HGAME 2022 Week1 writeup by nerowander

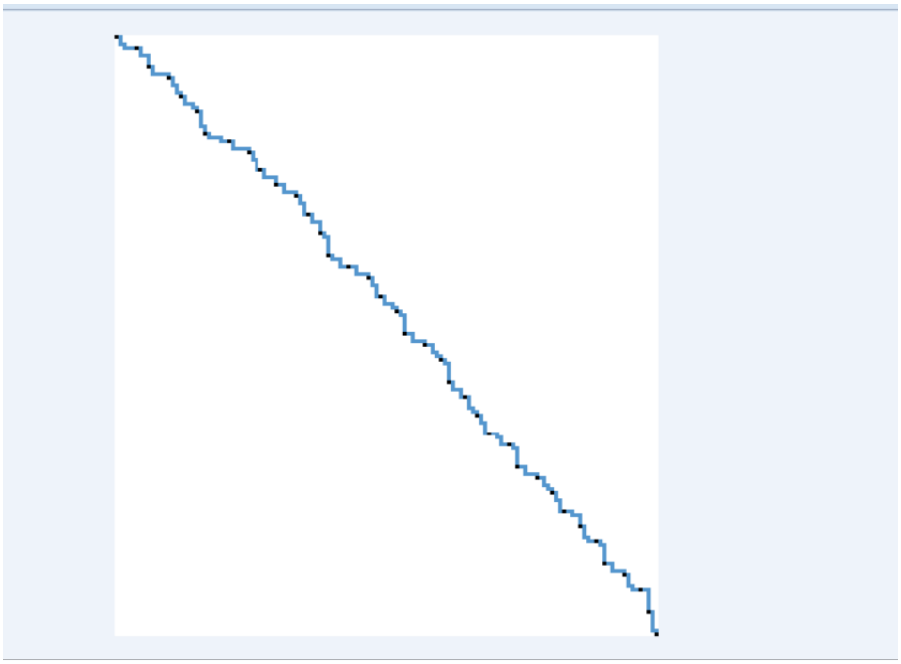
[TOC]

遇事不决问出题人，真的能帮你省很多不必要花费的时间，以及得到更好的学习机会

crypto

dancing line

点进去看是一张图片



发现每两个相邻的黑点之间走的步数都是 8 步

以 d 为右，s 为下

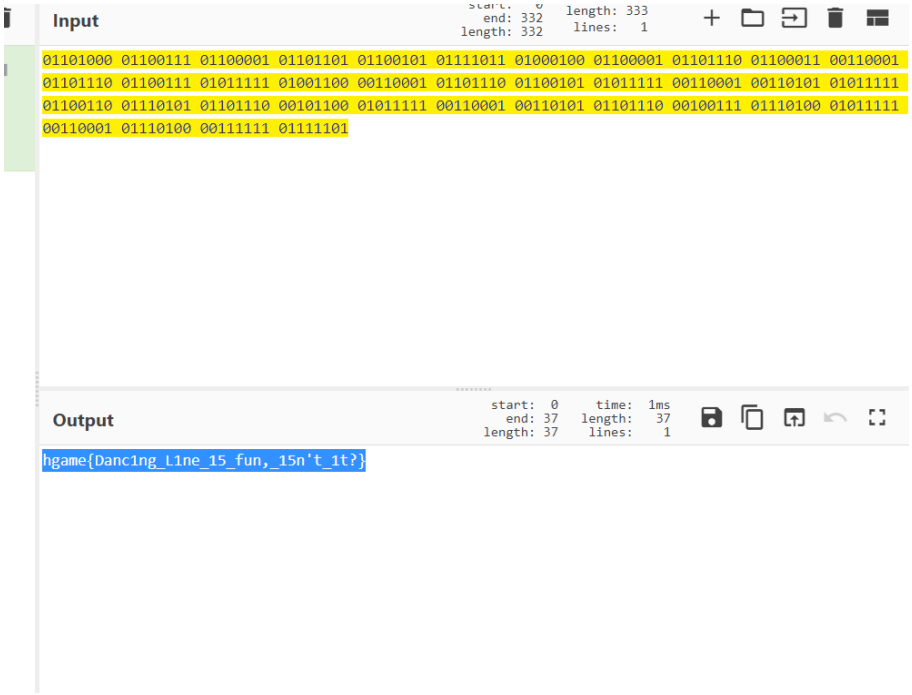
dssdsddd dssddsss dssddds dssdssds dssddsds dssssdss dsdddsdd dssddds dssdsssd dssddss ddssddds dssdsssd dssddsss dsdssss dsddssdd ddssddds dssdsssd dssddsds dsdssss ddssddds ddssdsds dsdssss dssddssd dsssdsds dssdsssd ddsdssdd dsdssss ddssddds ddssdsds dssdsssd ddsddsss dsssdsdd dsdssss ddssddds dsssdsdd ddssssss dsssssds

