

NTACTFWP

学号：23056034 姓名：汪杨峻 班级：电路 2301

Cry:

1. sign_in

看题目描述：

佛曰：冥藝涅訥遮奢都除哆悉冥心罰所諳娑隸呼哆朋俱特哆漫
梵姪罰帝大伽侄地彌梵遮娑幡道罰度奢。冥輸以諳怛密幡礙多
以耨奢迦哆漫南冥數參日怯竟怯吉冥智羯等鉢陀侄涅故遠訥老
諳穆梵栗有梵呼怯盧俱盧若盧度俱怖者夜一幡藝跋

直接与佛论禅解密得到 flag

佛曰：冥藝涅訥遮奢都除哆悉冥心罰所諳娑隸呼哆朋俱特哆漫梵姪罰帝大伽侄地彌梵遮娑幡道罰度奢。冥輸以諳怛密幡礙多以耨奢迦
哆漫南冥數參日怯竟怯吉冥智羯等鉢陀侄涅故遠訥老諳穆梵栗有梵呼怯盧俱盧若盧度俱怖者夜一幡藝跋

加密

解密

flag{fochan_Welcome_to_NTA2023}

2. 我不是猪，我是佩奇！哼唧！

下载附件看到图片和题目可知为猪圈密码

> 厂 < 匚 < 回 口 > < < 口 ✓

直接手撸得到 flag

┐	┌	└	┘	□	▤	┐	┌	└
┐	┌	└	┘	□	▤	┐	┌	└
┐	┌	└	┘	□	▤	┐	┌	└
┐	┌	└	┘	□	▤	┐	┌	└
┐	┌	└	┘	□	▤	┐	┌	└

明文: xiyounetyyds

3. new_base64

看题目描述和下载附件看自定义字典：

```
new_base64 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789{'
```

```
[5, 11, 0, 6, 62, 61, 57, 0, 53, 56, 56, 58, 0, 59, 53, 54, 52, 4, 56,
0, 5, 57, 2, 52, 2, 60, 60, 59, 60, 0, 1, 1, 59, 4, 58, 3, 54, 63]
```

然后根据密文写个脚本，得到 flag

```
# 自定义Base64字典
custom_base64 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789{'

# 密文数据
encoded_data = [5, 11, 0, 6, 62, 61, 57, 0, 53, 56, 56, 58, 0, 59, 53, 54, 52, 4, 56, 0, 5, 57, 2, 52, 2, 60, 60, 59, 60, 0, 1, 1, 59, 4, 58, 3, 54, 63]

# 解码Base64
try:
    decoded_chars = [custom_base64[i] for i in encoded_data]
    decoded_data = ''.join(decoded_chars)
    print('解码后的文本:', decoded_data)
except Exception as e:
    print('解码失败:', e)
```

```
Python 3.8.5 Shell
File Edit Shell Debug Options Window Help
Python 3.8.5 (tags/v3.8.5:580fbb0, Jul 20 2020, 15:57:54) [MSC v.1924 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: D:\python\3.py =====
解码后的文本: flag{95a1446a7120e4af5c0c8878abb7e6d2}
```

4. 我吃两碗 base

根据题目描述：

```
ZmxhZ3s1NDQ4Njk3MzlwNjkzNDVGNkU1NDYxNDM1ND
Q1NTIyMDU5NTk0NDUzMjB9IApUcnkgaXQgYWdhW4sI
GJ1dCB0aGlzIHRpbWUgaW4gYSBkaWZmZXJlbnQgd2F5
```

先放入 base 全家桶解一次密得到 fake flag

```

PS D:\misc\CTF-Tools(一键解密)> ./base
请贴入字符串: ZmxhZ3s1NDQ4Njk3MzIwNjkzNDVGbkU1NDYxNDM1NDQ1NTIyMDU5NTk0NDUzMjB9IApUcnkgaXQgYWdhaw4sIGJ1dCB0aGlzIHRpbWUgaW
4gYSBkaWZmZXJlbnQgd2F5
****base16****
not b16
****base62****
153993690445683818947796401258519609639543391514654510447950862843670129053545176318692315789787348995817489952468217597
16929642831671941908975046066751830421563953701485943210783657991124508789547405330743624658631560755324877719
not b62
****base64****
b flag{544869732069345F6E546143544552205959445320} \nTry it again, but this time in a different way'
not b64

