



记一次XSS闲鱼诈骗网站到主机上线再到信息收集的过程

原创 落幕 HACK学习呀

2020-01-15原文

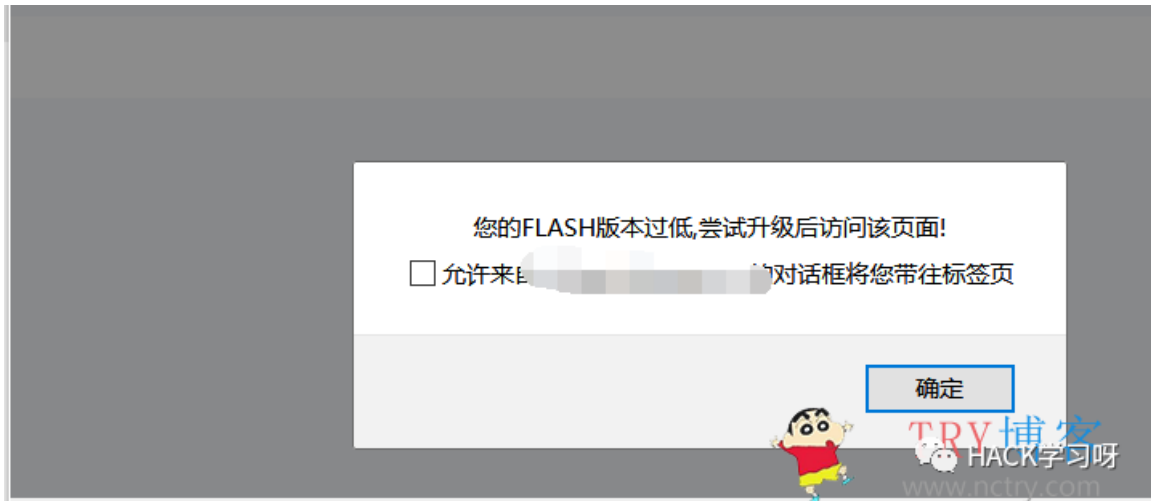
前言

距离上次搞闲鱼诈骗网站已经过去20多天了。这20多天里，搞了很多的钓鱼站，类似
什 么 黑 咖 的 
(已经下载到全站源码了，不过不会审计，有兴趣的大佬可以邮件联系我获取。)，
不过搞这些钓鱼站根本没用，相关部门也没进行管理。骗子们依然逍遥法外，所以最近依然在搞钓鱼网站，然后今天有了一些发现。就写下这篇文章，写的很乱。也是记录一下。希望能够提高大家的警惕性。 

