

# 2017信息安全大赛 MISC warm up 解题详解

原创

DDragon321 于 2019-07-23 15:16:14 发布 948 收藏 1

分类专栏: [CTF](#) 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/qq\\_43165101/article/details/96995745](https://blog.csdn.net/qq_43165101/article/details/96995745)

版权



[CTF 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

## 2017信息安全大赛 MISC warm up 解题详解

首先下载题目链接得到两个文件, 如图所示。

TF >



open\_forum.png



warmup\_3D871  
19B1FD69603E  
77BA1292A007  
C4B .zip

[https://blog.csdn.net/qq\\_43165101](https://blog.csdn.net/qq_43165101)

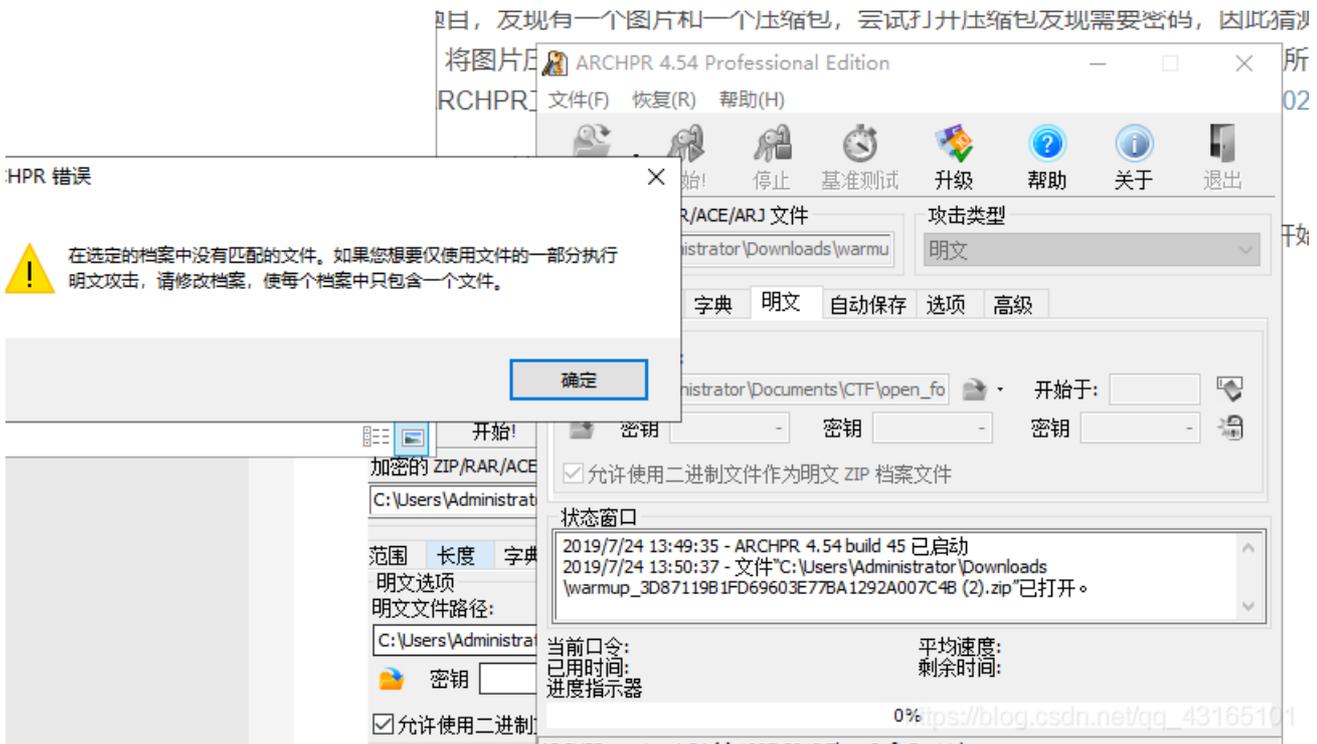
具体的题目链接可以查看爱春秋, <https://www.ichunqiu.com/battalion?t=1&r=58837>。

