攻防世界 Crypto高手进阶区 3分题 ecb,_it's_easy_as_123

原创

思源湖的鱼 于 2020-12-11 11:15:34 发布 388 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 crypto bmp 文件头

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111030717

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Crypto高手进阶区的3分题

本篇是ecb,_it's_easy_as_123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

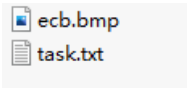
得到一个cry300文件

扔进winhex

00000000	50 4B 03 04 14 00 02 00 08 00 79 BE 37 45 C5 E2	PK y¾7EÅâ
00000016	95 8A C1 DF 00 00 90 48 3F 00 07 00 00 00 65 63	•ŠÁß H? ec
00000032	62 2E 62 6D 70 EC DD 79 58 55 D5 C2 F8 71 CD 29	b.bmpìÝyXUÕÂøqÍ)
00000048	45 D1 34 34 45 0D 4A 13 F3 15 C5 94 C1 21 EC 5A	EÑ44E J ó Å”Á!ìZ

是个zip

改后缀，解压



txt文件给出提示

Somebody leaked a still from the upcoming Happy Feet Three movie, which will be released in 4K, but Warner Bros. was smart enough to encrypt it. But those idiots used a black and white bmp format, and that wasn't their biggest mistake. Show 'em who's boss and get the flag.

