

# 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](#)

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\\_51867782/article/details/112776754](https://blog.csdn.net/weixin_51867782/article/details/112776754)

版权



[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

### 你猜猜

👍 8 最佳Writeup由ust\_x·u\_bj提供

难度系数: ★★★★★ 3.0

题目来源: ISCC-2017

题目描述: 我们刚刚拦截了, 敌军的文件传输获取一份机密文件, 请君速速破解。

题目场景: 暂无

题目附件: 附件1

[https://blog.csdn.net/weixin\\_51867782](https://blog.csdn.net/weixin_51867782)

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ASC I I HEX

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

选择剪贴板格式

- Unicode
- ANSI-ASCII
- IBM-ASCII
- ASCII Hex**

[https://blog.csdn.net/weixin\\_51867782](https://blog.csdn.net/weixin_51867782)

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		f1
0000020	61	67	2E	74	78	74	6C	9F	17	0D	35	D0	A4	58	26	A0	ag.txt1	5D*X&
0000030	3E	16	1F	B9	68	70	ED	DF	C7	C8	9A	11	86	2F	91	99	>	'hpiBÇÈ   /'
0000040	B4	CD	78	E7	50	4B	01	02	3F	00	0A	00	01	08	00	00	'ixçPK ?	
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	-	ÈòÑ \@
0000090	AA	05	CA	F2	D1	01	5C	AE	AA	05	CA	F2	D1	01	50	4B	è ÈòÑ \@è ÈòÑ PK	
00000A0	05	06	00	00	00	00	01	00	01	00	5A	00	00	00	44	00		Z 867782
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。打开后发现密码。用Ziperello破解，得到密码为123456，输入，得到flag: daczcasdqwdcsdzasd

The screenshot shows the Ziperello application window. The title bar reads "Ziperello". The main window has a blue header with the logo and the text "ziperello zip password recovery tool". On the right side of the header are buttons for "帮助" (Help), "关于" (About), and "退出" (Exit). The main content area is divided into two sections. The left section contains input fields for "当前密码长度" (Current password length) set to 0, "当前密码" (Current password) set to "123456", and "当前速度" (Current speed) set to "当前速度". Below these is a progress bar showing 0% completion, with "逝去时间: 00:00:00" (Elapsed time) and "剩余时间: 00:00:00" (Remaining time) labels. At the bottom of this section are "开始" (Start) and "停止" (Stop) buttons. The right section is titled "步骤 4" (Step 4) and contains the text: "准备就绪，请点击 [开始] 按钮" (Ready, please click the [Start] button) and a note: "注意：搜索进度条 (%) 及剩余时间字段显示的信息与当前的密码校验长度相关。破解 AES 算法加密的密码可能耗时较长。" (Note: The search progress bar (%) and remaining time field display information related to the current password verification length. Cracking AES algorithm encrypted passwords may take a long time). At the bottom of the window, there is a status bar with a "BACK" button, the text "步骤 4 / 4: 破解密码.Go", a URL "https://blog.csdn.net/wetxrx51267782", and a refresh icon.