

xctf攻防世界 MISC高手进阶区 János-the-Ripper

原创

18947943 于 2022-01-13 15:58:13 发布 190 收藏

分类专栏: [攻防世界misc之路](#) 文章标签: [安全 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/18947943/article/details/122475798>

版权



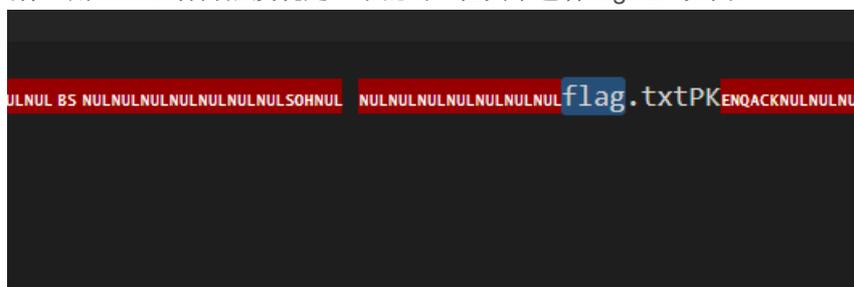
[攻防世界misc之路](#) 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

1. 打开环境, 下载附件

是一个misc100无后缀的文件, 用vscode打开后发现是一堆乱码, 但其中包含flag.txt, 如图:



2. 问题分析

1. 使用winhex打开文件

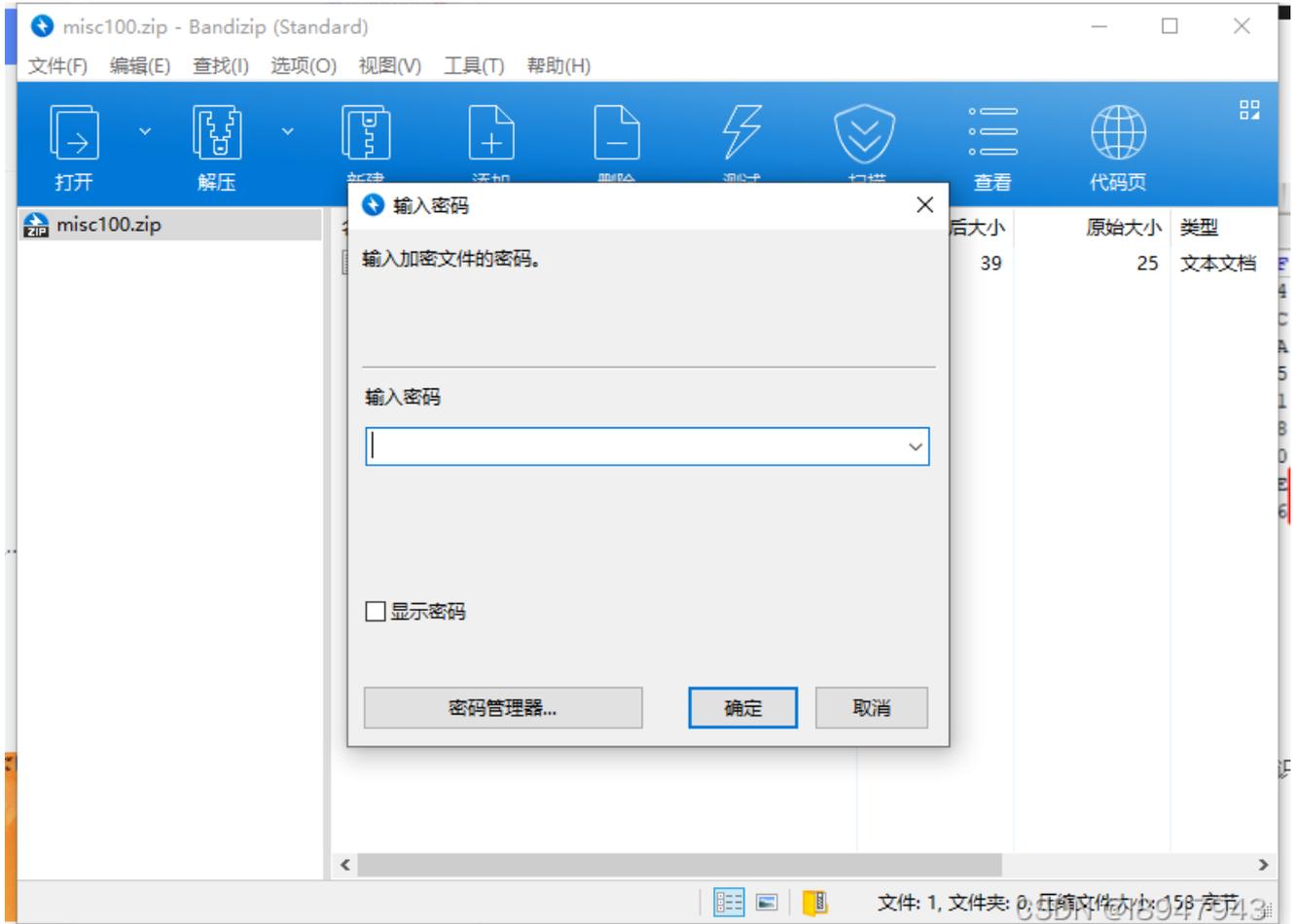
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII
00000000	50	4B	03	04	14	00	03	00	08	00	0E	A2	77	44	44	D4	PK	ewDDÔ
00000010	88	77	27	00	00	00	19	00	00	00	08	00	00	00	66	6C	^w'	fl
00000020	61	67	2E	74	78	74	00	10	01	4B	93	FF	03	EE	9C	FA	ag.txt	K"y iœú
00000030	D3	12	83	A1	57	88	57	8C	BF	41	AA	41	87	16	F6	85	Ó f;W^WQ;A^A† ö...	
00000040	FE	40	02	DA	73	CA	1F	AC	16	97	89	44	3A	50	4B	01	b@ ÚsÊ - -%D:PK	
00000050	02	14	00	14	00	03	00	08	00	0E	A2	77	44	44	D4	88	ewDDÔ^	
00000060	77	27	00	00	00	19	00	00	00	08	00	00	00	00	00	00	w'	
00000070	00	01	00	20	00	00	00	00	00	00	00	66	6C	61	67	2E	flag.	
00000080	74	78	74	50	4B	05	06	00	00	00	00	01	00	01	00	36	txtPK	6
00000090	00	00	00	4D	00	00	00	00	00								M	