目标：也是从闲鱼APP上获取到的链接 

XSS注入钓鱼

详细过程就不说了，可以去看我上篇文章。不过这次的xss注入里加入了flash弹窗钓鱼。效果如下:点这里查看详细过程

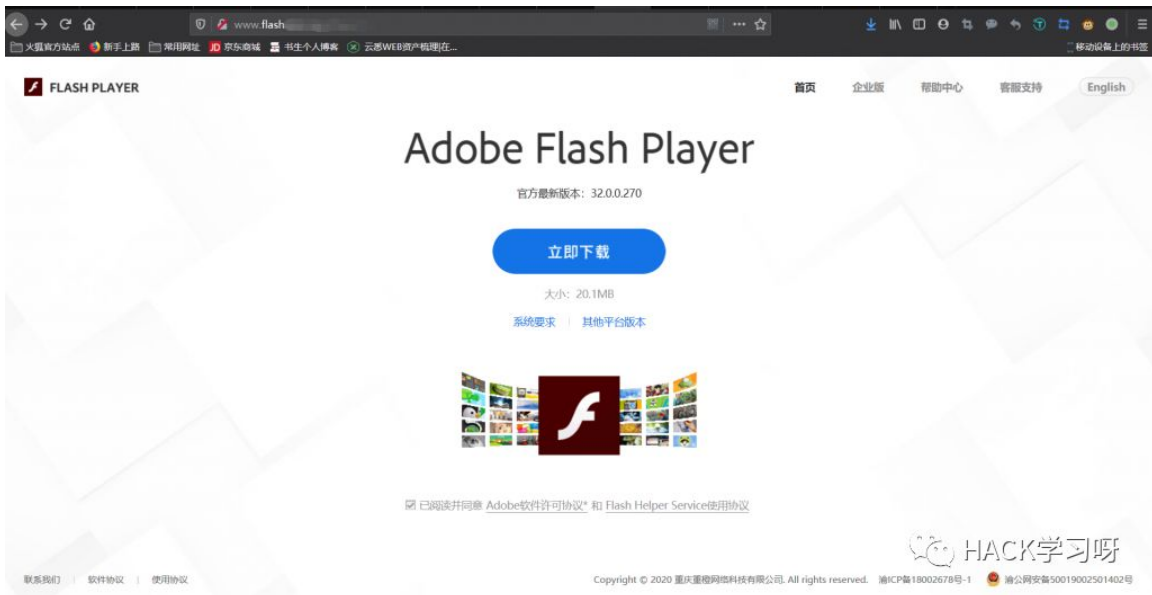


一个简单的xss弹窗跳转代码：

```
alert(" 您的 FLASH 版本过低 , 尝试 升级 后 访问 该 页面 !");  
window.location.href="填你的flash页面";
```

flash钓鱼

钓鱼页面：



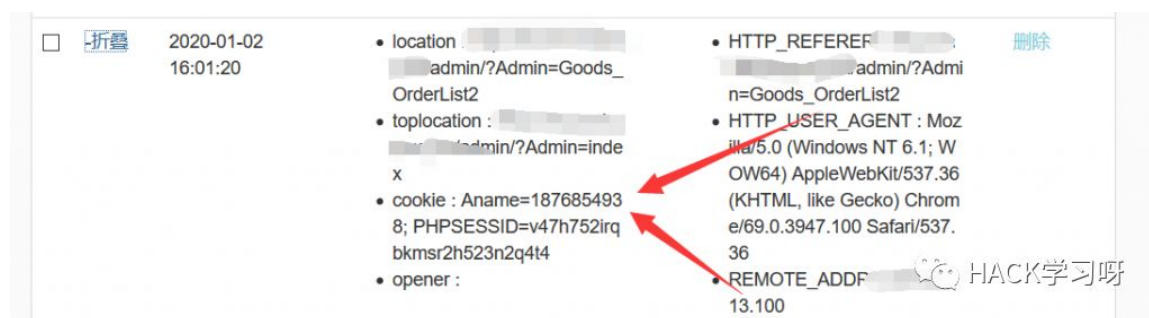
当然这个页面是我们自己伪造的，下载的文件是利用自解压程序捆绑了木马的（捆绑教程等下写），也是可以正常安装flash的。😏

