MISC-1

原创

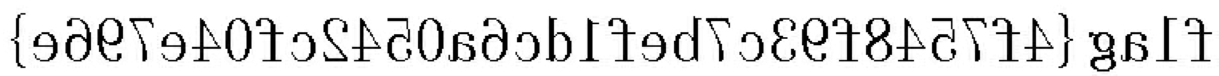
Re1y0n 于 2021-07-31 12:04:09 发布 29 收藏

分类专栏： CTF 文章标签： 其他

题目目录

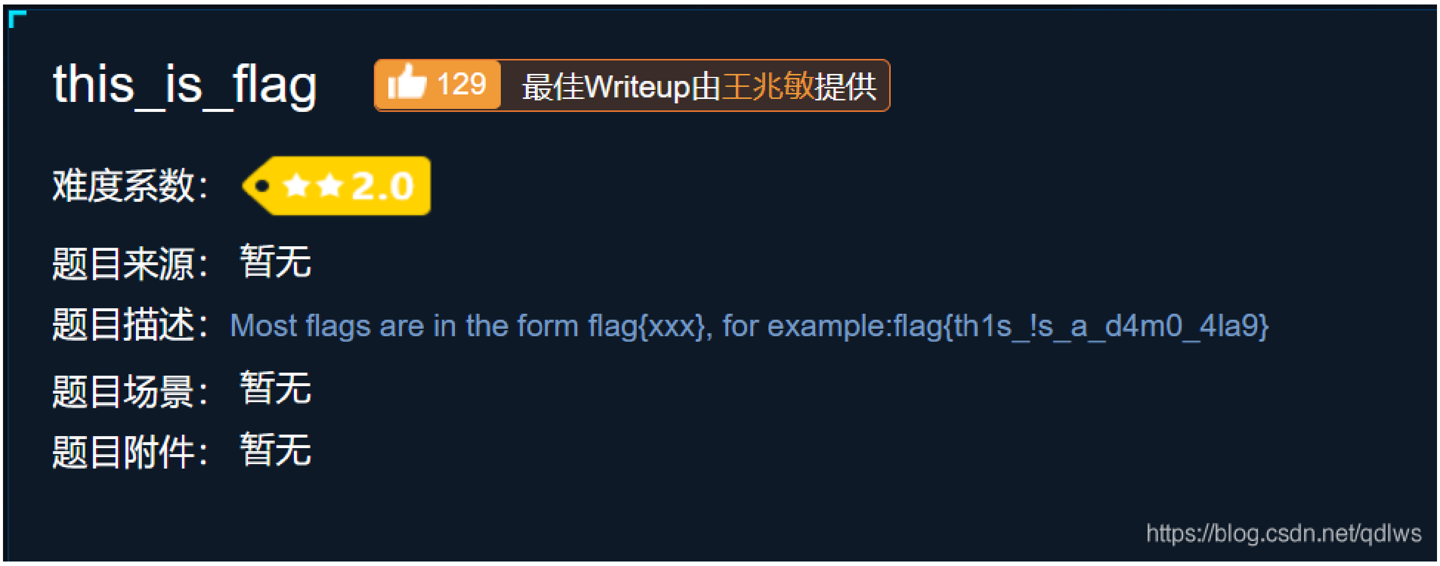
reverseMe

文件的内容



右键->编辑->旋转->水平翻转

this_is_flag:



试了两次：

flag{this_is_flag}和flag{th1s_!s_a_d4m0_4la9}

pdf:

