

记一次白嫖X站盒子App的渗透测试

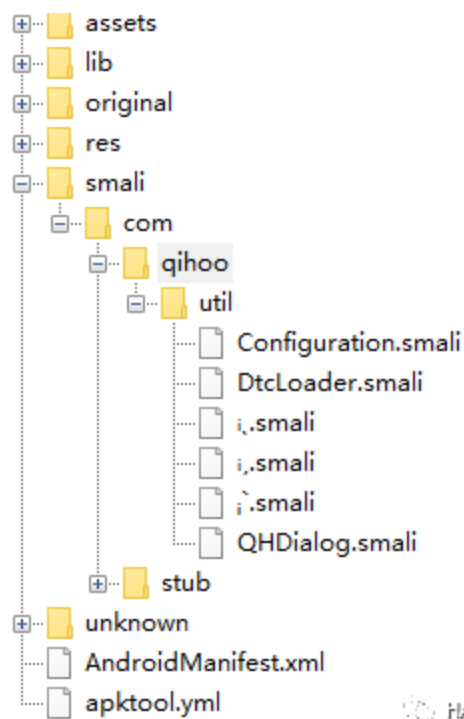
原创 cacker HACK学习呀

2020-07-29[原文](#)

无意间得到一个你懂的APP地址，为了保护祖国的花朵不受到摧残，能有一个健康、安全的网络环境.于是有了这个故事(给钱是不可能给钱的，只能白嫖这样才能维持生活这样子)。

 <p>龙珠</p> <p>4</p>	 <p>映客</p> <p>32</p>	 <p>樱花雨i</p> <p>127</p>
 <p>茄子i</p> <p>120</p>	 <p>逗艳</p> <p>79</p>	 <p>卡哇伊</p> <p>121</p>
 <p>Gboy</p> <p>120</p>	 <p>桃花运</p> <p>104</p>	 <p>一直播</p> <p>110</p>
 <p>优乐美</p> <p>125</p>	 <p>小天仙</p> <p>117</p>	 <p>小米粒</p> <p>120</p>
		

