攻防世界 Misc高手进阶区 5分题 picture2

原创

思源湖的鱼 于 2020-12-17 12:34:10 发布 643 收藏 1

分类专栏： ctf 文章标签： ctf 攻防世界 misc UUencode

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111311012

前言

继续ctf的旅程

攻防世界Misc高手进阶区的5分题

本篇是picture2的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

给了个png

扔进stegsolve
无果

扔进winhex

```
00000000  FF D8 FF E0 00 10 4A 46  49 46 00 01 01 00 00 01  ÿØÿà  JFIF
00000016  00 01 00 00 FF DB 00 43  00 0D 09 0A 0B 0A 08 0D      ÿÛ C
00000032  0B 0A 0B 0E 0E 0D 0F 13  20 15 13 12 12 13 27 1C                '
00000048  1E 17 20 2E 29 31 30 2E  29 2D 2C 33 3A 4A 3E 33    .)10.)-,3:J>3
00000064  36 46 37 2C 2D 40 57 41  46 4C 4E 52 53 52 32 3E  6F7,-@WAFLNRSR2>
```

看文件头FFD8FF发现是jpg文件

```
00038880  40 1F FF D9 78 9C AD 50  CB 92 A2 50 0C FD 20 16
00038896  C2 15 15 16 BD 08 EF DB  80 C5 43 04 D9 79 01 2F
00038912  F2 10 10 15 E4 EB 1B 6A  A6 BB 66 37 9B 4E A5 92
00038928  93 E4 54 4E 2A 3E 07 8A  24 B9 00 B3 83 52 0E 15
00038944  3B F6 FC 28 0A 21 9D 6B  95 87 25 2E E1 84 C4 32
00038960  CE 9C 8C 5E C0 B9 97 E9  2D B7 75 44 89 B0 5D 81
00038976  61 B4 3E AB DB 9D 7C F7  C4 1E 71 C4 E1 D7 7E 57
00038992  67 BD C5 34 AE DE 6C D8  AA 98 F8 09 27 8F 6E C4
00039008  FD C1 38 A2 0D C3 D5 07  75 F7 D2 12 91 56 1B 1C
00039024  5C 2F BB 0B B7 BA 1B B8  35 BA 6A 77 EB 4C 87 30
00039040  C8 DE DE 3C EB 39 E4 81  50 93 D5 C0 49 16 B8 78
00039056  05 FF BB 53 5E 86 7F 0C  FF 20 A9 20 C8 AB 64 0A
00039072  F4 BB 01 D2 0C B5 97 42  F9 E8 CC 0E AA 40 A1 7E
00039088  E4 E2 FD 00 87 37 C8 67  64 A0 87 2D 05 6A AF 49
00039104  F4 2F 7F 5E 7D 5C B0 31  2C E2 09 68 0F 37 8B BC
00039120  86 20 9E DA 57 7E 1D B9  AC E9 14 3C 83 CD 5C EC
00039136  0C D4 5C E6 5A 71 DB 20  A9 B5 22 0E 3F F3 13 EA
00039152  A9 A9 73 AF 64 ED D2 A4  3E CE BD 0D 8B F5 7D 4E
00039168  F4 81 12 5D 9B 52 B9 DC  2A 6E 43 B1 1A B7 44 0F
00039184  28 2E C6 21 8B F6 4D 1C  8E 3D 9E 80 C1 D7 85 57
00039200  3D 63 1F 46 4B 96 5A 72  05 81 84 62 99 86 63 E5
00039216  50 D6 C4 32 D0 7F B5 C3  FA F8 26 AC D7 A6 75 35
00039232  9D 43 F1 E9 45 9F 6F B2  C6 DB 1F CE F9 97 B2 0F
00039248  82 E5 4B C3 29 DA 4F 29  12 DF B1 0C 3B F3 FB 17
00039264  00 1F 5F 8A 8C C1 92
```


