

攻防世界crypto高手题之你猜猜

原创

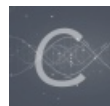
沐一·林 于 2021-09-08 16:45:12 发布 116 收藏 1

分类专栏: [CTF 密码学](#) 文章标签: [ctf](#)

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/xiao__1bai/article/details/120179268

版权



CTF 同时被 2 个专栏收录

167 篇文章 6 订阅

订阅专栏



密码学

51 篇文章 1 订阅

订阅专栏

攻防世界crypto高手题之你猜猜

继续开启全栈梦想之逆向之旅~

这题是攻防世界crypto高手题的你猜猜

你猜猜

👍 14 最佳Writeup由 [w1relesslab](#) · wffx提供

WP 建议

难度系数: ★★ 2.0

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

CSDN @沐一一沐, 一沐沐一

下载附件, 是一个.txt文件, 打开, 数字和字母:

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

往base家族想, 字母只有A~F, base16解码:

00AF150210CAF2D1015CAEAA05CAF2D1015CAEAA05CAF2D101504B05060000000010001005A000000440000000000

16进制转字符 字符转16进制 测试用例 清空结果 复制结果

广告 X

互动直播SDK

anyRTC音视频 SDK, 四行代码, 30分钟, 即可快速实现语音通话、直播等场景, 每月一万分钟免费。 anyRTC

打开

```

1 PK..
2 .....bm
3 |.....flag.txt|阶X& \ p T 鳶x瑞..?
4 .....bm
5 |.....$.....flag.txt
6 .....c\殼\殼.PK.....Z...D.....

```

CSDN @沐一一沐, 一沐沐一

(这里积累第一个经验)

嗯~好熟悉, 后来想起来是web题中bp抓过的数据, 查了资料发现是一个zip文件的16进制数据, 竟然这么短也能组成zip的数据, 也是开了眼界, zip里面也可以看到有个flag.txt文件。

一开始还直接修改成.zip后缀, 真是太天真了, 这是把hex数据放入txt文件啊。

打开winhex64复制粘贴成zip文件即可:

WinHex - [1.zip]

文件(E) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(I) 专业工具(I) 选项(O) 窗口(W) 帮助(H)

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII
00000000	50	4B	03	04	0A	00	01	08	00	00	62	6D	0A	49	F4	B5	PK	bm Iôµ
00000010	09	1F	1E	00	00	00	12	00	00	00	08	00	00	00	66	6C		fl
00000020	61	67	2E	74	78	74	6C	9F	17	0D	35	D0	A4	58	26	A0	ag.txtlÿ	5Ð=X&
00000030	3E	16	1F	B9	68	70	ED	DF	C7	C8	9A	11	86	2F	91	99	>	'hpißÇÈš +/\`™
00000040	B4	CD	78	E7	50	4B	01	02	3F	00	0A	00	01	08	00	00	'íxçPK	?
00000050	62	6D	0A	49	F4	B5	09	1F	1E	00	00	00	12	00	00	00	bm Iôµ	
00000060	08	00	24	00	00	00	00	00	00	00	20	00	00	00	00	00	\$	
00000070	00	00	66	6C	61	67	2E	74	78	74	0A	00	20	00	00	00	flag.txt	
00000080	00	00	01	00	18	00	AF	15	02	10	CA	F2	D1	01	5C	AE	-	ÈòÑ \@
00000090	AA	05	CA	F2	D1	01	5C	AE	AA	05	CA	F2	D1	01	50	4B	* ÈòÑ \@*	ÈòÑ PK
000000A0	05	06	00	00	00	00	01	00	01	00	5A	00	00	00	44	00	Z	D
000000B0	00	00	00	00														

CSDN @沐一一沐, 一沐沐一

解密的时候发现需要密码，也不是zip伪加密。嗯~查了资料，上网下载了Zipperello来爆破密码，密码组成只能一个个试了：



输入密码(E)

显示密码(S)