而bmp图片打不开

扔进winhex

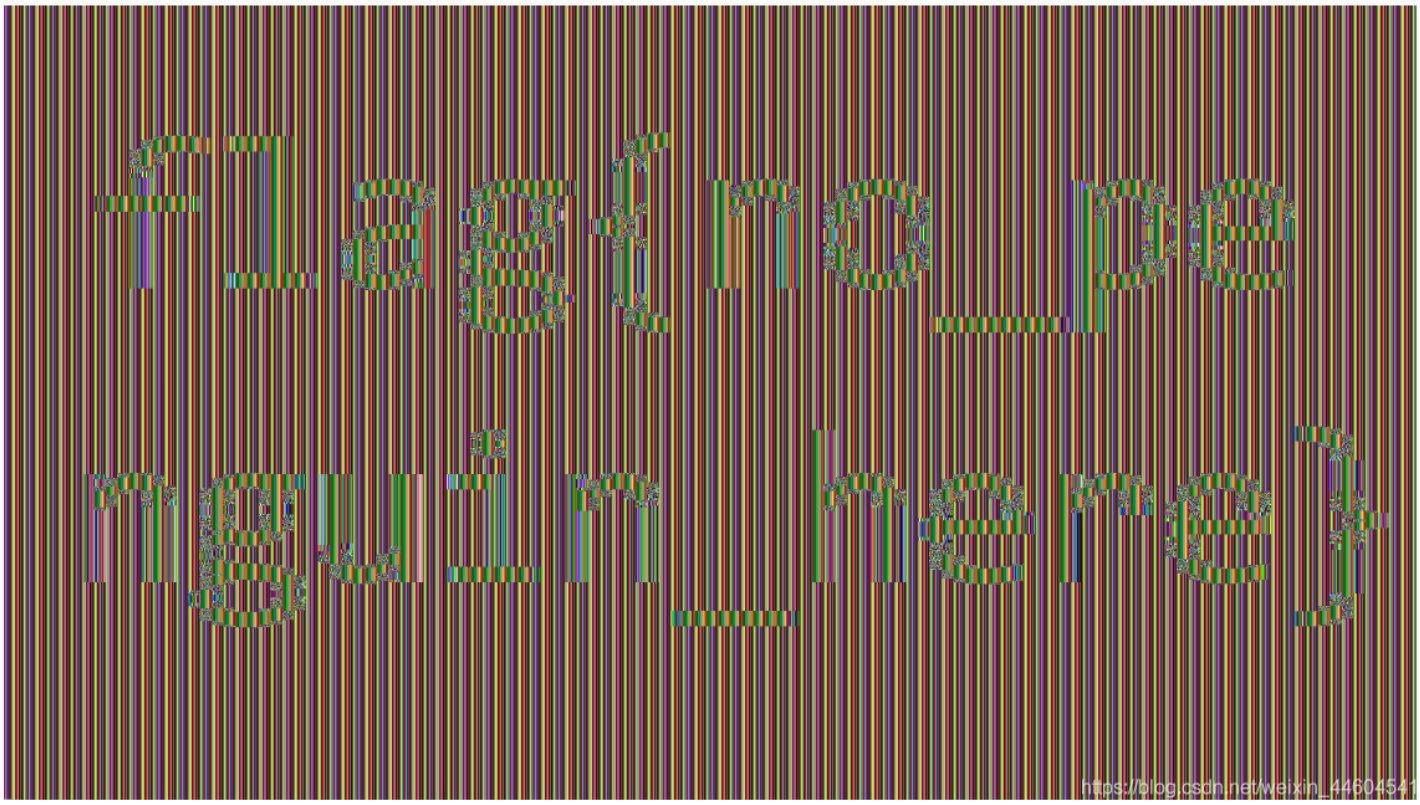
```
00000000  53 61 6C 74 65 64 5F 5F  AB 31 B5 E5 CA 3D B9 4D  Salted__«1µåÊ=¹M
00000016  F4 09 1A A5 DF 88 B7 2C  0E BD 8A 73 98 15 BA 69  ô  ¥ßˆ·, ½Šs˜ °i
00000032  A2 24 3E 09 94 CB 79 1E  EA A1 AD 33 C8 17 66 63  ¢$> "Ëy ê¡-3È fc
00000048  78 98 23 0B F0 AF 20 38  F1 AA 0B F4 69 1C EC CF  x˜# ð¯ 8ñª ôi ìÏ
00000064  FC D8 8E 3D 45 2A 99 B0  53 6B 50 0D 8A 3D C4 B7  üØŽ=E*™°SkP Š=Ä·
00000080  62 9C 6A 54 F0 59 20 13  22 4F B6 E2 B6 AA 0A 8B  bœjTðY  "O¶â¶ª ‹
00000096  5E 21 1A 9D CF 8C A2 F6  45 80 CB 9B B7 37 DA 7F  ^!  ÏŒ¢öE€Ë›·7Ú
00000112  73 50 88 CB DF 63 EE 22  D4 24 B3 B9 F4 24 AD 40  sPˆËßcî"Ô$³¹ô$-@
00000128  2F 09 E6 81 9B B5 13 88  01 FA 0A 47 78 09 65 23  / æ ›µ ˆ ú Gx e#
00000144  32 3F 8B 1E B8 20 9C 99  FC B5 46 01 0B C9 41 34  2?‹ ¸ œ™üµF  ÉA4
```

看文件头
发现被加密了

先不管加密
尝试改文件头

- 改为bmp的文件头
- 3840×2160大小
- 16色深（这里是查了wp才知道）

```
00000000  42 4D 76 48 3F 00 00 00  00 00 76 00 00 00 28 00  BMvH?     v   (
00000016  00 00 00 0F 00 00 70 08  00 00 01 00 04 00 00 00        p
00000032  00 00 00 48 3F 00 00 00  00 00 00 00 00 00 00 00     H?
00000048  00 00 00 00 00 00 00 00  00 00 00 00 80 00 00 80                 €  €
00000064  00 00 00 80 80 00 80 00  00 00 80 00 80 00 80 80     €€ €   € € €€
00000080  00 00 80 80 80 00 C0 C0  C0 00 00 00 FF 00 00 FF    €€€ ÀÀÀ   ÿ  ÿ
00000096  00 00 00 FF FF 00 FF 00  00 00 FF 00 FF 00 FF FF     ÿÿ ÿ   ÿ ÿ ÿÿ
00000112  00 00 FF FF FF 00 FF FF  FF FF FF FF FF FF FF FF    ÿÿÿ ÿÿÿÿÿÿÿÿ
```



得到flag

结语

对文件头要熟悉啊
色深是个有趣的点