CSDN @18947943

我们可以看到文件的开头为 504B, PK开头的文件, 我们知道这个开头的标识是zip文件, 详见: [各类文件的文件头标志](#)

改为zip文件

我们将文件修改成zip结尾的，发现需要解压密码，如图：



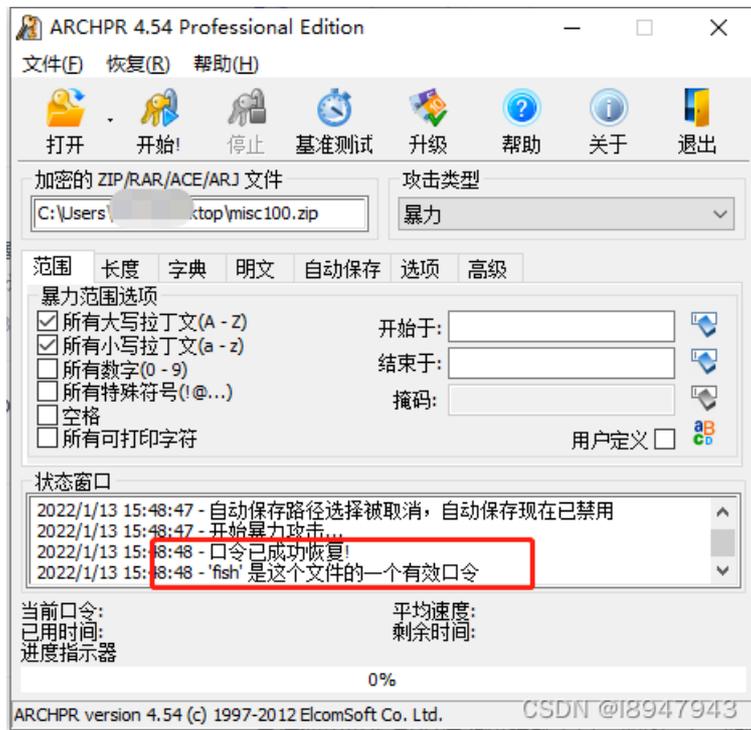
winhex中并没有伪加密，说明需要进行暴力破解。

掏出ARCHPR

附带工具下载链接：<https://zhangfa.lanzouw.com/iQmy8yq3tuh>

或者GitHub上下载：<https://github.com/cnsuhao/Advanced-Archive-Password-Recovery-Professional-Edition>

直接使用ARCHPR压缩包破解工具，如图，得到解压码'fish'，如图：



我们将zip解压，得到flag.txt。最终的答案为：`flag{ev3n::y0u::bru7us?!}`