看文件尾FFD9后面还有内容

foremost分离
失败

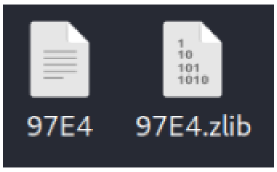
binwalk

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
38884         0x97E4          Zlib compressed data, default compression
```

导出

```
cy@kalifisher:~/ctf$ binwalk -e 1.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
38884         0x97E4          Zlib compressed data, default compression
```



打开得到一串base64


```
S1ADBBQAAQAAADkwl0xs4x98WgAAAE4AAAAEAAAAY29kZePegfAPrkdnhMG2gb86/AHHpS0GMqCrR9s21bP43SqmesL+oQGo50ljz4zIctqxIsTHV25+1mTE7vFc9gl5IUif7f1/rHIpHql7nqKPb+2M6nRLuwhU8mb/w1BLAQI/ABQAAQAAADkwl0xs4x98WgAAAE4AAAAEACQAAAAAAAAAIAAAAAAAAABjb2RlCgAgAAAAAAABABgAAFvDg4Xa0wE8gAmth9rTATyACa2H2tMBUEsFBgAAAAABAAEAVgAAAHwAAADcAFtQeXRob24gMi43XQ0KPj4+IKh9qH2ofQ0KDQpUcmFjZWJhY2sgKG1vc3QgcmVjZW50IGNhbGwgbGFzdCk6DQogIEZpbGUgIjxweXNoZWxsIzA+IiwgbGluZSAxLCBpbiA8bW9kdWxlPg0KICAgIKh9qH2ofQ0KWmVyb0RpdmlzaW9uRXJyb3I6IKh9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofSA8LSBwYXNzd29yZCA7KQ0KPj4+IAA=
```

解码

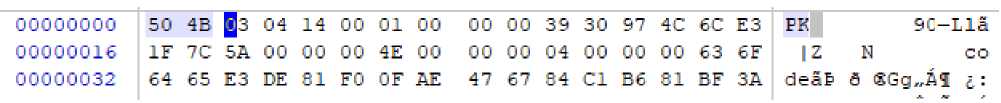
发现应该是个文件
而且开头KP
可能是PK的混淆

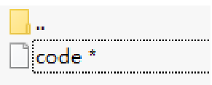
脚本保存文件

```python
import base64

t = "S1ADBBQAAQAAADkwl0xs4x98WgAAAE4AAAAEAAAAY29kZePegfAPrkdnhMG2gb86/AHHpS0GMqCrR9s21bP43SqmesL+oQGo50ljz4zIctqxIsTHV25+1mTE7vFc9gl5IUif7f1/rHIpHql7nqKPb+2M6nRLuwhU8mb/w1BLAQI/ABQAAQAAADkwl0xs4x98WgAAAE4AAAAEACQAAAAAAAAAIAAAAAAAAABjb2RlCgAgAAAAAAABABgAAFvDg4Xa0wE8gAmth9rTATyACa2H2tMBUEsFBgAAAAABAAEAVgAAAHwAAADcAFtQeXRob24gMi43XQ0KPj4+IKh9qH2ofQ0KDQpUcmFjZWJhY2sgKG1vc3QgcmVjZW50IGNhbGwgbGFzdCk6DQogIEZpbGUgIjxweXNoZWxsIzA+IiwgbGluZSAxLCBpbiA8bW9kdWxlPg0KICAgIKh9qH2ofQ0KWmVyb0RpdmlzaW9uRXJyb3I6IKh9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofah9qH2ofSA8LSBwYXNzd29yZCA7KQ0KPj4+IAA="
a = base64.b64decode(t)
with open('a', "bw") as f:
    f.write(a)
    f.close()
```

然后修改文件头





解压发现要密码
右边给了提示

```
[Python 2.7]
>>> [redacted]