pdf 98 最佳Writeup由S_O_L_R提供

难度系数: ★★★ 3.0

题目来源: csaw

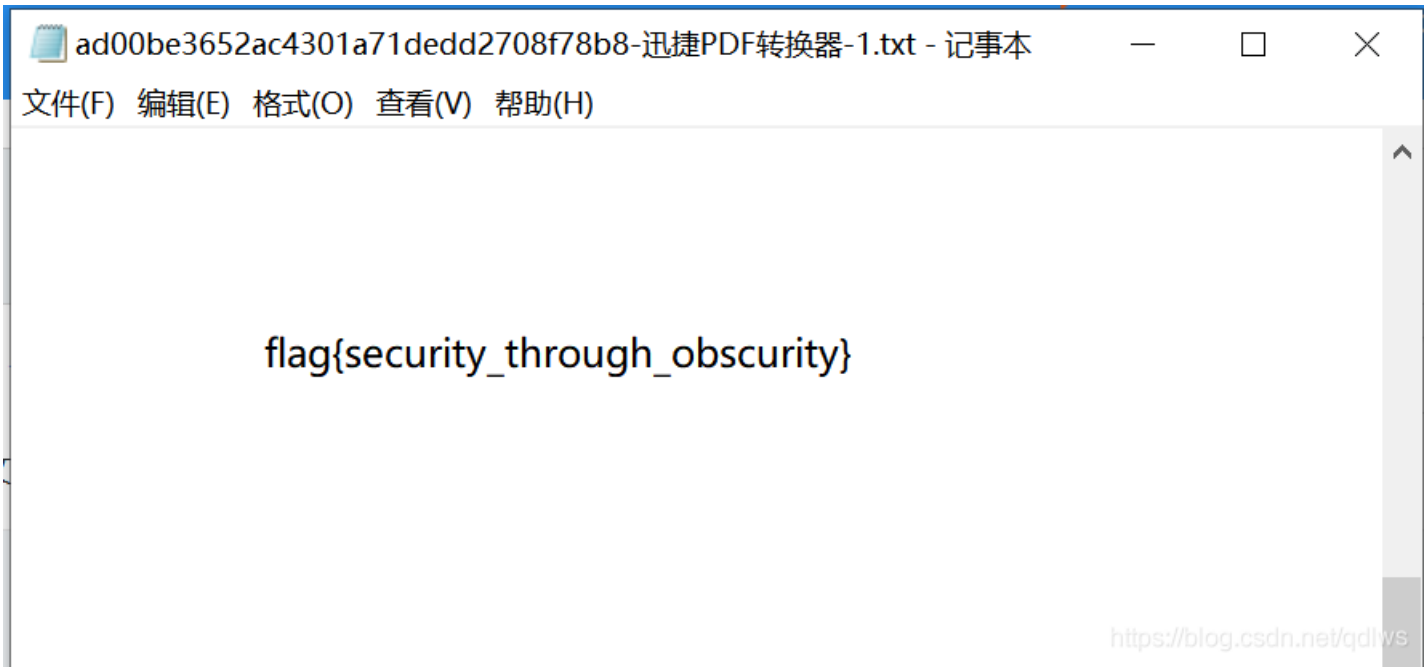
题目描述: 菜猫给了菜狗一张图，说图下面什么都没有

题目场景: 暂无

题目附件: 附件1

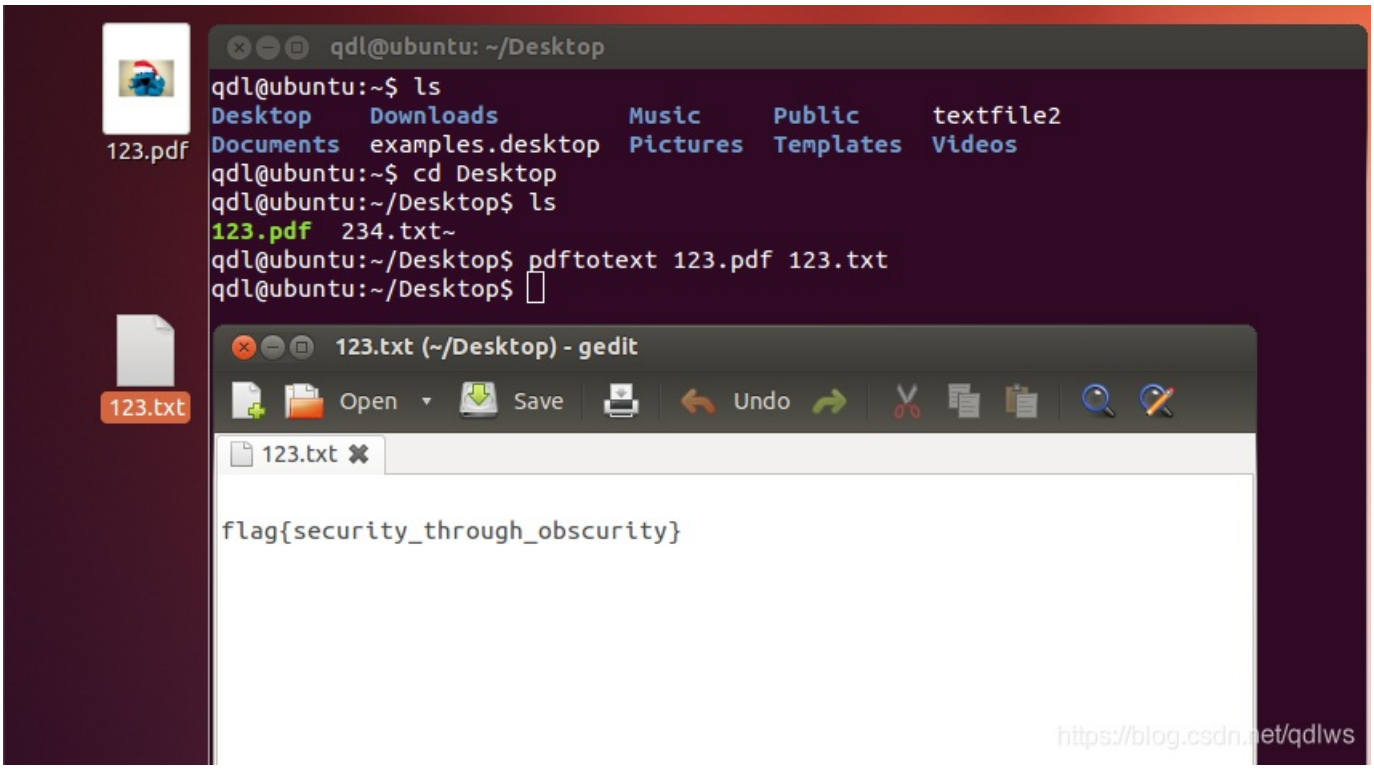
题目提示flag就在图片下面

利用在线转换器.转换成txt得到flag，本来想转换成word查看，但是转换成word一直打不开



看了大佬写的博客，还可以利用Linux自带工具pdftotext解题，于是乎尝试一番

```
pdftotext 123.pdf 123.txt
```



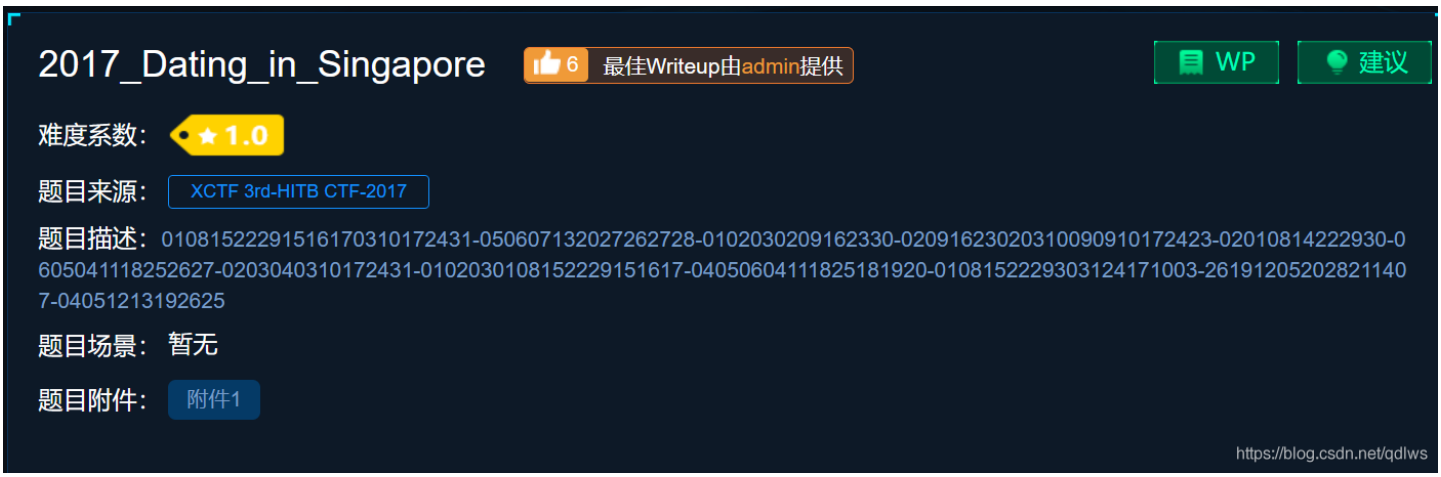
神奇的Modbus：

附件1是一个pcapng文件，使用wireshark打开

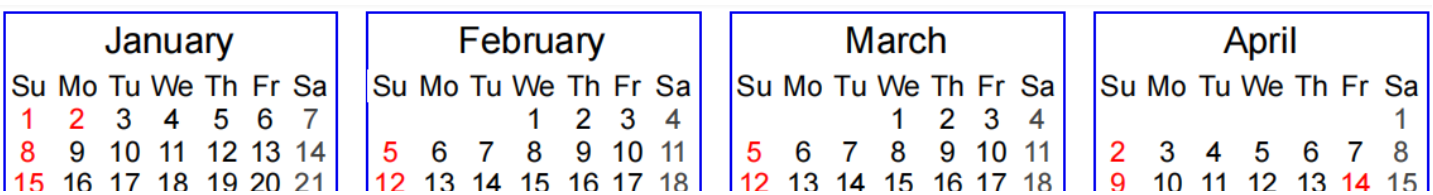
百度了一下，modbus是一个通讯协议，在wireshark中点击protocol进行分类，右键modbus通信协议的任意一条记录->追踪流->TCP流即得到字符串Easy_Mdbus

