XCTF攻防世界：MISC新手题解（1~6）

原创

CNwanku 于 2019-12-15 21:13:59 发布 1000 收藏 4

文章标签： XCTF linux 网络安全

本文链接：https://blog.csdn.net/qq_43233085/article/details/103553731

XCTF攻防世界：MISC新手题解（1~6）

this_is_flag

纯属签到题，直接将 flag 值复制提交就好。

ext3

先下载到linux系统上，用file看看文件类型。


```
root@kali:~/下载# file 5d6cda6e5ca0438cb40b367fd0ad5766
5d6cda6e5ca0438cb40b367fd0ad5766: Linux rev 1.0 ext3 filesystem data, UUID=cf6d7
bff-c377-403f-84ae-956ce3c99aaa
root@kali:~/下载#
```

是Linux文件，又是ext3格式，使用mount挂载上来。

```
root@kali:~/下载# mount 5d6cda6e5ca0438cb40b367fd0ad5766 /mnt
root@kali:~/下载#
```

查找一下flag文件的位置。

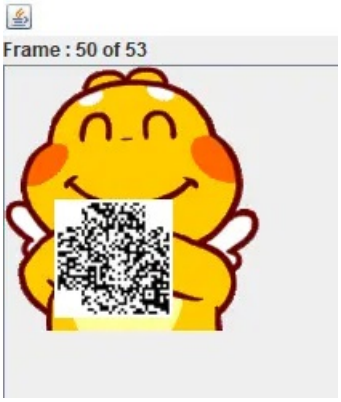
```
root@kali:~/下载# strings 5d6cda6e5ca0438cb40b367fd0ad5766 | grep flag
.flag.txt.swp
flag.txtt.swx
~root/Desktop/file/O7avZhikgKgbF/flag.txt
.flag.txt.swp
flag.txtt.swx
.flag.txt.swp
flag.txtt.swx
```

```
root@kali:~/下载# cd /mnt
root@kali:/mnt# ls
02CdWGSxGPX.bin  8A2MFawD4   ix1EMRHRpIc2  n            r
0GY1l            8DQFirm0D   j6uLMX        NgzQPW       Raf3SYj
0h3a5            8HhWfV9nK1  jE            Nv           rhZE1LZ6g
0l               8nwg        jj            o            Ruc9
0qsd             8RxQG4bvd   KxEQM         O7avZhikgKgbF  RZTOGd
0wDq5            FinD        LG6F          o8           scripts
0Xs              fm          Lh            OOoOs        sdb.cramfs
1                g           LlC6Z0zrgy.bin  orcA       sn
2X               gtj         LO0J8         oSx2p        SPaK8l2sYN
3                h           lost+found    OT           SrZznhSAj
3J               H           LvuGM         poiuy7Xdb    t
44aAm            H2Zj8FNbu   lWIRfzP       px6u         T
4A               hdi7        m             Q            TFGVOSwYd.txt
6JR3             hYuPvID     m9V0lIaElz    qkCN8
```

