

攻防世界 Misc新手练习区 1-12 全详解

原创

思源湖的鱼  于 2020-10-13 23:29:22 发布  2402  收藏 32

分类专栏: [ctf](#) 文章标签: [misc](#) [攻防世界](#) [ctf](#)

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/weixin_44604541/article/details/109058125

版权

CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

前言

对web有了一定了解

开始玩Misc

本篇是攻防世界 Misc新手练习区的全解

1、this_is_flag

this_is_flag  66 最佳Writeup由王兆敏提供

难度系数:    2.0

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/weixin_44604541

嗯

签到打卡

直接给出来了

2、pdf

pdf

👍 62 最佳Writeup由S_O_L_R提供

难度系数:  3.0

题目来源: [csaw](#)

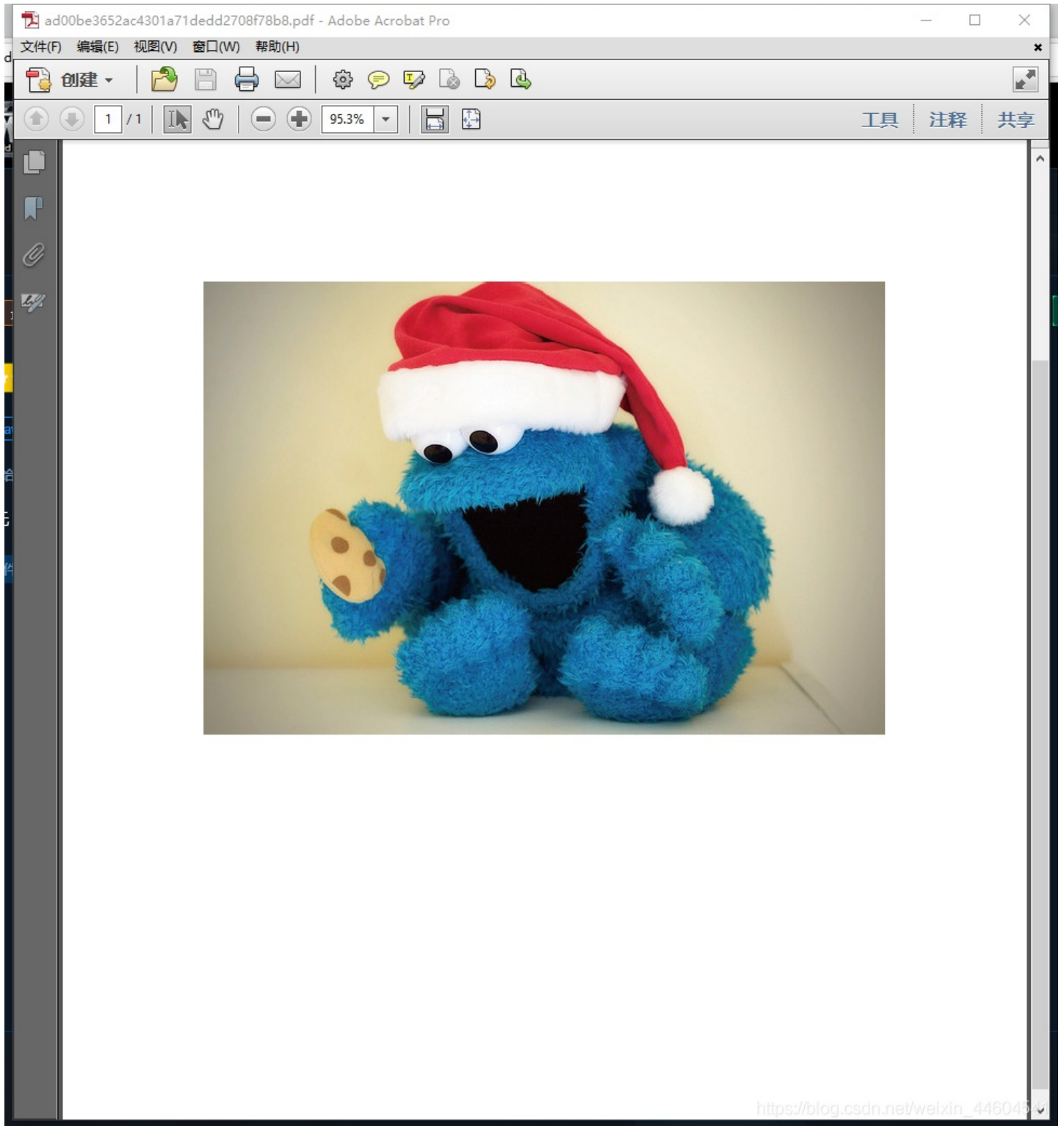
题目描述: 菜猫给了菜狗一张图, 说图下面什么都没有

题目场景: 暂无