```

然后把 {} 中的数字再跑一遍 base 全家桶得到 flag

```

PS D:\misc\CTF-Tools(一键解密)> ./base
请贴入字符串: 544869732069345F6E546143544552205959445320
****base16****
b'THis i4_nTaCTER YYDS '
not b16
****base62****
1558437410114620075086078942899891978923969499814415269211571359648
not b62
not b64
****base91****
bytearray(b'!\x94\xb1\xa6W\xe4)+\xd3\xeb\x07\x05\x10\xa6!\x84F\xcc\
not b91
****base92****
not b92
****base58****
not 58
****base85****
not b85
****base32****
not b32
****base36****
not b36
****IDAT****
b'THis i4_nTaCTER YYDS '
not IDAT

```

5. 米斯嘎，木斯嘎，神奇的阿斯克码

看题目描述可知直接 ASCII 码转换就可以得到 flag:

米斯嘎，木斯嘎，神奇的阿斯克码。

75

flag = [102, 108, 97, 103, 123, 48, 56, 97, 97, 102, 55, 98, 53, 100, 51, 98, 102, 49, 57, 55, 57, 99, 49, 102, 100, 49, 56, 51, 53, 49, 55, 99, 101, 99, 98, 50, 51, 125]

```
102 108 97 103 123 48 56 97 97 102 55 98 53 100 51 98 102 49 57 55 57 99 49
102 100 49 56 51 53 49 55 99 101 99 98 50 51 125

Result
flag {08aaf7b5d3bf1979c1fd183517cecb23}
```

6. 风中有朵雨做的云

看题目描述和附件可知为云影密码，找个脚本即可得到 flag

```
这咋还是乌云捏，地上影子灰蒙蒙的

8888420888884088881088884210888888210888888810842108888884108884210888882108888842084210888888421088
842108888210810888884210810884108888408884208888882108888801088884088888421088888842108888888410

Python 3.8.5 Shell
File Edit Shell Debug Options Window Help
a="8888420888884088881088884210888888210888888810842108888884108884210888882108
s=a.split('0')
print(s)
l=[]
for i in s:
    sum=0
    for j in i:
        sum+=eval(j)
    l.append(chr(sum+64))
print(''.join(l))

Python 3.8.5 (tags/v3.8.5:580fbb0, Jul 20 2020, 15:57:54) [MSC v.1924 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: D:\python\2.py =====
['888842', '888884', '88881', '8888421', '888888821', '88888881', '8421', '88888
841', '8888421', '8888821', '8888842', '8421', '888888421', '888421', '888821',
81', '88888421', '81', '8841', '88884', '88842', '88888821', '88888', '1', '8888
4', '88888421', '888888421', '888888841', '']
flag{yOu_knOw_cIoIUd`shAdow}@
>>>
```

7. where is my key

看到题目描述和附件：

钥匙好像藏在了 fz130

```

flag = "*****"
m = "flag{" + flag + "}"
c = ""
key = "****"
key_list = []
j = 0

for i in range(len(flag)):
    key_list.append(int(key[j]) ^ i)
    j += 1
    if j == 3:
        j = 0

for i in range(len(flag)):
    c += chr(ord(flag[i]) + key_list[i])

print(c)

#5:fch7@:>m>lC>pDtwLDHKxHQ}MMQMV}

