

攻防世界 Misc高手进阶区 3分题 5-1

原创

[思源湖的鱼](#) 于 2020-11-30 10:55:15 发布 529 收藏

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

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/110378348

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3分题

本篇是5-1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

下下来一个无后缀文件

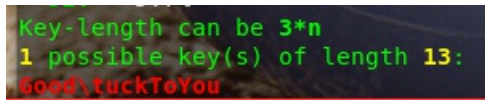
扔进winhex

00000000	13 07 0A 44 23 05 06 05	3D 01 3E 4F 19 2E 01 0A	D# = >O .
00000016	44 23 13 43 1F 3C 0A 79	01 1A 31 0A 03 44 2A 14	D# C < y 1 D*
00000032	0E 04 21 1C 35 16 55 26	01 01 0B 39 1B 00 0E 27	! 5 U& 9 '
00000048	55 79 4D 3C 33 4F 06 17	6C 14 43 1F 26 1A 2D 07	UyM<3O 1 C & -
00000064	55 32 01 06 12 29 07 10	0A 38 03 20 4F 14 24 04	U2) 8 O \$
00000080	01 0B 3B 19 06 0F 33 0A	3D 43 55 33 07 0E 10 6C	; 3 =CU3 1
00000096	14 43 18 3D 01 3E 03 10	67 02 0E 0A 6C 1C 0D 4B	C = > g 1 K
00000112	24 00 2A 1C 10 34 1C 06	0B 22 55 0C 0D 74 0E 79	\$ * 4 "U t y
00000128	08 1A 28 0B 4F 02 23 07	17 1E 3A 0A 79 02 00 34	(O # : y 4
00000144	1B 4F 06 29 55 0A 05 74	18 38 01 01 67 00 09 44	O)U t 8 g D
00000160	2D 55 14 02 32 0A 77 4D	55 13 07 06 17 6C 06 06	-U 2 wMU 1
00000176	1F 27 4F 34 0E 07 35 06	0E 03 29 55 02 18 74 0E	'O4 5)U t
00000192	79 0C 10 29 1B 1D 05 20	55 10 1E 36 05 3C 0C 01	y) U 6 <
00000208	A5 EF FB 05 22 11 43 19	31 0E 35 03 0C 6B 4F 0E	¥iû " C 1 5 kO
00000224	44 2F 10 0D 1F 26 0E 35	4F 05 35 00 0D 08 29 18	D/ & 5O 5)
00000240	81 EB C0 09 36 1D 55 33	07 0A 44 22 1A 15 0E 38	èÀ 6 U3 D" 8
00000256	4F 3E 0A 1B 22 1D 0E 08	20 0C 4D 4B 06 0A 38 0B	O> " MK 8
00000272	10 35 1C 4F 05 3E 10 43	1B 3B 06 2A 0A 11 67 1B	5 O > C ; * g
00000288	00 44 3D 00 06 18 20 06	36 01 55 30 07 0A 10 24	D= 6 UO \$
00000304	10 11 4B 3B 1D 79 01 1A	33 4F 1B 0C 29 06 06 4B	K; y 3O) K
00000320	27 06 37 08 19 22 4F 02	01 22 55 02 19 31 43 79	' 7 "O "U lCy
00000336	06 1B 67 09 0E 07 38 59	43 02 3A 4F 2E 0E 1B 33	g 8YC :O. 3
00000352	4F 00 02 6C 14 43 1C 3D	09 3C 43 55 28 1D 4F 0D	O 1 C = <CU(C
00000368	2A 55 10 1E 37 07 79 0B	10 34 06 1D 01 3F 55 02	*U 7 y 4 ?U
00000384	19 31 4F 3D 06 16 33 0E	1B 01 28 55 01 12 74 1B	1O= 3 (U t
00000400	31 0A 55 65 01 0A 0D 2B	1D 01 04 21 1D 31 00 1A	1 Ue + ! 1
00000416	23 4D 4F 02 2D 18 0A 07	3D 0A 2A 4F 14 29 0B 4F	#MO - = *O) O
00000432	10 24 10 0A 19 74 0B 38	1A 12 2F 1B 0A 16 3F 55	\$ t 8 / ?U
00000448	14 03 3B 4F 2B 0A 04 32	06 1D 01 6C 14 43 49 33	;O+ 2 1 CI3
00000464	00 36 0B 55 21 00 1D 10	39 1B 06 49 7A 4F 14 0E	6 U! 9 IzO
00000480	07 35 06 0E 03 29 55 0A	18 74 0E 79 0C 1A 2A 1F	5)U t y *
00000496	03 01 34 55 10 04 37 06	38 03 55 26 0C 1B 0D 3A	4U 7 8 U& :
00000512	1C 17 12 74 1B 31 0E 01	67 1B 0E 0F 29 06 43 1B	t 1 g) C
00000528	3B 03 30 1B 1C 24 0E 03	44 29 16 0C 05 3B 02 20	; 0 \$- D) ;

未知类型

查了查

用的是xortool



得到key: GoodLuckToYou

于是对文件做xor

```
key = 'GoodLuckToYou'
flag = ''
with open('1') as f:
    con = f.read()
    for i in range(len(con)):
        flag += chr(ord(con[i]) ^ ord(key[i%13]))
f = open('flag.txt', 'w')
f.write(flag)
f.close()
```

得到flag

结语

认识了新工具

- [xortool](#)



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)