

# xctf攻防世界 CRYPTO高手进阶区 你猜猜

原创

[18947943](#) 于 2022-02-10 16:39:14 发布 10574 收藏

分类专栏: [攻防世界crypto之路](#) 文章标签: [安全](#) [CRYPTO](#)

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/122863726>

版权



[攻防世界crypto之路](#) 专栏收录该内容

26 篇文章 0 订阅

订阅专栏

## 1. 进入环境，下载附件

题目给的一个txt文本:

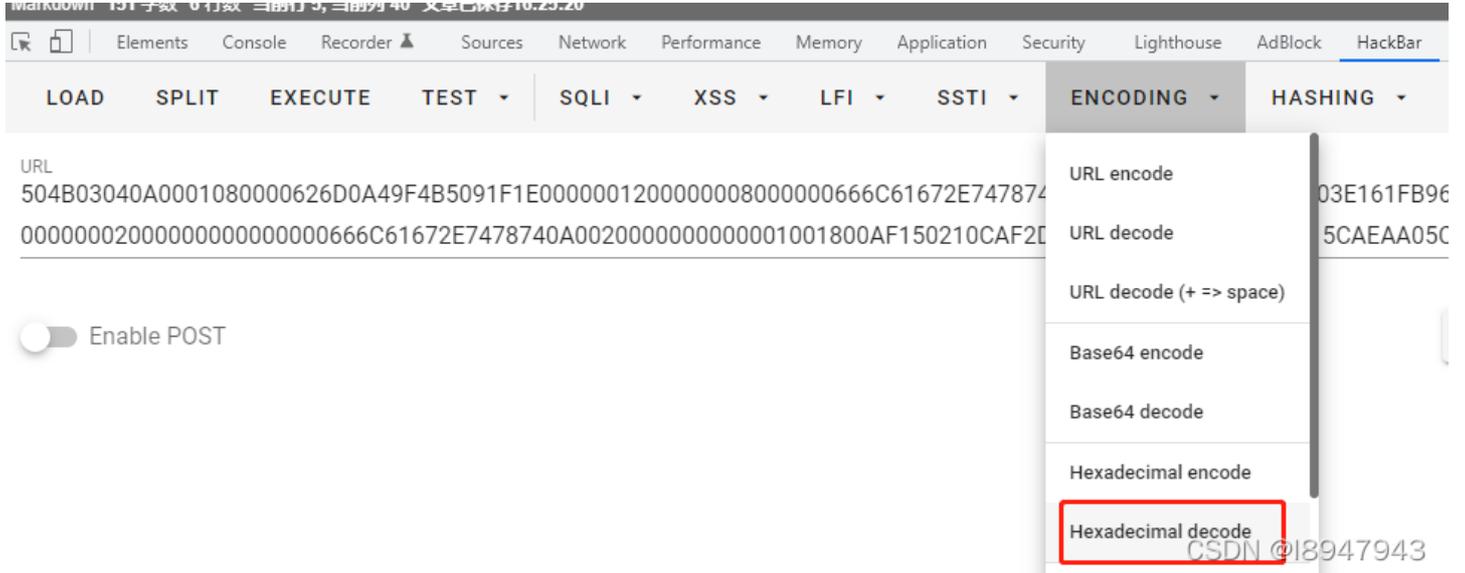
 a7cefaacd1684bfdabd71b0e848c3b83.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

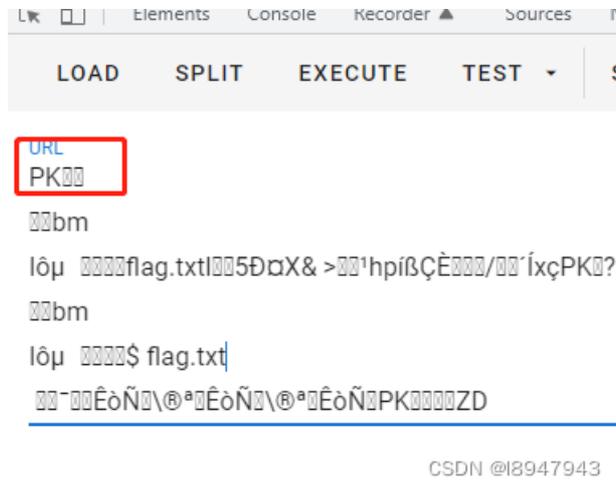
```
504B03040A0001080000626D0A49F4B5091F1E000000120000000800000066
```

## 2. 问题分析

可以看到上述字符串的范围都在0-F之间，我们尝试使用hackbar进行十六进制解码：

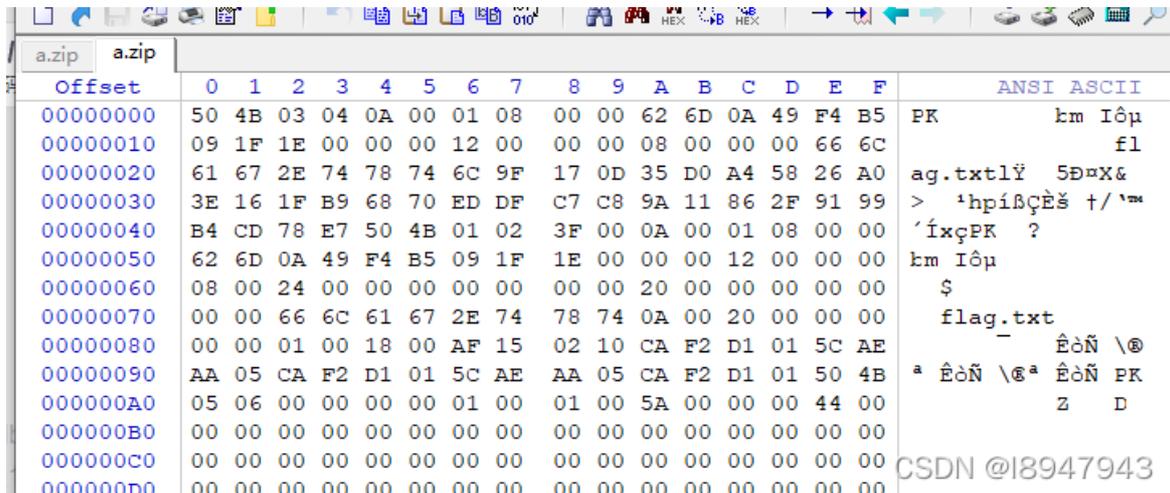


解码结果如图：



以PK开头的文件，做完misc方向就知道，是典型的zip文件开头。

尝试使用winhex新建一份文件，并将这些字符复制进去，并保存成.zip结尾的文件，如图：



打开压缩包，发现是个加密文件，在此尝试ziperllo进行暴力破解，下载链接：<https://zhangfa.lanzouw.com/idz1Xzuvxfe>

至于为什么不用ARCHPR，请看截图爆破时间：



而ziperello本身携带一些常用的字典可以跑，因此直接使用即可：



爆破后，压缩包密码为：123456。解压后，得到最终的flag。

最终答案为： `daczcasdqwcdsdzasd`