攻防世界 Crypto高手进阶区 5分题 x_xor_md5

原创

思源湖的鱼 于 2021-01-09 21:35:16 发布 387 收藏 2

分类专栏： ctf 文章标签： ctf 攻防世界 crypto md5 xor

本文链接：https://blog.csdn.net/weixin_44604541/article/details/112403221

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的5分题

本篇是x_xor_md5的writeup

发现攻防世界的题目分数是动态的

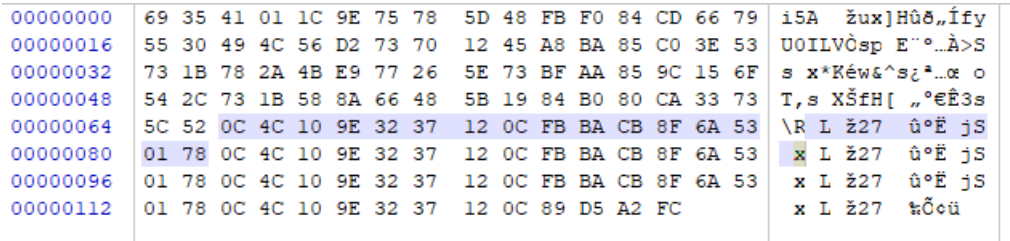
就仅以做题时的分数为准了

解题过程

题目描述

得到一个无后缀文件

扔进winhex



00000000	69 35 41 01 1C 9E 75 78 5D 48 FB F0 84 CD 66 79	i5A ž ux]Hûð„Ífy
00000016	55 30 49 4C 56 D2 73 70 12 45 A8 BA 85 C0 3E 53	U0ILVÒsp E¨º…À>S
00000032	73 1B 78 2A 4B E9 77 26 5E 73 BF AA 85 9C 15 6F	s x*Kéw&^s¿ª…œ o
00000048	54 2C 73 1B 58 8A 66 48 5B 19 84 B0 80 CA 33 73	T,s XŠfH[„°€Ê3s
00000064	5C 52 0C 4C 10 9E 32 37 12 0C FB BA CB 8F 6A 53	\R L ž27 ûºË jS
00000080	01 78 0C 4C 10 9E 32 37 12 0C FB BA CB 8F 6A 53	x L ž27 ûºË jS
00000096	01 78 0C 4C 10 9E 32 37 12 0C FB BA CB 8F 6A 53	x L ž27 ûºË jS
00000112	01 78 0C 4C 10 9E 32 37 12 0C 89 D5 A2 FC	x L ž27 ‰Õ¢ü

题目说xor

那猜测重复的就是key

拿`['01', '78', '0C', '4C', '10', '9E', '32', '37', '12', '0C', 'FB', 'BA', 'CB', '8F', '6A', '53']`
和每一行xor

得到

```
['68', '4d', '4d', '4d', '0c', '00', '47', '4f', '4f', '44', '00', '4a', '4f', '42', '0c', '2a',
'54', '48', '45', '00', '46', '4c', '41', '47', '00', '49', '53', '00', '4e', '4f', '54', '00',
'72', '63', '74', '66', '5b', '77', '45', '11', '4c', '7f', '44', '10', '4e', '13', '7f', '3c',
'55', '54', '7f', '57', '48', '14', '54', '7f', '49', '15', '7f', '0a', '4b', '45', '59', '20',
'5d', '2a', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00',
'00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00',
'00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '00',
'00', '00', '00', '00', '00', '00', '00', '00', '00', '00', '72', '6f', '69', '73']
```

转ascii
得到

```
hMMMGOODJOB*THEFLAGISNOTrctf[wE@L D@N@ <UT WH@T I@
KEY ]*rois

sandbox> exited with status 0
```

出现了ctf字样

回头审查
不应该出现0x00，0x00是绝对意义上的空，而空格 是 0x20

所以应该要和0x20异或

```
Hmmm, good job,
the flag is not RCTF{We1l_d0n3_@ut_wh4t_i5_*key}
                                                ROIS
```

ut前面这个位置不对
以及key这里多半是后面还有个星号

所以`00^2a`,那前面这个就是`1c^2a`得到36

于是得到

```
Hmmm, good job,
the flag is not RCTF{We1l_d0n3_6ut_wh4t_i5_*key*}
                                                ROIS
```

提交
错误

那在想题目里还有个md5
然后key位置应该是key

所以对`['01', '78', '0C', '4C', '10', '9E', '32', '37', '12', '0C', 'FB', 'BA', 'CB', '8F', '6A', '53']`
进行md5解密
得到`['21', '58', '2c', '6c', '30', 'be', '12', '17', '32', '2c', 'db', '9a', 'eb', 'af', '4a', '73']`
ascii得到`that`

所以flag是`RCTF{We1l_d0n3_6ut_wh4t_i5_that}`

结语

还是查了wp才做出来