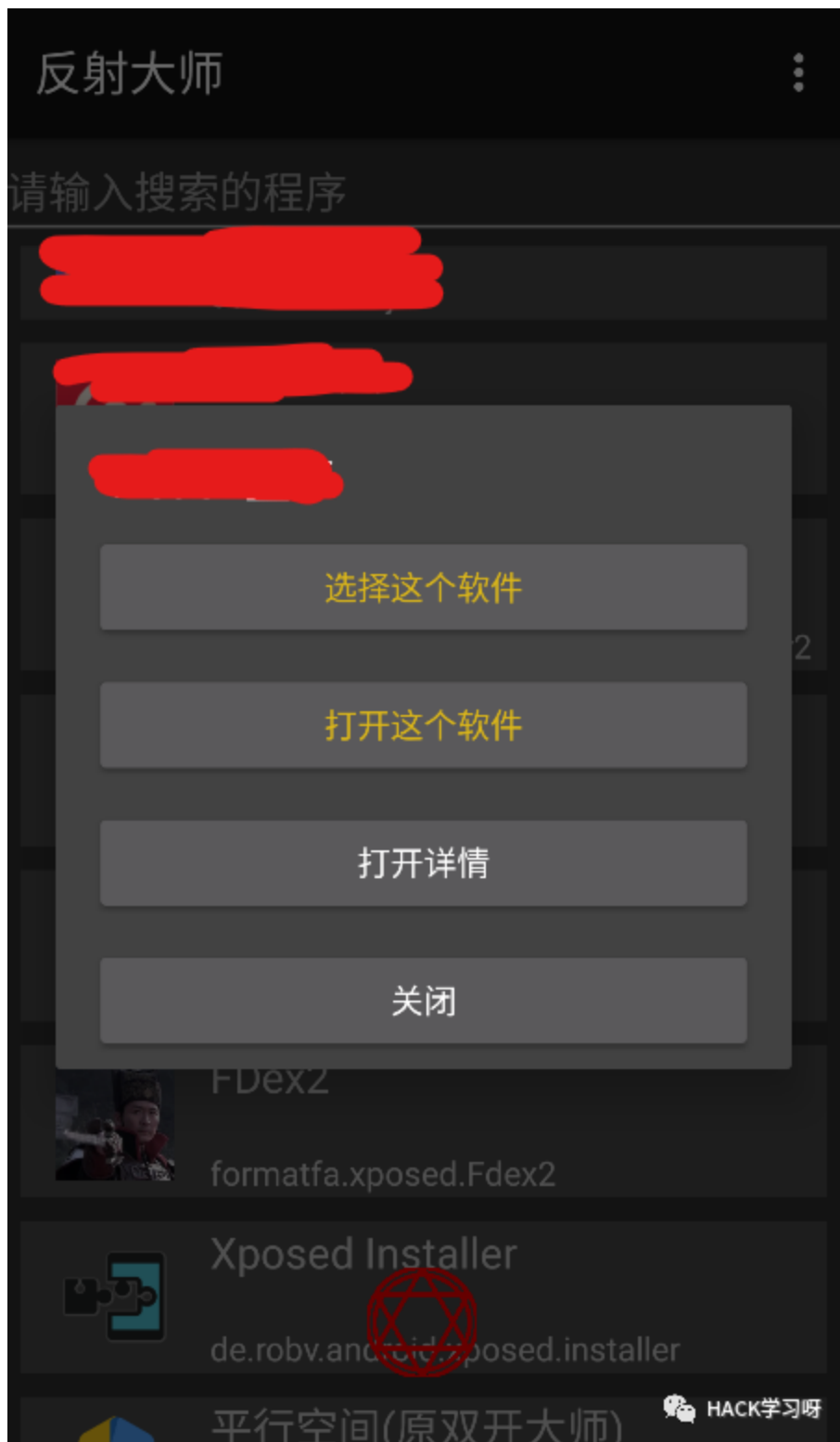
E4A写的**直播聚合盒子



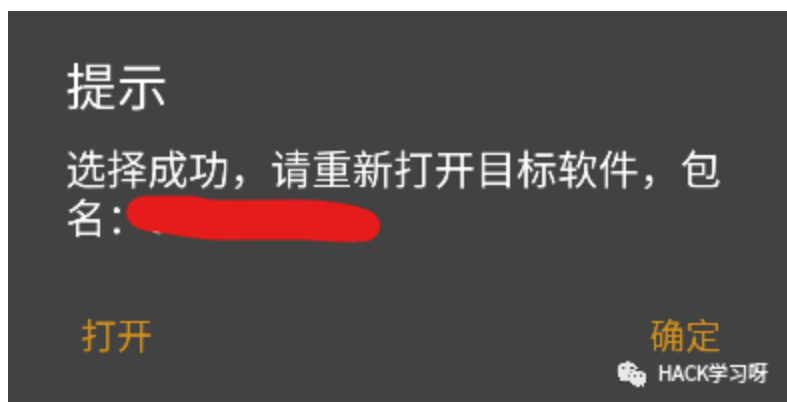
HACK学习呀

Apk反编译发现经过了360加固。这里我技术菜采用xposed+反射大师的方式进行自动脱壳（如果加壳的版本比较低）。

模拟器安装好xposed+反射大师后运行反射大师选择该app（都可以直接百度下载）



单击选择这个软件



然后选择打开，然后在目标软件的窗体上会多出一个六芒星的浮层。

缩小540 X 1440

当前ACTIVITY

VIEW获取(子)

HACK学习呀 点击六芒星然后选择当前activity。



长按选择写出dex

Tip

写出成功, 文件位于/storage/emulated/0/classes.dex/storage/emulated/0/classes.dex

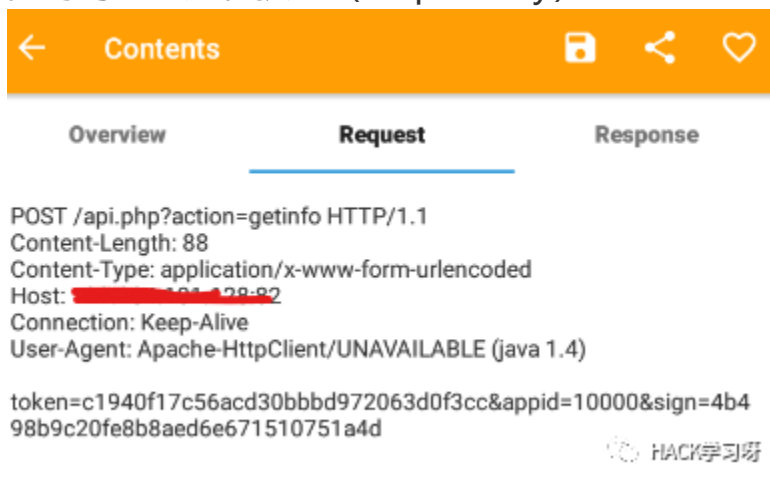
复制

OK

HACK学习呀

最后我们从模拟器中把提取的dex转换成jar就可以直接进行反编译了。

同时对APK进行抓包 (httpcanary)