等待主机上线

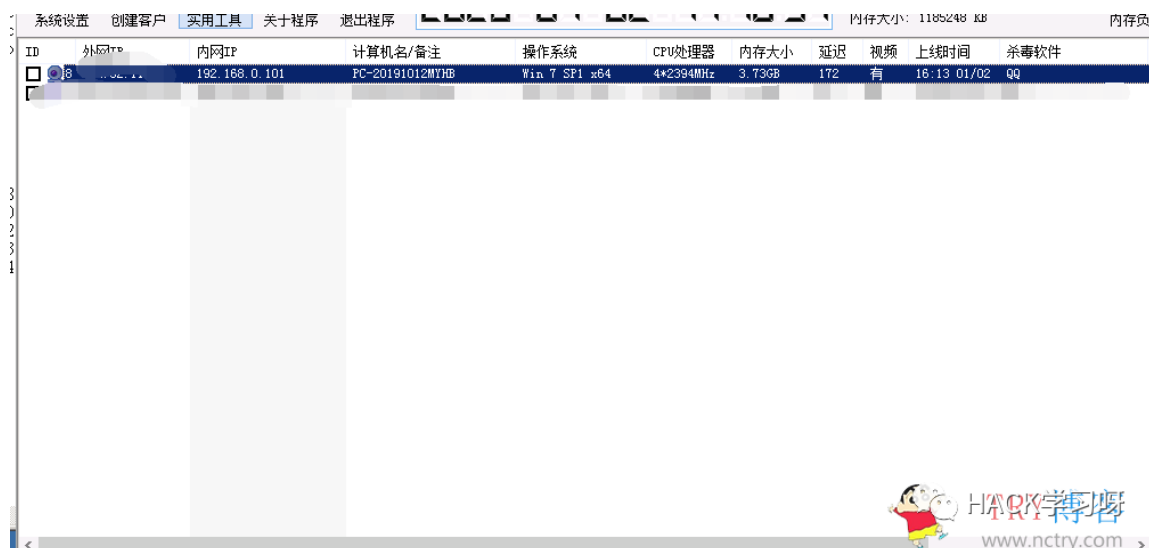
插入xss后，就耐心的等待骗子上线。但是有点警惕性的应该都不会上当的啦 😏

，不过运气不错，我们这个骗子好像警惕性有点低。😏
，哈哈。稍微等待了一会后，xss平台返回了一个管理员的cookie，然后再查看远控，主机已经成功上线！然后在xss平台里把弹窗代码取消掉。

