xctf攻防世界 MISC高手进阶区 我们的秘密是绿色的

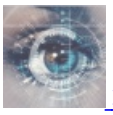
原创

l8947943 已于 2022-01-25 22:55:56 修改 7009 收藏 6

分类专栏： 攻防世界misc之路 文章标签： misc

于 2022-01-19 12:14:15 首次发布

本文链接：https://blog.csdn.net/l8947943/article/details/122576929



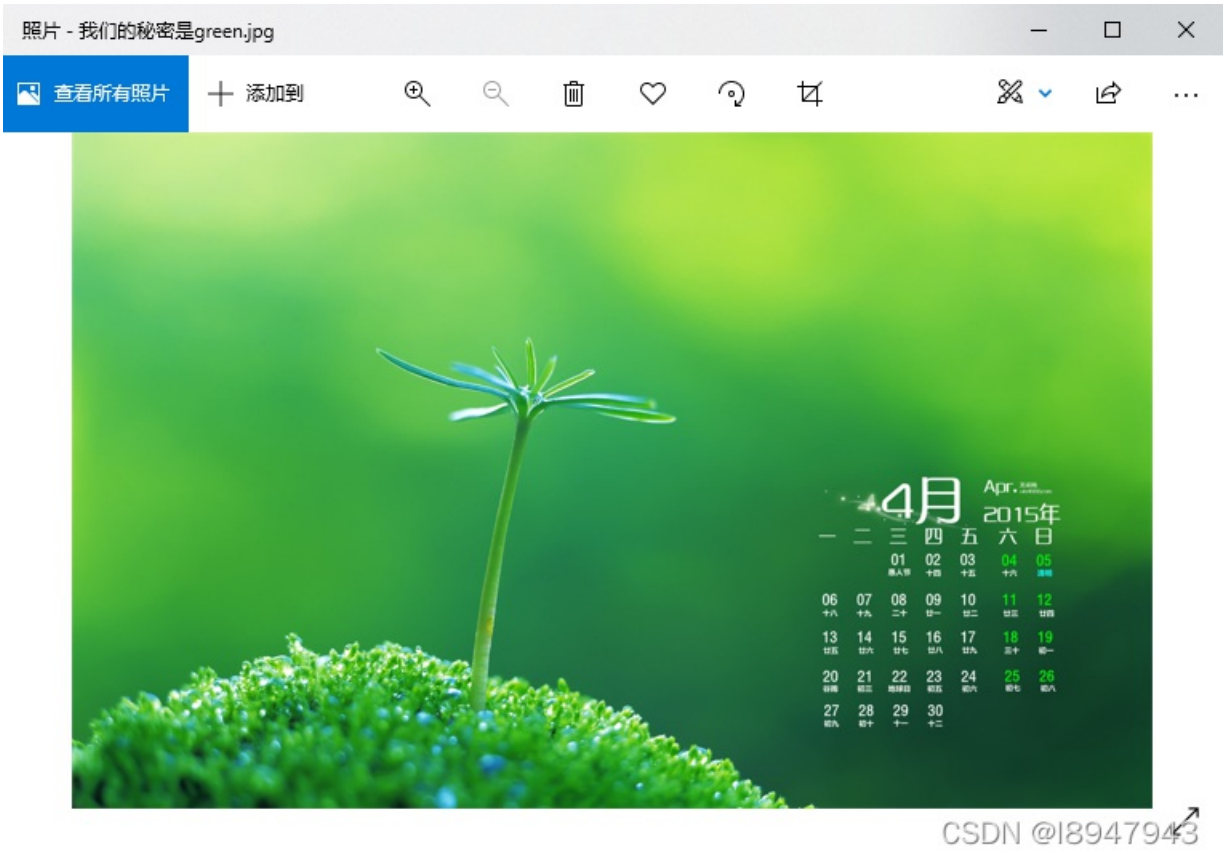
攻防世界misc之路 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