得到api接口地址, 发现是通过ip+端口的形式, 常规操作nmap+后台扫描器进行扫描

登入

账号

密码

☐ 记住我

登入

提示: 您还没有登陆, 请先登录!

© 2019 - eruyker. All rights reserved.

HACK学习呀

发现后台源码为某套开源网络验证系统，后台没有验证码，爆破也没成功

于是下载源码后进行本地搭建与审计。

易如意网络验证系统



首页

公告

应用

应用管理

+ 添加应用

会员

卡密

积分

商品

订单

统计

退出

应用设置

名称: app

APPID: 10000

复制

APPKEY: d52a2e5e3d8b850423865d30c637d24d

复制

Sign有效期: 100 秒

运营模式: ☒ 收费模式 ☐ 免费模式

设备校验: ☒ 开启 ☐ 关闭

提示: 开启设备校验之后, 用户登入时会校验上次登入的设备是否一致, 可防止VIP账号一人多用

应用状态: ☒ 开启 ☐ 关闭

提示: 关闭应用后, 改应用的用户无法进行任何操作!

同一IP注册间隔: 0 小时

提示: 可有效防止同一个IP在设置的时间间隔内无法再进行注册, 0为不限制

同一机器注册间隔: 0 小时

HACK学习呀

```
api.php
文字查找
$result = move_uploaded_file
查找
--函数列表--
json
Sign
md5Sign
get_pic
getcode
getIp
--变量列表--
$data
$data
$msg
$code
$data
$sign_t
$appkey
$prestr
$key
$pic_url
$server_url
$SERVER['REQUEST_URI']
$SERVER['SERVER_NAME']
$str
$mac
$strPol[rand
$
$strPol
$ip
$SERVER['REMOTE_ADDR']
$ini_data
$pay_qq_state
$pay_wx_state
$pay_rfb_state
$pay_appkey
$pay_appid
$pay_url
$pay_state
$app_extend_5
$app_extend_4
$app_extend_3
$app_extend_2
$app_extend_1
$app_extend_ini
$diary_vip
$inv_vip
$notice
$app_nurl
$app_nshow
389
} else {
390
    json(151, 'token已失效'); // token已失效
391
}
392
}
393
}
394
}
395
if ($action == 'alterpic') { // 上传头像
396
    $type = isset($_GET['type']) ? addslashes($_GET['type']) : 'e4a';
397
    $token = isset($_GET['token']) ? addslashes($_GET['token']) : '';
398
    if ($token == '') json(150, 'token不能为空'); // token不能为空
399
    $sql = "select * from eruyi_user where token = '$token'";
400
    $query = $db->query($sql);
401
    $have = $db->fetch_array($query);
402
    if ($have) {
403
        $user = $have['uid'];
404
    } else {
405
        json(151, 'token已失效'); // token已失效
406
    }
407
    $db->query("UPDATE `eruyi_user` SET `last_t` = '$last_t' WHERE token = '$token'"); // 活动
408
    $local_path = "./pic/";
409
    if (!file_exists($local_path)) mkdir($local_path);
410
    if ($type == 'bbp') {
411
        if ($SERVER['REQUEST METHOD'] == 'POST') {
412
            echo 1;
413
            foreach ($FILES as $name => $file) {
414
                $fn = $file['name'];
415
                $ft = strrpos($fn, '.');
416
                $fe = substr($fn, $ft);
417
                $fp = 'pic/' . $user . $fe;
418
                $result = move_uploaded_file($file['tmp_name'], $fp);
419
                $pic = "/" . $fp;
420
            }
421
            json(131, '提交方式不正确'); // 提交方式不正确
422
        } else if ($type == 'e4a') {
423
            $target_path = $local_path . $user . ".png";
424
            $result = move_uploaded_file($FILES['uploadedfile']['tmp_name'], $target_path);
425
            $pic = substr($target_path, 1);
426
        } else {
427
            json(132, '上传类型不支持'); // 上传类型不支持
428
        }
429
        if ($result) {

