攻防世界 Misc Ditf

原创

==Microsoft== 于 2022-03-05 12:41:50 发布 2344 收藏

分类专栏： Misc 文章标签： 安全 密码学 ctf misc

和你一起终身学习，这里是程序员Android

本文链接：https://blog.csdn.net/MrTreebook/article/details/123292179

版权

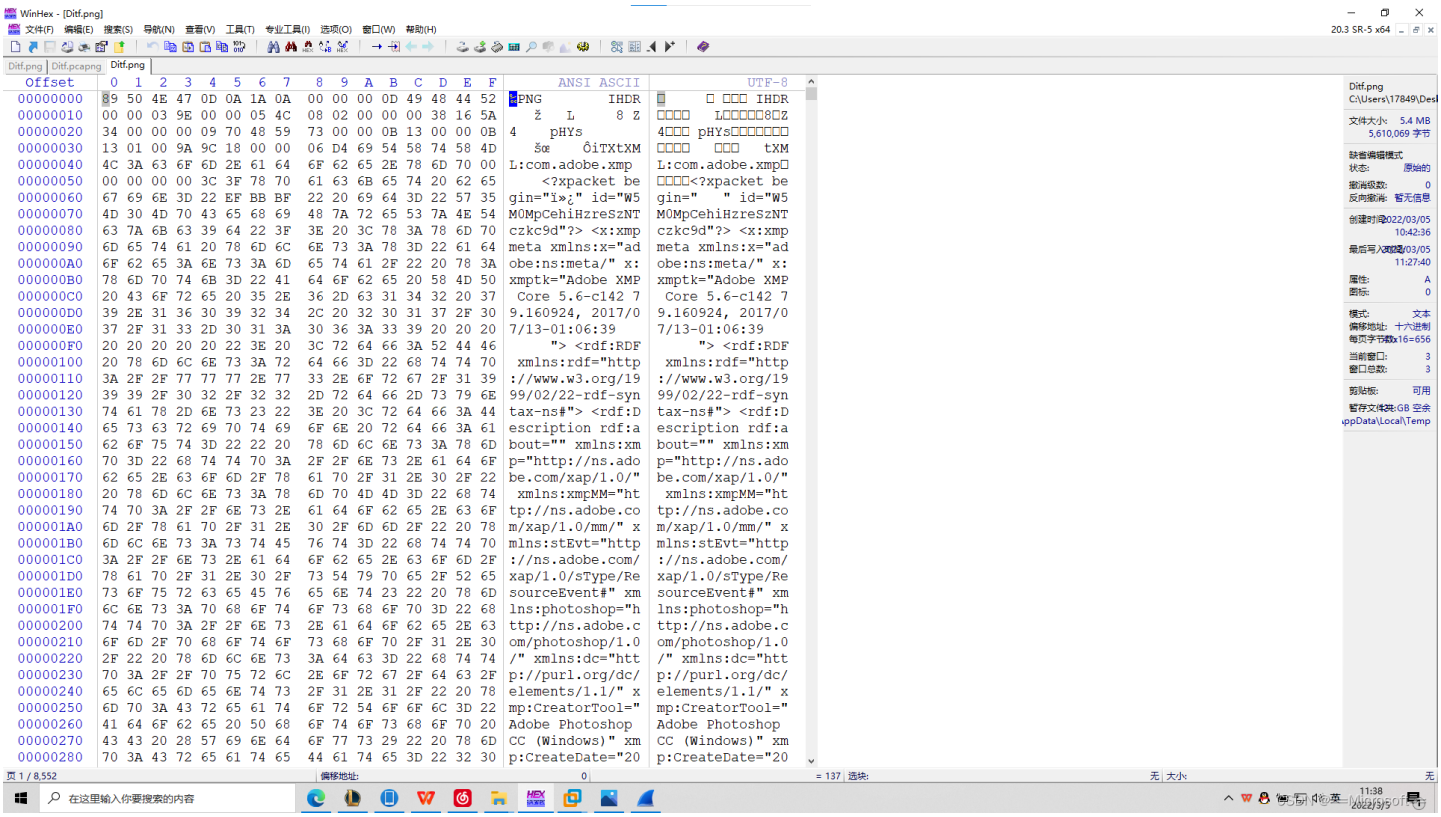
Misc 专栏收录该内容

50 篇文章 0 订阅

订阅专栏

攻防世界 Misc Ditf

1.winhex分析



- 看到了html代码，怀疑是一个网页

2.binwalk分析

```
┌──(mss㉿kali)-[~/Desktop/git/ctf-misc]
└─$ binwalk Ditf.png                                                148 ✕ 2 ⚙