使用base64对flag文件进行解码，得到flag值。

give_you_flag

打开是一个gif，用stegsolve分桢得到隐藏二维码

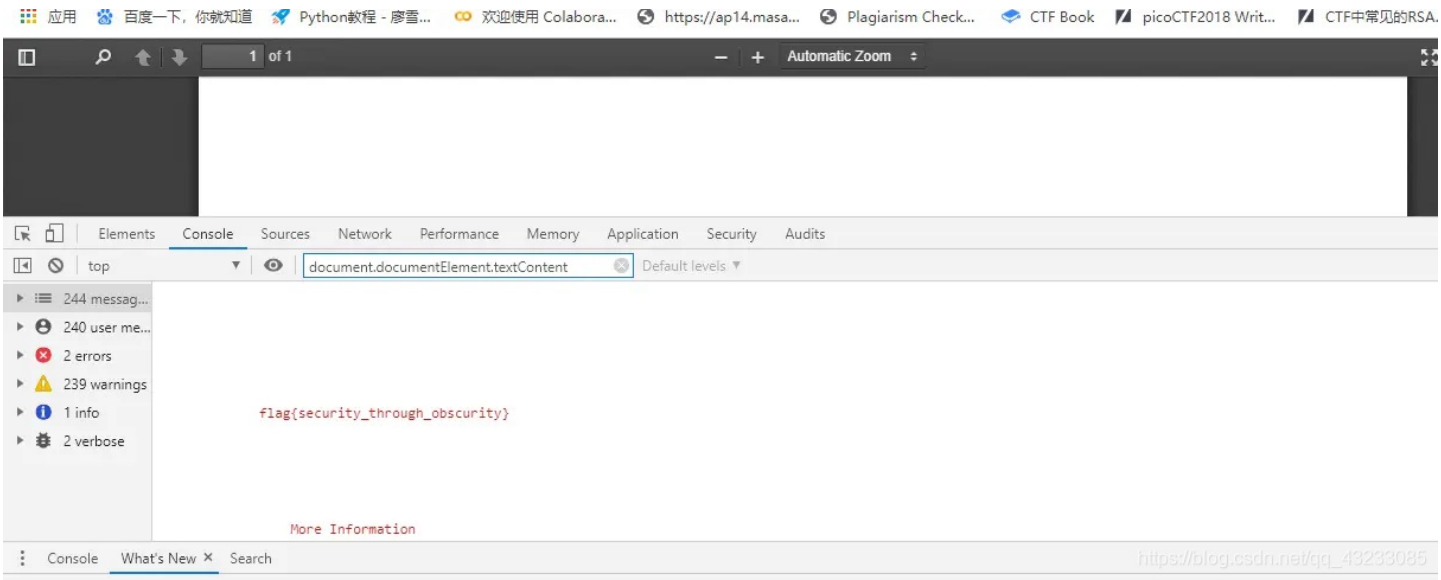


这个二维码少了三个角的定位符，没有定位符肯定是扫不出来东西的，手动画上定位符：

扫描得flag，为flag{e7d478cf6b915f50ab1277f78502a2c5}。

pdf

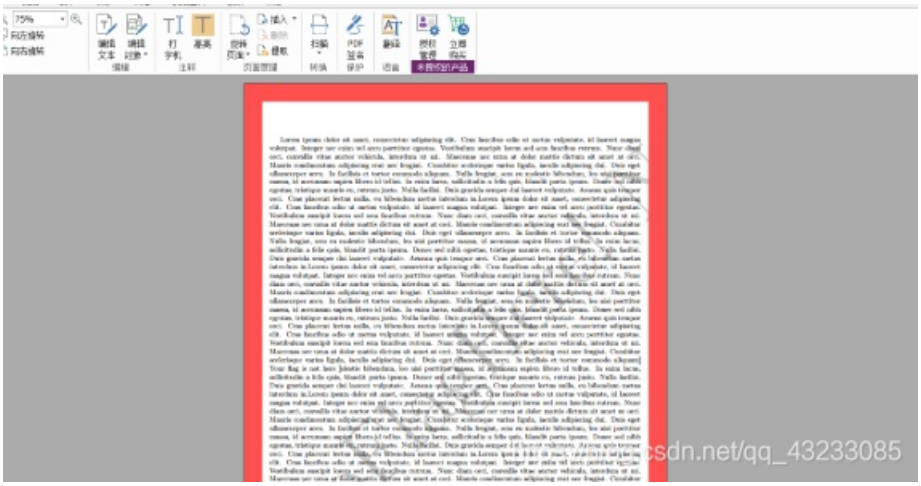
下载后是一个pdf
用谷歌浏览器打开后（在google上安装插件PDF Viewer，进入后一定要刷新！！！控制台输入document.documentElement.textContent）



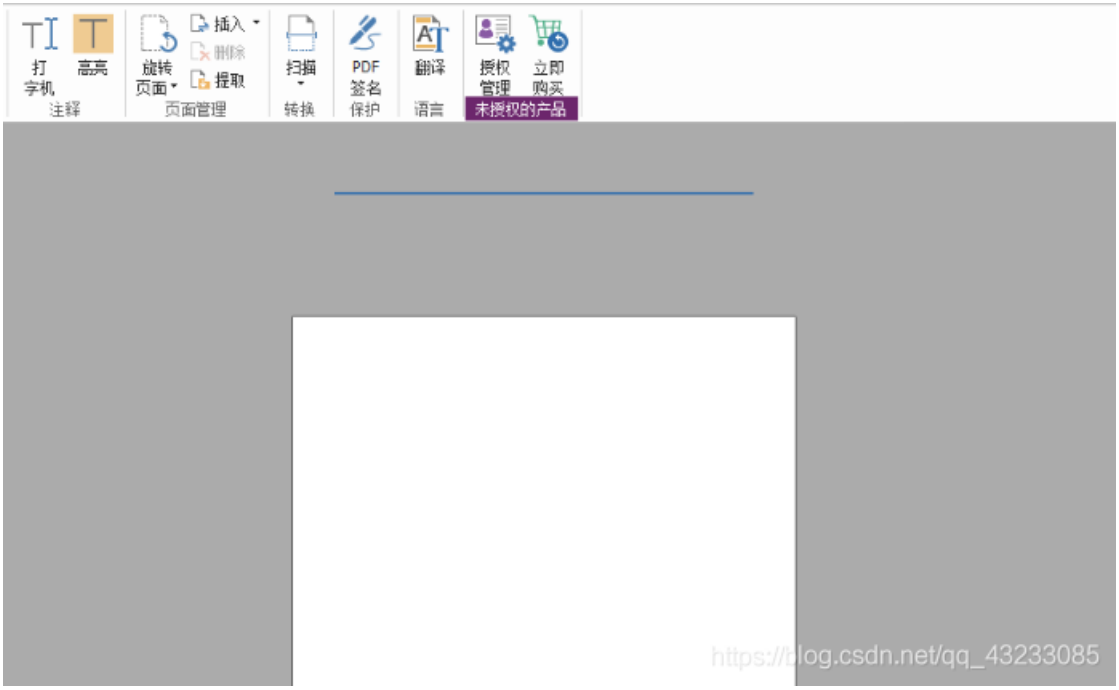
得到pdf上的文本flag{security_through_obscurity}