拿到题目, 发现有一个图片和一个压缩包, 尝试打开压缩包发现需要密码, 因此猜测图片即为压缩包的明文。

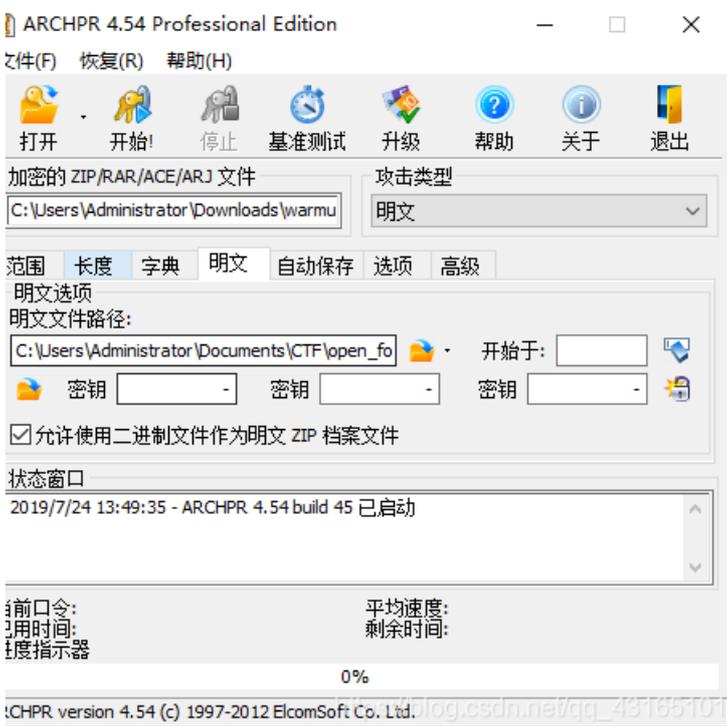
首先, 将图片压缩为zip文件, 因为此处要使用ARCHPR进行压缩包的破解工作, 所以要使文件的类型相同。

关于ARCHPR工具的下载可以参考csdn上的教程, [https://blog.csdn.net/weixin\\_40270867/article/details/83062134](https://blog.csdn.net/weixin_40270867/article/details/83062134)