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 926 x 1100, 8-bit/color RGB, non-interl
aced
1822          0x71E           Zlib compressed data, default compression
989714        0xF1A12         RAR archive data, version 4.x, first volume type:
MAIN_HEAD
                                                        CSDN @==Microsoft==
```

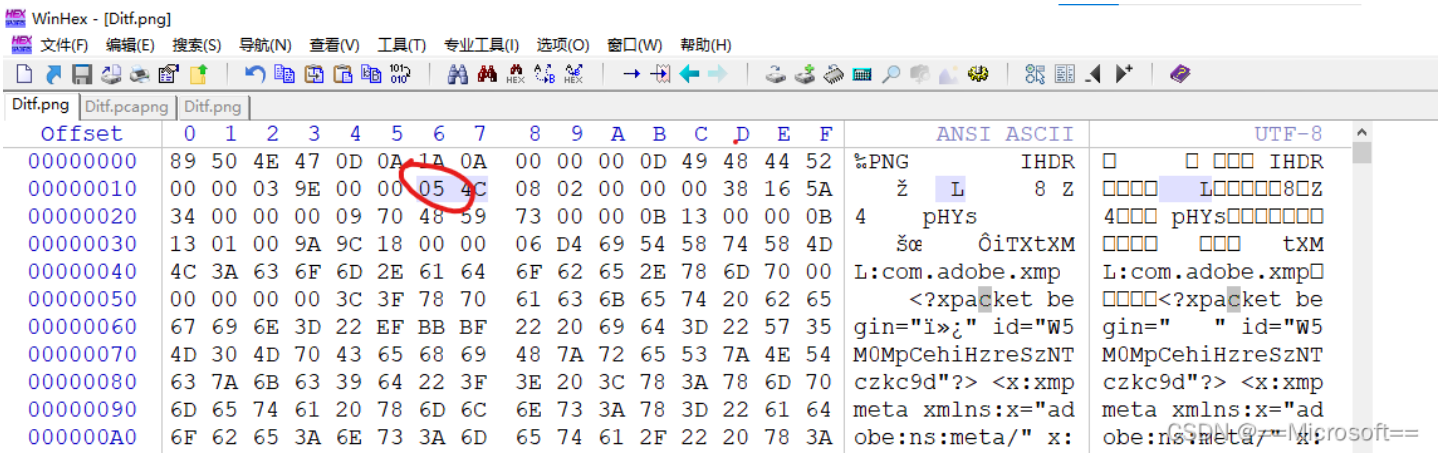
- 发现有一个rar文件

3.foremost分离

```
┌──(root㉿kali)-[/home/…/git/ctf-misc/output/png]
└─# foremost -i Ditf.png
```