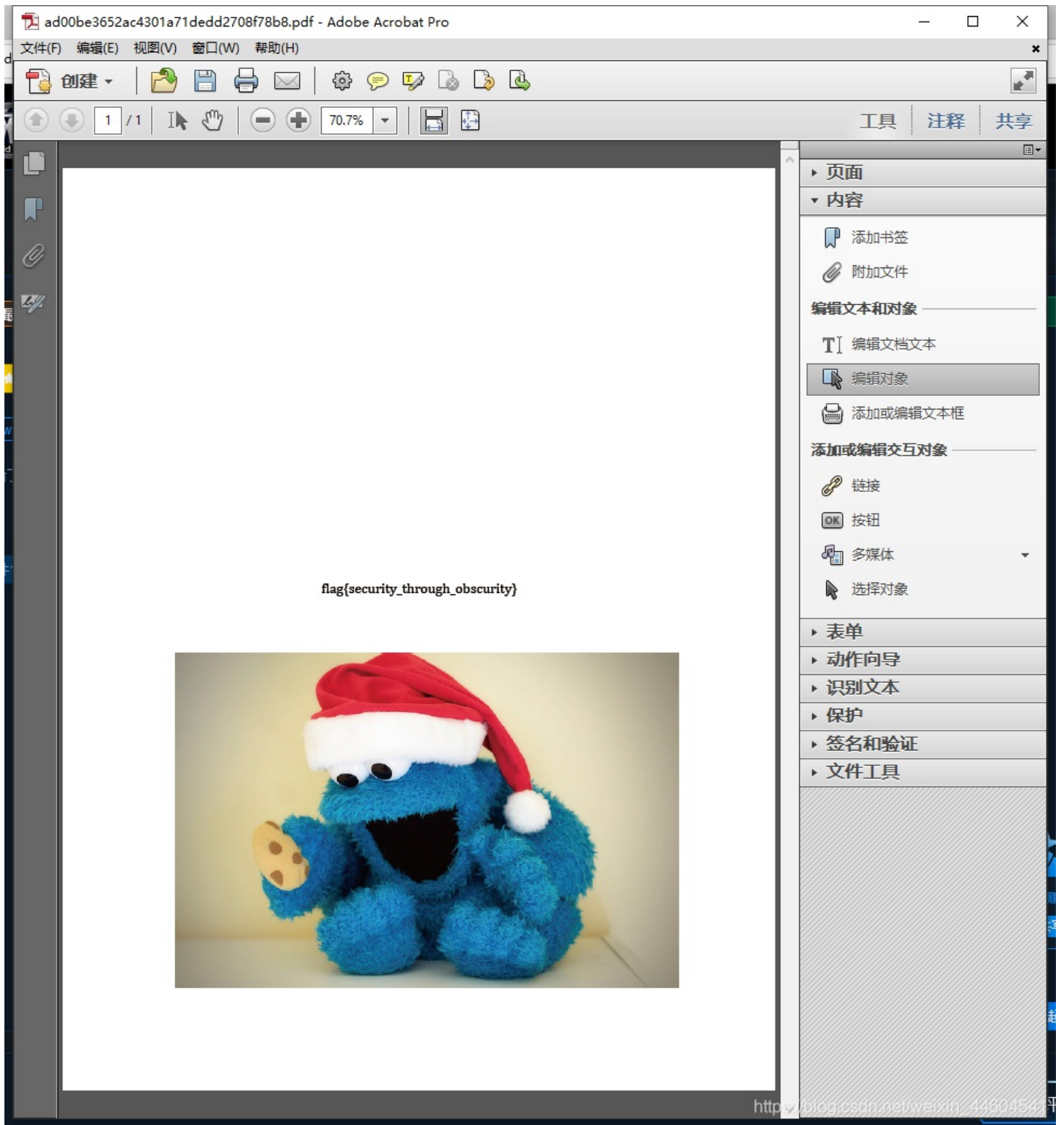
题目附件: [附件1](#)

https://blog.csdn.net/weixin_44604541

打开附件如下



根据提示
flag应该被图片挡住了



编辑下
挪开图片就有了

3、give_you_flag

give_you_flag 👍 59 最佳Writeup由testtestzrs提供

难度系数: ★★★★ 4.0

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

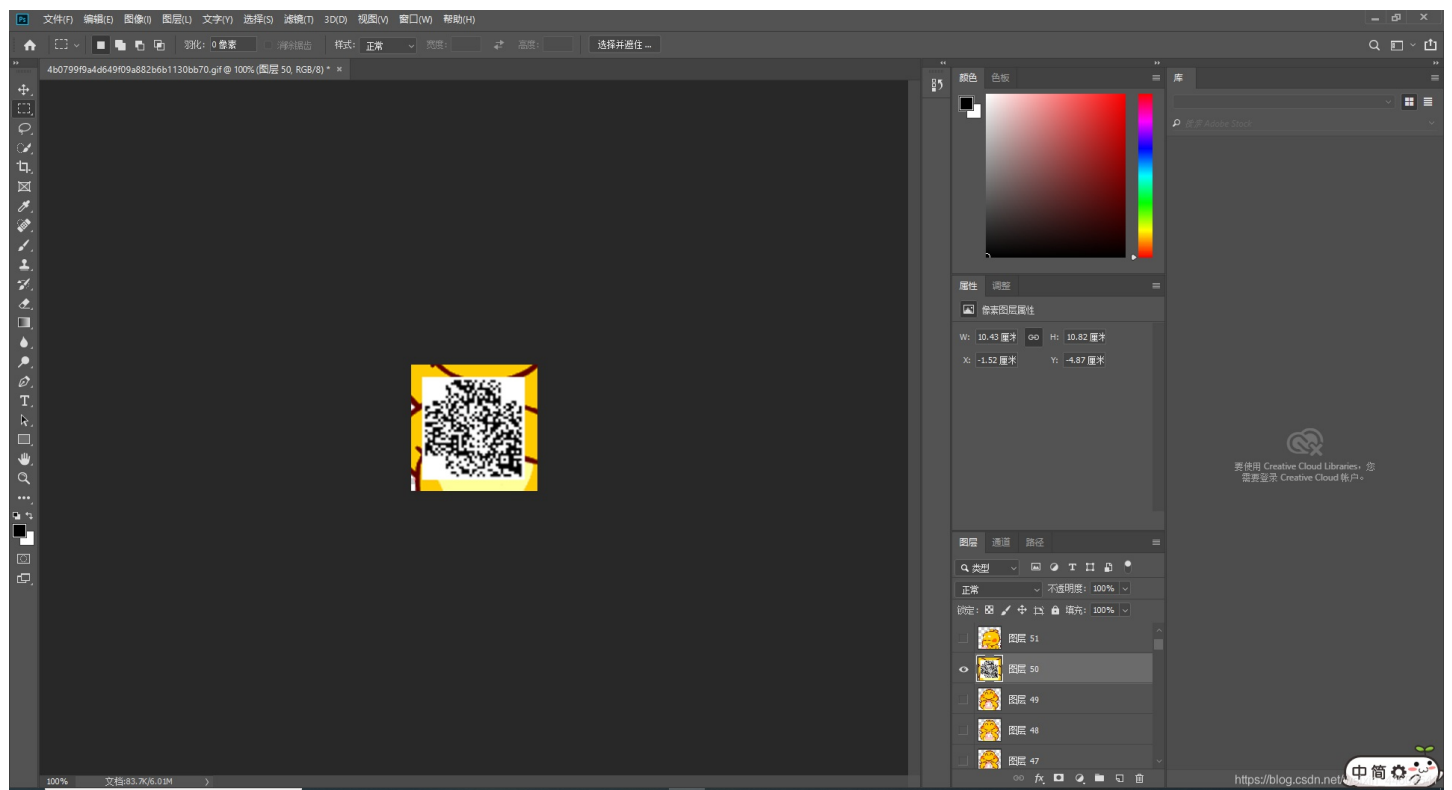
题目附件: 附件1

https://blog.csdn.net/weixin_44604541

打开是gif格式图片

有一张二维码一闪而过

打开ps



在第50帧发现残缺二维码

补上定位

再扫描



获得flag

4、坚持60s

坚持60s 👍 9 最佳Writeup由不要让我起名提供

难度系数: ★★★★ 4.0

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1

https://blog.csdn.net/weixin_44604541

下载下来是个jar



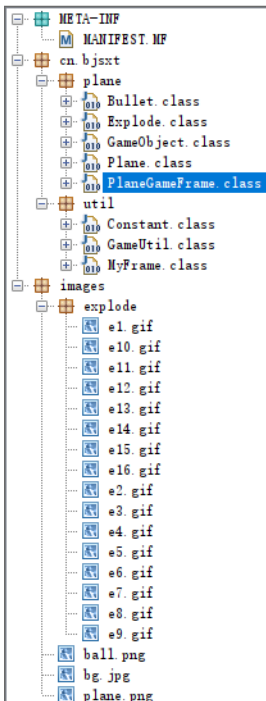
上下左右控制方块躲避障碍

.....



