2021年四川省大学生网络安全技能大赛 部分wp

原创

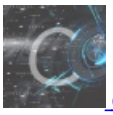
Je3Z 于 2021-05-15 13:46:08 发布 1075 收藏

分类专栏： ctf 文章标签： unctf

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/jvkyvly/article/details/116846240

版权


ctf 专栏收录该内容

31 篇文章 0 订阅

订阅专栏

加密解密

easy_pyc

在线反编译得到

```
#!/usr/bin/env python
# visit http://tool.lu/pyc/ for more information
import base64

def encode(yourflag):
	s = ''
	for i in yourflag:
		x = ord(i) ^ 62
		x = x + 6
		s += chr(x)

	return base64.b64encode(s)

tureflag = 'X1h1XOsMEWNiDxQQDgwTX15eZRFgFWMOFBATXhMMYw8PD2UMZUk='
flag = ''
print 'input your flag:'
yourflag = raw_input()
if encode(yourflag) == tureflag:
	print 'OHHHHHH~ correct!'
else:
	print 'emmm.. wrong'

```

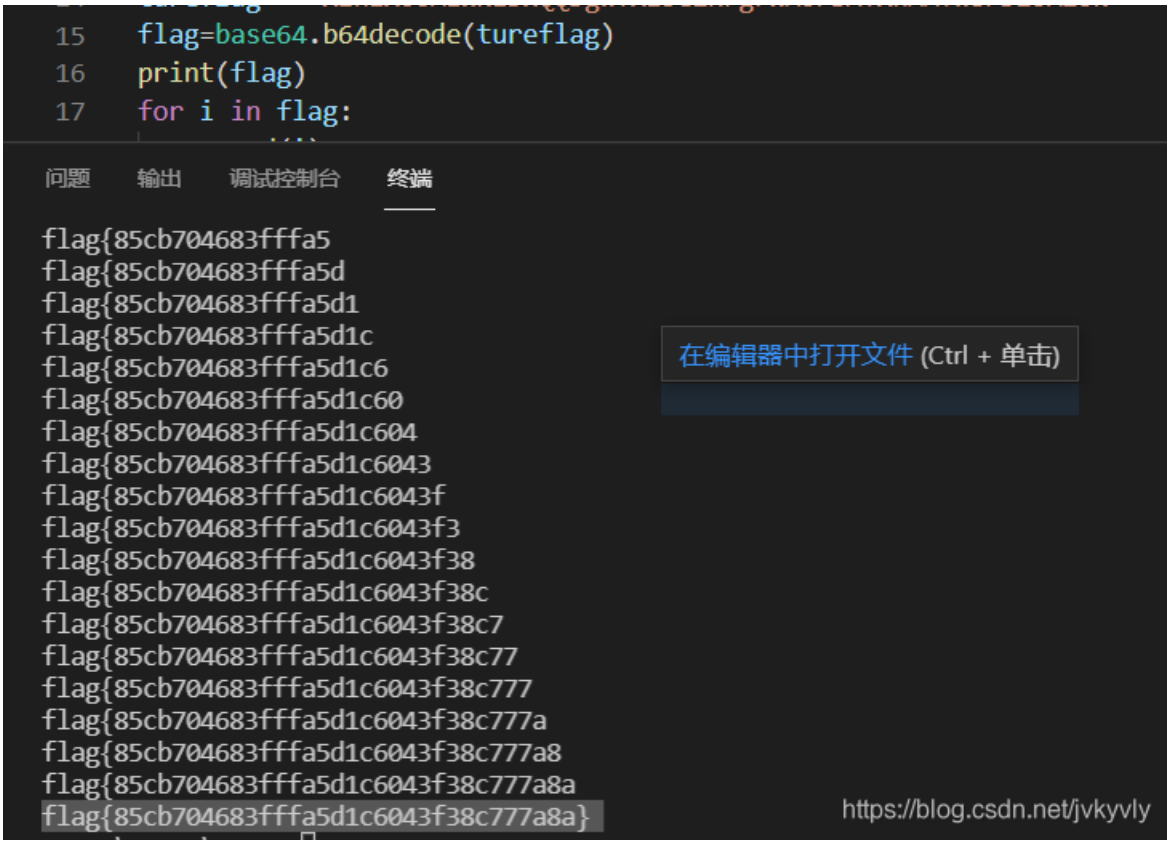
https://blog.csdn.net/jvkyvly

```python
#!/usr/bin/env python
# visit http://tool.lu/pyc/ for more information
import base64

def encode(yourflag):
    s = ''
    for i in yourflag:
        x = ord(i) ^ 62
        x = x + 6
        s += chr(x)

    return base64.b64encode(s)
zz=''
tureflag = 'XlhlX0sMEWNiDxQQDgwTXl5eZRFgFWMOFBATXhMMYw8PD2UMZUk='
flag=base64.b64decode(tureflag)
print(flag)
for i in flag:
    a=ord(i)
    a=a-6
    a=a^62
    zz+=chr(a)
    print(zz)
```

