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

本文链接：https://blog.csdn.net/xiao__1bai/article/details/120179268

CTF 同时被 2 个专栏收录

167 篇文章 6 订阅

订阅专栏

密码学

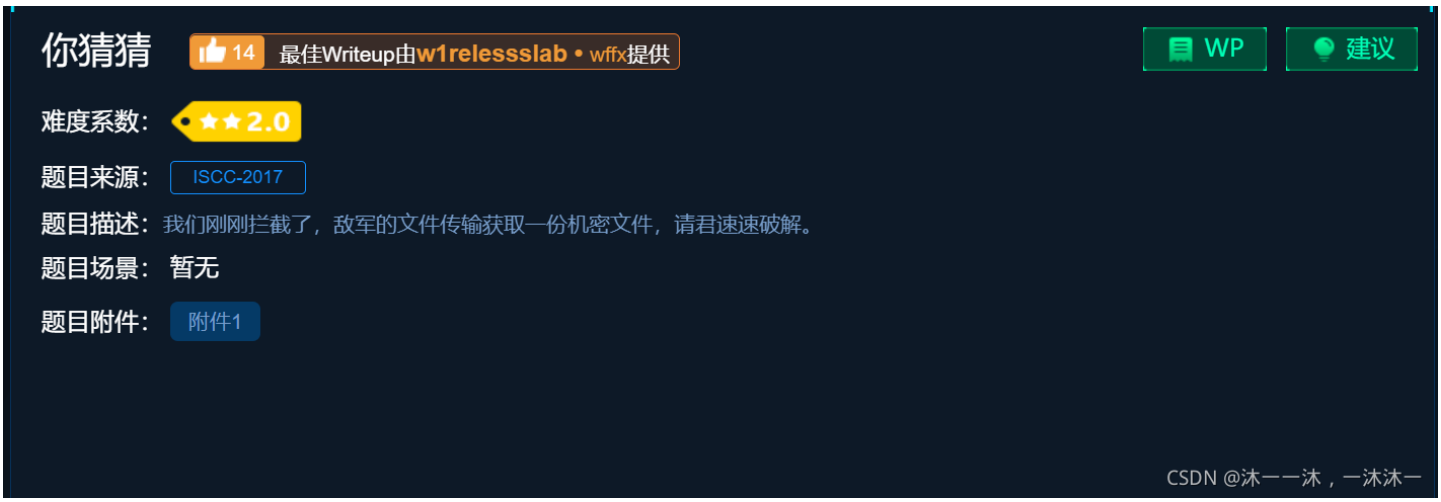
51 篇文章 1 订阅

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



.

.

下载附件，是一个.txt文件，打开，数字和字母：

```
504B03040A0001080000626D0A49F4B5091F1E0000001200000008000000666C61672E7478746C9F170D35D0A45826A03E161FB96870EDDF
C7C89A11862F9199B4CD78E7504B01023F000A0001080000626D0A49F4B5091F1E0000001200000008002400000000000000200000000000
0000666C61672E7478740A0020000000000000001001800AF150210CAF2D1015CAEAA05CAF2D1015CAEAA05CAF2D101504B050600000000100
01005A000000440000000000
```

.

.

往base家族想，字母只有A~F，base16解码：

00AF150210CAF2D1015CAEAA05CAF2D1015CAEAA05CAF2D101504B0506000000000100010058000000440000000000

16进制转字符 | 字符转16进制 | 测试用例 | 清空结果 | 复制结果


```
PK••
•••••bm
l剻••••••••••••flag.txtl吩X& \ p[8]Ţ•鶿x琋••?•
•••••bm
l剻••••••••••$••••••• •••••••flag.txt
• •••••••••ic\孮•\孮•PK••••••••••Z•••D•••••
```


.

.