充满了恶意

直接反编译看源码



```

}
}
}
if (!this.p.isLive()) {
    printInfo(g, "兄弟就死了的嘛", 50, 150, 200);
    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, 炊事班长咧兄弟", 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);
            break;
    }
}
}
}

public void printInfo(Graphics g, String str, int size, int x, int y) {
    Color c = g.getColor();
    g.setColor(Color.RED);
    Font f = new Font("宋体", 1, size);
    g.setFont(f);
    g.drawString(str, x, y);
    g.setColor(c);
}

public static void main(String[] args) {

```

https://blog.csdn.net/weixin_44604541

找到flag

开心的提交

...

错误

定睛一看

还得base64

文字加密解密

MD5加密/解密

URL加密

JS加/解密

JS混淆加密压缩

ESCAPE加/解密

BASE64

散列/

DajiDali_JinwanChiji

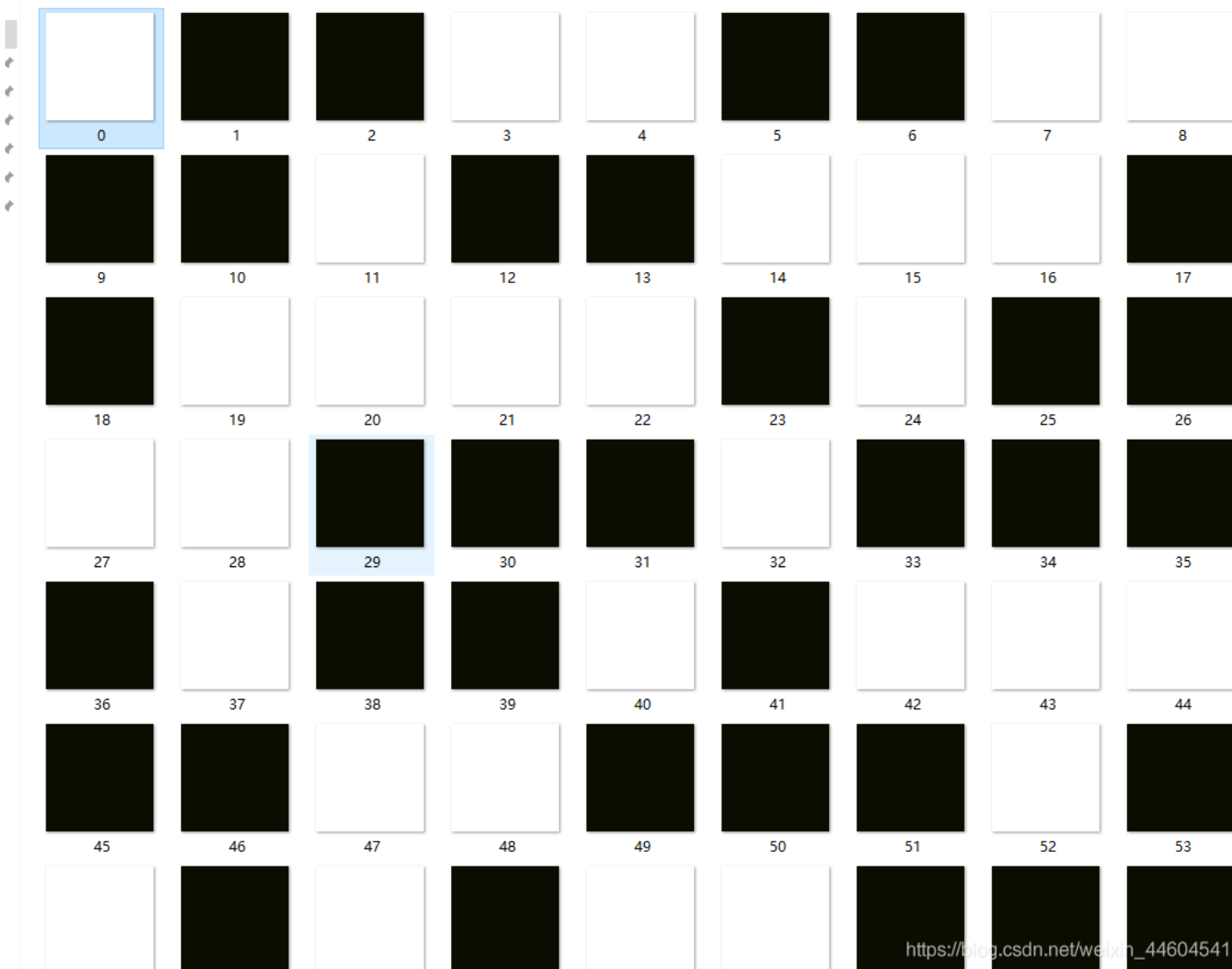
RGFqaURhbGlfSmlud2FuQ2hpamk=

获得flag

5、gif

下下来一个压缩包

解压后是104张图片



黑白黑白黑白

这不得是二进制?

```
01100110011011000110000101100111011110110100011001110101010011100101111101100111011010010100011001111101
```

简单写个脚本

```
flag=""
string="01100110011011000110000101100111011110110100011001110101010011100101111101100111011010010100011001111101"
for i in range(0,len(string),8):
    s=string[i:i+8]
    flag+=chr(int(s,2))
print (flag)
```

```
1 flag=""
2 string="01100110011011000110000101100111011110110100011001110101010011100101111101100111011010010100011001111101"
3 for i in range(0,len(string),8):
4     s=string[i:i+8]
5     flag+=chr(int(s,2))
6 print (flag)
```

```
flag(FuN_giF)
```

```
<completed in 160.00 ms>
```

https://blog.csdn.net/weixin_44604541

获得flag

6、掀桌子

掀桌子

👍 86 最佳Writeup由flag(not_here) • 渣渣焉提供

WP 建议

难度系数: ★★★★★ 4.0

题目来源: DDCTF2018

题目描述: 菜狗截获了一份报文如下c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfabe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2, 生气地掀翻了桌子(´•ω•)ノ(ノ)ノ