直接写脚本跑就行




```
flag{85cb704683fffa5d1c6043f38c777a8a}
```

em0ji

下载得到

☹😓😠😁{😁😂😈😂😇😇😄☝😁😑😊😄😇😂😠😓😁}

不用想前4个解密是 flag
直接网上搜em0ji
这个网址https://www.emojiall.com/zh-hans/emoji/%F0%9F%98%81

然后通过前面解码后是flag发现，解密就是简短代码的第一个字符

然后有一些没有，最后得到这个，再联想补全和测试即可

```
flag{ m jiisv rysimal }
```

```
flag{emojiisverysimple}
```

web

papapa

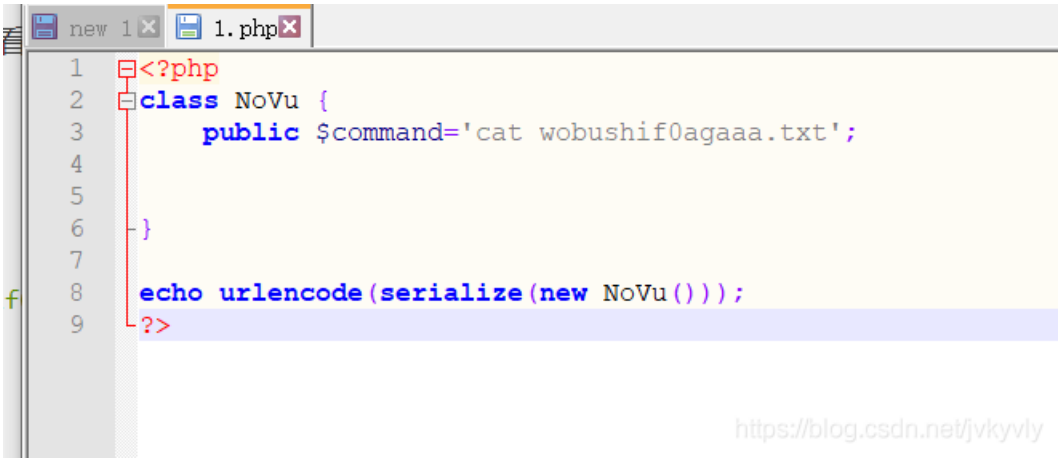
看robots.txt有提示mian.php

传参a得到

两次base64解码 再 16进制解码得到源码

md5数组绕过，正则那可以-绕过，也可以用%0a绕过

然后构造payload
先弄的ls，flag.txt里是假的，然后看到wobushif0agaaa.txt，是真的，读即可



最后payload

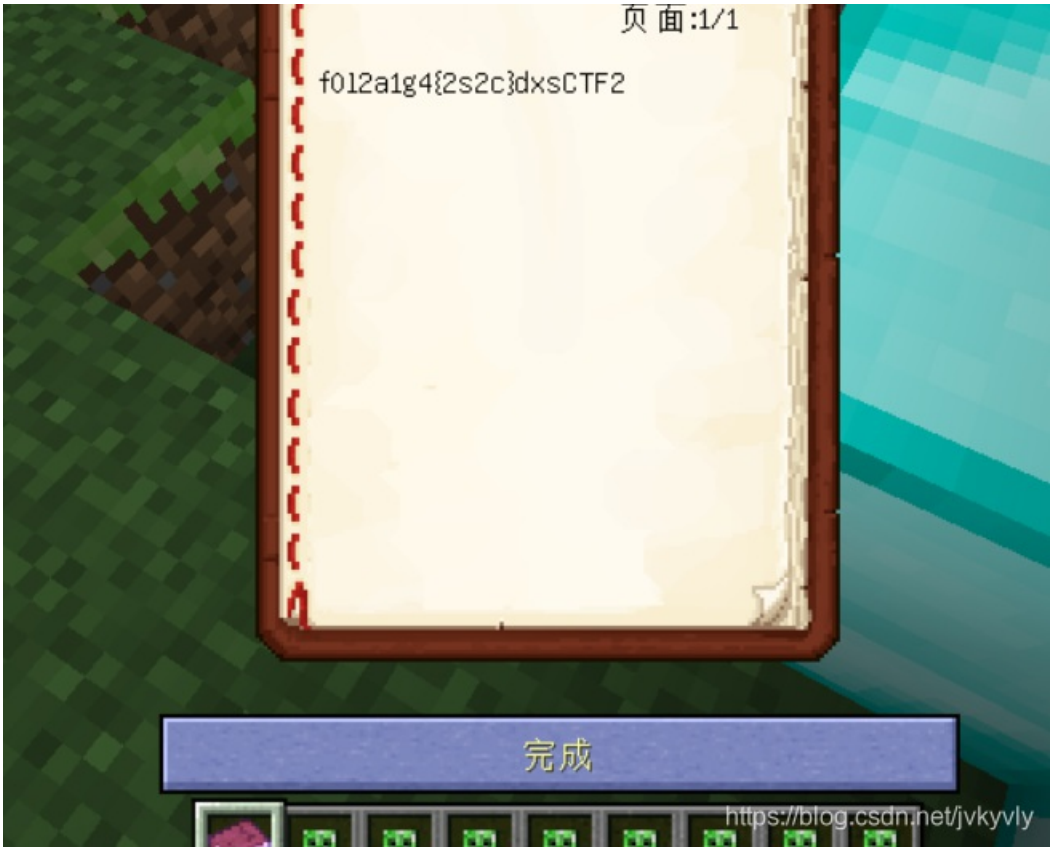
```
/main.php?a[]=1&b[]=2&c=-&d=O%3A4%3A"NoVu"%3A1%3A%7Bs%3A7%3A"command"%3Bs%3A22%3A"cat+wobushif0agaaa.txt"%3B%7D
```

```
flag{d90666230fc046c19ff11df9858702a0}
```

