

# 攻防世界 Misc高手进阶区 6分题 Mysterious-GIF

原创

思源湖的鱼  于 2021-01-27 23:48:40 发布  442  收藏

分类专栏: [ctf](#) 文章标签: [ctf](#) [攻防世界](#) [misc](#)

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/weixin\\_44604541/article/details/113252338](https://blog.csdn.net/weixin_44604541/article/details/113252338)

版权

## CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

### 前言

继续ctf的旅程

攻防世界Misc高手进阶区的6分题

本篇是Mysterious-GIF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

题目描述

**题目描述:** Aalekh是Felicity的铁杆粉丝, 他决定根据今年的Felicity主题制作一个GIF (图形交换格式)。一个晴朗的日子, 帕思, 一个动漫爱好者给了阿列克和阿尼美什一面旗帜, 把它藏在GIF里。突然, 亚列克想起了他以前制作的GIF, 决定把国旗藏在里面。他相信国旗是如此神秘, 只有那些费利西蒂的粉丝才能找到国旗。你是费利西蒂的粉丝吗? 如果是, 那么找到flag

得到一个gif



提示了隐藏文件  
那就binwalk看看

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	GIF image data, version "89a", 440 x 608
2670386	0x28BF32	Zip archive data, at least v1.0 to extract, compressed size: 112890, uncompressed size: 112890, name: temp.zip
2783320	0x2A7858	End of Zip archive, footer length: 22
2783420	0x2A78BC	End of Zip archive, footer length: 22

得到一个zip文件  
打开报错

再次binwalk

```

kali@kali:~/ctf/_mysterious.gif.extracted$ binwalk temp.zip
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         Zip archive data, at least v1.0 to extract, compressed size: 256, uncompressed size: 256, name: parta
a.enc
404         0x194      End of Zip archive, footer length: 22
426         0x1AA      Zip archive data, at least v1.0 to extract, compressed size: 256, uncompressed size: 256, name: parta
b.enc
830         0x33E      End of Zip archive, footer length: 22
852         0x354      Zip archive data, at least v1.0 to extract, compressed size: 256, uncompressed size: 256, name: parta
c.enc
1256        0x4E8      End of Zip archive, footer length: 22
1278        0x4FE      Zip archive data, at least v1.0 to extract, compressed size: 256, uncompressed size: 256, name: parta
d.enc
1682        0x692      End of Zip archive, footer length: 22
1704        0x6A8      Zip archive data, at least v1.0 to extract, compressed size: 256, uncompressed size: 256, name: parta
e.enc
2108        0x83C      End of Zip archive, footer length: 22
2130        0x852      Zip archive data, at least v1.0 to extract, compressed size: 256, uncompressed size: 256, name: parta
f.enc
2534        0x9E6      End of Zip archive, footer length: 22
2556        0x9FC      Zip archive data, at least v1.0 to extract, compressed size: 256, uncompressed size: 256, name: parta
g.enc
2960        0xB90      End of Zip archive, footer length: 22
2982        0xBA6      Zip archive data, at least v1.0 to extract, compressed size: 256, uncompressed size: 256, name: parta
h.enc
3386        0xD3A      End of Zip archive, footer length: 22
3408        0xD50      Zip archive data, at least v1.0 to extract, compressed size: 256, uncompressed size: 256, name: parta
i.enc
3812        0xEE4      End of Zip archive, footer length: 22
3834        0xEFA      Zip archive data, at least v1.0 to extract, compressed size: 256, uncompressed size: 256, name: parta

```

发现这个zip文件是一堆enc文件  
 从partaa.enc开始一直到partke.enc  
 共265个且都是256个字节

那现在就是要找下key

在图片里找到类似以下字符串

```

00000784 | 00 0A 00 00 00 21 FE 80 34 64 34 39 34 39 34 35 | !pE4d494945
00000800 | 37 36 37 37 34 39 34 32 34 31 34 34 34 31 34 65 | 767749424144414e
00000816 | 34 32 36 37 36 62 37 31 36 38 36 62 36 39 34 37 | 42676b71686b6947
00000832 | 33 39 37 37 33 30 34 32 34 31 35 31 34 35 34 36 | 3977304241514546
00000848 | 34 31 34 31 35 33 34 33 34 32 34 62 36 62 37 37 | 41415343424b6b77
00000864 | 36 37 36 37 35 33 36 63 34 31 36 37 34 35 34 31 | 6767536c41674541
00000880 | 34 31 36 66 34 39 34 32 34 31 35 31 34 34 36 34 | 416f494241514464
00000896 | 34 64 34 65 36 32 34 63 33 35 37 31 35 36 35 37 | 4d4e624c35715657
00000912 | 36 39 34 33 35 31 37 32 00 21 FF 0B 4E 45 54 53 | 69435172 !ÿ NETS