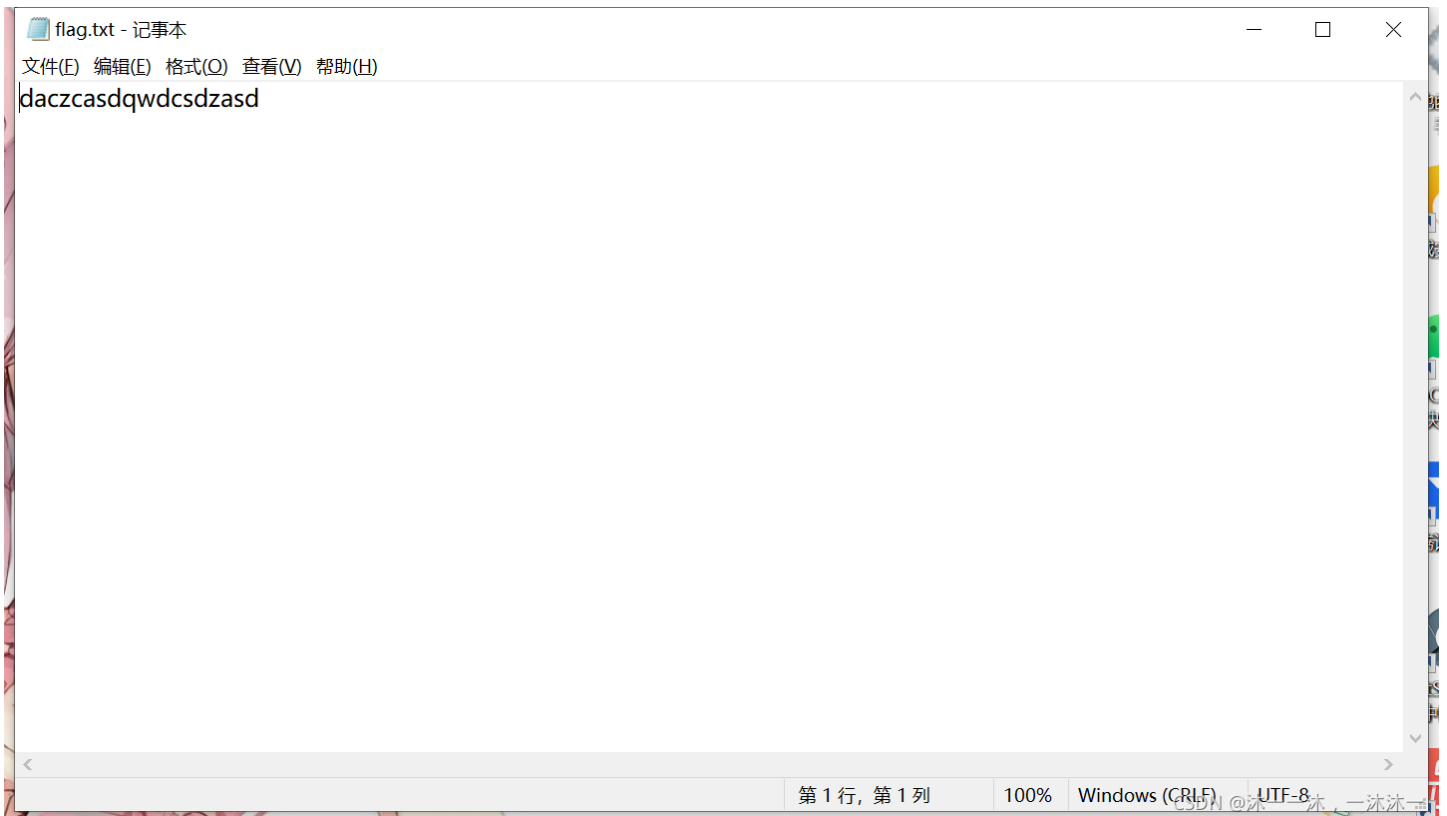
用于所有压缩文件(A)

整理密码(O)...

CSDN @沐一一沐，一沐沐一



拿到了密码123456，解压得到flag:



总结:

1:

(这里积累第一个经验)

嗯~好熟悉，后来想起来是web题中bp抓过的数据，查了资料发现是一个zip文件的16进制数据，竟然这么短也能组成zip的数据，也是开了眼界，zip里面也可以看到有个flag.txt文件。

一开始还直接修改成.zip后缀，真是太天真了，这是把hex数据放入txt文件啊。

解毕！敬礼！