Traceback (most recent call last):
  File "<pyshell#0>", line 1, in <module>
    [redacted]
ZeroDivisionError: [redacted]<- passwor
>>>
```

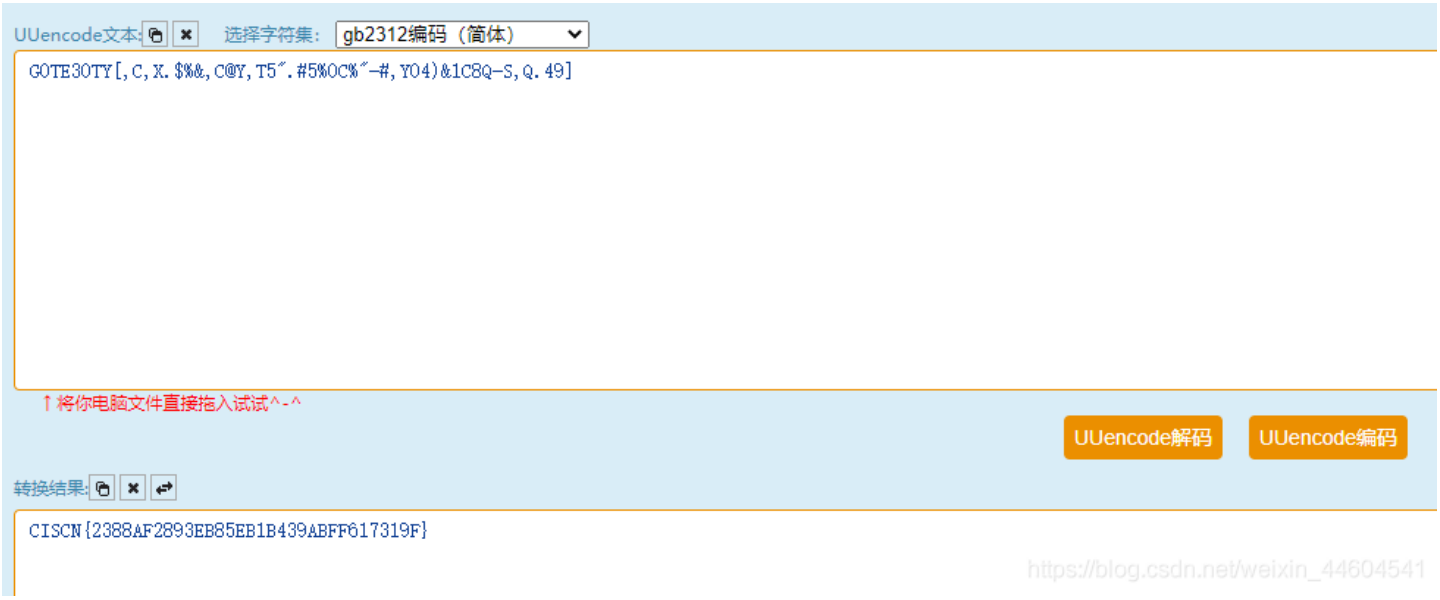
这里的报错信息是`integer division or modulo by zero`

解压得到code文件
扔进winhex

code

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	62	65	67	69	6E	20	36	34	34	20	6B	65	79	2E	74	78	begin 644 key.tx
00000016	74	0A	47	30	54	45	33	30	54	59	5B	2C	43	2C	58	2E	t G0TE30TY[,C,X.
00000032	24	25	26	2C	43	40	59	2C	54	35	22	2E	23	35	25	30	$%&,C@Y,T5".#5%0
00000048	43	25	22	2D	23	2C	59	30	34	29	26	31	43	38	51	2D	C%"-#,Y04)&1C8Q-
00000064	53	2C	51	2E	34	39	5D	0A	60	0A	65	6E	64	0A			S,Q.49] ` end

这是UUencode



得到flag

结语

知识点

- 文件头
- base64转文件
- binwalk
- UUencode