

MOCTF misc 杂项 writeup (持续更新)

原创

Um0 于 2019-03-15 21:01:57 发布 503 收藏

分类专栏: [MOCTF](#) 文章标签: [ctf](#) [moctf](#) [杂项](#) [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/qq_41358038/article/details/88583930

版权



[MOCTF 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

MOCTF misc 杂项 writeup (持续更新)

1. 我可是黑客

打开之后是张图片, 查看属性等操作后无果, 扔到winhex里, 在最低端发现了flag

```
00000F20  9C CE F3 AB FA 63 F4 E6 77 9D 5F D3 11 3D 5C 31  游螳鹞翻w_?.=\1
00000F30  F8 C9 FA 73 3B CE AF E9 8F D3 99 DE 75 7F 4C 44  蟹;??.?檐u.LD
00000F40  70 C7 E0 7E 9C CE F3 AB FA 64 D3 A7 F3 07 79 2A  p?解游螳鼓纓? y*
00000F50  6F B8 8F CE 22 4E 18 FC 13 FF 00 A8 72 3F C1 AB  o?.?"N.?. ?r?莲
00000F60  EA 63 FE A1 C8 FF 00 06 AF A9 88 93 86 3F 14 6F  汛 ?..?坨?.o
00000F70  B4 37 91 F2 D1 58 3E A4 99 5A DE 98 CF B3 FF 00  ? 戲裯>?欄迺銑 .
00000F80  28 41 FC 8B A8 89 66 18 FC 45 4B 2E BA D3 BB 2D  (A轟 f. 彝K.河?
00000F90  77 F7 62 64 10 B2 30 64 62 AC 39 82 0C 44 D0 C9  w?bd.?0db?9?.D猩
00000FA0  7D F7 E4 10 6E B5 9F 5D 9B 3D 93 16 A2 25 83 A1  }?? n?焯? ? ? 餽
00000FB0  FB 39 90 F6 53 65 2E 4B 0A C8 2A 4F 80 3E 1F E9  ? .?Se.K.?*0€. ?
00000FC0  32 F4 CA 95 5A F2 AB D0 B6 87 04 13 E2 0F 84 44  2?蘆Z? 案..? 灑
00000FD0  F3 5F EE BE 97 71 F2 16 EA 12 D0 08 0C 37 A9 E3  飢糴椽? ? ? .7十
00000FE0  5E 5C 94 A8 00 C0 EB 6D D9 11 30 A0 55 E1 DD A4  ^\敷.?雖? 0?U?莖
00000FF0  D8 7D 7B 3E 92 A5 DD 2A 95 ED 2B A4 93 E1 B3 A1  豨(>扭? 蟲+?撫场
00001000  11 2E 33 74 51 C5 C1 7E 91 B8 E5 66 59 C4 BB E4  ..3tQ?羆悖鉢Y?讳
00001010  AB F8 7A 09 67 2B F5 F5 DD 5D 60 25 58 EA 78 53  ★ z.g+貂葷`%X?xS
00001020  C0 9F 33 ED 11 35 6F 74 7F FF D9 00 00 00 00 00  罈3?.5ot. ? ....
00001030  6D 6F 63 74 66 7B 65 34 73 79 5F 31 6D 61 39 65  moctf{c1cy_1m00
00001040  5F 6D 31 73 63 7D  _mlscd
```

https://blog.csdn.net/qq_41358038

2. 假装安全

又是一张图片，直接foremost一下

(大家可以在找找在Windows上使用foremost的放大，非常方便，遇到图片隐写的题可以直接foremost一下，有时候会有奇效)

分离出了一个压缩包，发现有加密。

猜测为伪加密，用winhex打开压缩包

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	50	4E	03	04	14	00	00	08	08	00	14	69	0F	4B	05	42	PK.....i.K.B
00000010	E8	C6	18	00	00	00	16	00	00	00	08	00	00	00	66	6C	杵.....f1
00000020	61	67	2E	74	78	74	CB	4D	4E	73	2E	4A	CB	A9	0C	36	ag.txt...N\$.J...6
00000030	4C	CD	2F	A9	76	48	2D	CD	89	CF	49	A9	05	00	50	4B	L?/?vH-?增I?..PK
00000040	01	02	3F	00	14	00	00	08	08	00	14	69	0F	4B	05	42	..?...i.K.B
00000050	E8	C6	18	00	00	00	16	00	00	00	08	00	24	00	00	00	杵.....\$....
00000060	00	00	00	00	20	00	00	00	00	00	00	00	66	6C	61	67flag
00000070	2E	74	78	74	0A	00	20	00	00	00	00	00	01	00	18	00	.txt.....
00000080	9F	4A	58	8E	84	15	D3	01	DC	E1	95	32	8E	0F	D3	01	焯X?? ? 莪? z.?
00000090	DC	E1	95	32	8E	0F	D3	01	50	4B	05	06	00	00	00	00	莪? ? ? PK.....
000000A0	01	00	01	00	5A	00	00	00	3E	00	00	00	00	00	00	00Z...>.....

https://blog.csdn.net/qq_41353038

将这个9改为0，发现加密去掉了，打开里面的flag.txt，得到flag（还需要栅栏解密一下）

3.扫扫出奇迹

打开之后是个经过反色处理的二维码，这里介绍两个方法

- 打开QQ，发送图片，选中，就会发现图片被反色处理了



- 利用Windows系统自带的画图工具打开，
快捷键ctrl+shift+i
进行反色处理

两种方法都能得到正确的二维码，扫出flag

4.光阴似箭

打开后是一张图片，flag不断闪过

把图片下载下来，用StegSolve打开，Analyse，Frame Browser，就能翻到flag了

5.杰斯的魔法

```
document.write(unescape('%3Cscript%20language%20%3D%20%22javascript%22%3Ealert%28%22moctf%7Bscript_ls_magical%7D%22%29%3B%3C/script%3E'));
```

解题关键在这一部分

%7B 是 { 的url编码

%7D 是 } 的url编码

flag就显而易见了