```

```

00100768 | 00 0A 00 00 00 21 FE 80 35 38 33 32 37 37 33 36 | !pE58327736
00100784 | 33 39 37 31 32 66 33 37 37 39 33 33 35 33 36 38 | 39712f3779335368
00100800 | 34 39 35 30 37 35 36 35 37 30 37 34 37 38 36 36 | 4950756570747866
00100816 | 34 31 37 37 35 32 35 31 36 32 35 32 34 66 37 32 | 4177525162524f72
00100832 | 36 35 33 33 33 30 36 33 33 36 35 35 37 37 32 66 | 653330633655772f
00100848 | 36 66 34 62 33 38 37 37 36 35 35 61 35 34 37 38 | 6f4b3877655a5478
00100864 | 33 34 33 34 36 64 33 30 34 31 34 63 36 66 37 35 | 34346d30414c6f75
00100880 | 36 38 35 36 33 34 33 36 34 62 36 33 35 31 34 61 | 685634364b63514a
00100896 | 36 62 36 38 37 32 37 31 00 21 FF 0B 49 6D 61 67 | 6b687271 !ÿ Imag

```

汇总一下

4d494945767749424144414e42676b71686b6947397730424151454641415343424b6b776767536c41674541416f4942415144644d4e624c  
3571565769435172  
5832773639712f377933536849507565707478664177525162524f72653330633655772f6f4b3877655a547834346d30414c6f7568563436  
4b63514a6b687271  
67384f79337335593546563177434b3736367532574c775672574d49554a47316a4444725276595049635135557143703545445143696f52  
4d4763555a456732  
75766c3134324c44424161654f4c7a464d3465324a637a532b307238356d5052724353786a4c4b4c614c774949516e5a5849705853555256  
2f776a6877575231  
664a474738512b7563454170615873634e435546343462506d344850434a2f306d7244435457482f59324350564a6b4e6b2b6f305637564f  
74484b734d4c344e  
434e414a483434572f4952774a6e744e572b4e3848726770526b467567686d4e6a63776c456b7274554b4731735243792f2f57687544756e  
5632706853525176  
486f74425a76796441674d424141454367674542414a79614e336d6c6b756e772b617137704b5561677636437a6442477964394a78447941  
706b314b374f4938  
54426873464d2f33744246654131592f41762b7568434c727967726b4279652f6963372f2b30356f3853392b65674d6b52584e484b417579  
52336752696b7759  
7678454b634a676a5a5a4c524656794159372f6c477634774e42683362495044664631446739737a596e6b774948396c4c454679656d4d37  
34416941596c6371  
6456645a49452f6271325a344a4f307439484367485a4e6651374a645266656a4e4a51565955443031517535644d744f523465494d646257  
6b68625658773254  
45304837785178746a7754367a557270714576764f376533464845734249583635565258524c6276394f6f61794a786352715838654a6b52  
69344c2f597a6f34  
4b5470456d6b64754a4c58734677743361715154626a5a48584f6c5454344e45647348327030547343414543675945412f653162737a4f30  
61312b6342614451  
6a514f2b507673942734a464442336f314c47755484d4e53384644706e334a3436556b59796b353276496130763454636a715353484e4976  
585730544445556b  
624e4641314870557856786c7730426965656838426733486658795142685876645444376b306c73446d4d456f3455504b59533644356359  
577972776864356e  
4344304c72786562674f373552784c35514549452b34435649516b4367594541337638522f584b52564a5045346145656737705134755476  
6346786a454e4e65  
787866364b34787059344c6639636c49766465635268433274314864522b7853756c552f52536152727a4863773378672b4c31754f307331  
7435533766336e75  
3361696849586b636747537158435a3156487a426d65433430545673664179627337714a30785936543571384d6e78324f62355a336c4947  
7579686a65566174  
4649493253647a324a2f55436759454174654131357a516f6a53504e482b62676d62424e717465763247556a536f374932556b777243316e  
4559515334636266  
5064444364643066684d6444585534766e2b66575539686b58706d4b7043592b416363626c56554e744e4d4b6649423453484d78716a4269  
61386f31616e5a35  
726b6e6f5638576d4a4f50645a6259666478422f4b4432454434444243464756494c79417975657731506657436f64586969502f5a356a67  
742b6b4367594541  
727378716f61306f316f3975695237752b48735835494e6f5854394f4f475933715144576a55526e61435779774d756a525979355a774b36  
3930416f6f4c5253  
744e555633334b3453416868384b7153714f6830652b34636b5762354170666c38634b3561362b7638385430395838414164593550424733  
5465622b7673357a  
54704d75626c54434b4a773259617a4754385579564e38666635334e4f3951426f4533686d45796f642f4543675941396b307879434a7a63  
76654b6478727936  
706a51786b39465a7a3341744570316f635635566f776167562b4f4e657a2f4863634638474a4f384244716c5036586b634c5574736e7036  
7459526545494349  
484b7735432b667741586c4649746d30396145565458772b787a4c4a623253723667415450574d35715661756278667362356d58482f7744  
3969434c684a536f  
724b3052485a6b745062457335797444737142486435504646773d3d