```

直接逆向推个脚本然后 key 盲猜是 130 得到 flag

```


c = "5:fch7@:>m>lC>pDtwLDHKxHQ}MMQMV}"
key = "130"
key_list = []
j = 0
flag = ""

for i in range(len(c)):
    key_list.append(int(key[j]) ^ i)
    j += 1
    if j == 3:
        j = 0

for i in range(len(c)):
    flag += chr(ord(c[i]) - key_list[i])
m = "flag{" + flag + "}"

print(m)

```

 Python 3.8.5 Shell

File Edit Shell Debug Options Window Help

```

Python 3.8.5 (tags/v3.8.5:580fbb0, Jul 20 2020, 15:57:54)
[AMD64] on win32
Type "help", "copyright", "credits" or "license()" for more
>>>
===== RESTART: D:\python\4.py =====
flag{48daa2966e5a60b6af9447c18c33207a}
>>>

```

8. I am Julius Caesar

看题目描述可知为凯撒密码

I am Julius Caesar

100

Isip{Gpxpcbu_kg_Gyoslpj}

然后移位遍历后手撸 flag

qxnu {Lucuhgz_pl_Ldtxquo}	向右偏移了5位
ryov {Mvdviha_qm_Meuyrvp}	向右偏移了6位
szpw {Nwewjib_rn_Ntvzswq}	向右偏移了7位
taqx {Oxfxkjc_so_Ogwatxr}	向右偏移了8位
ubry {Pygylkd_tp_Phxbuys}	向右偏移了9位
vcsz {Qzhzmle_uq_Qiycvzt}	向右偏移了10位
wdta {Raiarmf_vr_Rjzdwaui}	向右偏移了11位
xeub {Sbjhng_ws_Skaexbv}	向右偏移了12位
yfvc {Tckcpoh_xt_Tlbfycw}	向右偏移了13位
zgwd {Udlhqqi_yu_Umcgzdx}	向右偏移了14位
ahxe {Vemerqj_zv_Vndhaey}	向右偏移了15位
biyf {Wfnfsrk_aw_Woeibfz}	向右偏移了16位
cjzg {Xgogtsl_bx_Xpfjcgai}	向右偏移了17位
dkah {Yhphutm_cy_Yqgkdhb}	向右偏移了18位
elbi {Ziqivun_dz_Zrhleic}	向右偏移了19位
fnci {Airjwvo_ea_Asimfid}	向右偏移了20位

flag {Welcome_to_Network}

9. 麻辣兔头!!!

看到题目可知为 rabbit 加密，打开附件看到一大串 ook

可知为 o0k 加密

Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook?
Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook? Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook.
Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook? Ook!
Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook! Ook. Ook? Ook! Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook.
Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook? Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook?
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook.
Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook? Ook. Ook.
Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook.
Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook?
Ook! Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook?
Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook? Ook. Ook.

解密得到下一层加密为 rabbit 加密，解密得到 flag

U2FsdGVkX18vD9yXN6V+1NjYFYFCgymFJQA91d7PSK1IdDacrXsNp4jEe3kCqR1aCoMbCTH1

Text to Ook!

Text to short Ook!