8 步为一个单位，可依次联想到二进制

用 0 代替 d，1 代替 s

```
01101000 01100111 01100001 01101101 01100101 01111011 01000100 01100001
01101110 01100011 00110001 01101110 01100111 01011111 01001100 00110001
01101110 01100101 01011111 00110001 00110101 01011111 01100110 01110101
01101110 00101100 01011111 00110001 00110101 01101110 00100111 01110100
01011111 00110001 01110100 00111111 01111101
```

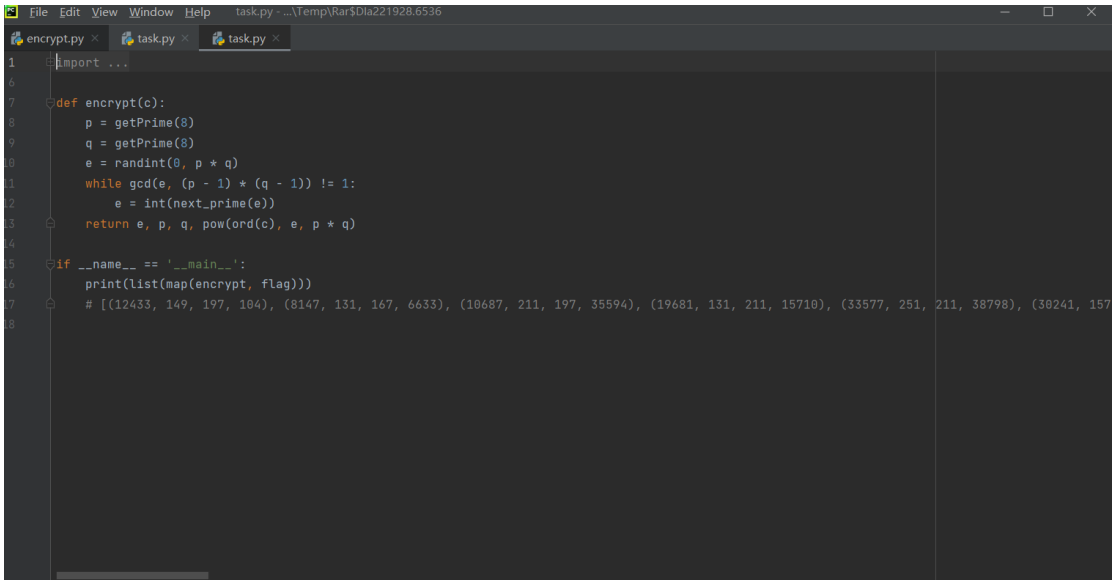
用 cyberchef 试一下



说实话，这道题的完成需要一定的脑洞

easy RSA

若干行 python 代码



去网上了解了一下 RSA 的一些参数

然后参考了一下网上大佬博客的脚本

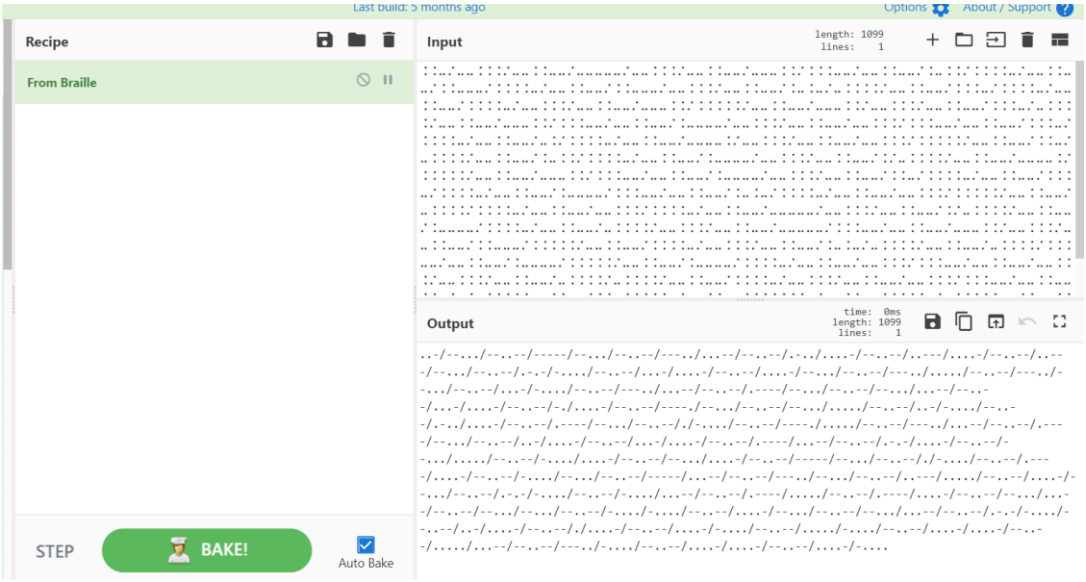
```
(22649, 211, 229, 7348), (1151, 179, 223, 17982), (8431, 251, 163, 30226), (38501, 193, 211, 30559), (14549, 211, 151, 21143), (24781, 239, 241, 45604), (8051, 179, 131, 7994), (863, 181, 131, 11493), (1117, 239, 157, 12579), (7561, 149, 199, 8960), (19813, 239, 229, 53463), (4943, 131, 157, 14606), (29077, 191, 181, 33446), (18583, 211, 163, 31800), (30643, 173, 191, 27293), (11617, 223, 251, 13448), (19051, 191, 151, 21676), (18367, 179, 157, 14139), (18861, 149, 191, 5139), (9581, 211, 193, 25595)]

#hgame{L00ks_l1ke_y0u've_mastered_RS4!}
def rsa_get_d(e, euler):
    k = 1
    while True:
        if (((euler * k) + 1) % e) == 0:
            return (euler * k + 1) // e
        k += 1

e=randint
euler=(p-1)*(q-1)
d = rsa_get_d(e, euler)

c = pow(m,e,p*q)
n = p*q
m = pow(c,d,n)
print(c)
```