显然是十六进制

转码得到

MIIEVwIBADANBgkqhkiG9w0BAQEFAASCBBKkwwggS1AgEAAoIBAQQdMNBLSqVwICQR  
X2w69q/7y3ShIPueptxfAwRQbROre30c6Uw/ok8weZTx44m0ALouhV46KcQJkhrq  
g80y3s5Y5FV1wCK766u2WLwVrWMIUJG1jDDrRvYPIcQ5UqCp5EDQCioRMGcUZEg2  
uv1142LDBAaeOLzFM4e2JczS+0r85mPRrCSxjLKLALwIIQnZXIPXSURV/wjhwWR1  
fJGG8Q+ucEApAXscNCUF44bPm4HPCJ/0mrDCTWH/Y2CPVJKnk+o0V7V0tHKsML4N  
CNAJH44W/IRwJntNW+N8HrgpRkFughmNjcw1EkrtUKG1sRCy//WhuDunV2phSRQv  
HotBZvydAgMBAAECggEBAJyaN3m1kunw+aq7pKUagv6CzdBGyd9JxDyApk1K7OI8  
TBhsFM/3tBFeA1Y/Av+uhCLrygrkBye/ic7/+05o8S9+egMkRXNHKAuyR3gRikwY  
vxEKcJgJZZLRFVYAY7/1Gv4wNBh3bIPDF1Dg9szYnkWIH91LEFyemM74AiAY1cq  
dVdZIE/bq2Z4J00t9HCgHZnfQ7JdRfejNJQVYUD01Qu5dMtOR4eIMdbWkhhbVXw2T  
E0H7xQxtjwT6zUrpqEvv07e3FHESBIX65VRXRLbv90oayJxcRqX8eJKRi4L/Yzo4  
KTPemkduJLXsFwt3aqQTbjZXH01TT4NEdsH2p0TsCAECgYEA/e1bsz00a1+cBaDQ  
jQ0+Pv9BsJFDB3o1LGuUHMNS8FDpn3J46UkYyk52vIa0v4TcjQSSHNIvXW0TDEUK  
bNFA1HpUxVx1w0Bieeh8Bg3HfXyQBhXvdTD7k01sDmMEo4UPKYS6D5cYwyrwhd5n  
CD0Lrxebg075RXL5QEIE+4CVIQkCgYEA3v8R/XKRVJPE4aEeg7pQ4uTvCFxjENNe  
xxf6K4xpY4L9c1IvdecRhC2t1HdR+xSu1U/RSaRrzHcw3xg+L1u00s1t5S7f3nu  
3aihIXkcgGSqXCZ1VHzBmeC40TVsfAybs7qJ0xY6T5q8Mnx20b5Z31IGuyhjeVat  
FII2Sdz2J/UCgYEateA15zQojsPNH+bgmbBNqtev2GUjSo7I2UkwrC1nEYQ54cbf  
PdDCdd0fhMdDXU4vn+fWU9hkXpmKpCY+Accb1VUNTnMKfIB4SHMxqjBia8o1anZ5  
rknoV8WmJOPdZbYfdxB/KD2ED4DBCFGVILyAyuew1PfwCodXiip/Z5jgt+kCgYEA  
rsxqoa0o1o9uiR7u+HsX5INoXT900GY3qQDWjURnaCwyMujRYy5ZwK690AooLRS  
tNUV33K4SAhh8KqSq0h0e+4ckWb5Apf18cK5a6+v88T09X8AAAdY5PBG3Teb+vs5z  
TpMub1TCKJw2YazGT8UyVN8ff53N09QBoE3hmEyod/ECgYA9k0xyCJzcveKdxry6  
pjQxk9FZz3AtEp1ocV5VowagV+ONez/HccF8GJ08BDq1P6XkcLUtsnp6tYReEICI  
HKw5C+fWAX1FItm09aEVTXw+xzLJb2Sr6gATPwM5qVaubxfsb5mXH/wD9iCLhJSO  
rK0RHZktPbEs5ytdsqBhd5PFFw==

这应该是key了

用openssl解密

得到一堆文件

显然是要拼的

```
cat part*>final
```

得到flag

# Flag Found:

FelicityIsFun



[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

## 结语

关键是找key