Ook! to Text

Text to Brainfuck

Brainfuck to Text

U2FsdGVkX18vD9yXN6V+1NjYFYFCgymFJQA91d7PSK1ldDacrXsNp4jEe3kCqRlaCoMbCTH1

自定义密码，例如：123456，如不需要密码时可以为空

Rabbit加密

Rabbit解密

清空输入框

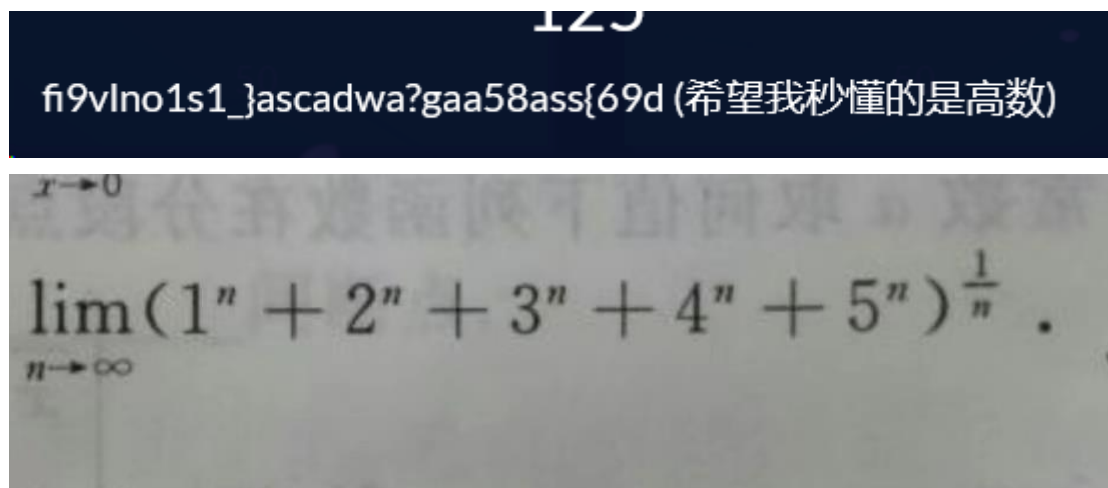
复制结果文本

flag{21232f297a57a5a743894a0e4a801fc3}

10. Railfence Cipher

根据题目可知这题是栅栏密码

打开附件和题目描述：



首先这个高数题答案是 5

然后尝试栅栏解密，key 为 5，得到 flag


```
fi9vlnolsl_}ascadwa?gaa58ass{69d
```

5

```
flag{asnioca65a19sd89awlv_asds?}
```

Misc:

1. trip

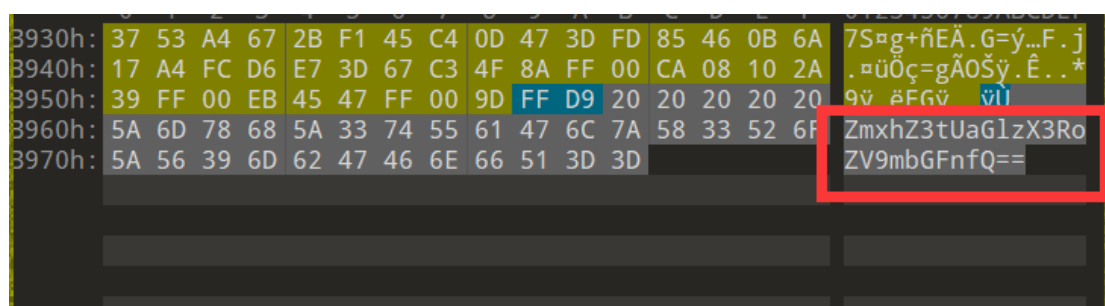
看到题目附件：



查询这些车次经过的站台，然后得到 flag{苏州站}

2. 010 上图

下载附件根据题目放入 010 看到 base 加密




解密得到 flag

```
PS D:\misc\CTF-Tools(一键解密)> ./base
请贴入字符串: ZmxhZ3tUaGlzX3RoZV9mbGFnfQ==
*****base16*****
not b16
not b62
*****base64*****
b'flag{This_the_flag}'
not b64
```

