misc攻防世界新手

原创

舞动的獾 于 2019-05-07 16:20:17 发布 3668 收藏 3

分类专栏： 网络安全misc 文章标签： ctf misc

本文链接：https://blog.csdn.net/Yu_csdnstory/article/details/89923557

网络安全misc 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

坚持60s

题目描述：

难度系数：

题目来源： 08067CTF

题目描述：菜狗发现最近菜猫不爱理他，反而迷上了菜鸡

题目场景： 暂无

题目附件： 附件0

解法过程：

进入题目会看到下载的一个附件，是一个Java写的程序，很有意思。

看文件类型，这就需要看出这个程序的基本的对象，就要用到java反编译器，这里使用**jd-gui**

下载地址：

下载jd-gui后直接解压，需要有Java环境

打开后会看到如下的页面儿：

```
int period = (int)((this.endTime.getTime() - this.startTime.getTime()) / 1000L);
printInfo(g, "你的持久度才" + period + "秒", 50, 150, 250);

switch (period / 10) {
case 0:
  printInfo(g, "真.头顶一片青青草原", 50, 150, 300);
  break;
case 1:
  printInfo(g, "这东西你也要抢着带？", 50, 150, 300);
  break;
case 2:
  printInfo(g, "如果梦想有颜色，那一定是原谅色", 40, 30, 300);
  break;
case 3:
  printInfo(g, "哟，炊事班长呀兄弟", 50, 150, 300);
  break;
case 4:
  printInfo(g, "加油你就是下一个老王", 50, 150, 300);
  break;
case 5:
  printInfo(g, "如果撑过一分钟我岂不是很没面子", 40, 30, 300);
  break;
case 6:
  printInfo(g, "flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}", 50, 150, 300);
```

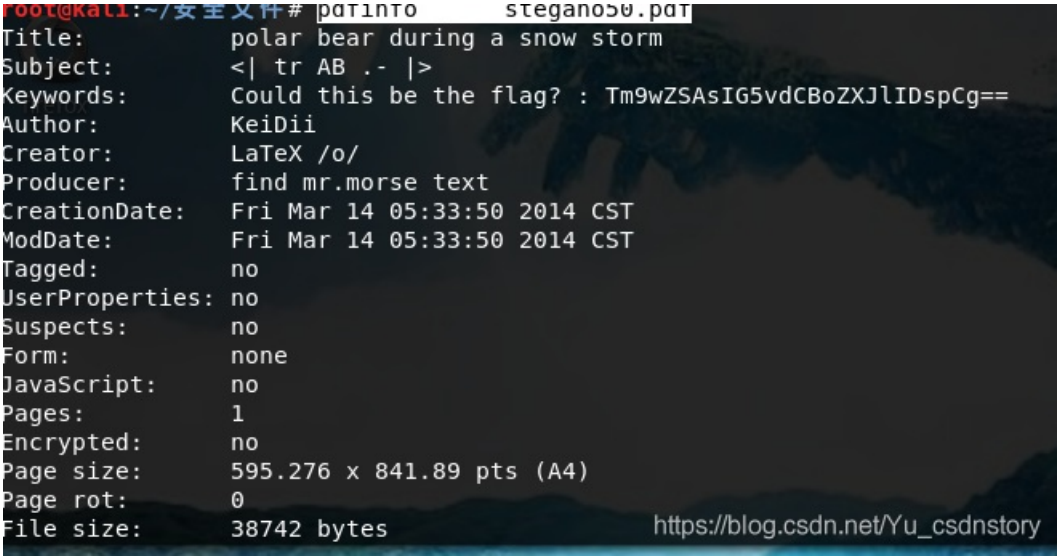

这时候看到的是经过base64加密后的flag，用解密工具解密就得到flag

stegano

首先下载附件，是个pdf文件 用linux kali打开，

```
pdfinfo      stegano50.pdf
```

如下图：



可以看到一个base64加密的字符串，用base64解密看看

```
gedit 1.txt
base64 -d 1.txt
```

创建文件1.txt,并输入base64加密的字符，解密得到：

Nope , not here ?