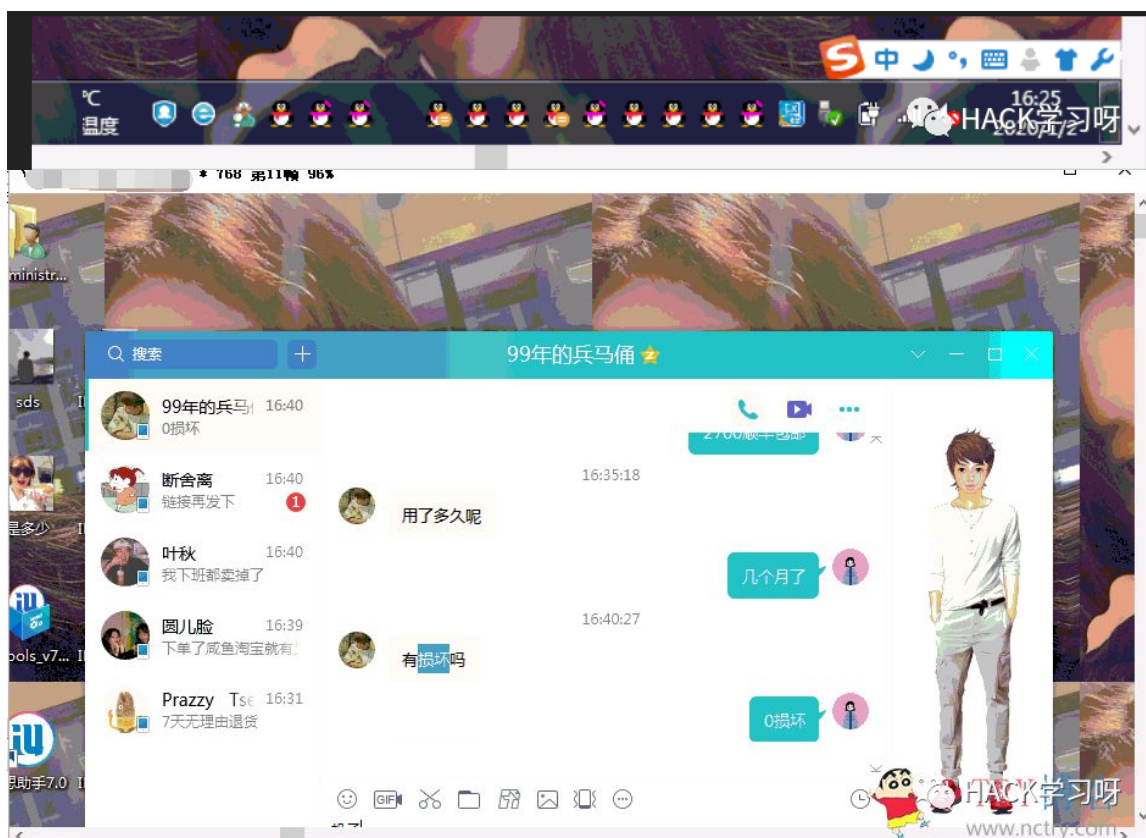
xss返回如下：



主机上线：（进行相关取证）



骗子桌面QQ截图：



(进行相关录屏录音取证，有兴趣的朋友可以找我获取🤖)

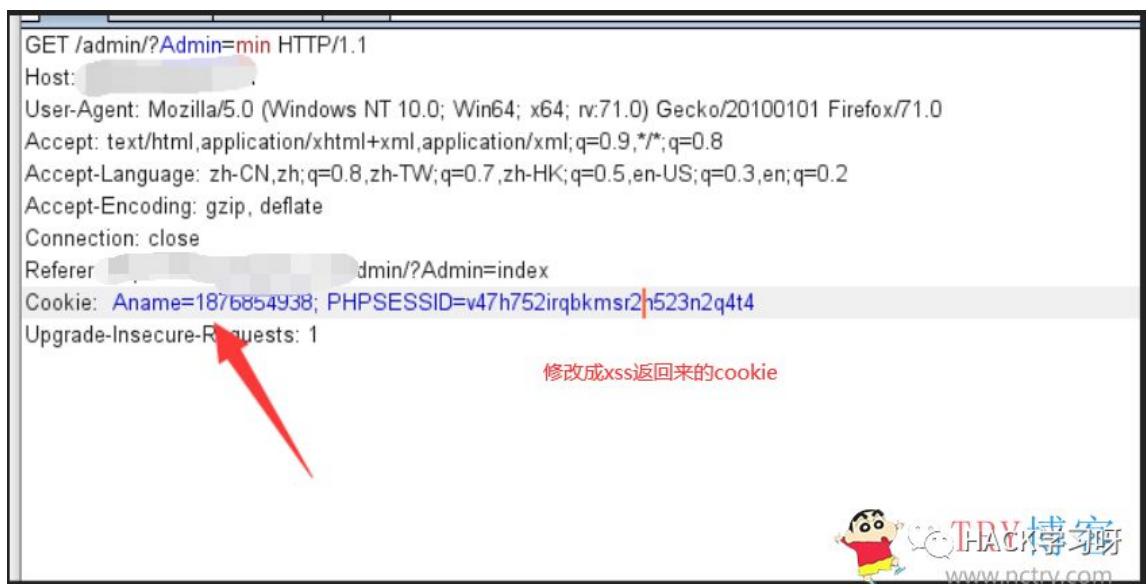
然后该骗子的电脑里没什么有用的信息，就一堆QQ号。。然后决定从诈骗网站中获取更多信息。