```

HACK学习呀

发现该套源码对外交互最主要的是api.php这个文件。

注入什么的都使用了addslashes进行了过滤，暂时没仔细看，不过发现了一处上传非常可疑。但是要使代码执行到这一地方就必须绕过sign签名校验。

```
$action = isset($_GET['action']) ? addslashes($_GET['action']) : '';
$appid = isset($_POST['appid']) ? (addslashes($_POST['appid']) : (isset($_GET['appid']) ? addslashes($_GET['appid']) : ''));
$sign = isset($_POST['sign']) ? (addslashes($_POST['sign']) : (isset($_GET['sign']) ? addslashes($_GET['sign']) : ''));

if ($action != '') {
    if ($appid == '') json(104, '应用id不能为空'); // 应用id为空
    if ($sign == '') json(105, '签名不能为空'); // 签名不为空
    $app_sql = "select * from eruyi_app where id = '$appid'";
    $app_query = $db->query($app_sql);
    $app_have = $db->fetch_array($app_query);
    if (!$app_have) json(107, '应用不存在'); // 应用不存在
    if ($app_have['state'] == 'n') json(108, $app_have['notice']); // 应用已关闭
    $t_sign = Sign($action, $app_have['key'], $app_have['sign_t']);
    if ($sign != $t_sign) json(109, '签名错误'); // 签名错误
}

function Sign($data, $appkey, $sign_t) {
    $data = $data . $appkey . floor(time() / $sign_t) * $sign_t;
    return md5($data);
}
```

HACK学习呀

回到校验处的代码跟进sign函数。

```
function Sign($data, $appkey, $sign_t) {
    $data = $data . $appkey . floor(time() / $sign_t) * $sign_t;
    return md5($data);
}
```

HACK学习呀

需要传入\$data,\$appkey,\$sign_t

通过上面的调用可以知道\$data就是get过来的action, \$app_have['key'],\$app_have['sign_t']的值我们并不知道。此时其实有2条路可以走。

第一种就是对\$app_have['key'],\$app_have['sign_t']的值进行破解

第二种就是反编译apk代码, 到里面找到\$app_have['key'],\$app_have['sign_t']的值。

APPKEY:


d52a2e5e3d8b850423865d30c637d24d

复制

Sign有效期:

100

秒

 HACK学习呀

在本地搭建的后台发现appkey的好像是一串md5
sign有效期也就是\$app_have['sign_t']默认是100秒,

```
$sql="select * from eruyi_app where name='$name'";  
$query=$db->query($sql);  
$have=$db->fetch_array($query);  
if($have){  
    echo "<script>alert('失败: 应用已存在');</script>";  
}  
else{  
    $key = md5(time());  
    $sql="INSERT INTO `eruyi_app` (  
        `name`,`key`,`charge`,`ipon`,`codeon`,`check_code`,`many_code`,`reg_award`,`inv_award`,`diary_award`,`  
        `reg_vip`,`reg_fen`,`inv_vip`,`inv_fen`,`diary_vip`,`diary_fen`,`app_bb`,`pay_url`,`pay_appid`,`pay_appkey`,`  
        `pay_notify`,`pay_state`,`pay_zfb`,`pay_wx`,`pay_qq`,`pay_zfb_state`,`pay_wx_state`,`pay_qq_state`) VALUES (  
        '$name','$key','$charge','$ipon','$codeon','$check_code','$many_code','$reg_award','$inv_award','$diary_award`,`  
        '$reg_vip','$reg_fen','$inv_vip','$inv_fen','$diary_vip','$diary_fen`,`$app_bb`,`$pay_url`,`$pay_appid`,`$pay_appkey`,`  
        '$pay_notify`,`$pay_state`,`$pay_zfb`,`$pay_wx`,`$pay_qq`,`$pay_zfb_state`,`$pay_wx_state`,`$pay_qq_state')";  
    $query=$db->query($sql);  
    if($query){  
        echo "<script>alert('应用创建成功');</script>";  
    }  
}
```

查看源码发现appkey的生成方式其实是调用time()函数得到时间戳进行md5加密, 那这就存在暴力破解的appkey的风险了。Appkey能够破解就可以伪造任意签名。