3. Seni0r h1gh school

看到附件有个引人注意的大招牌，搜店名得到位置



 客茶轩



百度一下

全部 视频 贴吧 问答 文库 笔记 筛选

八方客茶轩地址、电话、邮编、地图 -
图吧行业 - 图吧地图

9月8日 电话 八方客茶轩电话: 027-65389778 地址

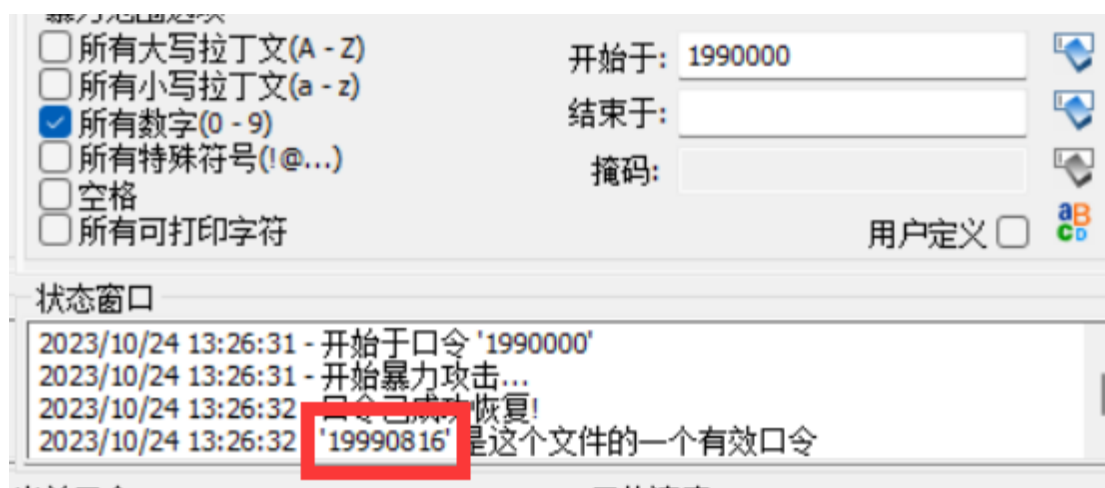


所以 flag {湖北省_武汉市_洪山高级中学}

4. zip 两连击

看题目描述，设置开头为 19900000 的八位数数字爆破得到压缩密码

李华使用自己的生日作为密码，我们只查到他的生日前三位为 199，你能解开这个压缩包吗？（虚拟设定，请勿带入现实）



解压得到第二个压缩包，放入 zipcracker 中识别为伪加密，提取出 flag

```
flag{xcicfnawdfg_Network}
```


	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52
0h:	00	00	04	B0	00	00	04	B0	08	02	00	00	00	64	43	24
0h:	98	00	00	00	09	70	48	59	73	00	00	0B	13	00	00	0B
0h:	13	01	00	9A	9C	18	00	00	20	00	49	44	41	54	78	5E



用 qr 解二维码得到 flag



请输入数据

已解码数据 1:

位置:(7.8,7.6)-(89.0,7.7)-(7.8,89.0)-(89.0,89.0)

颜色正常,正像

版本:3

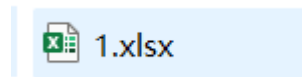
纠错等级:L,掩码:2

内容:

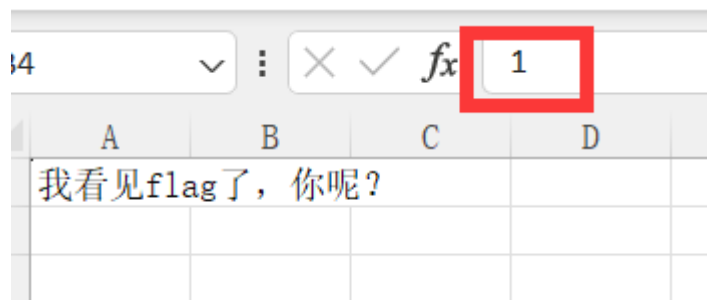
flag{4av8s6dvasdadfa?svasdV_Asdv45v}

6. EXCEL

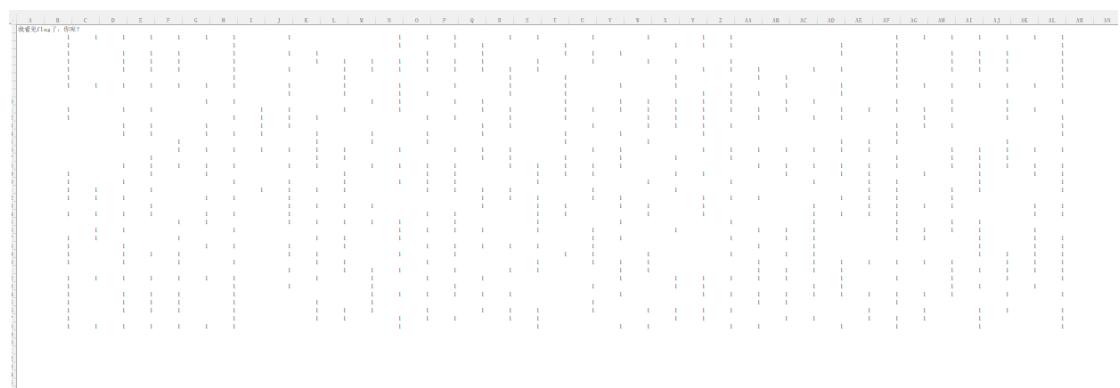
众所周知 Excel 文件本质是压缩包，所以将压缩文件后缀改为 xlsx 得到 Excel 文件



打开看到有字符无显示



选择大面积区域自定义单元格修改一波就显示了



修改 1 的格子为黑，然后改宽高得到二维码



再用 qr 解码得到 base 加密



已解码数据 1:

位置:(18.4,10.2)-(347.7,10.2)-(18.3,324.7)-(347.7,324.7)
颜色正常,正像
版本:5
纠错等级:H,掩码:5
内容:
ZmxhZ3tZb3VfZklhYVwxeV9mb1VuZF9NZS4xMTF9

解密 base 得到 flag

```
PS D:\misc\CTF-Tools(一键解密)> ./base
请贴入字符串: ZmxhZ3tZb3VfZklhYVwxeV9mb1VuZF9NZS4xMTF9
*****base16*****
not b16
*****base62*****
286440386521122633635061763251540602130432609565509208059130644931445279
not b62
*****base64*****
b'flag{You_finally_foUnd_Me.111}'
not b64
```

7. explosion

打开附件是个动图, 用 stegsolve 打开, 找到第 191 帧
有二维码, 但定位角给破坏了, 简单画图工具涂了下还
原二维码, 用 qr 解码得到 base, 解密得到 flag

Frame : 191 of 226



已解码数据 1:

位置:(17.2,11.0)-(322.5,11.9)-(16.6,320.2)-(322.2,321.0)

颜色正常, 正像

版本: 10

纠错等级:H, 掩码:0

内容:

R1kzRE1ZWldHRTNET04zQ0daU1RNWlJYR1EzRFNOUIJHVIRETU5KWEhBM1RBTIRER1pURE9NWldl
RTNHTU5URkc1U0E9PT09==

*****IDAT*****

```
b'flag{notia_explosion}'  
not IDAT
```

8. 裂开的 flag

附件是两个打不开的图片，放进 010 看到文件头被改了，还原打开得到 flag



Web:

1. 君子协议

打开题目看到：

In this little training challenge, you are going to learn about the Robots exclusion standard. The robots.txt file is used by web crawlers to check if they are allowed to crawl and index your website or only parts of it. Sometimes these files reveal the directory structure instead protecting the content from being crawled.

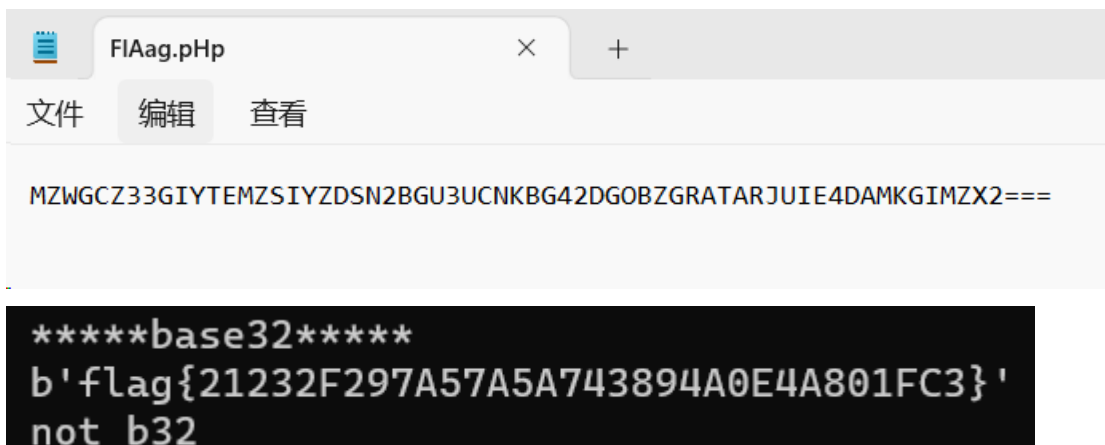
Enjoy!