- 打开rar文件发现需要密码
-

4.修改图片Ditf.png的高度

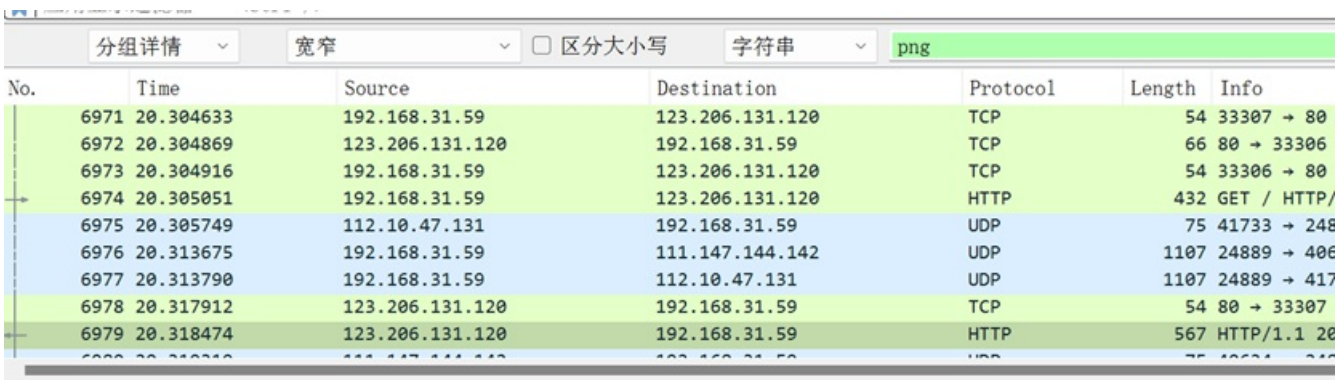


- 修改成05即可
- 再次打开图片可以看到密码

- 输入密码得到一个流量包文件

5.wireshark打开

- 搜索有关png的内容



```
  </head>\n
  <body>\n
  \t<img src="/kiss.png" />\n
  ZmxhZ3tPel80bmRfSGlyMF9sb3YzX0ZvcjN2ZXJ9\n
  </body>\n
</html>\n
\n
```

```
0000  3c 68 74 6d 6c 3e 0a 20  20 3c 68 65 61 64 3e 0a   <html>·   <head>·
0010  20 20 20 20 3c 6d 65 74  61 20 68 74 74 70 2d 65       <met a http-e
0020  71 75 69 76 3d 22 43 6f  6e 74 65 6e 74 2d 54 79   quiv="Co ntent-Ty
0030  70 65 22 20 63 6f 6e 74  65 6e 74 3d 22 74 65 78   pe" cont ent="tex
0040  74 2f 68 74 6d 6c 3b 20  63 68 61 72 73 65 74 3d   t/html;  charset=
0050  55 54 46 2d 38 22 20 2f  3e 0a 20 20 3c 2f 68 65   UTF-8" / >·  </he
0060  61 64 3e 0a 20 20 3c 62  6f 64 79 3e 0a 20 20 09   ad>·  <b ody>·  ·
0070  3c 69 6d 67 20 73 72 63  3d 22 2f 6b 69 73 73 2e   <img src ="/kiss.
0080  70 6e 67 22 20 2f 3e 0a  20 20 5a 6d 78 68 5a 33   png" />·  ZmxhZ3
0090  74 50 65 6c 38 30 62 6d  52 66 53 47 6c 79 4d 46   tPel80bm RfSGlyMF
00a0  39 73 62 33 59 7a 58 30  5a 76 63 6a 4e 32 5a 58   9sb3YzX0 ZvcjN2ZX
00b0  4a 39 0a 20 20 3c 2f 62  6f 64 79 3e 0a 3c 2f 68   J9·  </b ody>·</h
00c0  74 6d 6c 3e 0a 0a                                  tml>··
```


- 发现base64加密的内容
- 使用工具解密

6.exp

```
import base64
basecode = "ZmxhZ3tPel80bmRfSGlyMF9sb3YzX0ZvcjN2ZXJ9"
result = base64.b64decode(basecode)
print(result)
```

- 得到flag

```
PS C:\Users\17849\Desktop> python exp.py
b'flag{Oz_4nd_Hir0_lov3_For3ver}'
PS C:\Users\17849\Desktop>
```