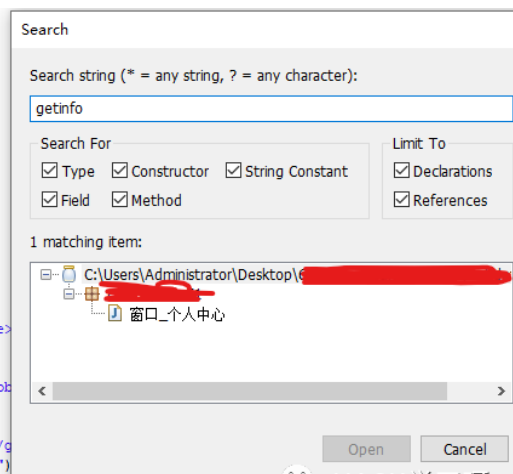
再次分析apk

```

public void 多线程16取网页源码完毕(String paramString)

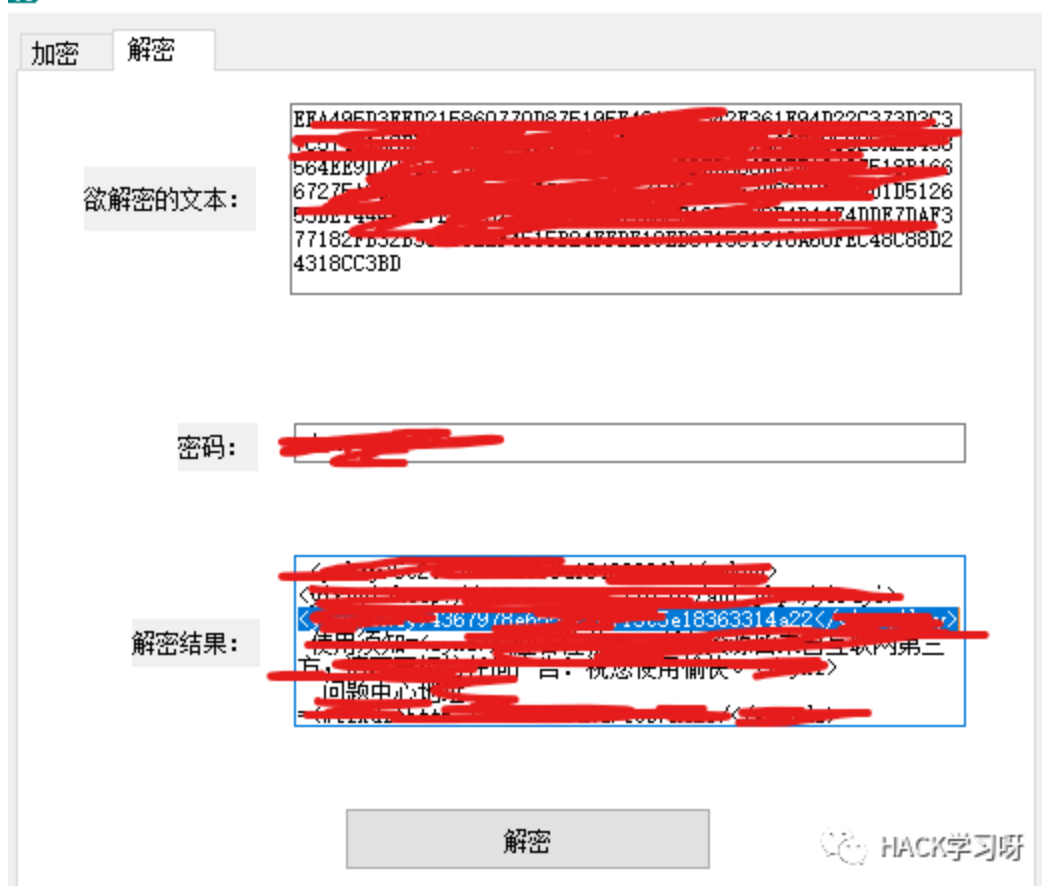
paramString = 加密操作.RC4解密(paramString, "true");
if (文本操作.取指定文本2(paramString, "<title>", "</title>").equals(""))
{
    if (this.线路 == true)
    {
        this.多线程1.开始取网页源码("http://[redacted]k1", "utf-8");
        this.线路 = false;
        return;
    }
    this.ok工具类1.简单信息框(0, "错误", "连接服务器错误");
    return;
}
公用模块.软件名称 = 文本操作.取指定文本2(paramString, "<title>", "</title>");
this.更新方式 = 文本操作.取指定文本2(paramString, "<gxfs>", "</gxfs>");
this.软件状态 = 文本操作.取指定文本2(paramString, "<tyrj>", "</tyrj>");
this.最新版本号 = 转换操作.到数值(文本操作.取指定文本2(paramString, "<xzbb>"));
this.下载地址 = 文本操作.取指定文本2(paramString, "<xzzz>", "</xzzz>");
this.更新说明 = 文本操作.取指定文本2(paramString, "<gxsm>", "</gxsm>");
公用模块.滚动标签公告 = 文本操作.取指定文本2(paramString, "<gdbqgg>", "</gdbqgg>");
公用模块.弹窗公告 = 文本操作.取指定文本2(paramString, "<tcgg>", "</tcgg>");
公用模块.QQ号 = 文本操作.取指定文本2(paramString, "<qq>", "</qq>");
公用模块.QQ群KEY = 文本操作.取指定文本2(paramString, "<qqq>", "</qqq>");
公用模块.搜索一 = 文本操作.取指定文本2(paramString, "<搜索一>", "</搜索一>");