明示查看 robots.txt，然后得到：

```
User-agent: *  
Disallow: /FlAag.pHp
```

```
User-agent: Yandex  
Disallow: *
```

打开得到 base，解密得到 flag



2. 302 jump

打开题目看到电击后无法跳转的按钮，用 bp 抓包得到

flag

```
=9 Content-Type: text/html; charset=
.0
.1 flag{We1c0me T0000 NTA!}
```

3. 功德+1

打开题目是敲木鱼游戏，直接看源码得到 js 文件。里面有段 base，解码得到 flag

```
cache.count += times;

if (cache.count > 1000000) {
    alert(atob("ZmxhZ3tPME8wSyFCMHVkbGU1c19CZW5lXmYxY2VuY2V9"))
}

localStorage.setItem('x_dzmy', JSON.stringify(cache));
```

```
PS D:\misc\CTF-Tools(一键解密)> ./base
请贴入字符串: ZmxhZ3tPME8wSyFCMHVkbGU1c19CZW5lXmYxY2VuY2V9
****base16****
not b16
****base62****
4232539395205635284555948221106635670889035795405587744852981383652
not b62
****base64****
b'flag{0000K!B0udle5s_Bene^f1cence}'
not b64
```

4. 奇怪的按钮

打开题目是个不能按的按钮，去检查—>控制器把 disabled “” 删了就可以按了，得到 flag

按下按钮获得flag

flag



按下按钮获得flag

flag

flag{fa966345577ba81af?aawrr23@#WEfwef}

5. getpost

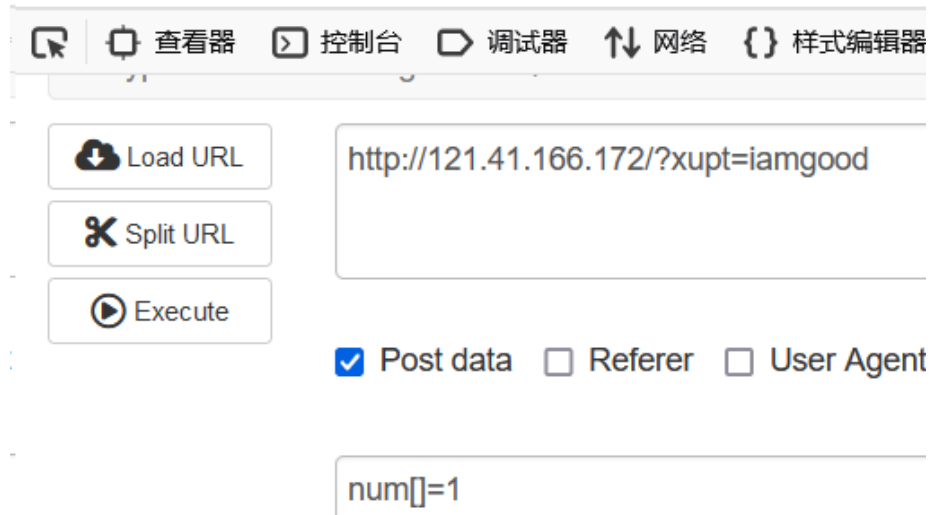
看题目：

```
include "error.php";
highlight_file('./index.php');
//num是一个数字哦!
if(isset($_POST['num']) && isset($_GET['xupt'])) {
    $num = $_POST['num'];
    $xupt = (String)$_GET['xupt'];

    if(preg_match("/([0-9]|cat|find|vim|ls|al|find|touch|echo)/", $num)) {
        echo $error;
        die;
    }
    else if(preg_match("/*flag\.php\.*/", $xupt)){
        echo $error;
        die;
    }
    else if(preg_match("/*flag\.php\.*/", $num)){
        echo $error;
        die;
    }
    else if ($num !== null && $xupt !== null && $xupt === 'iamgood') {
        echo $flag;
    }
}
```