一个字一个字打出来就可以了

Matryoshka

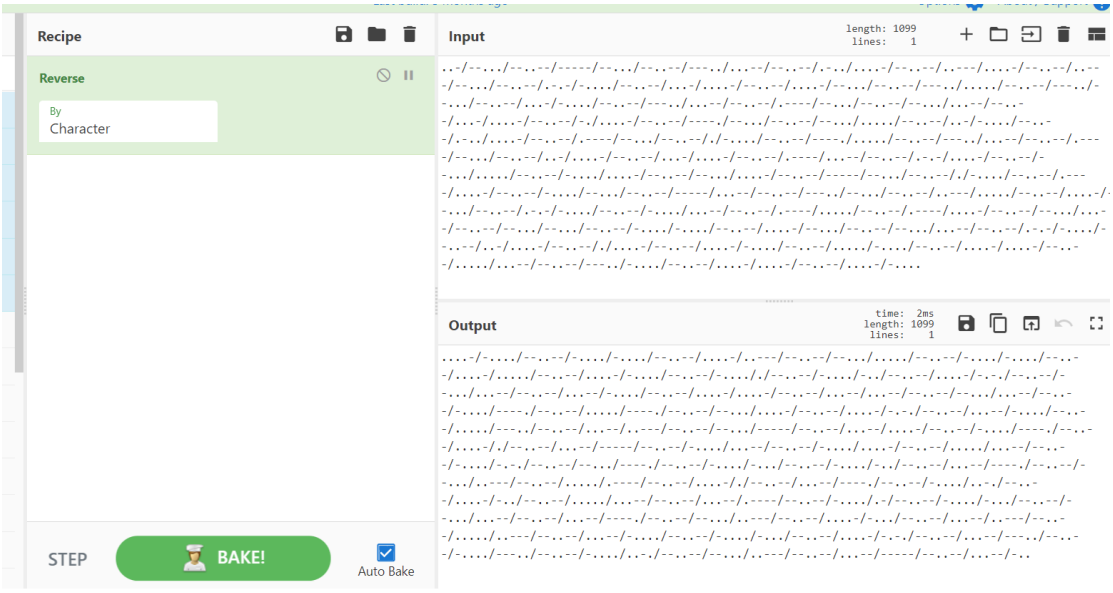
说实话这道题是真的卡了我很久，不过也让我了解了一些我没见过的密码和编码类型，出题的师傅辛苦了