```



搜索getinfo发现了请求了一个网页然后进行rc4解密。直接访问是乱码，于是进行rc4解密

这其实也有点坑调用的是e4a的解密，于是我还特地下了个e4a利用e4a提供的rc4演示工具解密才成功



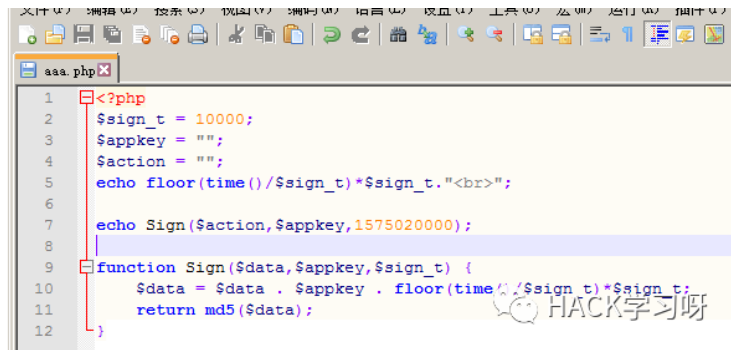
然后从解密的文件中得到了appkey值，但是还需要个sign_t的值才行。

继续从源码中

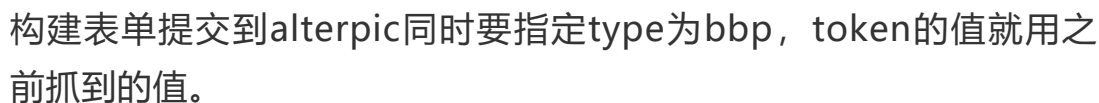
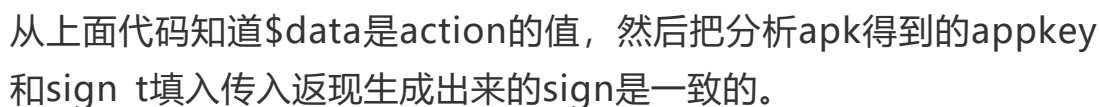
```
@SimpleDataElement
public static int sign_t = AsyncHttpClient.DEFAULT_SOCKET_TIMEOUT;
@SimpleDataElement
public static final int DEFAULT_SOCKET_TIMEOUT = 10000;
public static final String ENCODING_GZIP = "gzip";
```

得到sign_t的值为10000，然后开始伪造签名

1575270000
0f09973adcef65d503a0ca22d42733e3



1575270000
4b498b9c20fe8b8aed6e671510751a4d



```
{
  "code": 131,
  "msg": "提交方式不正确",
  "data": [
    [
      "pic/10.png"
    ]
  ]
}
```