提交发现并不正确，少了一个字母o，flag应为为sctf{Easy_Modbus}

2017_Dating_in_Singapore:



附件1：



22	23	24	25	26	27	28
29	30	31				

6:◐ 12:○ 20:◑ 28:●

19	20	21	22	23	24	25
26	27	28				

4:◐ 11:○ 19:◑ 26:●

19	20	21	22	23	24	25
26	27	28	29	30	31	

5:◐ 12:○ 20:◑ 28:●

16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

4:◐ 11:○ 19:◑ 26:●

May

Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

3:◐ 11:○ 19:◑ 26:●

June

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

1:◐ 9:○ 17:◑ 24:●

July

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

1:◐ 9:○ 17:◑ 23:● 30:◐

August

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

8:○ 15:◑ 22:● 29:◐

September

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

6:○ 13:◑ 20:● 28:◐

October

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

6:○ 12:◑ 20:● 28:◐

November

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

4:○ 11:◑ 18:● 27:◐

December

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

3:○ 10:◑ 18:● 26:◐

有用的信息只有题目中的那一串数字和附件1中的日历，将数字进行处理

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
0108152229151617031017243l-
0506071320272627 28-
0102030209162330-
020916230203100909101724 23-
020108142229 30-
0605041118252627-
0203040310172431-
0102030108152229151617-
0405060411182518 1920-
0108152229303124171003-
2619120520282114 07-
04051213192625
```


我一开始解读第一行的时候认为是从1月8号开始，但是后面就让我难以继续了，如果是一位数的月份前面也应该有个0，15月的话，想想就觉得自己有点憨，思考了一番无果，无聊数位数，第一行竟然是偶数，又数了两行，新即兹哇一兹摸你肚子，我悟了，数了一下行数，十二行，一行对应一个月啊，这下我彻底悟了，对数字进行两两分组

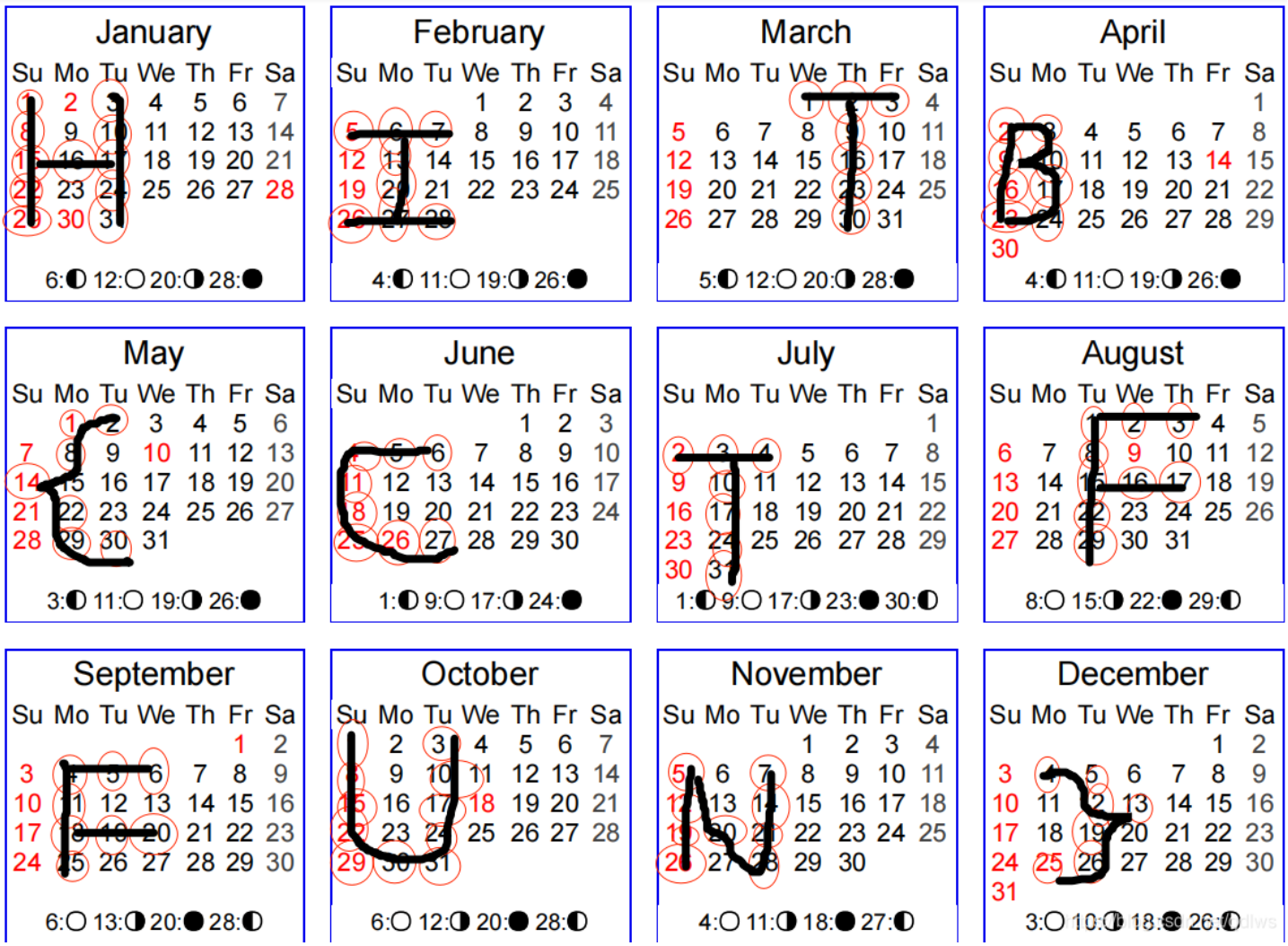
*新建文本文档.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

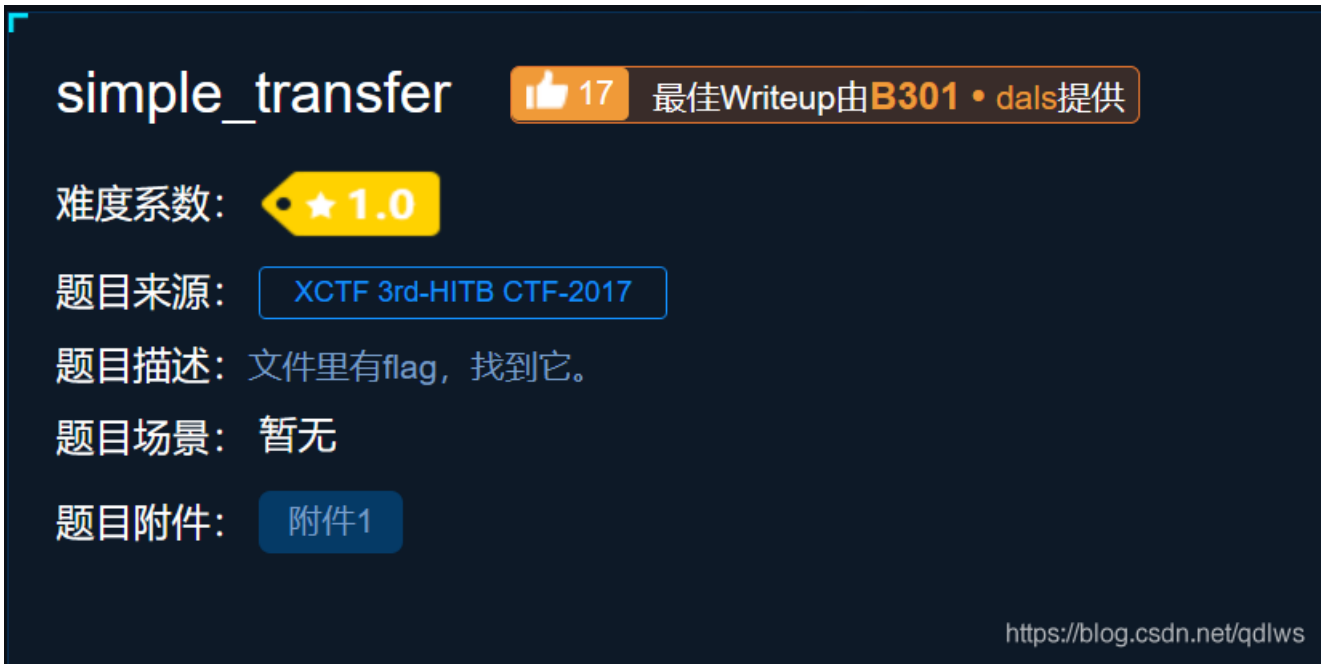
```
01 08 15 22 29 15 16 17 03 10 17 24 31- 26位
05 06 07 13 20 27 26 27 28- 18位
01 02 03 02 09 16 23 30- 16位
```

02 09 16 23 02 03 10 09 09 10 17 24 23- 26位
02 01 08 14 22 29 30- 14位
06 05 04 11 18 25 26 27- 16位
02 03 04 03 10 17 24 31- 16位
01 02 03 01 08 15 22 29 15 16 17- 22位
04 05 06 04 11 18 25 18 19 20- 20位
01 08 15 22 29 30 31 24 17 10 03- 22位
26 19 12 05 20 28 21 14 07- 18位
04 05 12 13 19 26 25 14位

然后就在附件上不停的画圈圈，最后连起来得到flag



simple_transfer：



附件1是一个pcap文件，wireshark打开，点击protocol，从后往前一条一条地找，找了很久才找到这个file.pdf

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 … <Ctrl-/>

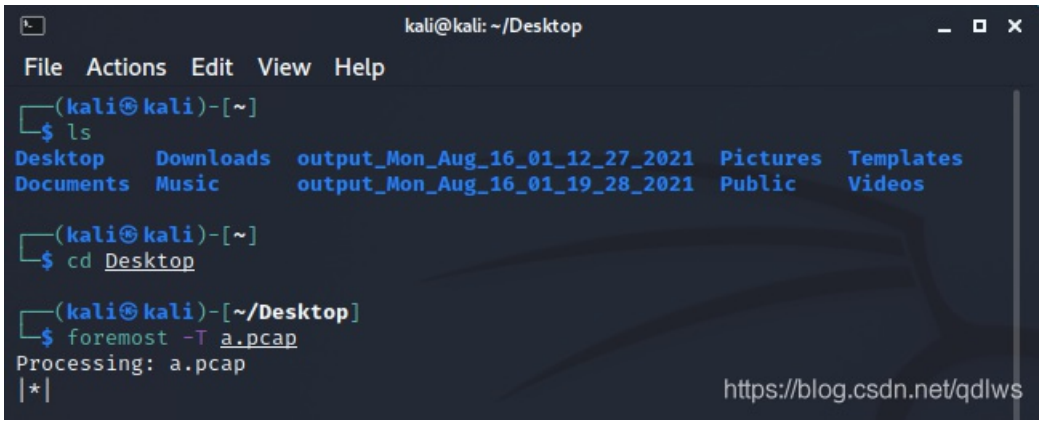
No.	Time	Source	Destination	Protocol	Length	Info
4308	62.583851	10.0.2.5	10.0.2.4	NFS	174	V4 Call (Reply In 4314) SETCLIENTID_CONFIRM
4307	62.583814	10.0.2.4	10.0.2.5	NFS	130	V4 Reply (Call In 4306) SETCLIENTID
4306	62.583621	10.0.2.5	10.0.2.4	NFS	242	V4 Call (Reply In 4307) SETCLIENTID
4304	62.583488	10.0.2.4	10.0.2.5	NFS	122	V4 Reply (Call In 4303) LOOKUP Status: NFS4ERR_NOENT
4303	62.583091	10.0.2.5	10.0.2.4	NFS	230	V4 Call (Reply In 4304) LOOKUP DH: 0x0163bd75/file.pdf
4301	61.845888	10.0.2.4	10.0.2.5	NFS	266	V4 Reply (Call In 4300) GETATTR
4300	61.845705	10.0.2.5	10.0.2.4	NFS	210	V4 Call (Reply In 4301) GETATTR FH: 0x0163bd75
4298	61.844943	10.0.2.4	10.0.2.5	NFS	266	V4 Reply (Call In 4297) GETATTR