1. 进入环境，下载附件

给了一张图片，是个日历，如图：



嗯，确实绿色！

2. 问题分析

绿色的含义

使用binwalk进行分析，并没有什么有用的信息，

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.02
30            0x1E            TIFF image data, big-endian, offset of first image
directory: 8
```

读题，题目说：我们的秘密是绿色的。观察到图片上有翠绿色的字体，0405111218192526。不知道是什么东东，感觉像个密码一样。没有思路了，看了看wp，全是盲区，这些工具都没怎么用过。。。跟着wp不断学习吧。

使用Our Secret

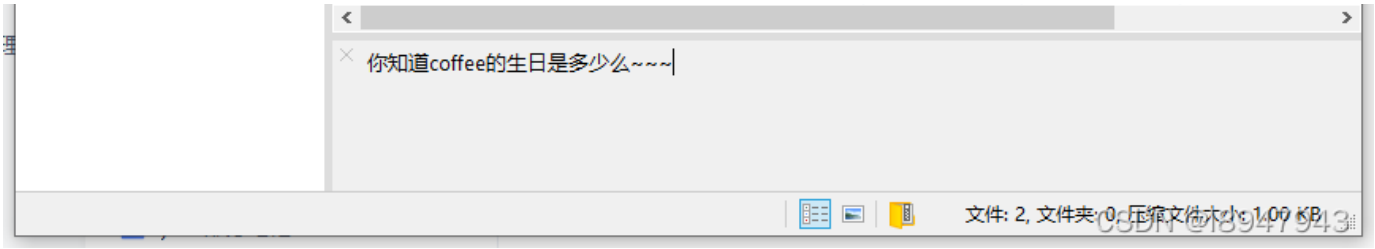
工具下载地址：https://www.cr173.com/soft/80335.html

打开图片，并使用上述密码，如图：

得到一个zip压缩包。

打开压缩包

发现需要密码，但是有提示，问coffee的生日，如图：