题目场景: 暂无

题目附件: 暂无

https://blog.csdn.net/weixin_44604541

就是这串东西解码呗

```
c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfabe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2
```

试了试

。。。

真的掀桌子了

不是任何现成的加密手段

再定睛一看

只有a-f和数字

这怕不是16进制

转换为10进制看看

```
import re
a = 'c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfabe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2'
a = re.findall('{2}',a)
a = [int(i, 16) for i in a]
print(a)
```

```
1 import re
2 a = 'c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfabe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2'
3 a = re.findall('{2}',a)
4 a = [int(i, 16) for i in a]
5 print(a)
```

```
[200, 233, 172, 160, 198, 242, 229, 243, 232, 196, 239, 231, 161, 160, 212, 232, 229, 160, 230, 236, 225, 231, 160, 233, 243, 186, 160, 232, 234, 250, 227, 249, 228, 234, 250, 226, 234, 228, 227, 234, 235, 250, 235, 227, 245, 231, 233, 243, 228, 227, 232, 234, 249, 234, 243, 226, 228, 230, 242]
```

<<completed in 454.00 ms>

数字在160到250之间

哽住

。。。。。

然后突然想到

160=128+32

这不得是ascii码

```
a = [chr(i - 128) for i in a]
s = "".join(a)
print(s)
```

```
1 import re
2 a = 'c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baae8eafae3f9e4eafae2eae4e3
3 a = re.findall('.{2}',a)
4 a = [int(i, 16) for i in a]
5 print(a)
6 a = [chr(i - 128) for i in a]
7 s = "".join(a)
8 print(s)
```

[200, 233, 172, 160, 198, 242, 229, 243, 232, 196, 239, 231, 161, 160, 212, 232, 229, 160, 230, 236, 225, 231, 160, 233, 243, 186, 160, 232, 234, 250, 227, 249, 228, 234, 250, 226, 234, 228, 227, 234, 235, 250, 235, 227, 245, 231, 233, 243, 228, 227, 232, 234, 249, 234, 243, 226, 228, 230, 242]

Hi, FreshDog! The flag is:
hjzcydjzbdjckzkcugisdchjyjsbdf
<completed in 382.00 ms>

https://blog.csdn.net/weixin_44604541

获得flag

是该掀桌子

蛋疼

7、如来十三掌

是个word文件

内容如下

夜哆悉譜多苦奢陀奢諦冥神哆盧穆幡三侄三即諸譜即冥迦冥隸數顛耶迦奢若吉佉陀
語怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧幡豆蒙密離怯婆幡礙他哆提哆
多鉢以南哆心曰姪罰蒙訥神。舍切真怯勝訥得俱沙罰娑是怯遠得訥數罰輸哆遠薩得
槃漫夢盧幡亦醜訥娑幡瑟輸譜尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿幡沙蘇
輸奢恐豆侄得罰提哆伽譜沙楞鉢三死怯摩大蘇者數一遮

我*&.....%¥#

这是啥加密

查了查

一个网站与佛论禅

与佛论禅

MzkuM3gvMUAwnzuvn3cgozMLMTuvqzAenJchMUAeqzWenzEmLJW9

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

命由己造，相由心生

佛曰：夜哆悉譜多苦奢陀奢諦冥神哆盧穆幡三侄三即諸譜即冥迦冥隸數顛耶迦奢若吉佉陀語怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧幡豆蒙密離怯婆幡礙他哆提哆多鉢以南哆心曰姪罰蒙訥神。舍切真怯勝訥得俱沙罰娑是怯遠得訥數罰輸哆遠薩得槃漫夢盧幡亦醜訥娑幡瑟輸譜尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿幡沙蘇輸奢恐豆侄得罰提哆伽譜沙楞鉢三死怯摩大蘇者數一遮

https://blog.csdn.net/weixin_44604541

获得字符串

MzkuM3gvMUAwnzuvn3cgozMLMTuvqzAenJchMUAeqzWenzEmLJW9

还是蛋疼

这是啥加密

题目为什么是十三掌？

跟13有关的加密

rot13



ROT13解密计算器

字符串

MzkuM3gvMUAwnzuvn3cgozMIMTuvqzAenJchMUAeqzWenzEmLJW9

计算

解码结果

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

复制

https://blog.csdn.net/weixin_44604541

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

。。。。

蛋碎了

又是一番折腾

都陷入怀疑了

然后

发现还得再来一个base64

文字加密解密

MD5加密/解密

URL加密

JS加/解密

JS混淆加密压缩

ESCAPE加/解密

BASE64

散列/哈希

迅雷, 快车, 旋风URL加密

flag{bdscjhbkmfrdhbckijndskvbkjdsab}

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

多行

Base64加密

Base64解密

清空结果

https://blog.csdn.net/weixin_44604541

获得flag

生活不易

唉声叹气

佛了

8、stegano

下下来是个pdf

搜索flag



无内容

挠头

...

查了查

得用chrome打开pdf

再ctrlA→ctrlC

黏贴到txt文件中

会出现BABABABA

NoFlagHere! NoFlagHere! NoFlagHere! XXX
BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA AB
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laore

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 AB
BBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB

瞅着就是摩斯密码
转换下

```
a = 'BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA B  
a = a.replace("A", ".")  
a = a.replace("B", "-")  
print(a)
```

<completed in 97.00 ms>
https://blog.csdn.net/weixin_44604541

.....
.....