信息收集

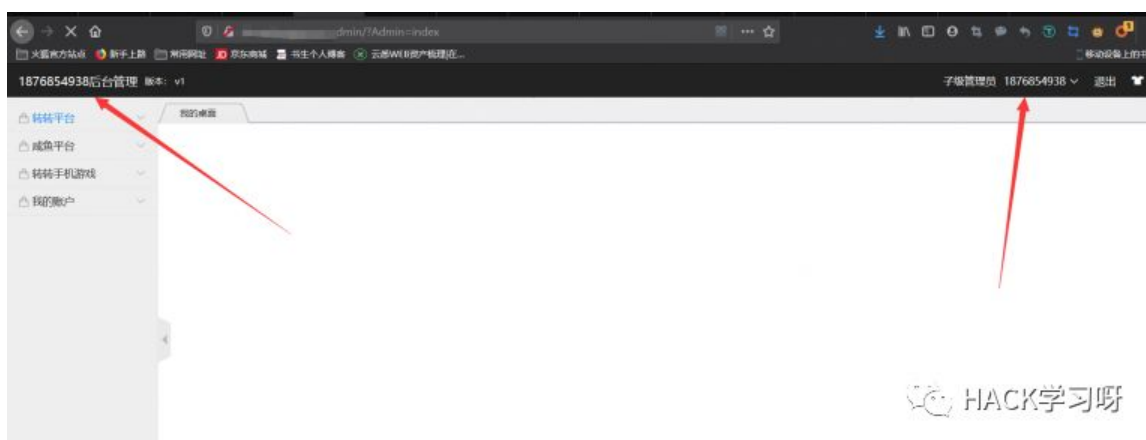
网站后台：<http://xxx.cn/Surplus.php>（扫描出来的）

利用之前xss返回来的cookie进行登录。

利用burp修改cookie进行登录，成功进入后台。

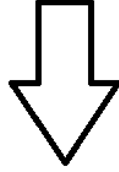


进入后台后发现不是管理员权限?? , 原来是一个小弟?



得想办法搞到管理员权限。然后通过查看cookie, 发现可能存在越权访问。

```
Aname=1876854938; 这里是xss返回的cookie, 用户名是1876854938  
PHPSESSID=v47h752irqbkmsr2h523n2q4t4
```



```
Aname=admin;  
PHPSESSID=v47h752irqbkmsr2h523n2q4t4
```