```
Opcode: PUTFH (22)
  FileHandle
    length: 28
    [hash (CRC-32): 0x0163bd75]
    FileHandle: 01000700bb230600000000005c7536b9c59642ef9c9651d4…
```

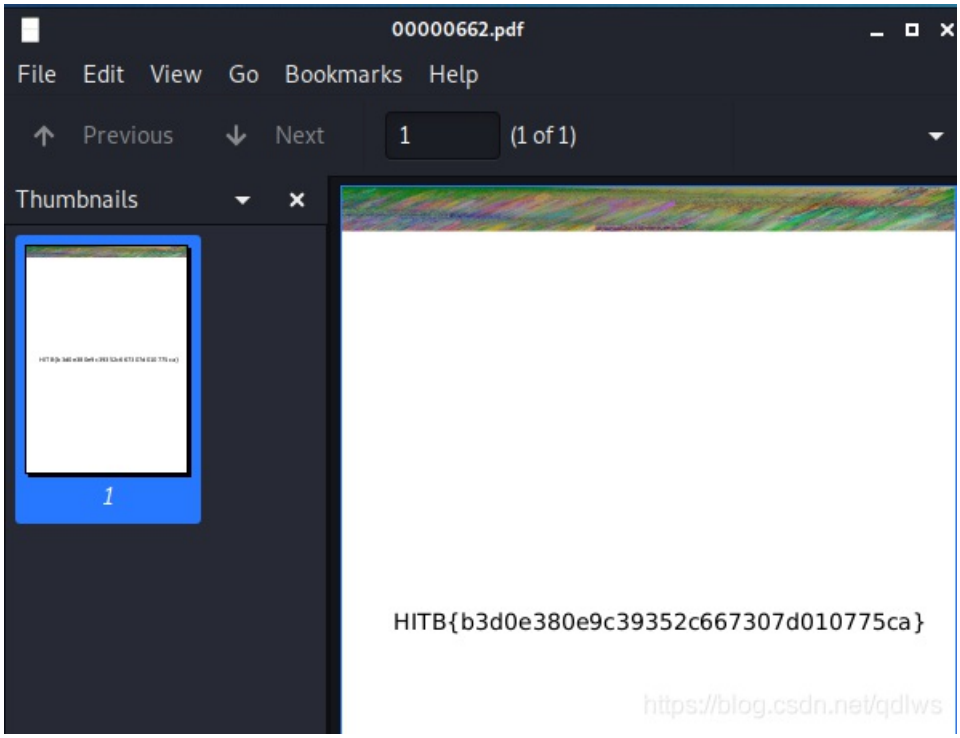
```
0000  08 00 27 1f c2 a8 08 00  27 f3 75 4b 08 00 45 00   ··'····· '·uK··E·
0010  00 d8 09 72 40 00 40 06  18 a6 0a 00 02 05 0a 00   ···r@·@· ········
0020  02 04 03 56 08 01 bb 86  59 19 29 a2 bc 04 80 18   ···V···· Y·)·····
0030  01 49 18 d3 00 00 01 01  08 0a 00 02 4d 2f 00 02   ·I····· ····M/··
0040  49 cb 80 00 00 a0 7f c0  e6 45 00 00 00 00 00 00   I····· ·E······
0050  00 02 00 01 86 a3 00 00  00 04 00 00 00 01 00 00   ····· ····· ·····
0060  00 01 00 00 00 24 01 06  27 38 00 00 00 0a 63 74   ·····$·· '8····ct
0070  66 2d 63 6c 69 65 6e 74  00 00 00 00 00 00 00 00   f-client ····· ·····
0080  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ····· ····· ·····
0090  00 00 00 00 00 00 00 00  00 00 00 00 04 00 00 00   ····· ····· ·····
00a0  00 16 00 00 00 1c 01 00  07 00 bb 23 06 00 00 00   ····· ····· ···#····
00b0  00 00 5c 75 36 b9 c5 96  42 ef 9c 96 51 d4 3c 03   ··\u6··· B···Q·<·
00c0  75 59 00 00 00 0f 00 00  00 08 66 69 6c 65 2e 70   uY····· ····file.p
00d0  64 66 00 00 00 0a 00 00  00 09 00 00 00 02 00 10   df····· ····· ·····
00e0  01 1a 00 b0 a2 3a                                  ····· :
```


将文件更名拖进kali linux，foremost指令分离文件