看来不在这里，然后用火狐的控制台试试，输入

```
document.documentElement.textContent
```

弹出以下关键内容

BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB

这应该是莫斯电文，把A看成.,B看成-

转换结果入下：

```
-.-. --- -. --. .-. .- - ..- .-.. .- - .. --- -. ... --..-- ..-. .-.. .- --. ---... .---- -. ...- .---- ..... .----
--- -... .-.. ...-- -- ...-- ..... ..... ....- --. ...--
```

转换地址

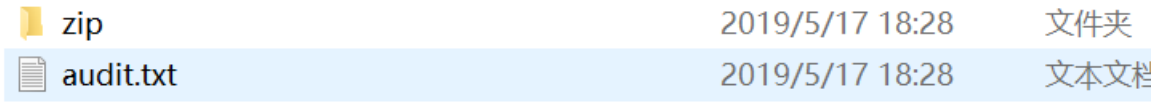
结果得到flag

```
CONGRATULATIONSFLAG1NV151BL3M3554G3
```

功夫再高，也怕菜刀

有一个附件，直接下载，发现这个是winshark文件包，

首先用foremost分析，输出为一个zip文件，里面含有一个flag.txt,但是拥有密码

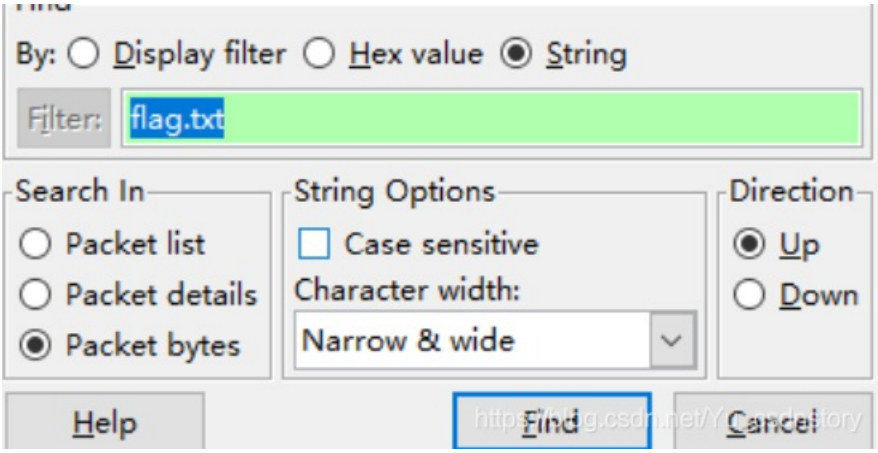


foremost下载地址

使用方法

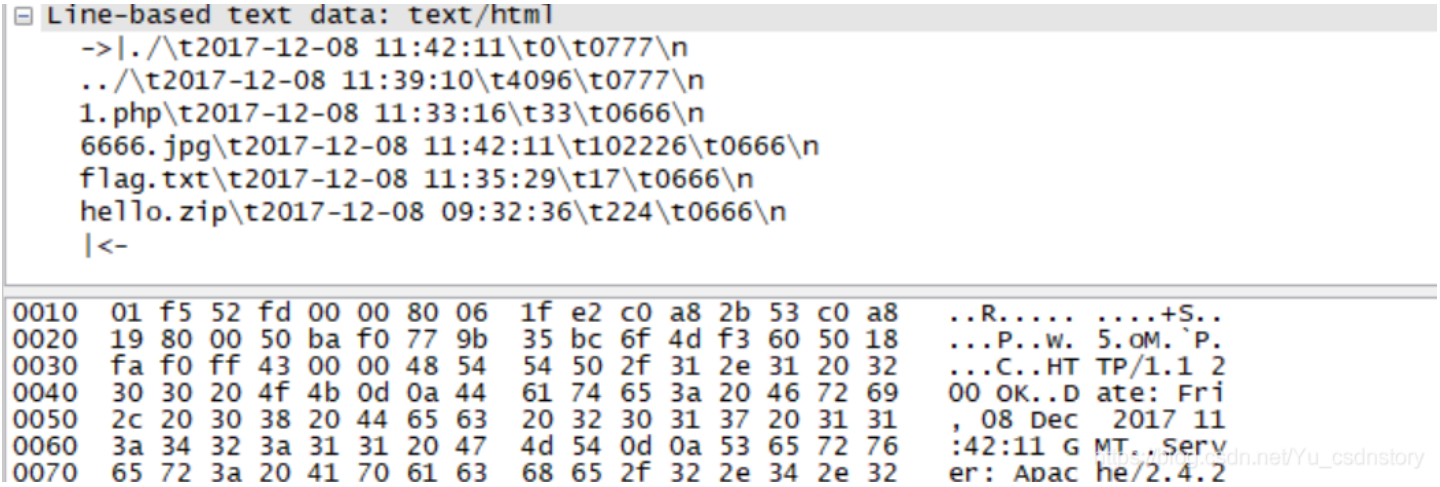
用winshark打开文件，筛选数据，在搜索框搜索flag.txt

快捷键ctrl+F



winshark搜索功能的使用

搜寻包，并进行分析，ctrl+B选择下一个筛选内容找到1150这个包时，发现了一个图片，6666.jpg



通过tcp跟踪流，将图片分离出来

```
upload/1.php HTTP/1.1
User-Agent: Java/1.8.0_151
Host: 192.168.43.83
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 204999

aa=@eval.(base64_decode($_POST
[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpOOBzZXRfdGltZV9saW1pdCgwKTt
c2V0X21hZ2ljX3F1b3RlC19ydW50aW1lKDApO2VjaG8oIi0%
2BfCIpOzskZj1iYXNlNjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JGM9JF9QT1NUWyJ6MiJdOyRjPXN0cl9yZXBs
WNlKCJcciIsIiIsJGMpOyRjPXN0cl9yZXBsYWNlKCJcbiIsIiIsJGMpOyRidWY9IiI7Zm9yKCRpPTA7JGk8c3R
bGVuKCRjKTskaSs9MikkYnVmLj11cmxkZWNvZGUoIiUiLnN1YnN0cigkYywkaSwyKSk7ZWNobyhAZndyaXRlKG
vcGVuKCRmLCJ3IiksJGJ1Zik%2FIjEiOiIwIik7O2VjaG8oInw8LSIpO2RpZSgpOw%3D%
3D&z1=RDpcd2FtcDY0XHd3d1x1cGxvYWRcNjY2Ni5qcGc%
3D&z2=FFD8FFE000104A464946000101010078007800000FFDB0043000101010101010101010101010101
1010101010101010101010101010101010101010101010101010101010101010101010101010101010101010
0101010101FFDB0043010101010101010101010101010101010101010101010101010101010101010101010101