提交后提示提交方法不正确，其实已经上传成功，文件名是/pic/用户id+上传的格式。用户id在getinfo的返回包中可以看到。

	名称	日期	大小	属性
	0.png	2018-03-04 17:36:42	8.8 Kb	0755
	1.png	2019-11-29 17:29:05	7.04 Kb	0644
	10.png	2019-09-16 17:56:30	2.01 Kb	0755
	100.png	2019-11-29 17:29:05	7.04 Kb	0644
	2.png	2019-09-16 09:52:32	229.99 Kb	0755
	28.png	2019-11-19 20:49:33	333.59 Kb	0644
	29.png	2019-11-20 01:52:12	39.34 Kb	0644
	350.png	2019-11-21 23:43:24	4.23 Kb	0644
	42.png	2019-11-19 21:19:38	1.36 Mb	0644
	964.png	2019-11-29 17:21:55	4.78 Kb	0644
	979.png	2019-11-29 08:18:16	1.25 Mb	0644

Getshell成功。

额外发现：

```
vip.php
1 <?php
2 include("include/global.php");
3 $ipList = array('192.168.0.13','127.0.0.1');//可添加多个安全IP, 只有安全IP才可调用该接口
4
5 if(!in_array(getIP(),$ipList)) json(100,'安全IP校验失败');
6
7 $user = isset($_GET['user']) ? addslashes($_GET['user']) : '';
8 $day = isset($_GET['day']) ? addslashes($_GET['day']) : '';
9 if($user == '') json(101,'用户账号不能为空');
10 if($day == '') json(102,'增加天数不能为空');
11
12 $sql="select * from eruyi_user where `user`='$user'";
13 $query=$db->query($sql);
14 $have=$db->fetch_array($query);
15 if(!$have) json(103,'没有找到该用户');
16 if($have['vip']=='999999999') json(104,'该用户已是永久会员');
17 if($have['vip']>time()){
18     if($day == '9999'){
19         $sql="UPDATE `eruyi_user` SET `vip`='999999999' WHERE user='$user'";
20     }else{
21         $sql="UPDATE `eruyi_user` SET `vip`='$vip'+$day*86400 WHERE user='$user'";
22     }
23 }else{
24     if($day == '9999'){
25         $vip = '999999999';
26     }else{
27         $vip = time()+$day*86400;
28     }
29     $sql="UPDATE `eruyi_user` SET `vip`='$vip' WHERE user='$user'";
30 }
31 $query=$db->query($sql);
32 if($query){
33     json(200,'增加成功');
34 }else{
35     json(201,'增加失败');
36 }
37
38
39 function getIP() {
40     if (getenv('HTTP_CLIENT_IP')) {
41         $ip = getenv('HTTP_CLIENT_IP');
42     } elseif (getenv('HTTP_X_FORWARDED_FOR')) {
43         $ip = getenv('HTTP_X_FORWARDED_FOR');
44     } elseif (getenv('HTTP_X_FORWARDED')) {
45         $ip = getenv('HTTP_X_FORWARDED');
```

其实在这套源码中存在一个vip.php文件

```
function getIP() {  
    if (getenv('HTTP_CLIENT_IP')) {  
        $ip = getenv('HTTP_CLIENT_IP');  
    } elseif (getenv('HTTP_X_FORWARDED_FOR')) {  
        $ip = getenv('HTTP_X_FORWARDED_FOR');  
    } elseif (getenv('HTTP_X_FORWARDED')) {  
        $ip = getenv('HTTP_X_FORWARDED');  
    } elseif (getenv('HTTP_FORWARDED_FOR')) {  
        $ip = getenv('HTTP_FORWARDED_FOR');  
    } elseif (getenv('HTTP_FORWARDED')) {  
        $ip = getenv('HTTP_FORWARDED');  
    } else {  
        $ip = $_SERVER['REMOTE_ADDR'];  
    }  
    return $ip;  
}
```