解码得到

congratulations,flag:1nv151b13m3554g3

获得flag

一开始用adobe看pdf
啥都么得
BABABA也么得

9、SimpleRAR

SimpleRAR 49 最佳Writeup由它山提供

难度系数: 5.0

题目来源: 08067CTF

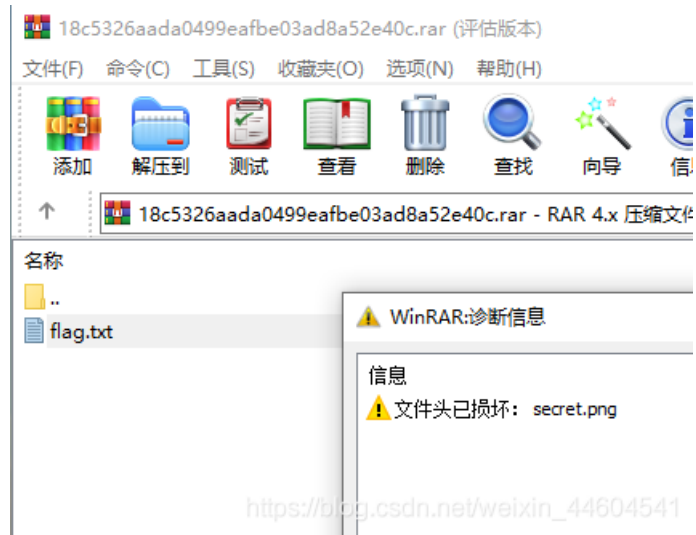
题目描述: 菜狗最近学会了拼图, 这是他刚拼好的, 可是却搞错了一块(ps:双图层)

题目场景: 暂无

题目附件: [附件1](#) https://blog.csdn.net/weixin_44604541

下载下来一个rar

但是解压报错



https://blog.csdn.net/weixin_44604541

用winhex打开看看

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	Övt -
00000020	00	00	00	02	C7	88	67	36	6D	BB	4E	4B	1D	30	08	00	Ç^g6m»NK 0
00000030	20	00	00	00	66	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	7A	20	90	2F	00	3A	15	00	00	42	16	00	00	e"<z / : B
00000060	02	BC	E9	8C	2F	6E	84	4F	4B	1D	33	0A	00	20	00	00	4éG/n„OK 3
00000070	00	73	65	63	72	65	74	2E	70	6E	67	00	F0	40	AB	18	secret.png δ@«
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

寻找secret.png

查了下

这里的问题是

png是文件块，应该用74

但这里是7A，变成子块了

参考RAR文件格式官方说明书的翻译[中英对照]

修改下

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	Övt -
00000020	00	00	00	02	C7	88	67	36	6D	BB	4E	4B	1D	30	08	00	Ç^g6m»NK 0
00000030	20	00	00	00	66	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	7A	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	4éG/n„OK 3
00000070	00	73	65	63	72	65	74	2E	70	6E	67	00	F0	40	AB	18	secret.png δ@«
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

打开rar文件

18c5326aada0499eafbe03ad8a52e40c.rar (评估版本)

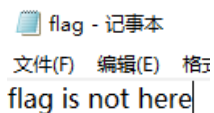
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)



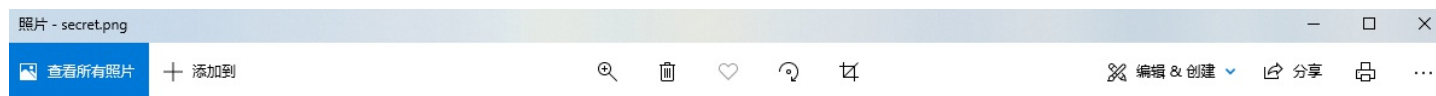
18c5326aada0499eafbe03ad8a52e40c.rar - RAR 4.x 压缩文件, 解包大小为 5,714 字节

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
flag.txt	16	16	文本文档	2017/10/14 23:27	366788C7
secret.png	5,698	5,434	PNG 文件	2017/10/15 16:35	2F8CE9BC

flag.txt里没东西



secret.png文件全空白



https://blog.csdn.net/weixin_44604544

用ps看看

结果提示不是png文件

...

那继续winhex打开

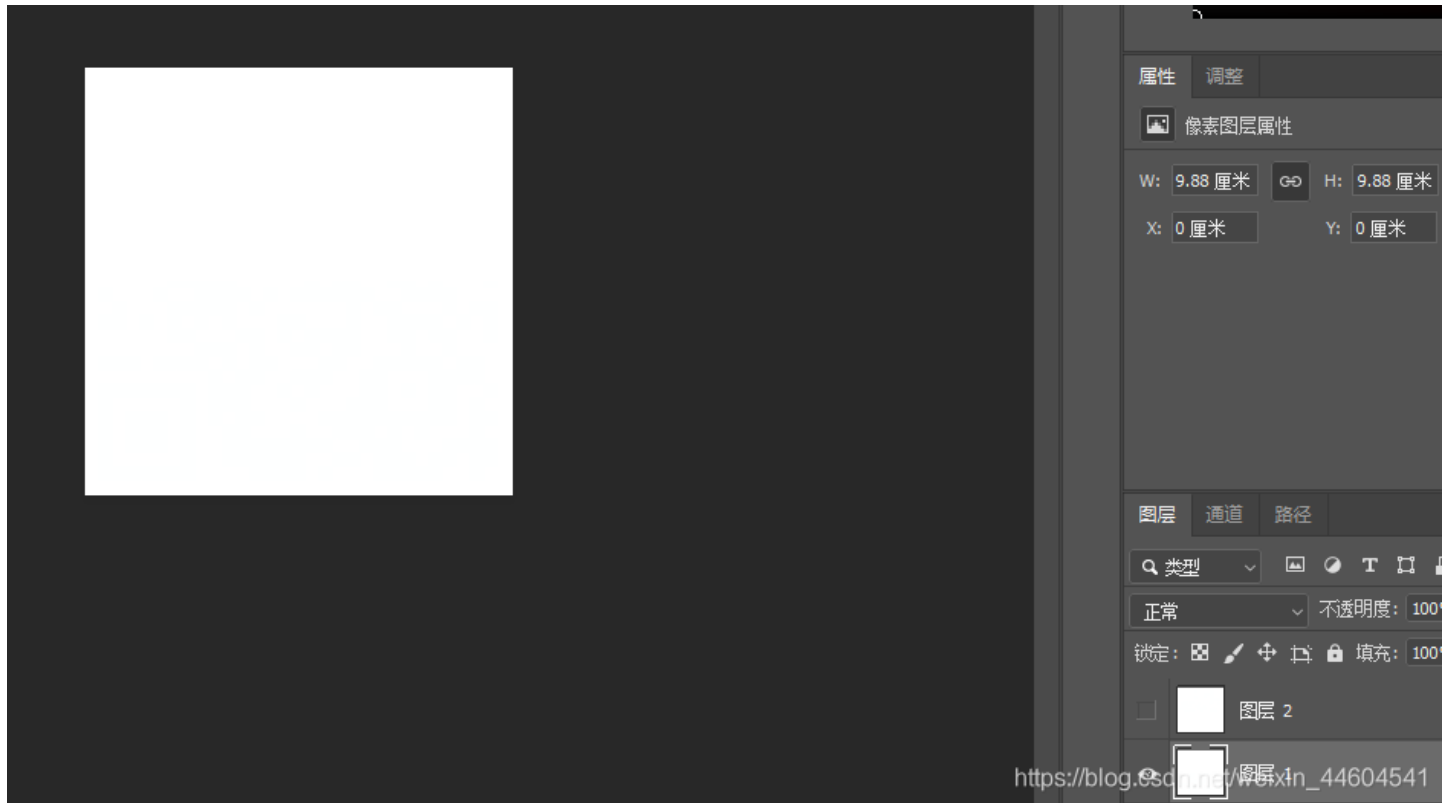
secret.png																ANSI ASCII		
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
00000000	47	49	46	38	39	61	18	01	18	01	91	02	00	FE	FF	FF	GI	89a \ pÿÿ
00000016	FF	FF	FF	FF	FF	FF	00	00	00	21	FF	0B	58	4D	50	20	ÿÿÿÿÿÿ	!ÿ XMP
00000032	44	61	74	61	58	4D	50	3C	3F	78	70	61	63	6B	65	74	DataXMP<?xpacket	