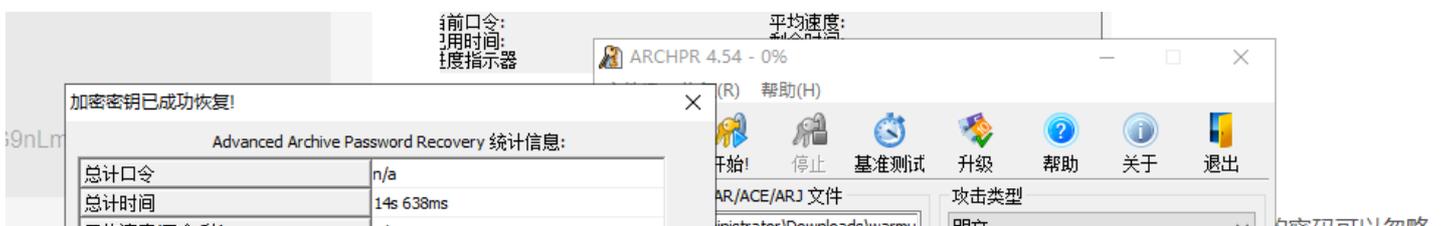
使用该工具破解，选择明文，然后选择对应文件，发现提示如下错误。

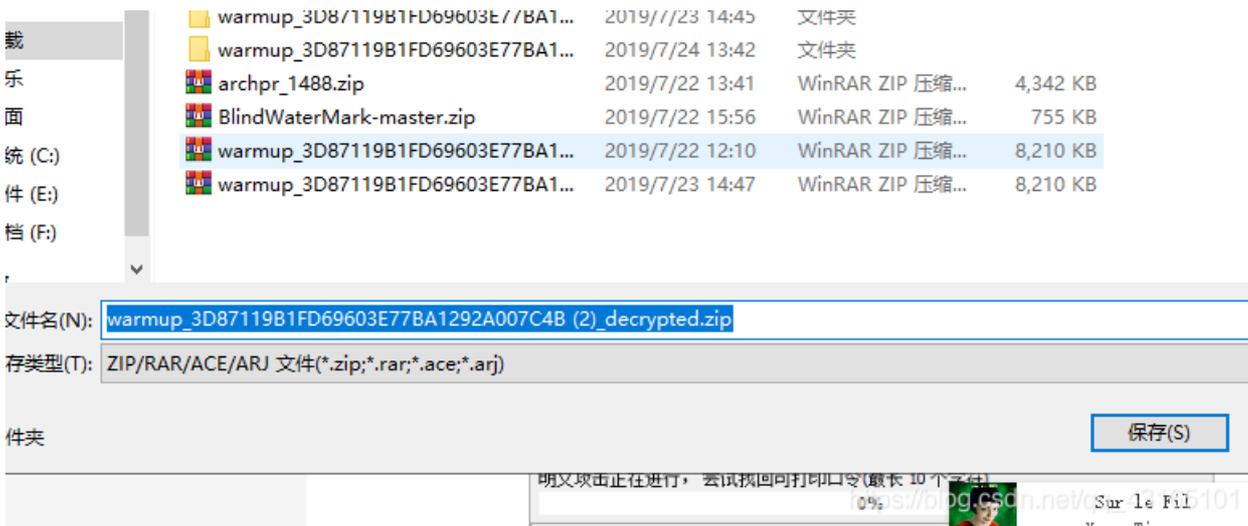
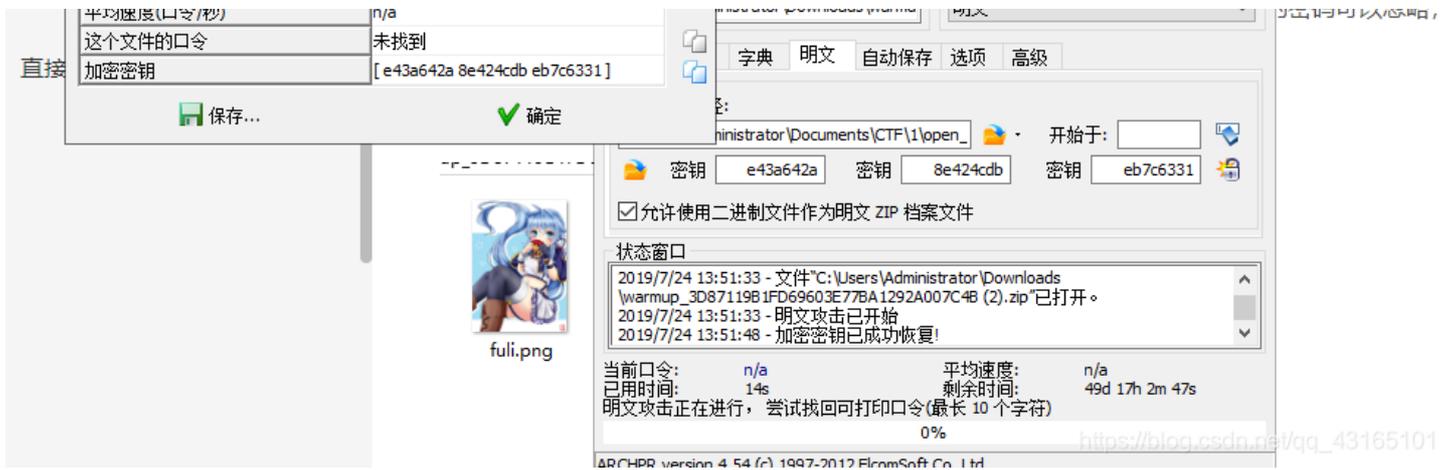


分析是压缩包的格式不一致，采用winrar再次压缩得到zip文件。再次尝试，发现开始破解。



刚开始以为破解时间很久，其实只需要几秒就可以破解，后面应该是在计算具体的密码可以忽略，直接另存为就可以得到破解的文件。





破解的文件如图所示



猜测采用的是盲水印算法，根据github上的py脚本，可以直接破

解， <https://github.com/chishaxie/BlindWaterMark/blob/master/README.md>

注意这里采用的是python2编写的脚本，所以运行时也要用python2不然会报错。另外因为调用了opencv的库所以需要安装python对应的opencv库。具体脚本运行时还需要一些其他的库再自行安装。

破解的结果如图

```
PS C:\Users\Administrator\Downloads>warmup_3D87119B1FD69603E77BA1292A007C4B (2)_decrypted> python2 bwm.py decode fuli.png fuli2.png watermark.png
image<fuli.png> + image(encoded)<fuli2.png> -> watermark<watermark.png>
```





fuli.png



fuli2.png



open\_forum.png



watermark.png

