

xctf攻防世界 MISC高手进阶区 再见李华

原创

[18947943](#) 于 2022-01-17 13:26:22 发布 5747 收藏

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

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/122537741>

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. 进入环境, 下载附件

题目给了一个压缩包, 包含一张jpg图片, 如图:



CSDN @18947943

没有其他信息, 猜测是md5的加密玩意, 但是少内容

2. 问题分析

1. 丢入 StegSolve

一通乱点，没有发现隐藏的内容，通道分析也没有什么奇怪的点。

2. 丢入 winhex

文件头FFD8FF开头的，emmm，没问题，拉到最后瞅瞅，发现了猫腻，如图：

```
248 00 92 14 9E A1 77 63 34 57 74 00 03 00 62 8A EB ' zjwc4Wt bSë
264 84 2D 14 8C 5B BB B9 FF D9 50 4B 03 04 14 00 01 "- G[ ]¹yÜPK
280 08 08 00 ED A1 0B 49 05 02 71 1B 25 00 00 00 1A i; I q %
296 00 00 00 07 00 00 00 6B 65 79 2E 74 78 74 1F B8 key.txt .
312 6D CB A3 14 44 0A 7B 05 9B B6 EA 30 C9 9E 7C C2 mÈ£ D { }ÿè0Éž|Ä
328 AF B2 CF 43 47 6A 85 68 0B 8A 76 FB D5 C7 F2 EF ~²iCGj...h ŠvûÖÇòì
344 99 45 98 50 4B 01 02 3F 00 14 00 01 08 08 00 ED "E~PK ? i
360 A1 0B 49 05 02 71 1B 25 00 00 00 1A 00 00 00 07 i I q %
376 00 24 00 00 00 00 00 00 00 20 00 00 00 00 00 00 s
392 00 6B 65 79 2E 74 78 74 0A 00 20 00 00 00 00 00 key.txt
408 01 00 18 00 B2 8D 26 0A CA F3 D1 01 B2 8D 26 0A & ÉóÑ &
424 CA F3 D1 01 A1 97 97 00 AC F3 D1 01 50 4B 05 06 ÉóÑ i-- -óÑ PK
440 00 00 00 00 01 00 01 00 59 00 00 00 4A 00 00 00 Y J
456 00 00
```

隐写包含一个key.txt，果断分离呗

3. 丢入 kali进行 foremost

```
foremost -i mail2LiHua.jpg -o res
```

结果如图：



```
zhangfa@kali: ~/下载
文件 动作 编辑 查看 帮助
(zhangfa@kali)~[~/下载]
$ foremost -i mail2LiHua.jpg -o res
Processing: mail2LiHua.jpg
|foundat:key.txt[m*D]
{|0e|CGj|h
|vCGj|hE?PK?
*
```

果然有东西，打开瞅瞅，发现是个.zip压缩包，需要打开密码

4. 暴力破解

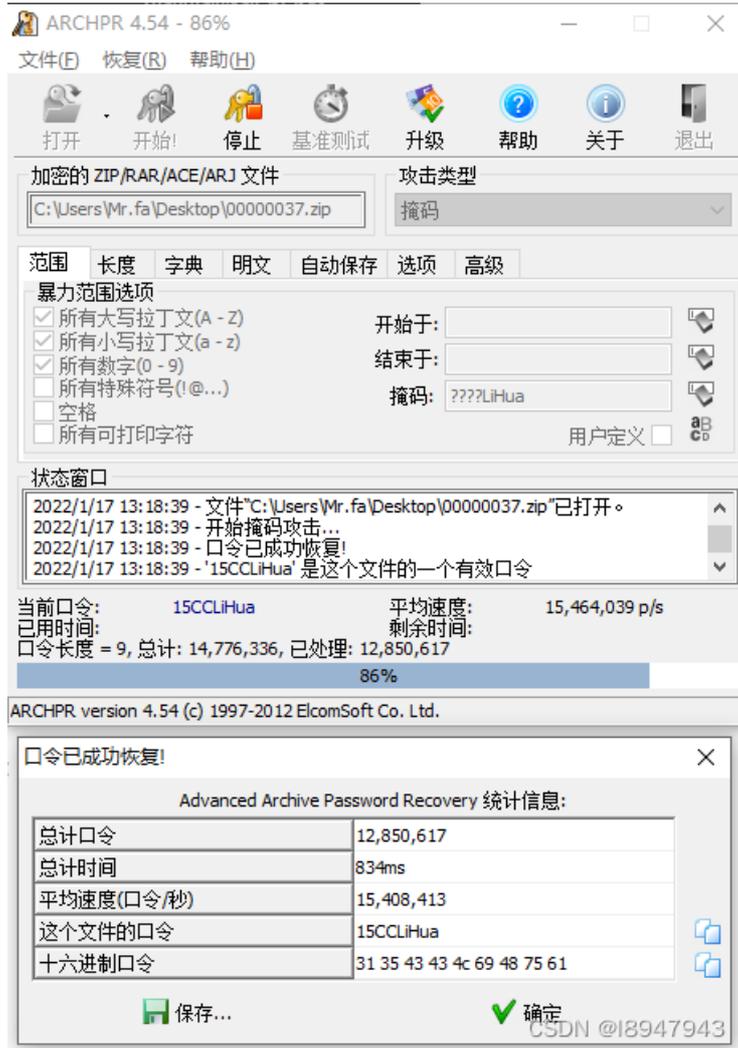
先分析，题目提示：假如你是李华（LiHua），收到乔帮主一封密信，没有任何特殊字符，请输入密码，不少于1000个字。同学，记得署名哦~

emmm，LiHua收款信件，且要用于签名，那就不用这个作为压缩密码试试，发现打不开！

看了看其他人的wp，使用的掩码匹配！不过神仙们，你们怎么知道构造几位字符啊，我一点都找不到位数方向。。。

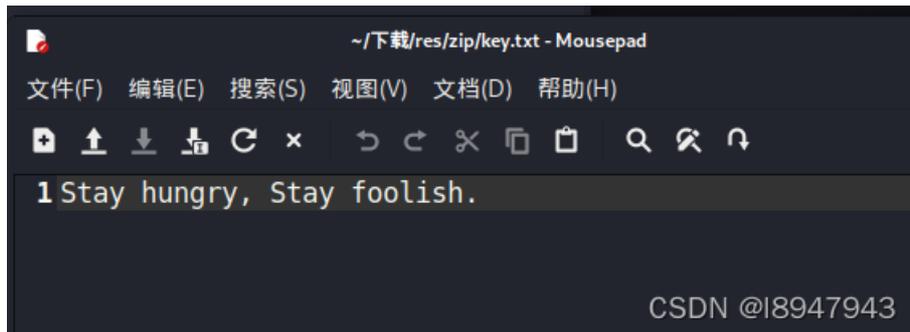
妈的，吃完饭想了想，明白了为啥用四位，继续补充。题目说不少于1000字，这1000指的不是真的1000个，而是四位字符!!! 所以构造的是???LiHua。真各种脑洞猜

使用工具ARCHPR，如图：

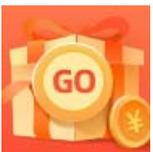


解压码为：15CCLiHua

解压结果如图：



最终的答案为： Stay hungry, Stay foolish.



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)