1010101010101010101010101010101010101010101010101010101010101010101FFC00011080139012E20301220
021101031101FFC4001F0000010501010101010100000000000000000102030405060708090A0BFFC400B5
0000201030302040305050404000001 7D01020300041105122131410613516107227114328191A1082342B
```

可以将它保存下来，然后进行分离操作，在sublimetext打开，用find分别搜索**FFD8FF和FFD9**将之间的字符全部复制，然后新建winhex文件，粘贴复制的字符，保存为.jpg文件

几种类型文件的字符编码开头

保存后的图片如下：

在图片里看到了密码，输入得到flag

base64stego

本来以为又要与佛论禅了，结果发现它的加密是假的

用WinRAR的修复功能直接修复解压，发现了一个txt文件

打开文件，进行base64解码，结果如下：

base64解码地址

Steganography is the art and science of writing hidden messages in such a way that no one

意思是说，隐写是个很好的解决方法

马上上网查了查，发现base64可以隐写的，并发现了大佬们的脚本代码

```
#coding=utf-8
def get_base64_diff_value(s1, s2):
    base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
    res = 0
    for i in xrange(len(s2)):
        if s1[i] != s2[i]:
            return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))
    return res


def solve_stego():
    with open('D:\\火狐下载\\1.txt', 'rb') as f:
        file_lines = f.readlines()
        bin_str = ''
        for line in file_lines:
            steg_line = line.replace('\n', '')
            norm_line = line.replace('\n', '').decode('base64').encode('base64').replace('\n', '')
            diff = get_base64_diff_value(steg_line, norm_line)
            print diff
            pads_num = steg_line.count('=')
            if diff:
                bin_str += bin(diff)[2:].zfill(pads_num * 2)
            else:
                bin_str += '0' * pads_num * 2
            print goflag(bin_str)


def goflag(bin_str):
    res_str = ''
    for i in xrange(0, len(bin_str), 8):
        res_str += chr(int(bin_str[i:i + 8], 2))
    return res_str


if __name__ == '__main__':
    solve_stego()
```

脚本原地址

这个是python2的脚本，所以运行要用python2来运行，否则出错这里无法解决，编码符设置我为ANSI

跑下脚本，得到flag