发现原来是个gif

改后缀名

然后扔ps

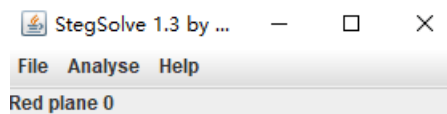
...



还是没东西啊

...

扔stegsolve

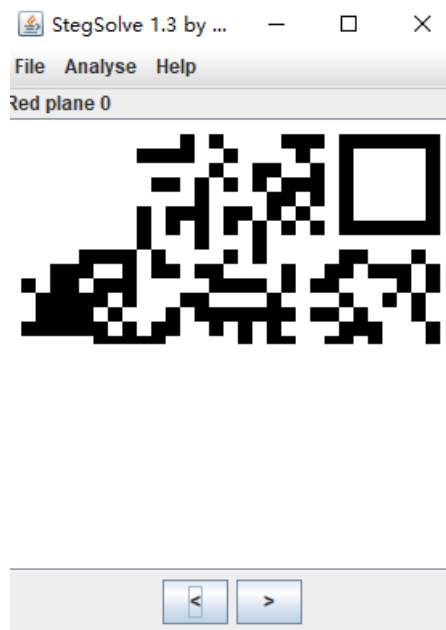


但只有一半二维码

。 。 。

想到ps打开的时候有两个图层

把另一个导出来看看



发现另一半

又是ps



已解码数据 1:

位置:(21.5,24.0)-(347.7,23.7)-(21.5,343.2)-(347.7,342.8)
颜色正常, 正像
版本: 3
纠错等级:H, 掩码:4
内容:
[flag{yanji4n_bu_we1shi}](https://blog.csdn.net/weixin_44604541)