misc

我的世界

直接进去捡到书打开，然后栅栏密码



f012a1g4{2s2c}dxsCTF2

每组字数 14 加密 解密

f1ag{scdxsCTF2021422}

https://blog.csdn.net/jvkyvly

提交这个显示错误。。。

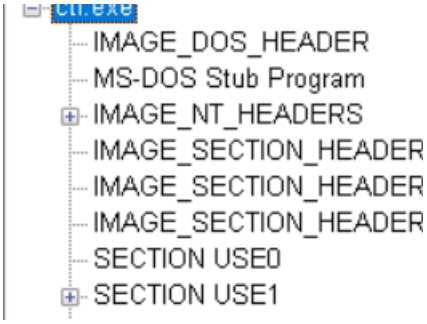
然后洞里面看的这个

牌子是有个这个，然后上面有个地图，然后感觉有猫腻，看不清，到地图上看

看到这个，尝试了一下加到flag后面，结果就对了

```
flag{scdxsCTF2021422CTF515}
```

Pack

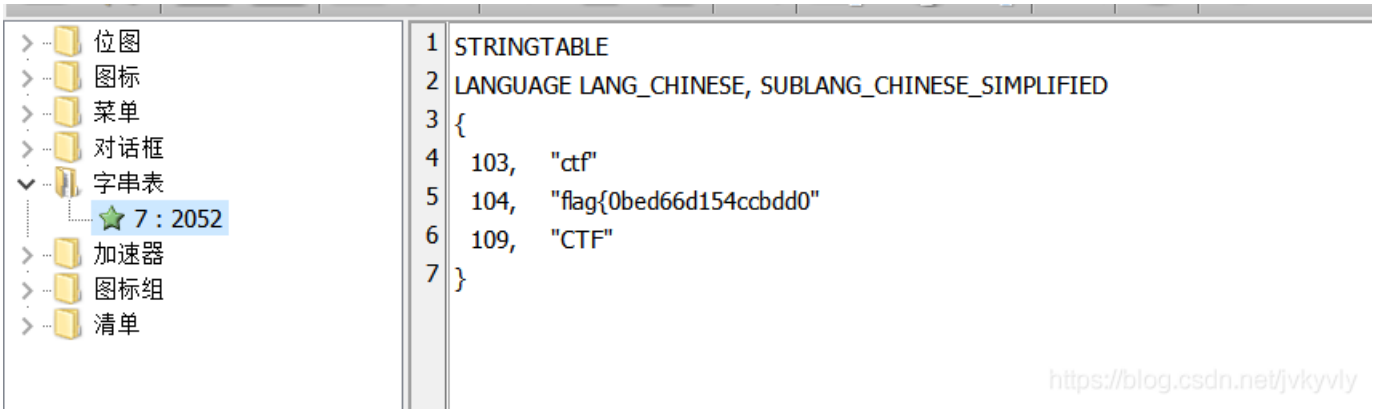


可以看到UPX节区名错了

```
1D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
1E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
1F0  55 50 58 30 00 00 00 00 00 00 0F 00 00 10 00 00  UPX0............
200  00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00  ................
210  00 00 00 00 80 00 00 E0 55 50 58 31 00 00 00 00  ....€..àUPX1....
220  00 00 05 00 00 10 0F 00 00 F2 04 00 00 04 00 00  .........ò......
230  00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 E0  ............@..à
240  2E 72 73 72 63 00 00 00 00 C0 00 00 00 10 14 00  .rsrc....À......
250  00 BE 00 00 00 F6 04 00 00 00 00 00 00 00 00 00  .¾...ö..........
```