这里是修改后的cookie, 猜测管理员用户名是admin, 后端验证的是Aname参

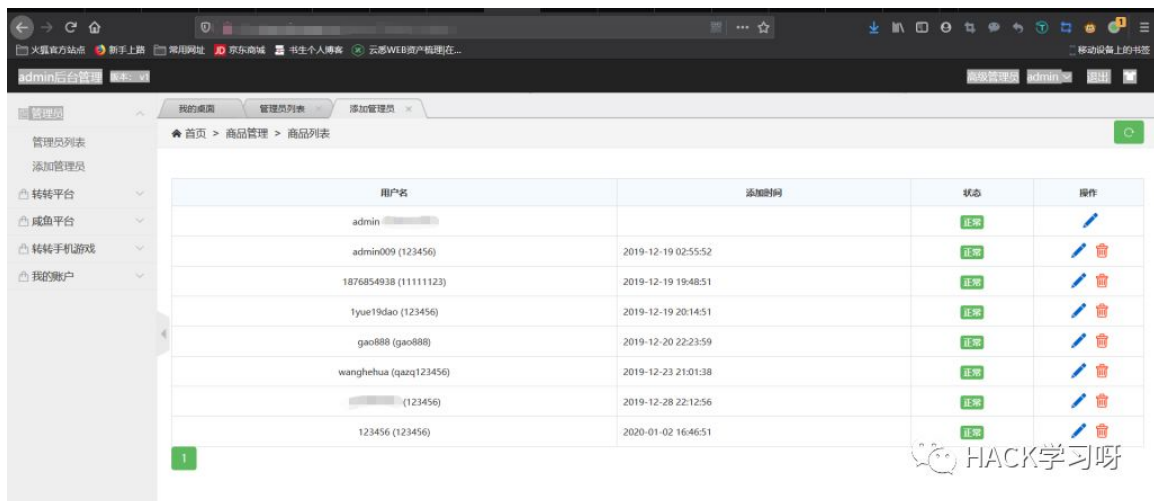


HACK学习呀
www.nctry.com

利用修改后的cookie进行登录, 运气不错, 成功用管理员权限进入后台! 哈哈。



查看管理员密码:发现管理员密码貌似是一个QQ号?? ? QQ是: 243XXXXXXX



用户名	添加时间	状态	操作
admin		正常	编辑 删除
admin009 (123456)	2019-12-19 02:55:52	正常	编辑 删除
1876854938 (11111123)	2019-12-19 19:48:51	正常	编辑 删除
1yue19dao (123456)	2019-12-19 20:14:51	正常	编辑 删除
gao888 (gao888)	2019-12-20 22:23:59	正常	编辑 删除
wanghehua (qazq123456)	2019-12-23 21:01:38	正常	编辑 删除
(123456)	2019-12-28 22:12:56	正常	编辑 删除
123456 (123456)	2020-01-02 16:46:51	正常	编辑 删除



HACK学习呀

哈哈, 有了QQ号就好办了。然后通过百度查询他QQ号的相关信息。



贴吧账号：



还有微信什么的就不发出来了。希望大佬们能出手，让这些骗子去吃过年牢饭吧，哈

哈

。

，写的比较乱，目前证据也挺乱的，有这个骗子用过的QQ等，还有骗子骗人的过程



录屏以及录音（摄像头打开黑屏~~）。但是还是无从下手的感觉，我太菜了。



奥利给！



推荐阅读：

渗透学习-如何搞定一个在闲鱼搞诈骗的网站

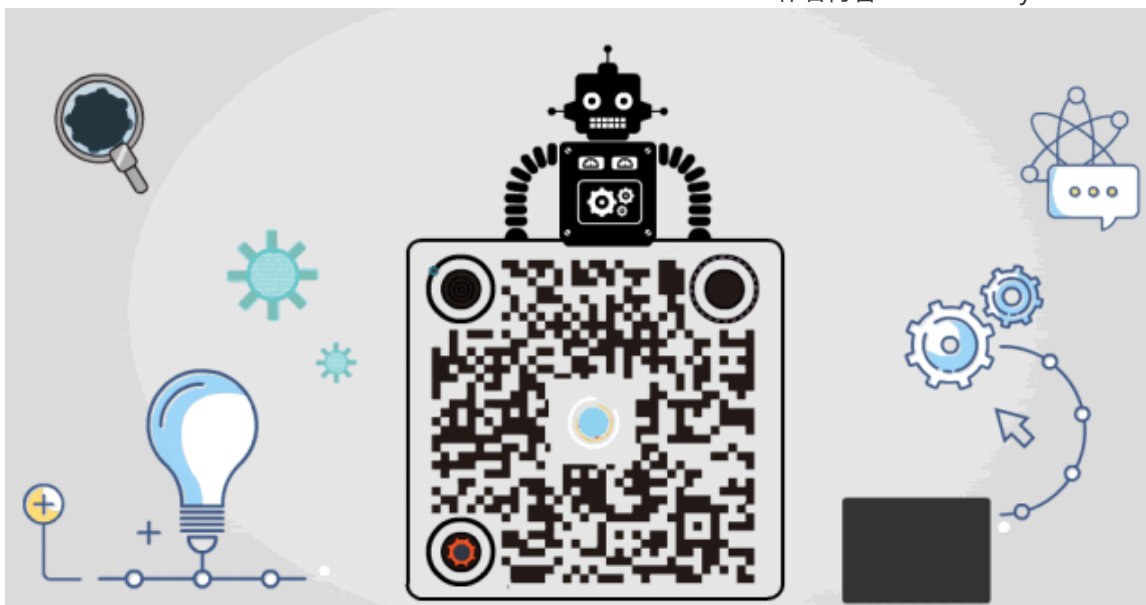
<http://www.nctry.com/1163.html>

希望大家警惕此类骗局，淘宝或者咸鱼站外交易，尽量别交易，避免被骗

天上不会掉馅饼

原创投稿作者：落幕

作者博客：www.nctry.com



精选留言

用户设置不下载评论