(这里积累第一个经验)

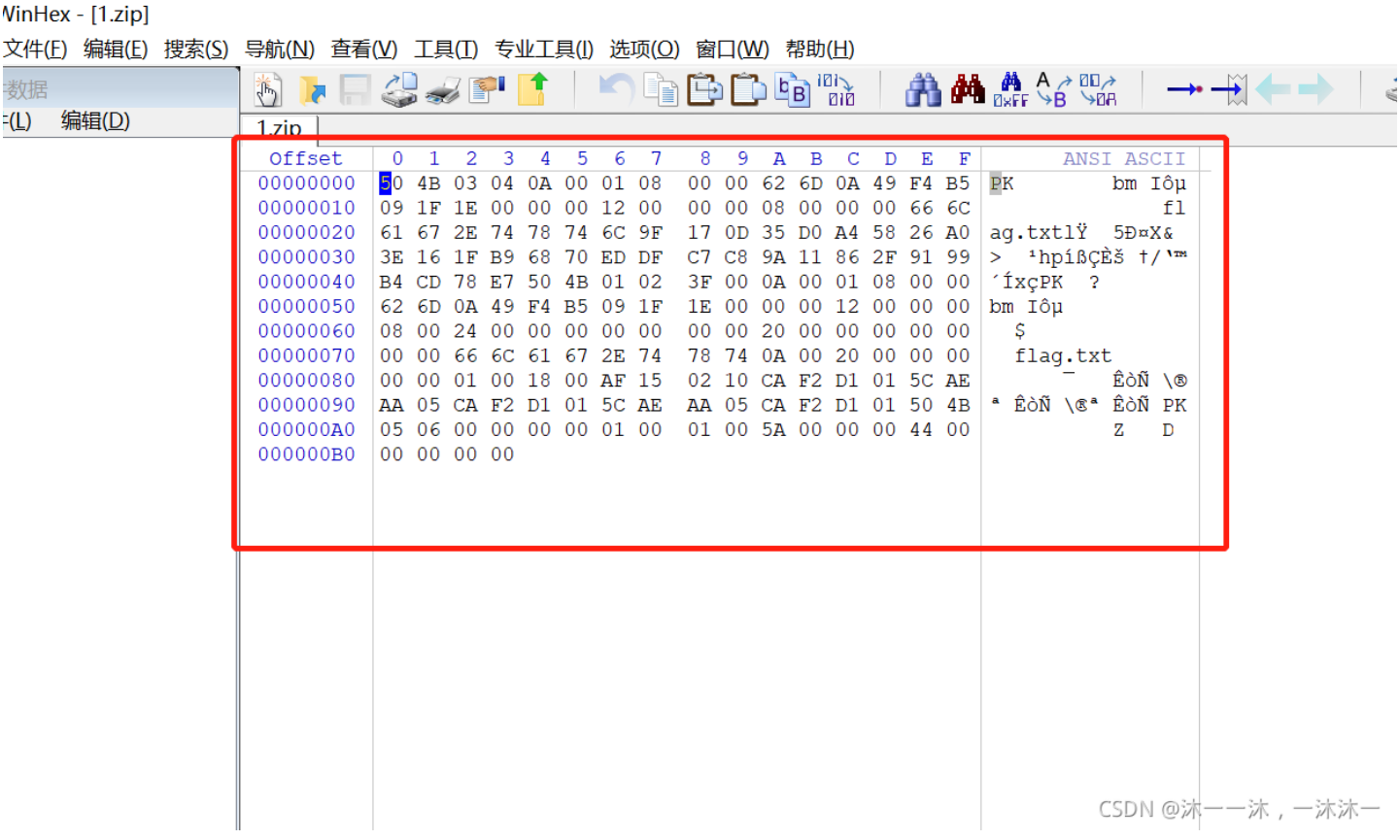
嗯~好熟悉，后来想起来是web题中bp抓过的数据，查了资料发现是一个zip文件的16进制数据，竟然这么短也能组成zip的数据，也是开了眼界，zip里面也可以看到有个flag.txt文件。

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：



.