打开文件，一看是 Braille 盲文

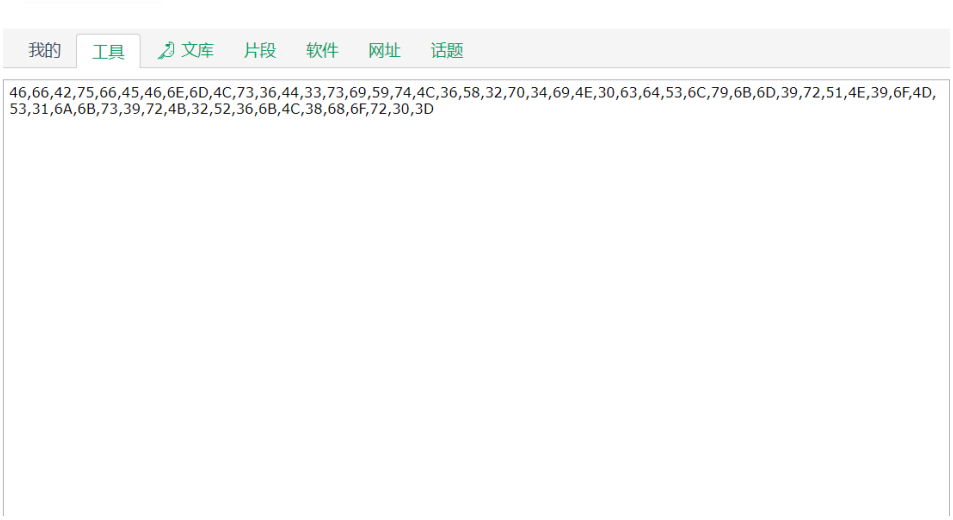


将它们翻译出来，是摩斯电码的形式

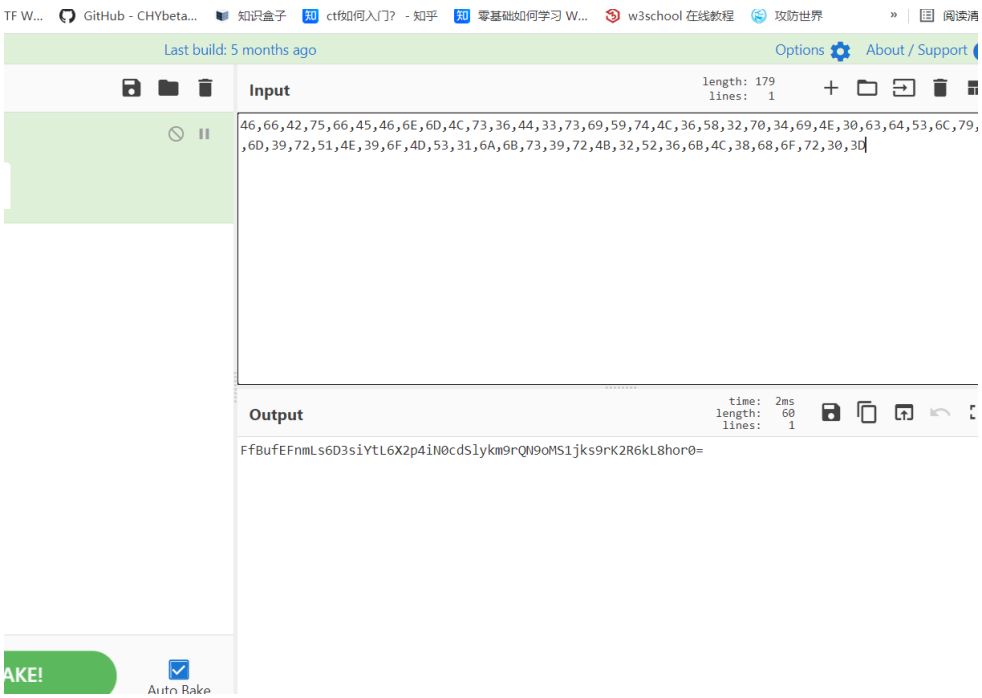
但是后来出题的学长提示，摩斯电码是第三步而不是第二步，后来我和出题的学长交流了一下，原来 reverse（倒序）也是一种替换编码



