攻防世界 Misc高手进阶区 3分题 miscmisc

原创

思源湖的鱼 于 2020-11-12 12:46:53 发布 479 收藏 3

分类专栏： ctf 文章标签： 攻防世界 ctf misc 网络安全 明文攻击

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109641236

CTF

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Misc高手进阶区的3分题

本篇是miscmisc的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

下下来一个png文件

扔进stegsolve

无果

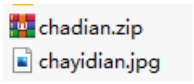
扔进winhex

发现flag.zip

```
00046160  D8 CE AD 26 00 00 00 34  00 00 00 08 00 00 00 66  ØÎ-&   4       f
00046176  6C 61 67 2E 74 78 74 69  A0 A3 EE 51 00 2E 4A 93  lag.txti £îQ .J"
00046192  94 69 DC 1F B8 30 9D 13  DF 89 C7 54 33 D4 6C 43  "iÜ ¸0  ß‰ÇT3ÔlC
00046208  C0 73 9F B5 2B B3 63 69  1C 68 EE C0 58 50 4B 07  ÀsŸµ+³ci hîÀXPK
00046224  08 F9 D8 CE AD 26 00 00  00 34 00 00 00 50 4B 03   ùØÎ-&   4   PK
00046240  04 14 00 09 00 08 00 D7  5C 4C 4F AA A0 ED 46 61         ×\LOª íFa
00046256  6F 04 00 7E 6F 04 00 08  00 00 00 66 6C 61 67 2E  o  ~o       flag.
00046272  7A 69 70 C4 65 9C 67 89  F6 86 CC 17 6D CD 34 BD  zipÄeœg‰ö†Ì mÍ4½
00046288  BA 66 7B 3D 48 AF 91 A0  B6 1F 6B 66 33 8F AE CE  °f{=H¯' ¶ kf3 ®Î
```