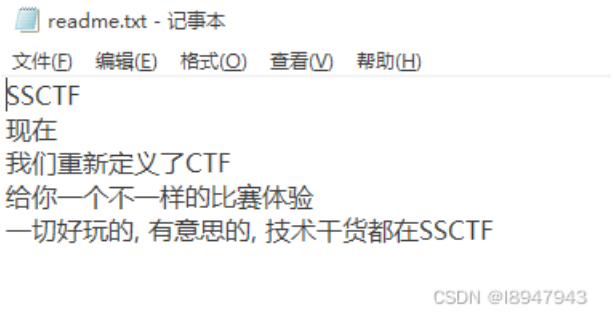


生日不就是××××-××-××，一共八位，且为纯数字。使用暴力破解工具：ARCHPR

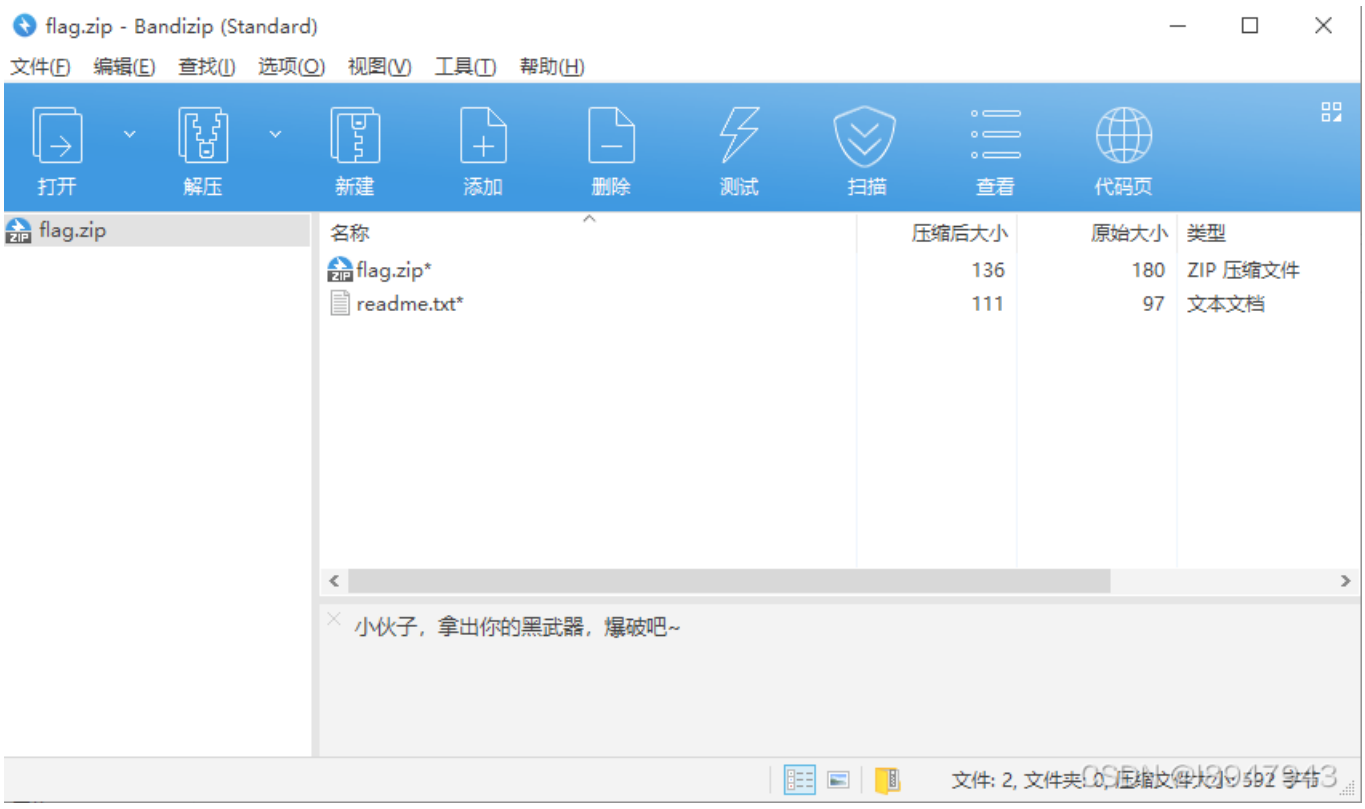
尝试解压码：19950822

4. **继续探索压缩包**

解压得到两个压缩文件，先看readme：

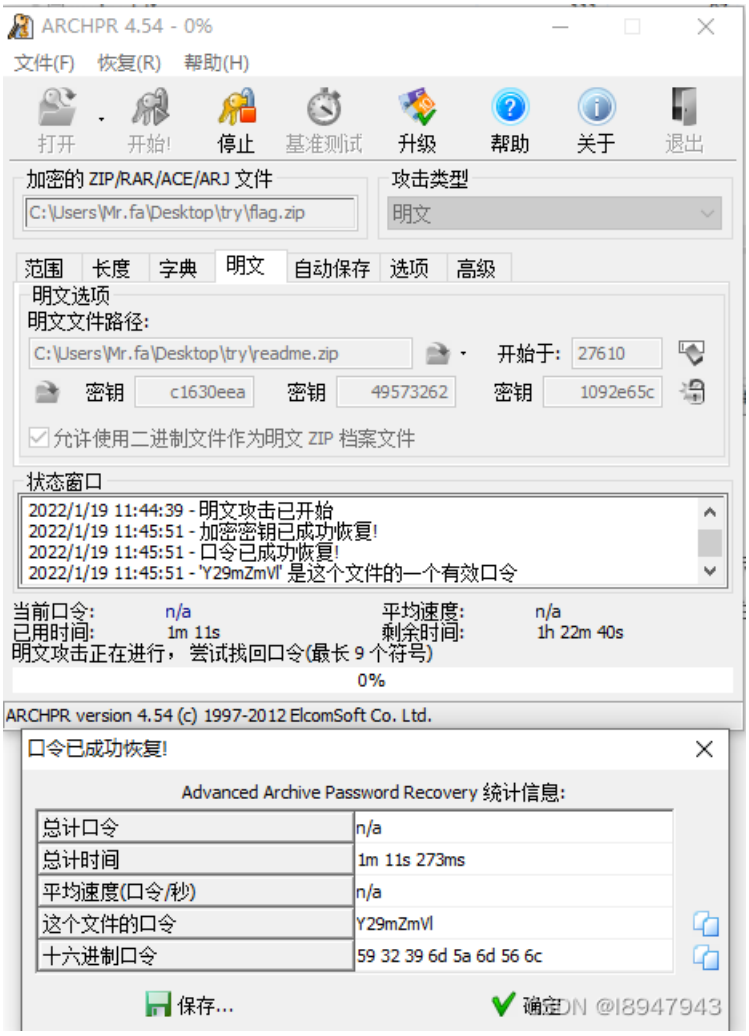


估计是SSCTF又是什么新的工具吧，先继续压缩文件：



我草，还踏马有解压密码，你搁这搁这搁这呢？俄罗斯套娃啊？

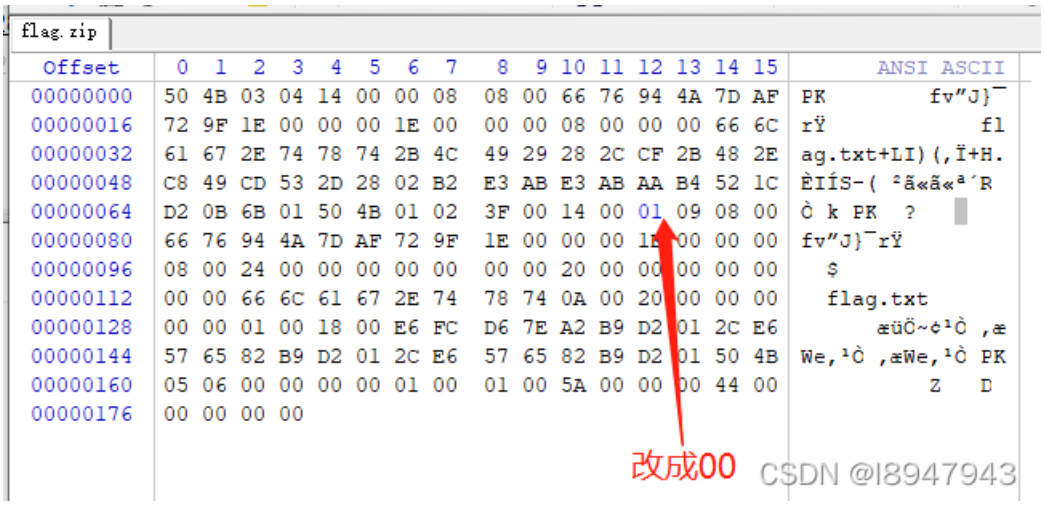
wp提示明文攻击，还没接触过，先跟着尝试。这块有踩坑，原始文件用什么压缩，对应目标文件一定也要跟上，明文攻击才能奏效（推荐用WinRAR，bandizip容易导致ARCHPR出现“在选定的档案中没有匹配的文件”），如图：



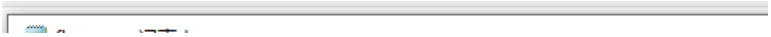
文件口令为：Y29mZmVl

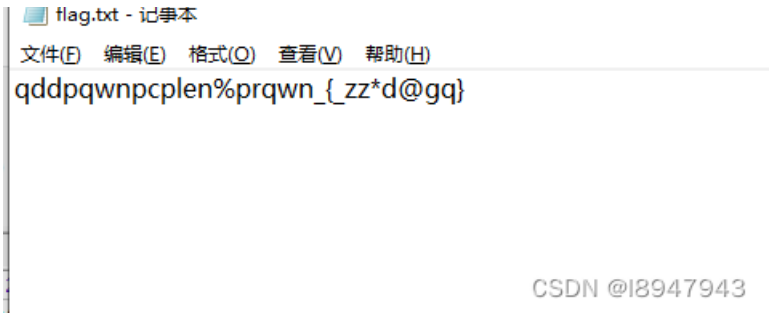