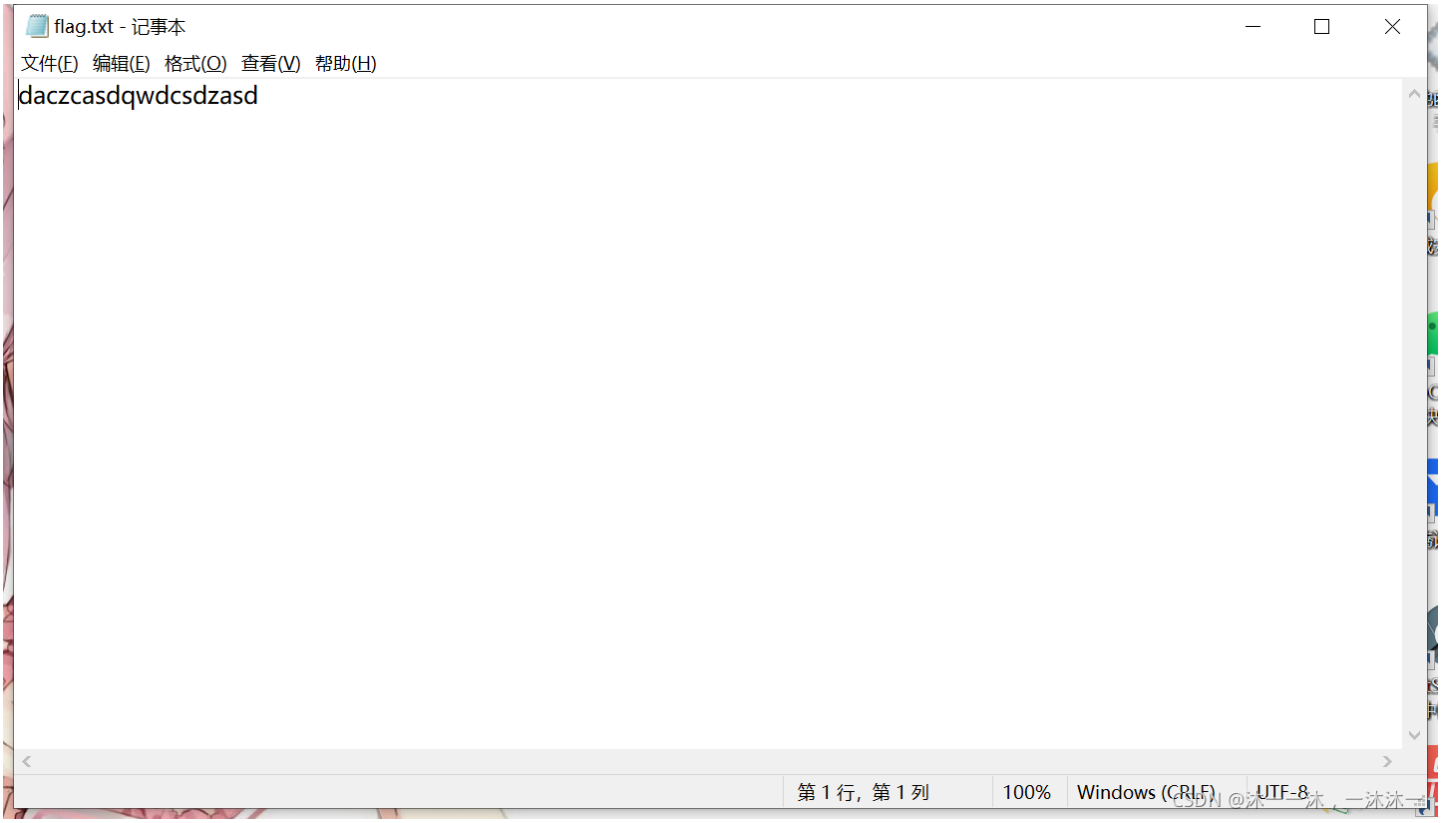
.

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Ziperello来爆破密码，密码组成只能一个个试了：

.

.

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！