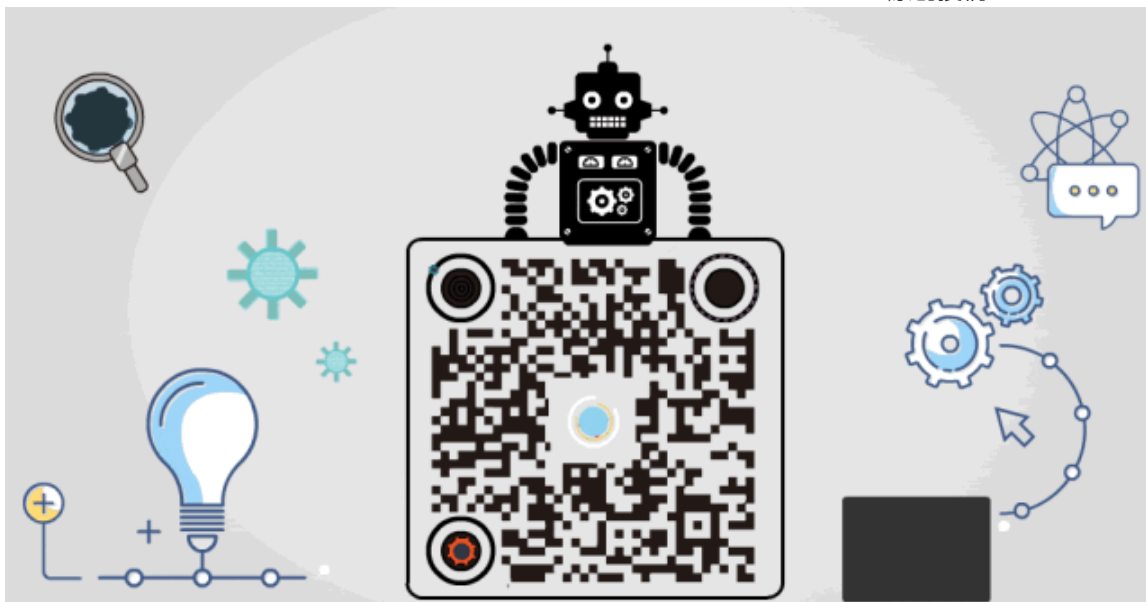
HACK学习呀

获取ip的方法改xff头就可以伪造，也可以直接获取永久VIP。



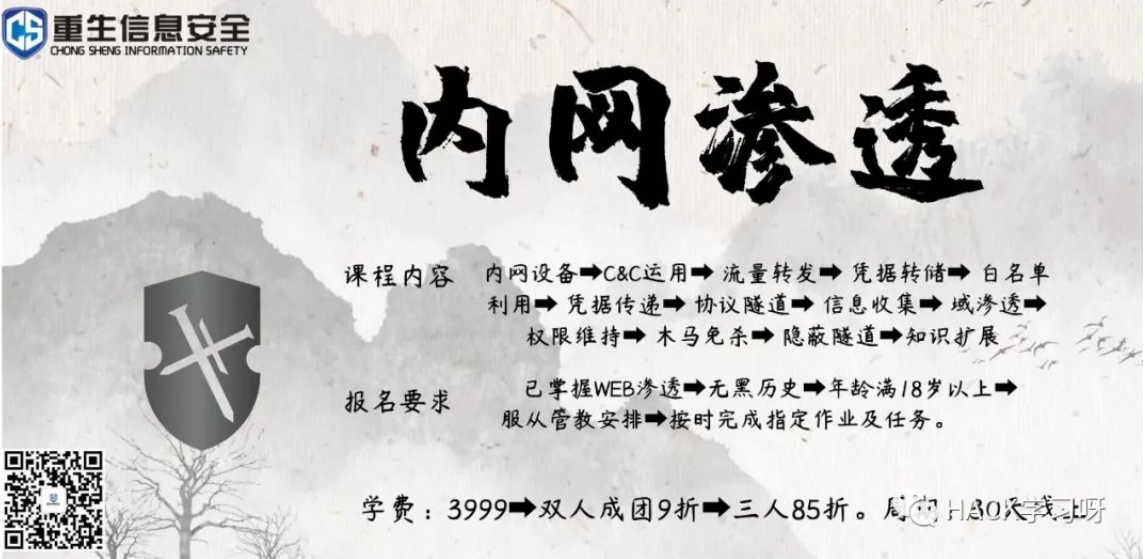
点赞，转发，在看

原创投稿：cacker



一则广告

添加记得注明来源：HACK学习



重生信息安全
CHONG SHENG INFORMATION SAFETY

内网渗透

课程内容 内网设备→C&C运用→流量转发→凭据转储→白名单利用→凭据传递→协议隧道→信息收集→域渗透→权限维持→木马免杀→隐蔽隧道→知识扩展

报名要求 已掌握WEB渗透→无黑历史→年龄满18岁以上→服从管教安排→按时完成指定作业及任务。

学费：3999→双人成团9折→三人85折。周周HACK学习呀

精选留言

用户设置不下载评论