```
foremost -T 文件名
```



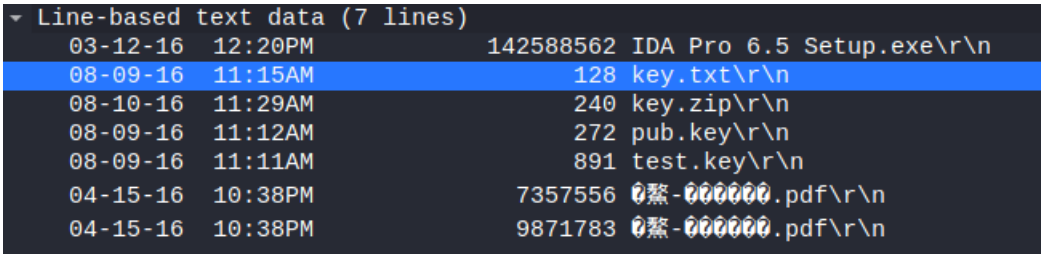
然后桌面上就会多出一个文件，进入文件打开pdf得到flag



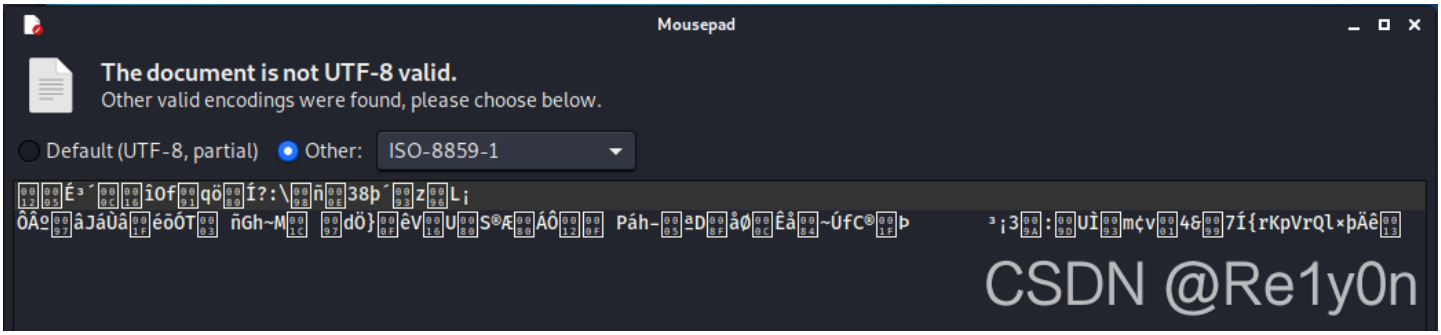
看了一下大佬的博客，大佬使用wireshark的统计->协议分级查看，通过协议的字节百分比占用基本全在nfs协议上来过滤nfs，然后观察报文发现file.pdf，我发现还可以点protocol将协议分类然后每一种协议都右键->追踪流查看

就在其中：

附件1解压wireshark打开，搜索关键词，当关键词为key时



foremost命令分离文件，在文件zip中发现key.txt文件，但是打开却是乱码

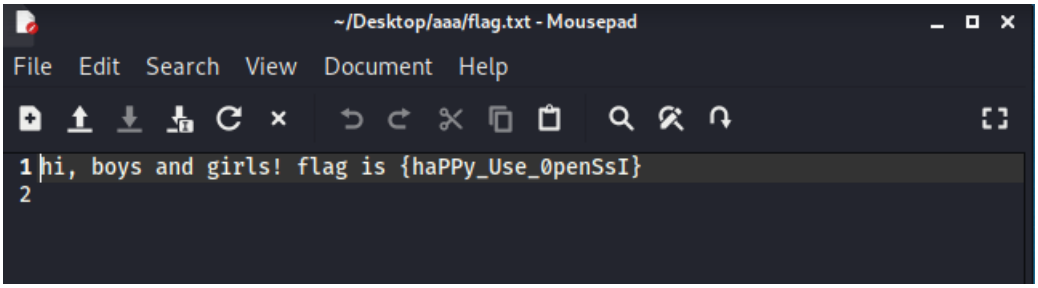


猜想可能需要密钥才能打开，搜索PRIVATE，followTCP流就可以看到密钥

新建rsa.txt文件，将密钥粘贴到rsa.txt中，要和key.txt放在一个目录下，openssl解密，得到flag.txt

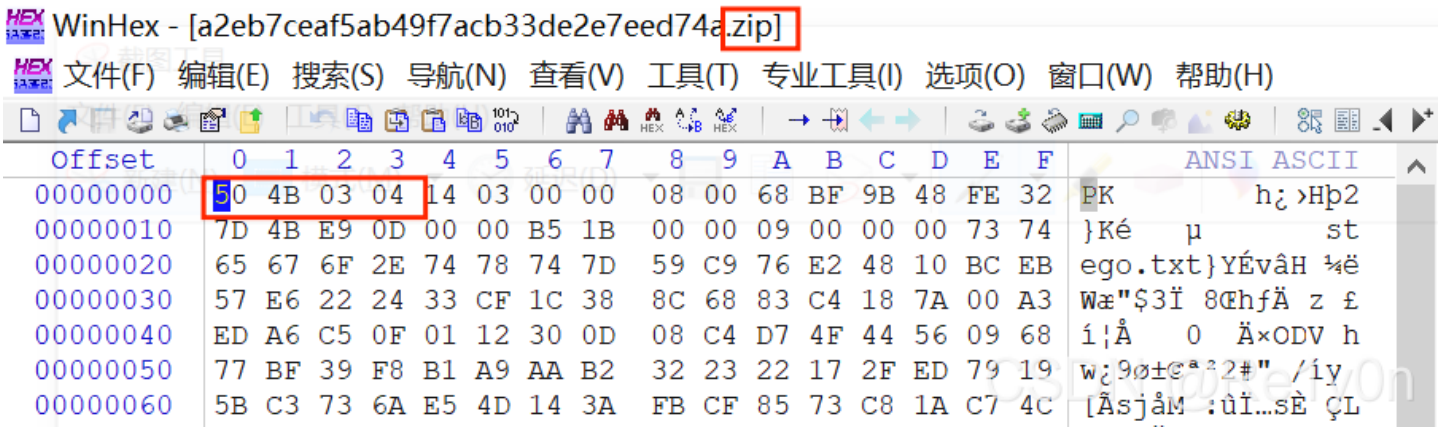
```
openssl rsautl -decrypt -in key.txt -inkey rsa.txt -out flag.txt