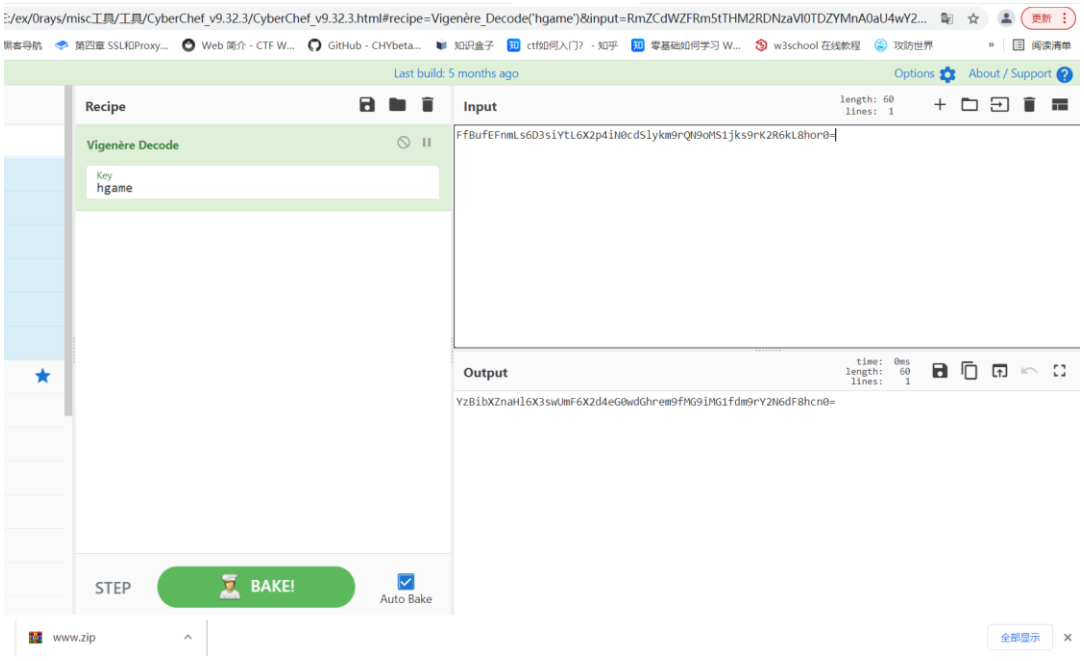
reverse 完之后，将 morse 解码



得到一串 hex 字符

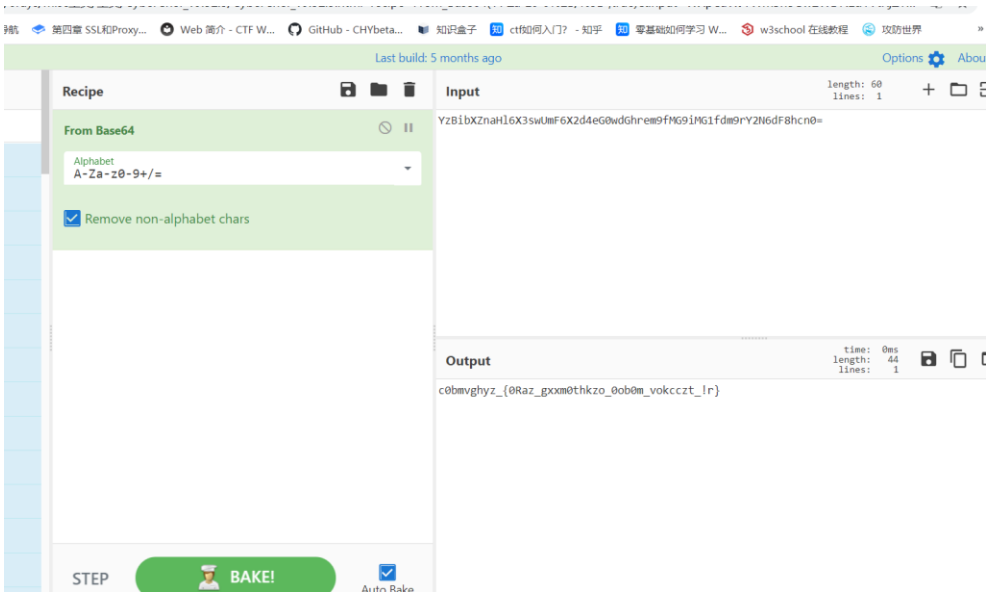


解码 hex，下一步就是根据"hgame"的密钥解密 vigenere

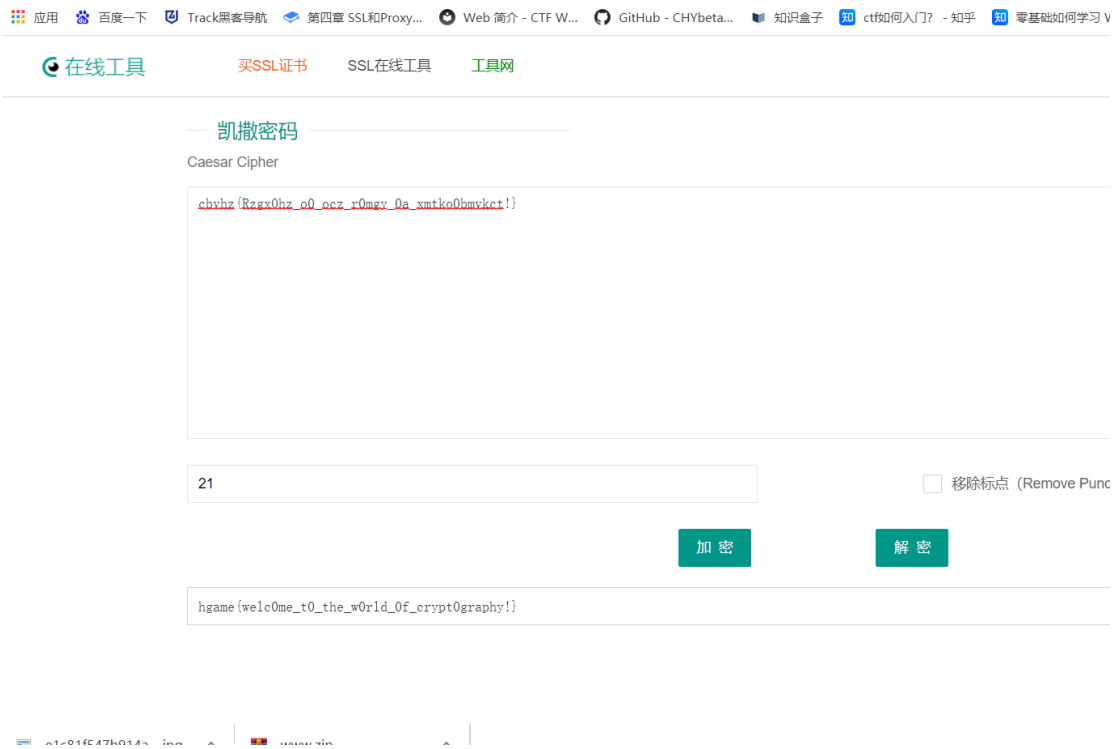


可以推理出下两步，一步是置换密码，一种是其他的编码形式