stegano

用编辑器打开附件，我用的是福昕PDF编辑器



可以看到，到处都是无用的干扰信息，全部干掉！



缩小页面，选择“编辑对象”后框选页面外的一大片区域，发现在页面上方隐藏着一行字符串，将其复制出来：
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
看到AB首先想到的是培根密码，但是培根密码是5个一组，于是又想到摩斯密码，将A替换为.，B替换为-，放到在线摩斯密码加解密网站上解密，得到flag

---

摩斯密码在线翻译

英文摩斯密码翻译工具 可以对英文和数字进行摩斯电码加密解密。如果用到汉字，请使用：中文摩斯密码翻译

输入摩尔斯电码，点击“解密”，即可将摩尔斯电码翻译成可识别的字符。

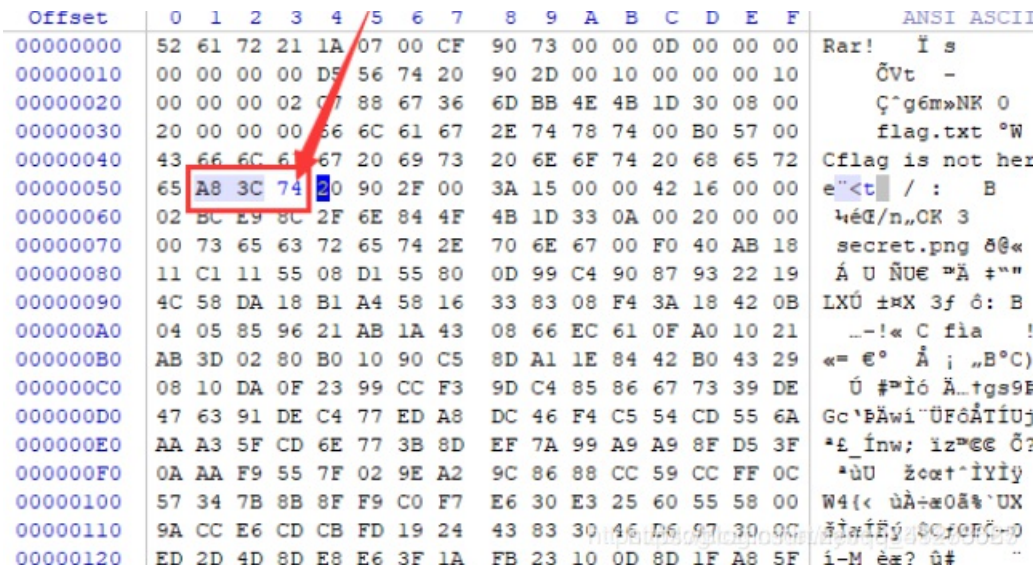
-.-. --- -. --. .-. .- - ..- .-.. .- - .. --- -. ... --..-- ..-. .-.. .- --. ---... .---- -. ...- .---- ..... .---- -... .-.. ...-- -- ...-- ....- --. ...--

得到flag{1nv151bl3m3554g3}。

SimpleRAR

下载文件，解压，里面还有个flag压缩包，解压flag压缩包的时候报错：

我们把它拖进HxD中查看一下，检查文件头，发现0x74位置被修改为0x7A，故修改还原。
再次解压flag.rar，即可得到secret.png，一个白白的图片。



再次把它拖进去！发现是一个gif文件，改一下后缀名。

再次打开发现还是啥也没有。这次再把它拖进stegsolve，一波检查，发现R通道含有半个二维码。
使用stegsolve帧功能模块，得到两张不同的帧图片。

这个时候就要使用伟大的ps工具把它p到一起，还顺带学习了一下ps功能…
扫码得到flag{yanji4n_bu_we1shi}