-in 需要解密的文件 -inkey 密钥 -out 输出的文件
```

打开得到flag

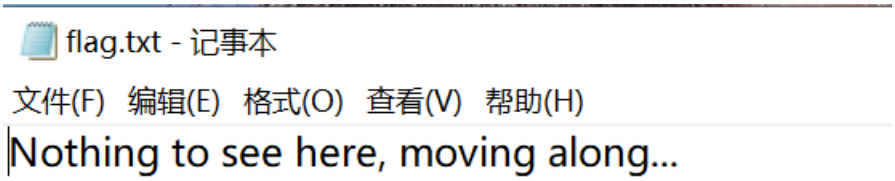


MISCall:

附件1是一个无后缀文件，winhex打开，发现时zip文件



解压得到flag.txt和.git文件

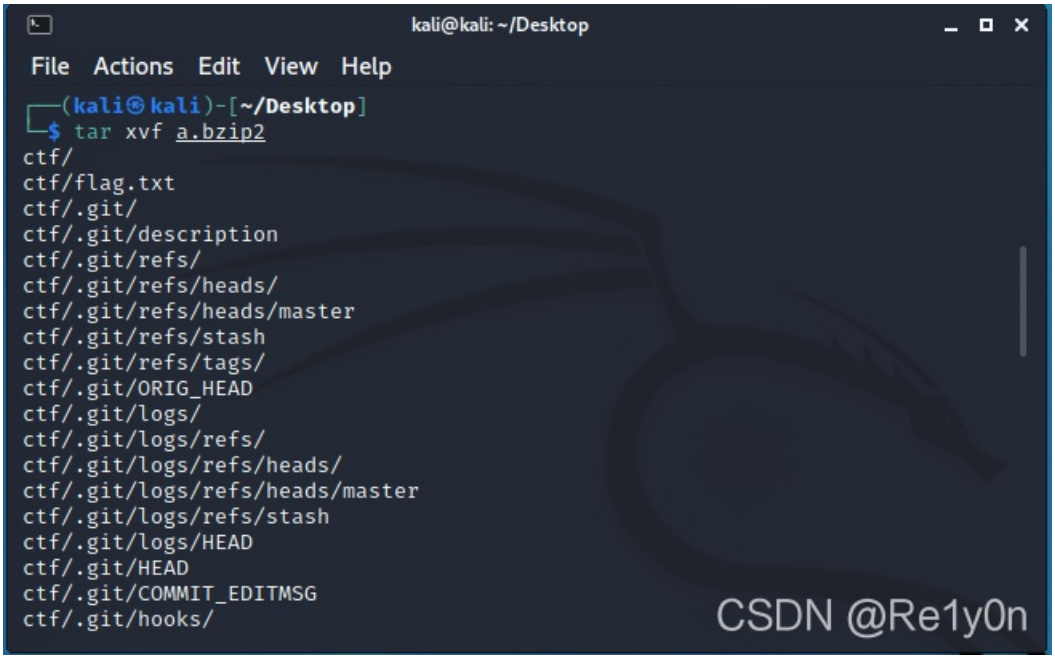


意料之外，这个.git文件不知道该怎么处理，百度了一下，这道题需要用Linux指令来解，解题参考

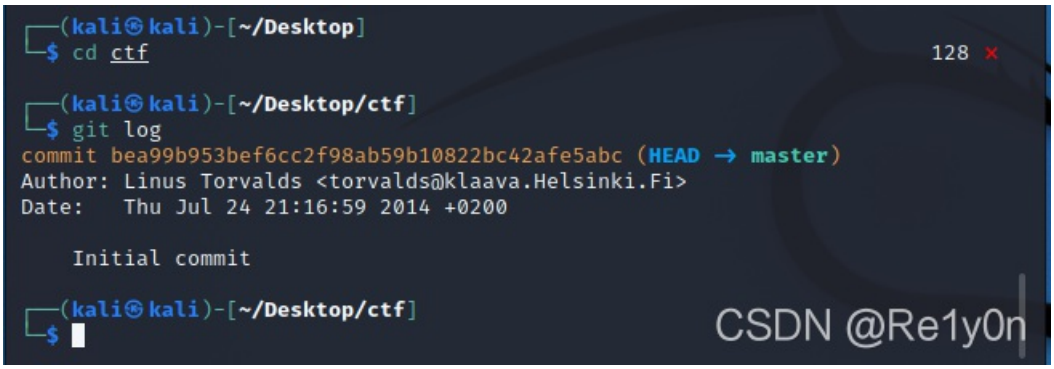
题外之外，这个.git文件不知道该怎么处理，百度了一下，这道题需要用Linux指令来解，解题参考

以下解题过程是按照解题参考的实操

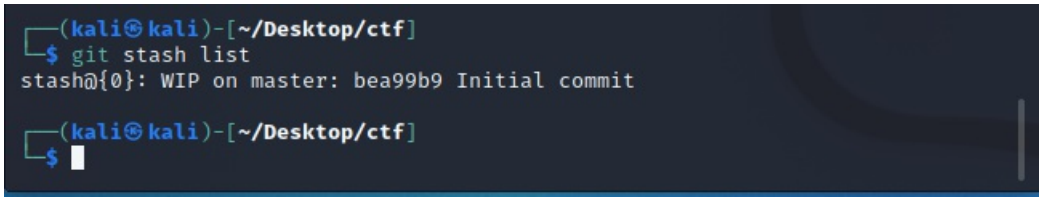
修改后缀然后解压



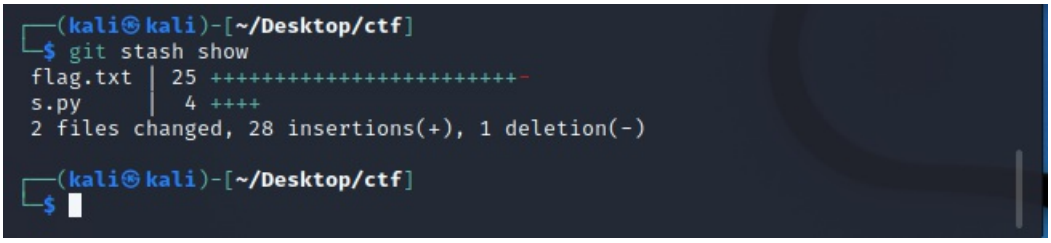
查看git记录



查看修改列表，储存列表中有一条记录



校验列表中的存储文件



把列表中的文件恢复

直接执行 git stash apply 时，会 提示文件覆盖 自动终止，可以先把flag.txt删除再执行

