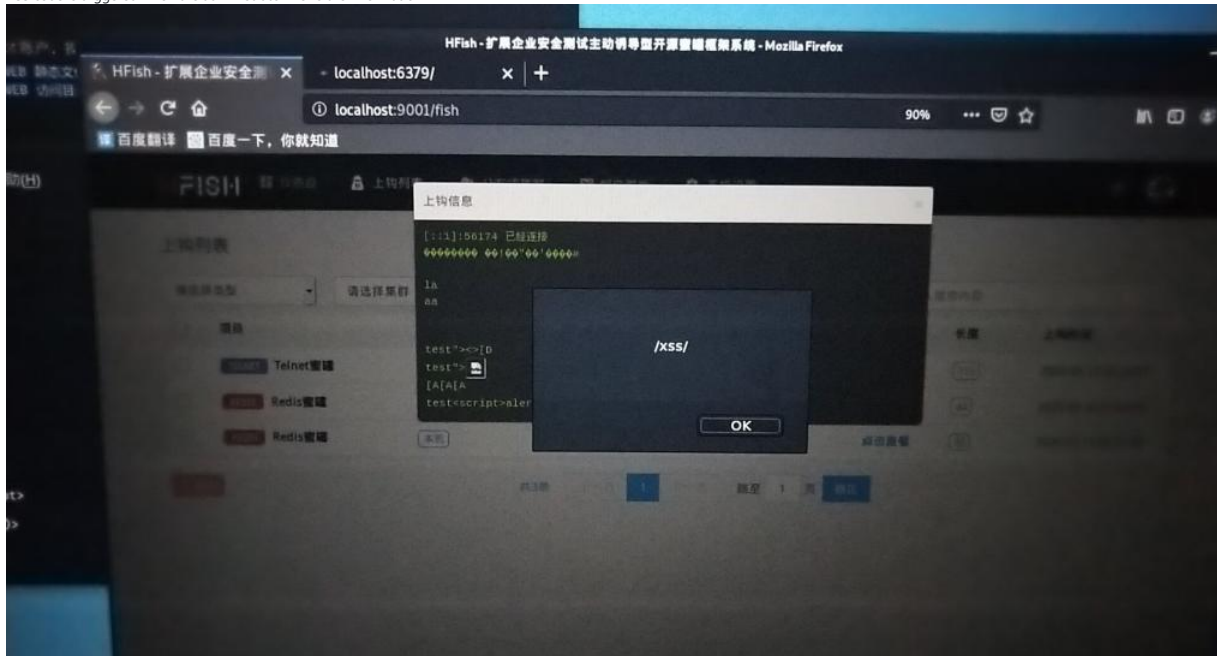
In any phishing interface, where the password needs to be entered, the use of img tags can cause XSS attacks.

Insert XSS payload where the password is entered

192.168.11.129:9000



XSS code is triggered when the administrator views the information



Use the following code to get a cookie.


```

```

	+全部	时间	接收的内容	Request Headers	操作
	折叠	2020-03-15 11:16:15	<ul style="list-style-type: none">location : http://192.168.11.129:9001/fishtoplocation : http://192.168.11.129:9001/fishcookie : HFish=MTU4NDIxMTMyOHxE^{di}1CQkFFQ180SUFBUKFCRUF^{BQVZ}QLUNBQUIHYzNSeWFXNW5EQW9BQ0dselgyeHZaMmx1Qm5OMGNibHVad3dlQUFWaFpHMXBiZ1p6ZEhKcGJY01CZ0FFZEdsdFpRWnpkSEpwYm1jTUZRQVRNakF5TUMwd015MHhOU0F3TWpvME1qb3dPQT09fkouiA_XL-nG_hif-pGEhHy2Hcr5m8MgaHW1Vjsos7T6opener :	<ul style="list-style-type: none">HTTP_REFERER : http://192.168.11.129:9001/fishHTTP_USER_AGENT : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36REMOTE_ADDR : 127.0.0.1	删除

sanjinhub commented on Mar 17, 2020

收到，等新版本

 sanjinhub closed this as completed on Apr 10, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

