

绕过思路就是

在 action 前面加一个/

action/=javascript:

就可以绕过

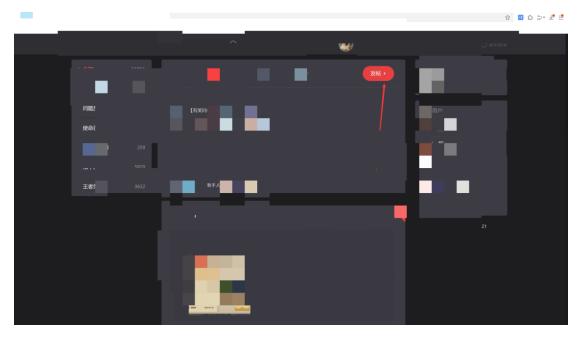
知道思路后,回到主题。

漏洞详细:

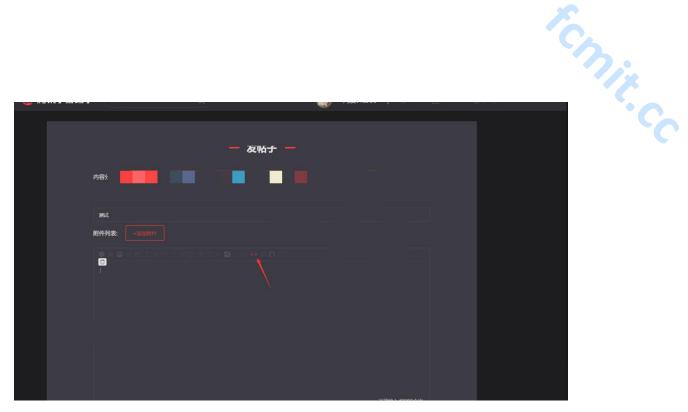
某T厂家论坛存在 xss 漏洞

url: https://bbbb.xxxxx.com/

登录之后我们点发帖



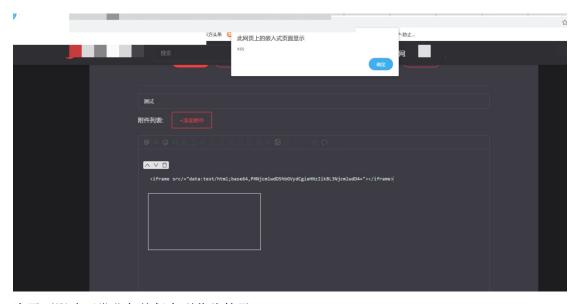
然后点击行内代码



综合我上面绕过的方法组合的 poc

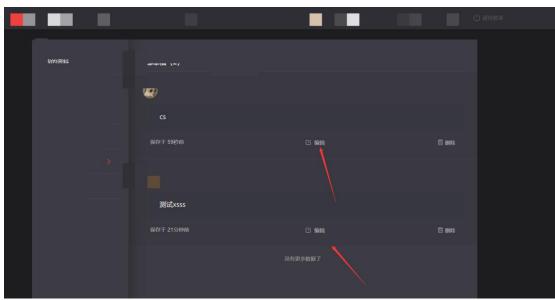
bypassPoc: <iframe src/="data:text/html;base64,

PHNjcmlwdD5hbGVydCgieHNzlik8L3NjcmlwdD4="></iframe>



为了不影响正常业务就保存到草稿箱了

C. C.



草稿箱打开也正常弹出

