

# 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](#)

版权声明：本文为博主原创文章，遵循[CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：[https://blog.csdn.net/qq\\_43233085/article/details/103553731](https://blog.csdn.net/qq_43233085/article/details/103553731)

版权

## XCTF攻防世界：MISC新手题解（1~6）

[this\\_is\\_flag](#)

[ext3](#)

[give\\_you\\_flag](#)

[pdf](#)

[stegano](#)

[SimpleRAR](#)

### this\_is\_flag

纯属签到题，直接将 flag 值复制提交就好。

**this\_is\_flag**  9 最佳Writeup由王兆敏提供

难度系数： ★ 1.0

题目来源：暂无

题目描述：Most flags are in the form flag{xxx}, for example:flag{th1s\_is\_a\_d4m0\_4la9}

题目场景：暂无

题目附件：暂无

[https://blog.csdn.net/qq\\_43233085](https://blog.csdn.net/qq_43233085)

### ext3

**ext3**  77 最佳Writeup由hackcat提供

难度系数： ★ 1.0

题目来源：[bugku](#)

题目描述：今天是菜狗的生日，他收到了一个linux系统光盘

题目场景：暂无

题目附件：[附件1](#)

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/07avZhikgKgbF/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       07avZhikgKgbF  RZTOgd
0wDq5         FinD       LG6F        o8      scripts
0Xs           fm         Lh          00o0s  sdb.cramfs
1             g         LlC6Z0zrgy.bin  orcA   sn
2X            gtj       L00J8       oSx2p  SPaK8l2sYN
3             h         lost+found  OT      SrZznhsAj
3J            H         LvuGM       poiuy7Xdb  t
44aAm        H2Zj8FNbu  lWIRfzP     px6u   T
4A           hdi7      m           Q       TFGV0SwYd.txt
6JR3        hYuPvID   m9V0lIaElz  qkCN8
```

```
6w0aZE1VbSW 1 M10 Qm0Y1d
7H7geLLS5 imgLDpt4BY Mnuc QQY3sF63w
root@kali:/mnt# cd 07avZhikgKgbF/
root@kali:/mnt/07avZhikgKgbF# ls
flag.txt
root@kali:/mnt/07avZhikgKgbF# cat flag.txt
ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2piaannor3ncmltcang=
https://blog.csdn.net/qq_43233085
```

使用base64对flag文件进行解码，得到flag值。