https://blog.csdn.net/weixin_44604541

得到flag

10、base64stego

base64stego

👍 97 最佳Writeup由CTFshow • zEr0_0提供

难度系数: ★★★★★ 5.0

题目来源: olympicCTF

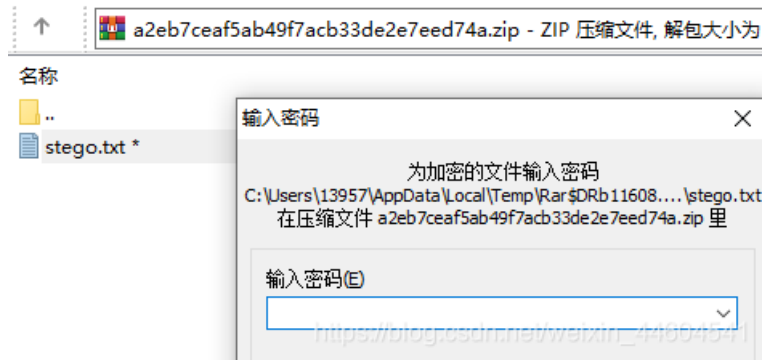
题目描述: 菜狗经过几天的学习, 终于发现了如来十三掌最后一步的精髓

题目场景: 暂无

题目附件: 附件1

https://blog.csdn.net/weixin_44604541

下载下来一个zip文件
解压要密码



挠头
这没有任何信息啊

查了查
伪加密
winrar修复功能修复一下就可以打开了
(还有这样的)
伪加密专题

得到一大串base64

stego - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
U3RIZ2Fub2dyYXBoeSBpcyB0aGUgYXJ0IGFuZCBzY2llbmNlIG9m
IHdyaXRpbmcaGlkZGVuIG1lc3NhZ2VzIGlulHN1Y2ggYSB3YXkgdGhhdCBubyBvbV=
LCBhcGFydCBmcm9tIHRoZSBzZW5kZXIgaW5kIGludGVuZGVkIHJlY2lwaWVudCwgc3VzcGU=
Y3RzIHRoZSBleGlzdGVuY2Ugb2YgdGhllG1lc3M=
YWdlLCBhIGZvc0g2Ygc2VjdXJpdHkgdGhyb3VnaCBvYnNjdXJpdHkuIFS=
aGUgd29yZCBzdGVnYW5vZ3JhcGh5IGlzlG9mIEdyZWVrIG9yaWdpbiBhbmQgbWVhbnMglmNvbmluY2
bGVkIHdyaXRpbmciIGZyb20gdGhllEdyZWVrIHdvcmlzIHNoZWdhbm9zIG1lYW5pbmclmNv
dmVyZWQgb3IgcHJvdGVjdGVkIiwgYW5kIGdyYXBoZWlulG1lYW5pbmclnRvIHc=
cmI0ZSulFRoZSBmaXJzdCBzZW5kIGludGVuZGVkIHJlY2lwaWVudCwgc3VzcGU=
YW5uZXMgVHJpdGhllbWl1cyBpbiBoaXMgU3RIZ2Fub2dyYXBoaWEsIGEdHJlYV==
dGlzZSBvbiBjcnlwdG9ncmFwaHkgYW5kIHNoZWdhbm9ncmFwaHkgZGlzZ8==
dWlzZWQgYXMGYSBib29rIG9uIG1hZ2JlLiBHZW5lcmFsbHksIG1lc3P=
YWdlcyB3aWxsIGFwcGVhcnB0byBiZSBzY21ldGhpbmclZG9yIHNoZWdhbm9zIG1lYW5pbmcl
Y2xlcwgc2hvcHBpbmclZG9yIHNoZWdhbm9zIG1lYW5pbmclZG9yIHNoZWdhbm9zIG1lYW5pbmcl
aGVyIGNvdmlvY2VudGV4dCBhbmQsIGNsYXNzaWNhbGx5LCB0aGUgaGlkZGVuIG1lc3NhZ2UgbWF5IGl
c2libGUgaW5rIGludHdlZW4gdGhllHZpc2libGUgbGluZXMgY2YgYSBwcmI2YXRlIGxldHRlci4NCg0K
VGhIGFkdmludGVuZSBvZiBzdGVnYW5vZ3JhcGh5LCBvdmluY2VzIG1lYW5pbmclZG9yIHNoZWdh
eXB0b2dyYXBoeSBhbG9uZSwwgaXMgdGhhdCBtZXNzYWdlcyBkbyBub3QgYXR0cmFjdCBhdHRlbnRpb25=
IHRvIHRoZW1zZWx2ZXMuIFBsYWlubHkgdmlzaWJsZSBibmNyeXB0ZWQgbWVzc2FnZXOXbW8gbWF0dC
aG93IHVuYnJlYWthYm91dG9yIG9uIG1hZ2JlLiBHZW5lcmFsbHksIG1lc3P=
dXNwaWNpb24sIGFuZCBtYXkgYW4gdGhllbHJlcyBiZSBpbmNyaW1pbmF0aW5nIP==
aW4gY291bnRyaWVzIHdoZXJlIGVuY3J5cHRpb24gaXMgaWxsZWdhbC4gVGhlcmlmY291bnRyaWVz
IHdoZXJlYXMGY3J5cHRvZ3JhcGh5IHByb3RlY3RzIHRoZSBjb250ZW50cyBvZj==
IGEdyZWVzc2FnZSwwgaXMgdGhhdCBtZXNzYWdlcyBkbyBub3QgYXR0cmFjdCBhdHRlbnRpb25=
b3R0IG1lc3NhZ2VzIGFuZCBjb21tdW5pY2F0aW5nIHhcnRpbmclZG9yIHNoZWdhbm9ncmFwaHkgYW
```

查了查

是base64隐写

脚本

```
# -*- coding: cp936 -*-
import base64
b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
with open('stego.txt', 'rb') as f:
    bin_str = ''
    for line in f.readlines():
        stegb64 = str(line, "utf-8").strip("\n")
        rowb64 = str(base64.b64encode(base64.b64decode(stegb64)), "utf-8").strip("\n")
        offset = abs(b64chars.index(stegb64.replace('=', ''))[-1]) - b64chars.index(rowb64.replace('=', ''))[-1])
        equalnum = stegb64.count('=') #no equalnum no offset
        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)
    print("".join([chr(int(bin_str[i:i + 8], 2)) for i in range(0, len(bin_str), 8)])) #8 位一组
```


ZmxhZ3tzYWpiY2lienNrampbmJoc2J2Y2pianN6Y3N6Ymt6an0=

瞅着是base64

文字加密解密 MD5加密/解密 URL加密 JS加/解密 JS混淆加密压缩 ESCAPE加/解密 **BASE64** 散列/哈希 迅雷, 快车, 旋风URL加密

flag(sajbcibzskjcnbhsbvcjbszcszpkzj)

ZmxhZ3tzYWpiY2lienNrampbmJoc2J2Y2pianN6Y3N6Ymt6an0=

多行
 Base64加密
Base64解密
清空结果

得到flag

12、功夫再高也怕菜刀

下下来一个pcapng文件

这应该是个流量文件

wireshark

搜索flag

```

Line-based text data: text/html (7 lines)
->|./\t2017-12-08 11:42:11\t0\t0777\n
..\t2017-12-08 11:39:10\t4096\t0777\n
1.php\t2017-12-08 11:33:16\t33\t0666\n
6666.jpg\t2017-12-08 11:42:11\t102226\t0666\n
flag.txt\t2017-12-08 11:35:29\t17\t0666\n
hello.zip\t2017-12-08 09:32:36\t224\t0666\n
|<-
  
```

追踪该TCP流

注: jpg格式以FFD8FF开头, 以FFD9结尾