要 num 不能有数字和那些命令，且不为 null 为一个数字，xupt 得为 iamgood，那直接给 num 来个数组绕过得到 flag

flag{nice!!good_job}



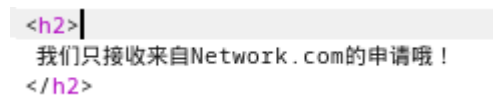
5. NTAuser

打开题目：

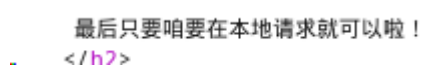


看到 cookie 是 user=guest

给他改成 NTAuser 进入第二层



我们加个 Referer:Network.com 伪造链接来源进入下一层



最后加个 X-Forwarded-For:127.0.0.1 表示本地请求得到 flag

```
<div class="center">
  <h2>
    flag{c0ngratul@tion!you_find_it!}
  </h2>
</div>
```

Pwn:

1. 瑞士军刀

nc 地址即可得到 shell

```
# nc 39.101.68.110 9233
ls
bin
dev
flag
lib
lib32
lib64
pwn0
cat flag
flag{f07dbe44-3daf-4d01-9a36-b9183be367fe}
```

2. 扫雷

nc 题目，输一局得到雷的地图然后通关游戏获得 shell

```
请输入排雷的位置:>1
1
0 1 2 3 4 5 6 7 8 9
1 1 0 0 0 0 0 0 0 1
2 0 1 0 0 0 0 0 1 0
3 0 0 1 0 0 0 1 0 0
4 0 0 0 1 0 1 0 0 0
5 0 0 0 0 1 0 0 0 0
6 0 0 0 0 1 0 0 0 0
7 0 0 0 0 0 0 0 0 0
8 0 0 0 0 0 0 0 0 0
9 0 0 0 0 0 0 0 0 0
很遗憾，排雷失败，你被炸糊了 ...
```

```
恭喜你，排雷成功 ...
0 1 2 3 4 5 6 7 8 9
1 1 0 0 0 0 0 0 0 1
2 0 1 0 0 0 0 0 1 0
3 0 0 1 0 0 0 1 0 0
4 0 0 0 1 0 1 0 0 0
5 0 0 0 0 1 0 0 0 0
6 0 0 0 0 1 0 0 0 0
7 0 0 0 0 0 0 0 0 0
8 0 0 0 0 0 0 0 0 0
9 0 0 0 0 0 0 0 0 0
ls
bin
dev
```

没看到 flag, ls -lR 遍历目录看到 flag 地址

```
./mine/failure:
total 4
-rwxr----- 1 0 1000 28 Oct 16 10:51 flag
cd ./mine/failure
```

```
ls
flag
cat flag
flag{Zhen_de_j1n_l1n_le!!!}
```

得到 flag

3. 馅饼

看 ida 其实已经拿到 shell 了但是给关闭了输出

```
close(1);
close(2);
execve("/bin/sh", 0LL, 0LL);
return 0;
```

可以用 1>&0 来重新定向得到 flag

```
nc 39.101.68.110 9145
ls
ls 0>&1
ls 1>&0
bin
dev
flag
lib
lib32
lib64
libexec
libx32
pwn3
cat flag 1>&0
flag{Sanntaa_wants_t0_make_more_4nd_m0re_money!!!}
```