修改保存

然后upx脱壳，再用ResourceHacker_zh.exe打开，一顿乱翻



然后还有一个皮皮虾的那个，看二进制视图，最后那有个base64

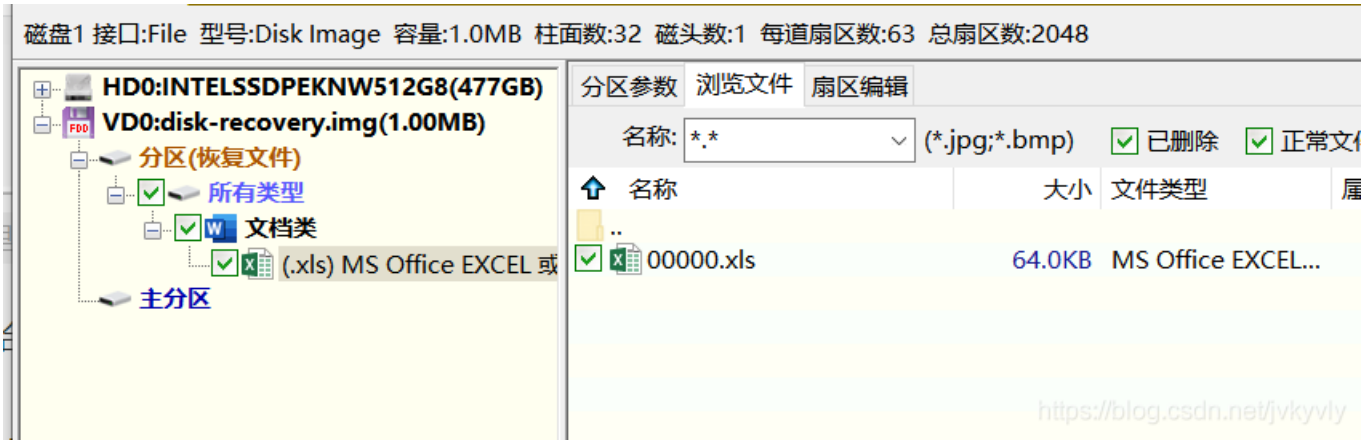
```
# N2E2MzQyYWJmOTdhNWNmY30=
```

解密组合一下即可

```
flag{0bed66d154ccbdd07a6342abf97a5cfc}
```

disk-recover

下载解压题目得到upload.pcapng文件，再用7-Zip解压，得到已损img，然后恢复



打开得到flag


```
flag{E7A10C15E26AA5750070EF756AAA1F7C}
```

RE

easy_re

脱壳，然后ida f5打开

```
  v9 = __readfsqword(0x28u);
  strcpy(v5, "'- &:8.4a 3$a&3$ 5```<");
  v6 = 0;
  v7 = 0;
  for ( i = 0; i < (unsigned __int64)j_strlen_ifunc(v5, argv); ++i )
    v8[i] = v5[i] ^ 0x41;
  return 0;
}
```

直接写脚本

```
a="'- &:8.4a 3$a&3$ 5```<"
b=''
for i in a:
    b+=chr(ord(i)^0x41)
print(b)
```

```
flag{you are great!!!}
```

base变形计

upx脱壳，然后发现是变表base，也和题目呼应，密文动调得到或者自己算也行。动调第一个输入要是42，然后输入flag，39这个字符

```
import base64
s1 = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/"
s2 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"

a=[0x50,0x67,0x72,0x62,0x50,0x19,0x79,0x1e,0x47,0x5e,0x4f,0x72,0x44,0x5d,0x5f,0x1b,0x44,0x70,0x62,0x63,0x47,0x5d
,0x47,0x72,0x45,0x5e,0x50,0x63,0x47,0x70,0x5b,0x18,0x50,0x60,0x69,0x1f,0x53,0x5d,0x4c,0x66,0x45,0x5e,0x53,0x72,0
x53,0x70,0x5b,0x7d,0x53,0x19,0x1a,0x17]
flag=""
for i in a:
    flag+=chr(42^i)

flag=base64.b64decode(flag.translate(str.maketrans(s1, s2)))
```

```
flag{you are great!!!}
```

官方wp