```
└─$ ls

┌──(kali㉿kali)-[~/Desktop/ctf]
└─$ git stash apply
On branch master
Changes to be committed:
  (use "git restore --staged <file>..." to unstage)
        new file:   s.py

Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        modified:   flag.txt


┌──(kali㉿kali)-[~/Desktop/ctf]
└─$
```

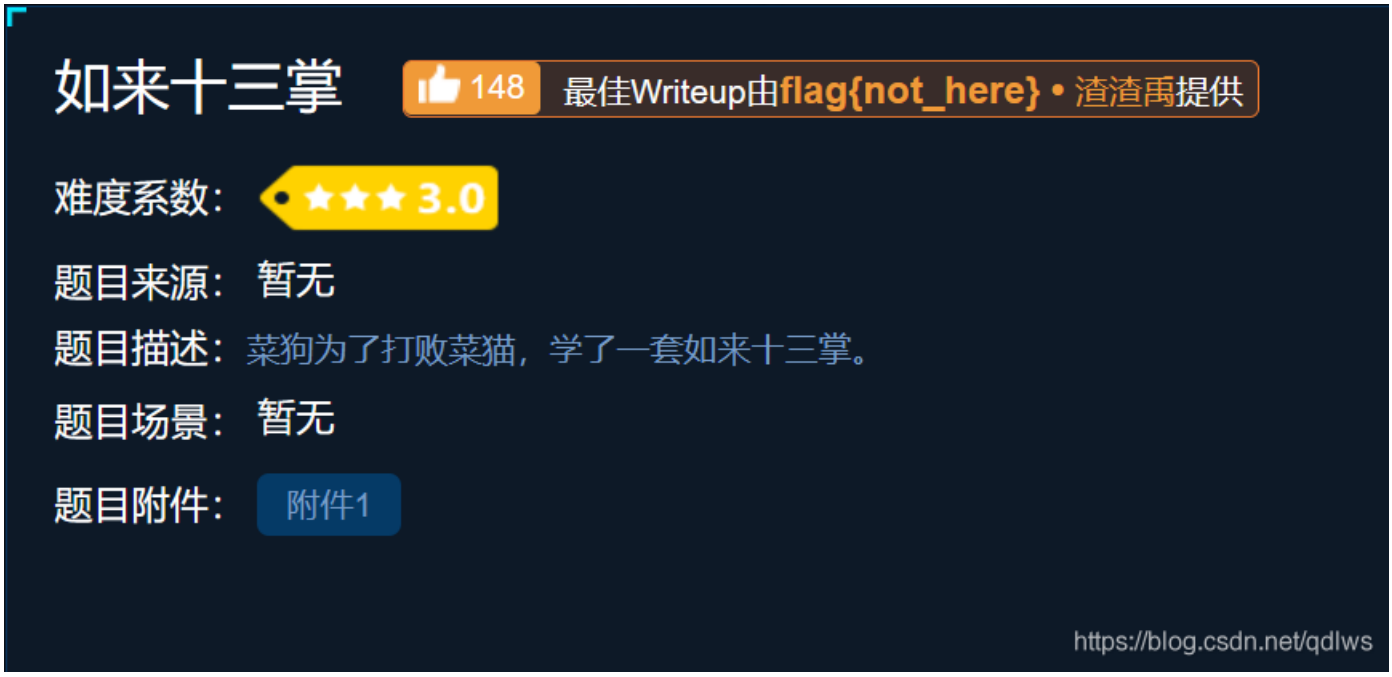

运行s.py得到flag

```
┌──(kali㉿kali)-[~/Desktop/ctf]
└─$ ./s.py
NCN4dd992213ae6b76f27d7340f0dde1222888df4d3

