攻防世界——你猜猜

原创

Irving- 于 2021-01-18 13:59:58 发布 392 收藏 2

分类专栏： 题解

本文链接：https://blog.csdn.net/weixin_51867782/article/details/112776754

题解 专栏收录该内容

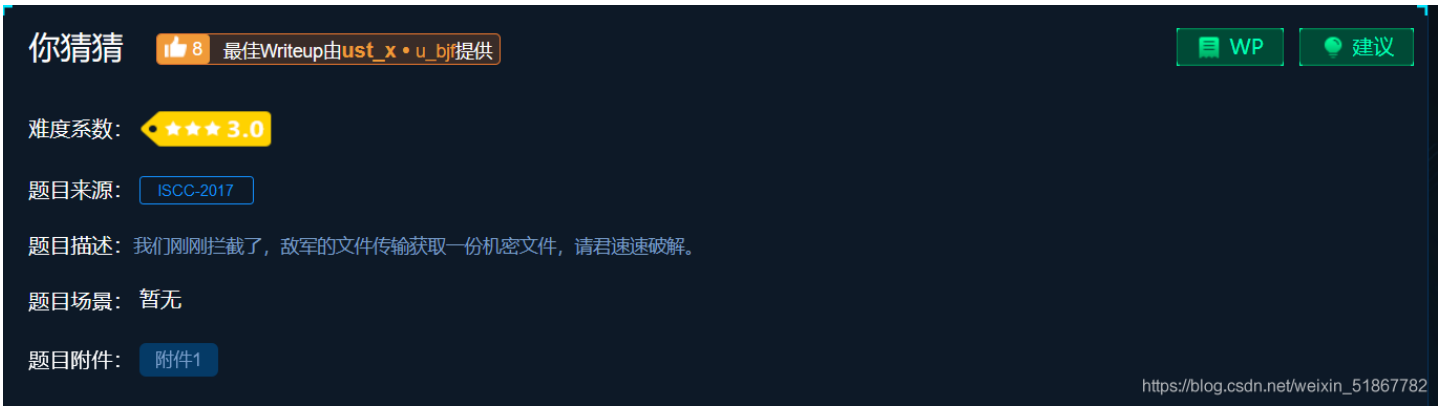
8 篇文章 0 订阅

订阅专栏

攻防世界——你猜猜

原理：zip文件头，zip密码暴力破解

工具：winhex,Ziperello



拿到文件后，发现是504B0304开头的。这是zip文件头，打开winhex，将那段16进制复制进去，选择ASCⅠⅠHEX

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0000000	50	4B	03	04	0A	00	01	08	00	00	62	6D	0A	49	F4	B5	PK bm Iôµ
0000010	09	1F	1E	00	00	00	12	00	00	00	08	00	00	00	66	6C	fl
0000020	61	67	2E	74	78	74	6C	9F	17	0D	35	D0	A4	58	26	A0	ag.txtl▌ 5Ð¤X&
0000030	3E	16	1F	B9	68	70	ED	DF	C7	C8	9A	11	86	2F	91	99	> ¹hpíßÇÈ▌ ▌/'▌
0000040	B4	CD	78	E7	50	4B	01	02	3F	00	0A	00	01	08	00	00	´ÍxçPK ?
0000050	62	6D	0A	49	F4	B5	09	1F	1E	00	00	00	12	00	00	00	bm Iôµ
0000060	08	00	24	00	00	00	00	00	00	00	20	00	00	00	00	00	$
0000070	00	00	66	6C	61	67	2E	74	78	74	0A	00	20	00	00	00	flag.txt
0000080	00	00	01	00	18	00	AF	15	02	10	CA	F2	D1	01	5C	AE	¯ ÊòÑ \®
0000090	AA	05	CA	F2	D1	01	5C	AE	AA	05	CA	F2	D1	01	50	4B	ª ÊòÑ \®ª ÊòÑ PK
00000A0	05	06	00	00	00	00	01	00	01	00	5A	00	00	00	44	00	Z D
00000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

保存该文件得到一个压缩包flag.zip。打开后发现有密码。用Ziperello破解，得到密码为123456，输入，得到flag：daczcasdqwdcsdzasd