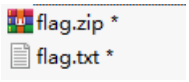
改后缀

解压



chadian.zip里有flag

解压要密码



尝试伪加密和AZPR暴力破解

无果

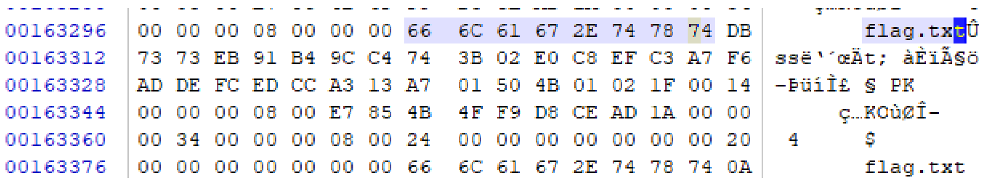
看看jpg

扔进stegsolve

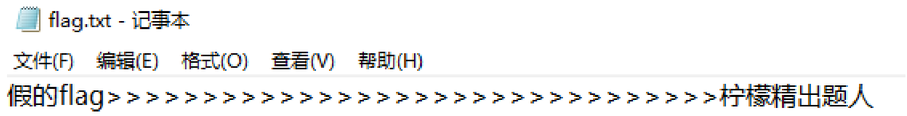
无果

扔进winhex

发现flag.txt

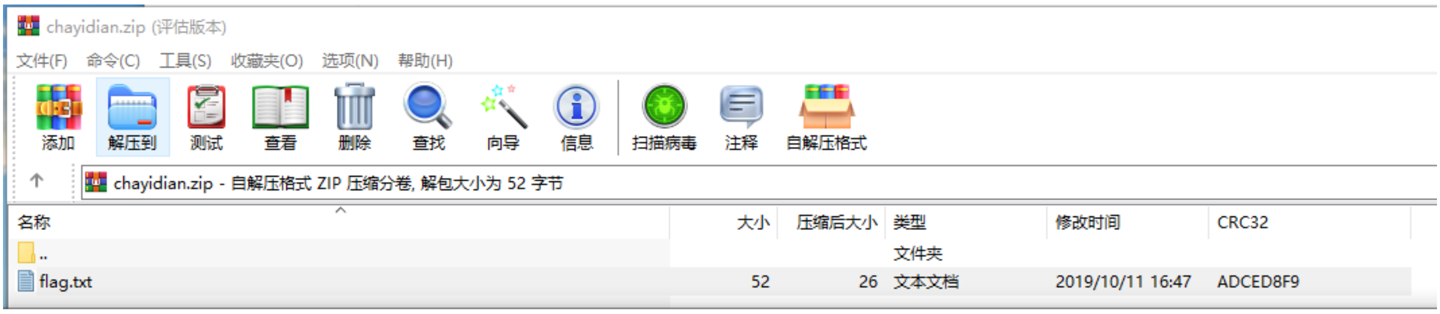


改后缀
解压

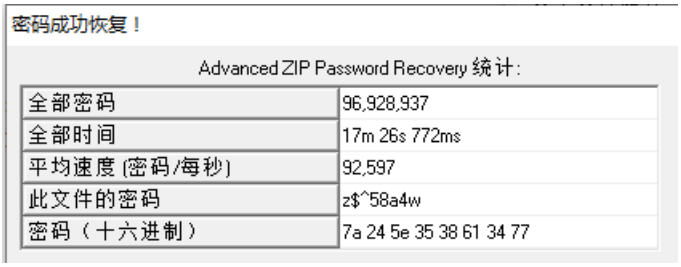


。。。。。。

突然想起前面的chadian.zip
也有个flag.txt
对比一看
CRC32一样

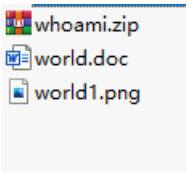


那就是明文攻击了



得到解压密码 `z$^58a4w`

解压
得到



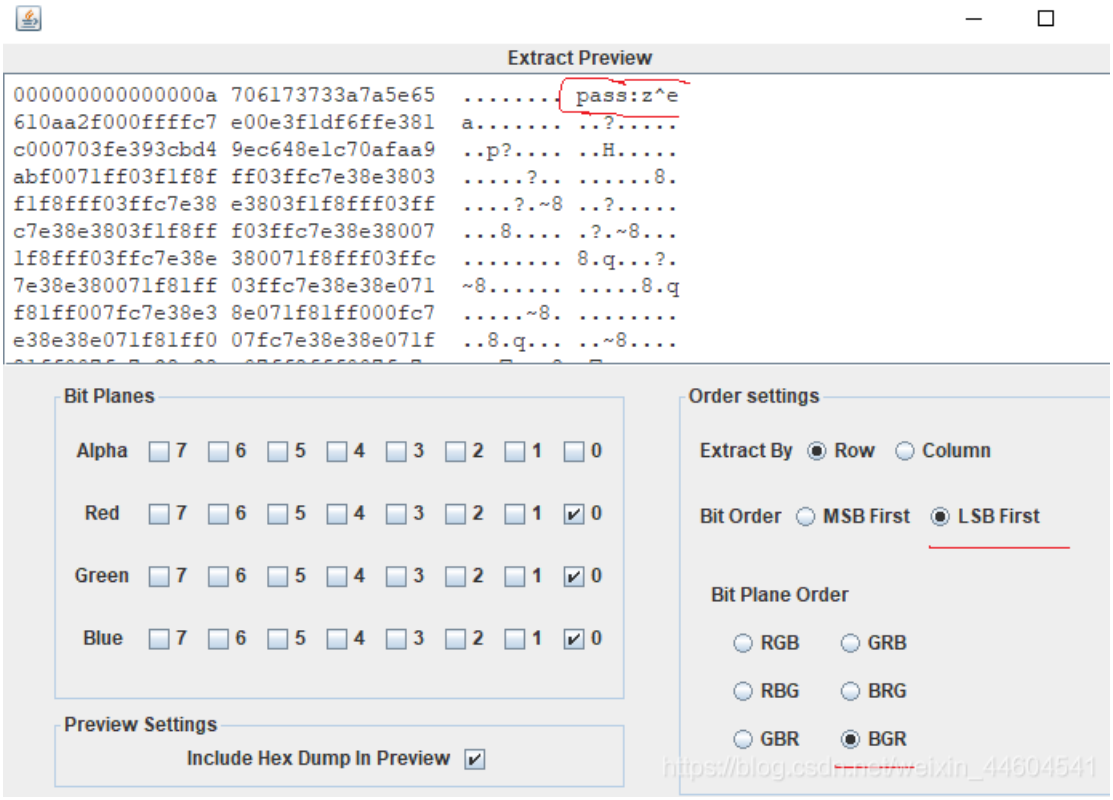
whoami里面又需要密码

word文件

除了这个就差一点点了

png文件

扔进stegsolve
得到一部分解压密码

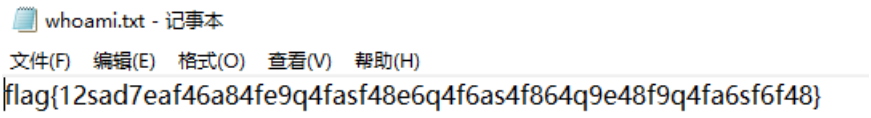


还有一部分应该在word里
全选-字体-隐藏

除了这个就差一点点了
Zdfaw1234
3daeghalz
2aeaqrqfa
Weasa65fa
Ezafasfasf3
Sadera85fa
Daaszffasfz
Asdfafsfaff
Sad54656a8

。。。
但这还是很多啊
一行行一列列的试

试出来是`z^ea4zaa3azf8`
难顶



得到flag

结语

真·还差亿点点
套娃套中套

知识点

- 图片隐写
- 文字隐藏
- 明文攻击