```
root@kali:/mnt/07avZhikgKgbF# base64 -d flag.txt
flag{sajbcibzskjjcnbhsbvcjbjyszczsbkzj}root@kali:/mnt/07avZhikgKgbF#
root@kali:/mnt/07avZhikgKgbF#
root@kali:/mnt/07avZhikgKgbF#
```

## give\_you\_flag

give\_you\_flag 👍 16 最佳Writeup由testtestzrs提供

难度系数: ★ 1.0

题目来源: 暂无

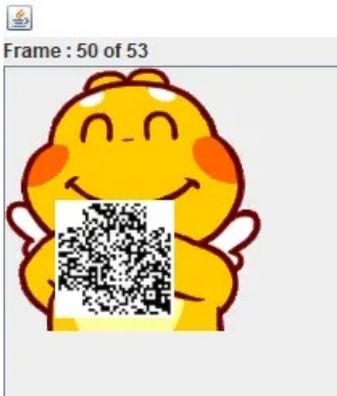
题目描述: 菜狗找到了文件中的彩蛋很开心, 给菜猫发了个表情包

题目场景: 暂无

题目附件: 附件1

[https://blog.csdn.net/qq\\_43233085](https://blog.csdn.net/qq_43233085)

打开是一个gif, 用stegsolve分帧得到隐藏二维码



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

pdf 👍 11 最佳Writeup由S\_O\_L\_R提供

难度系数: ★ 1.0

题目来源: CSAW

题目描述: 菜猫给了菜狗一张图, 说图下面什么都没有

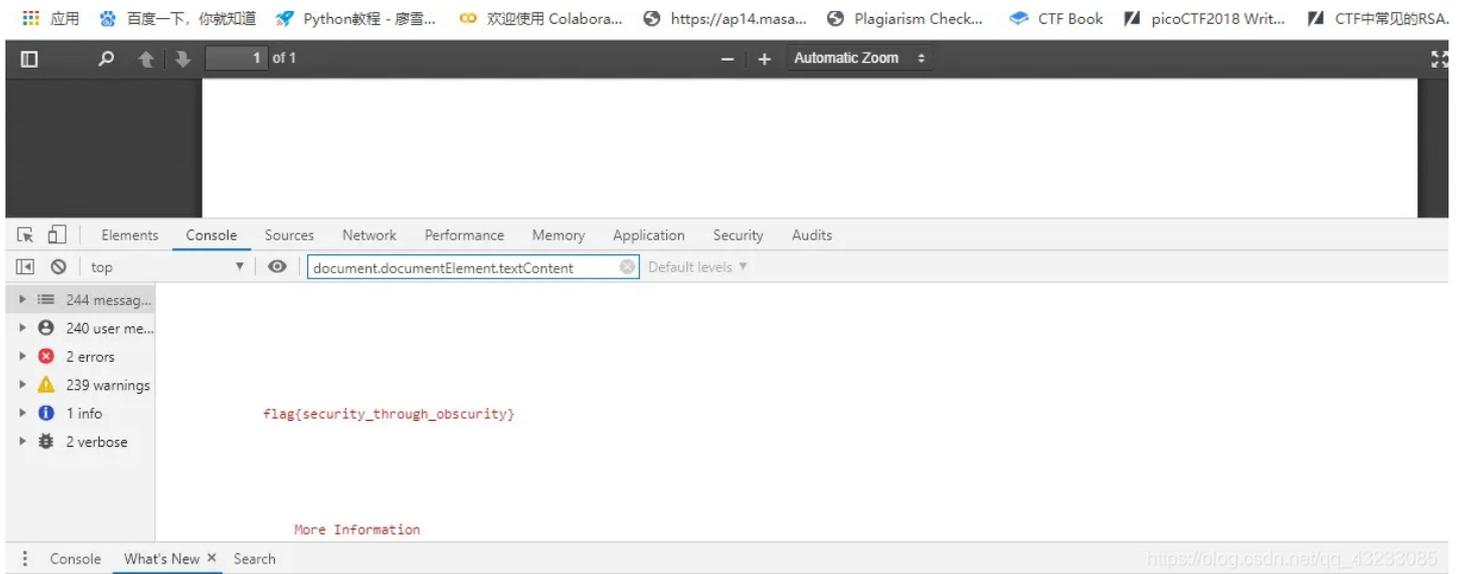
题目场景: 暂无

题目附件: 附件1

[https://blog.csdn.net/qq\\_43233085](https://blog.csdn.net/qq_43233085)

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

stegano 👍 149 最佳Writeup由LK-TEAM • 来自南方的羊提供

难度系数: ★ 1.0

题目来源: CONFidence-DS-CTF-Teaser

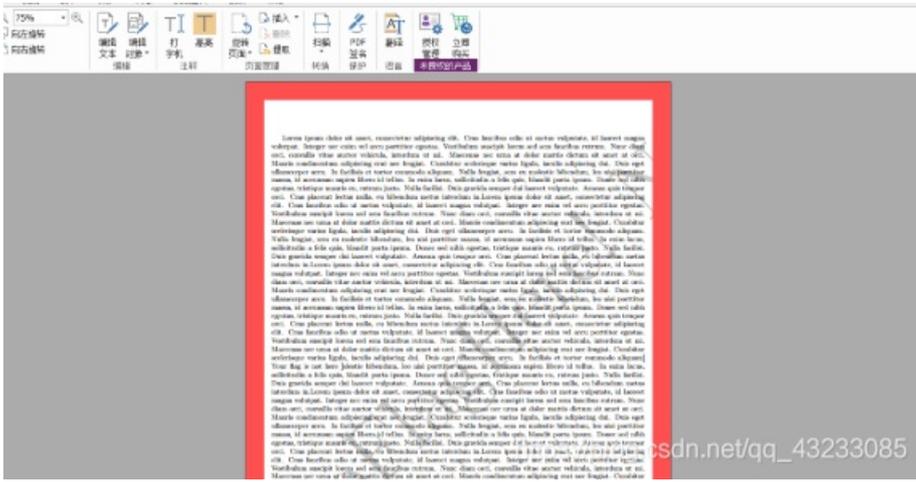
题目描述: 菜狗收到了图后很开心, 玩起了pdf 提交格式为flag{xxx}, 解密字符需小写

题目场景: 暂无

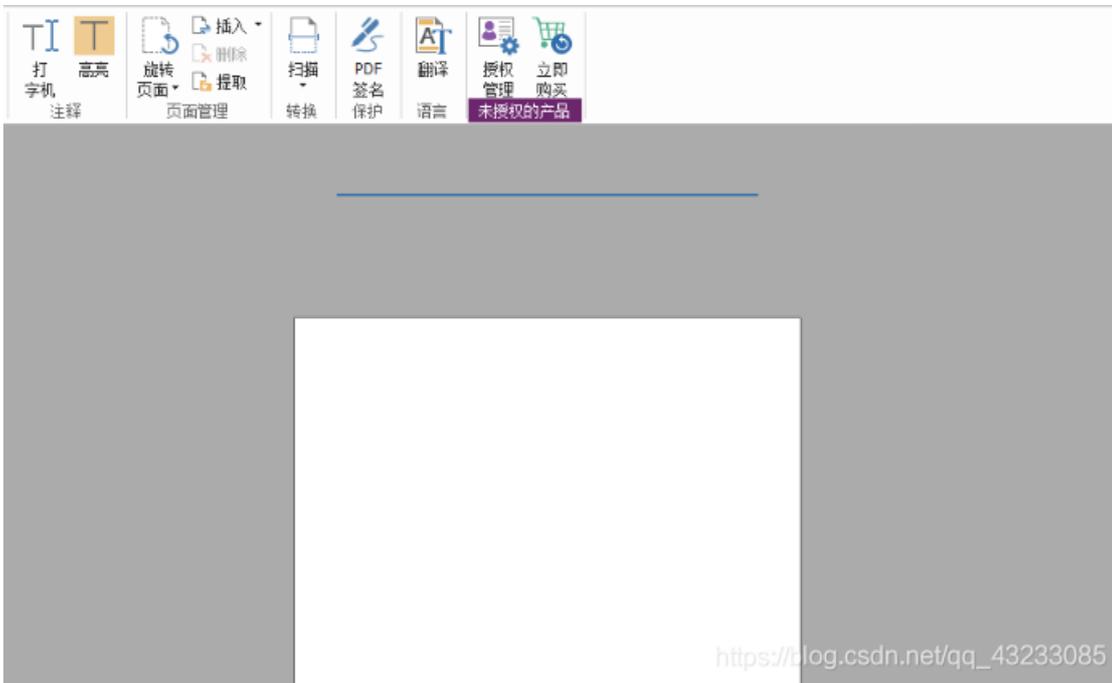
题目附件: 附件1

[https://blog.csdn.net/qq\\_43233085](https://blog.csdn.net/qq_43233085)

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。

-----  
-----  
-----

解密

congratulations,flag:1nv151bl3m3554g3

推荐: 中文摩斯密码翻译 >

[https://blog.csdn.net/qq\\_43233085](https://blog.csdn.net/qq_43233085)

得到flag{1nv151bl3m3554g3}。

## SimpleRAR

SimpleRAR 👍 10 最佳Writeup由它山提供

难度系数: ★ 1.0

题目来源: 08067CTF

题目描述: 菜狗最近学会了拼图, 这是他刚拼好的, 可是却搞错了一块(ps:双图层)

题目场景: 暂无

题目附件: 附件1

[https://blog.csdn.net/qq\\_43233085](https://blog.csdn.net/qq_43233085)