```

aa=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRp
c3BsYXlfZXJyb3JzIiwicCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0
X21hZ2ljX3F1b3Rlc19ydW50aw1lKDApO2VjaG8oIi0%2BfcIpOzskZj
1iYXNlNjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JGM9JF9QT1NUWyJ6Mi
JdOyRjPjXN0cl9yZXBsYWwNlKJCcciIsIiIsJGMpOyRjPjXN0cl9yZXBsYW
NlKJCcbiIsIiIsJGMpOyRidWY9IiI7Zm9yKCRpPTA7JGk8c3RybGVuKC
RjKTSkaSs9MikkYnVmLj11cmxkZWVZGUoIiUiLnN1YnN0cigkYywkas
wyKSk7ZWNobyhAZndyaXRlKGZvcGVuKCRmLCJ3IiksJGJ1Zik%2FIjEi
OiIwIik7O2VjaG8oInw8LSIpO2RpZSgpOw%3D%3D&z1=RDpcd2FtcDY0
XHd3d1x1cGxvYWRcNjY2Ni5qcGc%3D&z2=FFD8FFE000104A46494600
  
```

复制所有内容

粘贴到winhex中, 选择ASCII Hex格式

保存为jpg文件

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00001E90	8C	79	7B	01	7F	99	CD	B0	3D	66	97	3F	3D	E4	D9	E7	Ëy(¨í°=f-?=aùç
00001EA0	62	F5	5C	F0	31	8C	60	3E	7B	29	C7	6B	AF	3D	75	7D	bõ\ðlè'>()çk¯=u)
00001EB0	1A	F5	BA	7A	F5	95	FF	00	9A	69	2E	69	4A	CA	EE	FF	õ°zõ•ÿ sí.iJÈiy
00001EC0	00	E5	B3	7A	35	A5	AD	E9	1E	5D	7D	D8	3E	6A	D2	6E	â°z5¥-é }}ø>jòn
00001ED0	05	B7	E2	36	31	83	2E	DE	96	96	DF	C1	02	76	F3	A5	·â6lf.ð--ðÁ vó¥
00001EE0	E0	1E	AC	73	CE	4B	31	15	DC	E4	F4	11	37	97	91	8E	à -síKl Úaõ 7-`ž
00001EF0	45	A5	B7	73	EF	34	D9	E0	9C	31	2D	D8	B6	04	E4	0E	E¥·s14Ùàæ1-ø¥ a
00001F00	08	CC	8A	24	3E	50	23	9B	BB	9E	8F	33	7F	D3	08	B1	ìš>p#>>ž 3 Ó ±
00001F10	C6	7E	87	EF	39	15	DF	1C	80	4C	AA	24	19	FF	00	A7	Æ~+19 ß eL°\$ ý S
00001F20	CB	A3	E8	3A	98	21	EF	D0	1F	4C	B0	C7	6C	15	DF	DD	Èèè:~!1ð L°çl ßÝ
00001F30	6F	3D	BA	A5	AF	7B	AF	55	FF	00	2E	CE	49	B7	66	9E	o=°¥~{~Uy .íi·fž
00001F40	DE	5A	25	AA	5A	2F	9D	AC	EF	65	A3	D5	54	64	07	E6	èž*Z/ -1eíøTð æ
00001F50	61	B3	F7	67	CB	3E	50	39	C5	AD	B8	FB	F3	C8	7B	CB	a°+gÈ>P9À-,úóÈ{È
00001F60	26	09	18	E7	9C	8C	12	98	85	89	F9	04	63	1F	2B	7D	& çøæ ~..kù c +)
00001F70	9D	5C	71	0C	7F	F2	D2	F2	5F	47	20	31	52	72	46	06	\q òòò_G 1RrF
00001F80	32	15	41	9E	41	B5	1B	7F	EF	01	94	79	CE	3A	DC	DC	2 AžAµ i "yí:ÜÜ
00001F90	7F	0D	BC	64	63	F7	31	93	C8	4C	0E	A4	75	5A	AD	27	¼dc÷1"ÈL =uZ-'
00001FA0	FC	B4	32	12	7E	61	F6	82	BF	F2	D2	4F	F9	67	67	16	ü'2 ~aõ,¿òòùgg
00001FB0	32	02	A9	C0	6D	B9	1C	13	D1	57	3D	91	8E	AB	CB	F0	2 @Àm¹ ÑW='ž«Èð
00001FC0	76	5E	4D	2D	BE	56	BF	D8	82	7C	92	6B	77	DB	AE	BD	v^M-¼V¿ø, 'kwÜG¼
00001FD0	97	5D	77	7D	75	D6	CE	CE	53	B4	04	8C	21	45	3D	C5	-]w)uóíís' @!E=À
00001FE0	B2	BF	19	6C	7E	F2	F6	6C	F6	1C	94	1D	06	07	F7	4E	°¿ 1~òòlò " ÷N
00001FF0	6B	92	00	4D	99	71	B8	F9	2A	DF	F2	DA	63	C3	DC	48	k' M°q,ù*BòúçÀUH
00002000	0F	02	38	C9	F9	77	75	03	07	8F	30	99	DF	92	FB	DB	8Èùwu 0°B'úÜ
00002010	03	00	DD	32	76	1D	63	B2	87	FD	A3	81	BC	2E	00	03	Ý2v c°+ý£ ¼.
00002020	92	42	90	D5	E5	27	E7	DD	F2	65	47	9C	57	A5	BC	03	'B Óá'çÝòeGøW¥¼
00002030	EE	5B	46	09	E2	49	30	01	EA	46	4E	7A	48	6B	AE	11	l[è a10 eFNzHkø

得到图片



高兴的提交

错误

...

头疼

用binwalk跑一下

发现文件包含

还有一个zip文件

```
root@kali:~/Downloads/misc/14# binwalk 19ae303d520c4790b0401569b354e6a2.pcapng
```

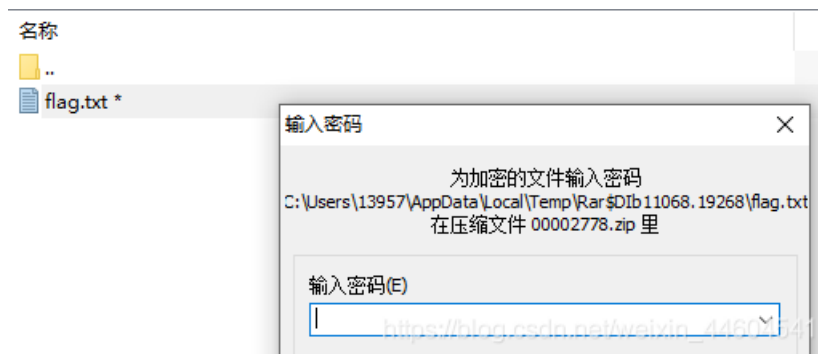
DECIMAL	HEXADECIMAL	DESCRIPTION
663085	0xA1E2D	xz compressed data
664045	0xA21ED	xz compressed data
812025	0xC63F9	xz compressed data
814001	0xC6BB1	xz compressed data
1238637	0x12E66D	xz compressed data
1240937	0x12EF69	xz compressed data
1391563	0x153BCB	xz compressed data
1393067	0x1541AB	xz compressed data
1406647	0x1576B7	xz compressed data
1412887	0x158F17	xz compressed data
1422689	0x15B561	Zip archive data, encrypted at least v2.0 to extract, compressed size: 52, uncompressed size: 40, name: flag.txt

https://blog.csdn.net/weixin_44604541

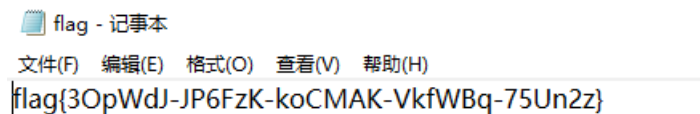
查了查
用foremost进行分离
foremost使用教程



得到zip文件
里面有flag.txt
但是需要密码
这应该是之前图片里的 `Th1s_1s_p4sswd_!!!`



成功打开



得到flag

结语

简单水了水misc新手区

还是学到好些东西的

- [ps的灵活使用](#)
- [jd-gui反编译jar](#)
- [base64以及base64隐写](#)
- [进制与ASCII码转换](#)
- [与佛论禅。。这个真的佛了](#)
- [rot13加密](#)
- [pdf隐写](#)
- [摩斯密码](#)
- [gif隐写](#)
- [RAR文件格式官方说明书的翻译\[中英对照\]](#)
- [zip伪加密](#)
- [binwalk文件包含](#)
- [foremost文件分离](#)



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)