

攻防世界 Crypto高手进阶区 3分题 你猜猜

原创

思源湖的鱼  于 2020-12-08 13:06:57 发布  235  收藏

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

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/110870973

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Crypto高手进阶区的3分题

本篇是你猜猜的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

得到一串16进制

```
504B03040A0001080000626D0A49F4B5091F1E0000001200000008000000666C61672E7478746C9F170D35D0A45826A03E161FB96870EDDF
C7C89A11862F9199B4CD78E7504B01023F000A0001080000626D0A49F4B5091F1E00000012000000080024000000000000200000000000
0000666C61672E7478740A002000000000001001800AF150210CAF2D1015CAEAA05CAF2D1015CAEAA05CAF2D101504B050600000000100
01005A000000440000000000
```

看到开头 `504B0304`

就知道是个zip文件

用winhex保存为zip文件

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
00000000	50	4B	03	04	0A	00	01	08	00	00	62	6D	0A	49	F4	B5	PK	bm Iôµ
00000016	09	1F	1E	00	00	00	12	00	00	00	08	00	00	00	66	6C		f1
00000032	61	67	2E	74	78	74	6C	9F	17	0D	35	D0	A4	58	26	A0	ag.txtlÿ	5ÐHX&
00000048	3E	16	1F	B9	68	70	ED	DF	C7	C8	9A	11	86	2F	91	99	>	'hpi&ÇÈš +/'™
00000064	B4	CD	78	E7	50	4B	01	02	3F	00	0A	00	01	08	00	00	'ixçPK	?
00000080	62	6D	0A	49	F4	B5	09	1F	1E	00	00	00	12	00	00	00	bm Iôµ	
00000096	08	00	24	00	00	00	00	00	00	00	20	00	00	00	00	00	\$	
00000112	00	00	66	6C	61	67	2E	74	78	74	0A	00	20	00	00	00	flag.txt	
00000128	00	00	01	00	18	00	AF	15	02	10	CA	F2	D1	01	5C	AE	-	ÈòÑ \@
00000144	AA	05	CA	F2	D1	01	5C	AE	AA	05	CA	F2	D1	01	50	4B	* ÈòÑ \@*	ÈòÑ PK
00000160	05	06	00	00	00	00	01	00	01	00	5A	00	00	00	44	00	Z	D
00000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00000208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		

1.zip (评估版本)

文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)

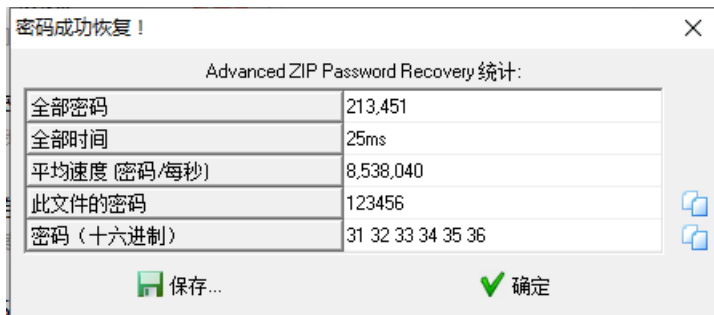


1.zip - ZIP 压缩文件, 解包大小为 18 字节

名称	大小	压缩后大小
..		
flag.txt *	18	30

解压发现要密码

用ZAPR爆破



flag - 记事本

文件(F) 编辑(E) 格式(O) 查看

daczcasdqwcdsdzasd

得到flag

结语

这应该放到misc中