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:

### WinRAR:诊断信息

信息

❗ 文件头已损坏: secret.png

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。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar! ĩ s
00000010	00	00	00	00	D5	56	74	20	90	2D	00	10	00	00	00	10	Œvt -
00000020	00	00	00	02	07	88	67	36	6D	BB	4E	4B	1D	30	08	00	Ç`g6m»NK 0
00000030	20	00	00	00	36	6C	61	67	2E	74	78	74	00	B0	57	00	flag.txt °W
00000040	43	66	6C	61	67	20	69	73	20	6E	6F	74	20	68	65	72	Cflag is not her
00000050	65	A8	3C	74	20	90	2F	00	3A	15	00	00	42	16	00	00	e"<t / : B
00000060	02	BC	E9	8C	2F	6E	84	4F	4B	1D	33	0A	00	20	00	00	4éQ/n„OK 3
00000070	00	73	65	63	72	65	74	2E	70	6E	67	00	F0	40	AB	18	secret.png 8@«
00000080	11	C1	11	55	08	D1	55	80	0D	99	C4	90	87	93	22	19	Á U ÑUE »Ä ±""
00000090	4C	58	DA	18	B1	A4	58	16	33	83	08	F4	3A	18	42	0B	LXÚ ±»X 3f ó: B
000000A0	04	05	85	96	21	AB	1A	43	08	66	EC	61	0F	A0	10	21	...!« C fia !
000000B0	AB	3D	02	80	B0	10	90	C5	8D	A1	1E	84	42	B0	43	29	«= e° Á ; „B°C)
000000C0	08	10	DA	0F	23	99	CC	F3	9D	C4	85	86	67	73	39	DE	Ú #»ió Ä..tgs9E
000000D0	47	63	91	DE	C4	77	ED	AB	DC	46	F4	C5	54	CD	55	6A	Gc`pÄwi`ÜFóÄTIUj
000000E0	AA	A3	5F	CD	6E	77	3B	8D	EF	7A	99	A9	8F	D5	3F		*f ínw; iz»EE Ó?
000000F0	0A	AA	F9	55	7F	02	9E	A2	9C	86	88	CC	59	CC	FF	0C	*ùU žcøt`iYiÿ
00000100	57	34	7B	8B	8F	F9	C0	F7	E6	30	E3	25	60	55	58	00	W4{< úÄ±«0Ä%`UX
00000110	9A	CC	E6	CD	CB	FD	19	24	43	83	30	46	D6	97	30	9C	Äi»iÿÿ`CC`CFÿ»0
00000120	ED	2D	4D	8D	E8	E6	3F	1A	FB	23	10	0D	8D	1F	A8	5F	i-M èæ? ú# "

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}