5. **还有压缩密码**

   扔进winhex，发现是伪加密，如何判断伪加密：https://blog.csdn.net/u011377996/article/details/79286958



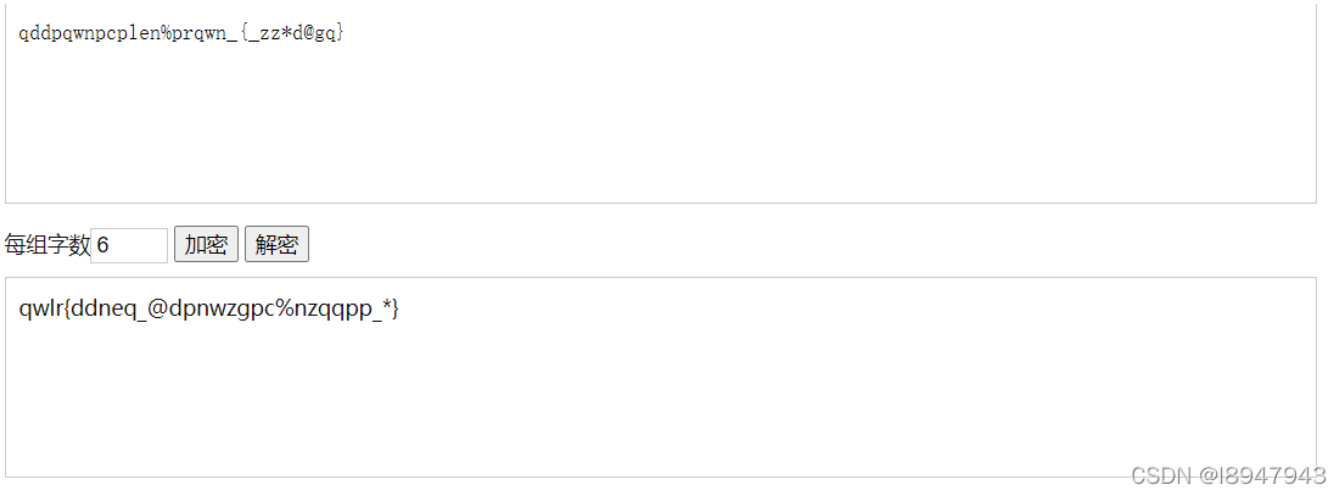
修改00为01，解压得到flag：





6. **栅栏解密**

https://www.qqxiuzi.cn/bianma/zhalanmima.php 在线解密，不太懂这个玩意，后面再回头看吧！看wp说解密密码（2，3，5，6，10，15几个因数，不懂，，，）如图：



组数为6的时候，还需要凯撒，https://www.qqxiuzi.cn/bianma/kaisamima.php 再继续：

得到最终答案：`flag{ssctf_@seclover%coffee_*}`

3. 总结

- 涉及很多没见过的工具，难
- 暴力破解踩坑好烦
- 明文攻击不懂
- 栅栏加密和凯撒加密等知识需要补充
- 为什么其他的wp这么优秀，都怎么学习的，每日一膜

这个题2分，我觉得能有5分的感觉，干不动哎，休息一下吧！