┌──(kali㉿kali)-[~/Desktop/ctf]
└─$
```

如来十三掌：

菜狗为了打败菜猫，学了一套如来十三掌



附件1：

夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙吶神。舍切真怯勝吶得俱沙罰娑是怯遠得吶數罰輸哆遠薩得槃漫夢盧皤亦醯吶娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮

如果不是看了别人的writeup，怎么能想到“与佛论禅”这个玩意儿

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

心不动，万物皆不动

佛曰：夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集逮俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙吶神。舍切真怯勝吶得俱沙罰娑是怯逮得吶數罰輪哆逮薩得槃漫夢盧皤亦醯吶娑皤瑟輪諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輪奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮

然后进行rot13解码

rot13

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

Rot13 编码 Rot13 解码 拷贝 剪切 粘贴 清除

最后base64解码得到flag

Base64.us Base64 在线编码解码 (最好用的 Base64 在线工具)

Base64 | URLEncode | MD5 | TimeStamp

请输入要进行 Base64 编码或解码的字符

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

编码 (Encode) 解码 (Decode) ↕交换 (编码快捷键: Ctrl + Enter)

Base64 编码或解码的结果:

编/解码后自动全选

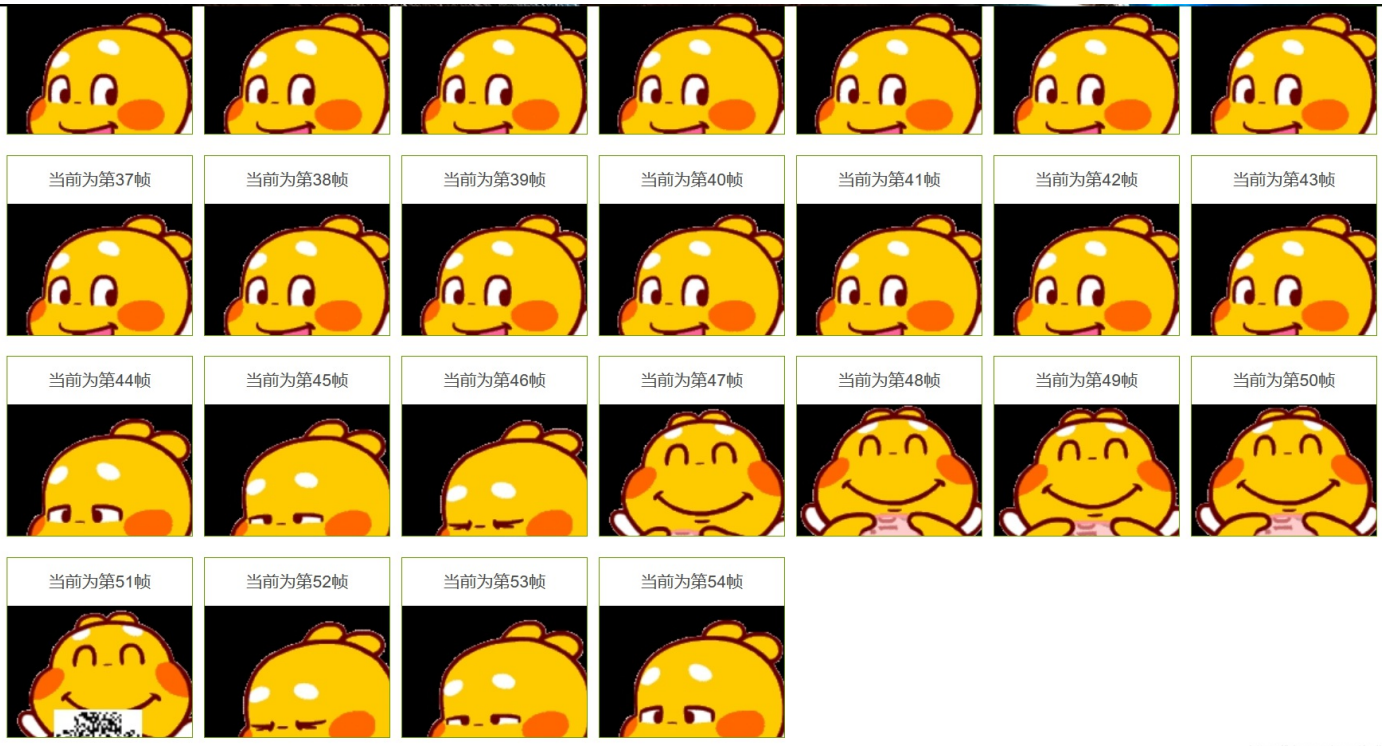
flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

离谱，想不到真就一点都做不出来

give_you_flag：

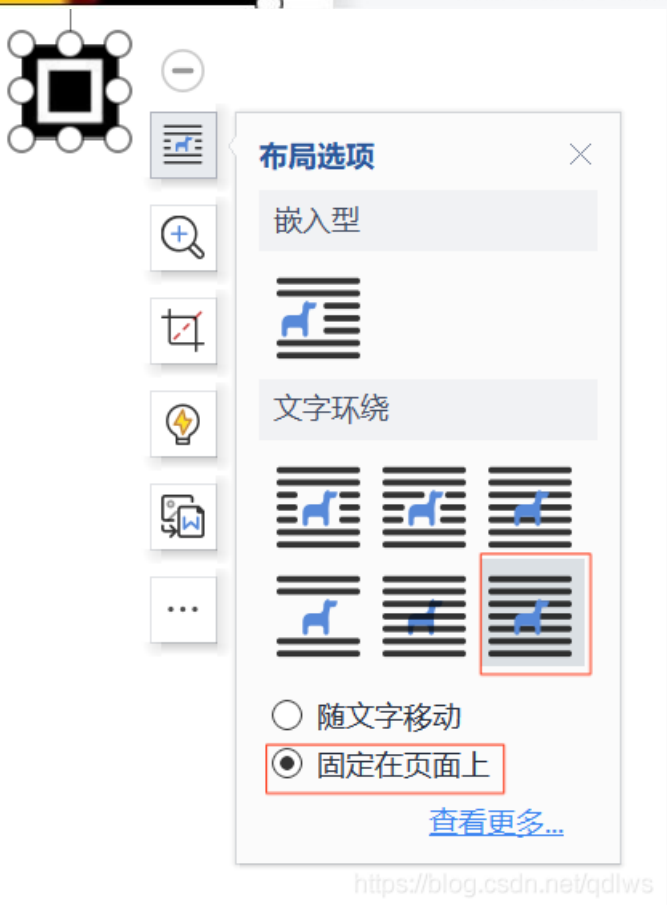
附件是一个动图，动图的播放过程中出现了一个二维码，但是因为太快扫不上，然后我就录频录下来，使用0.25倍速观看，然后发现这个二维码少了二维码定位符符号，使用在线工具 https://www.qtool.net/gif.分解GIF动画

将第51帧保存下来



将保存的图片用word打开调整到合适大小，建议调小一点，图片放大会比较模糊，将三个二维码定位符符号放于三个角不断的调整位置直到能够扫上为止


文字环绕
随文字移动
固定在页面上
查看更多...
https://blog.csdn.net/qdlws


布局选项
嵌入型
文字环绕
随文字移动
固定在页面上
查看更多...
https://blog.csdn.net/qdlws

用微信扫一扫得到flag