vigenere 解密完后，推测是 base64 的形式



最后栅栏密码和凯撒密码结合一下，然后就可以了（注意一下大小写，有的工具会把大写变成小写）



IoT

饭卡的 uno

打开附件，放进 010 editor 拉到底部即可

（010 editor 过期了，网上也没找到有效的激活码，截图就截不了了，sorry……）

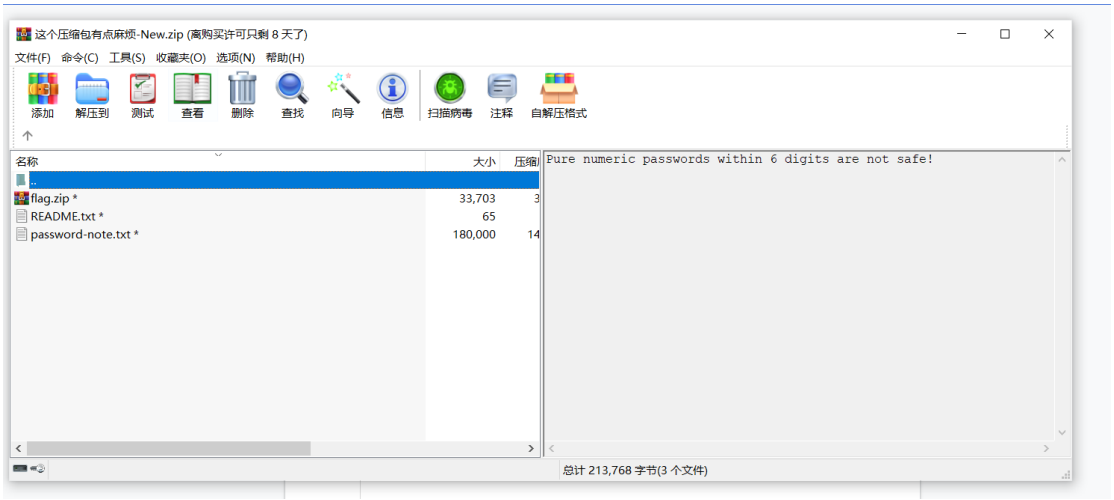
MISC

欢迎欢迎！热烈欢迎！

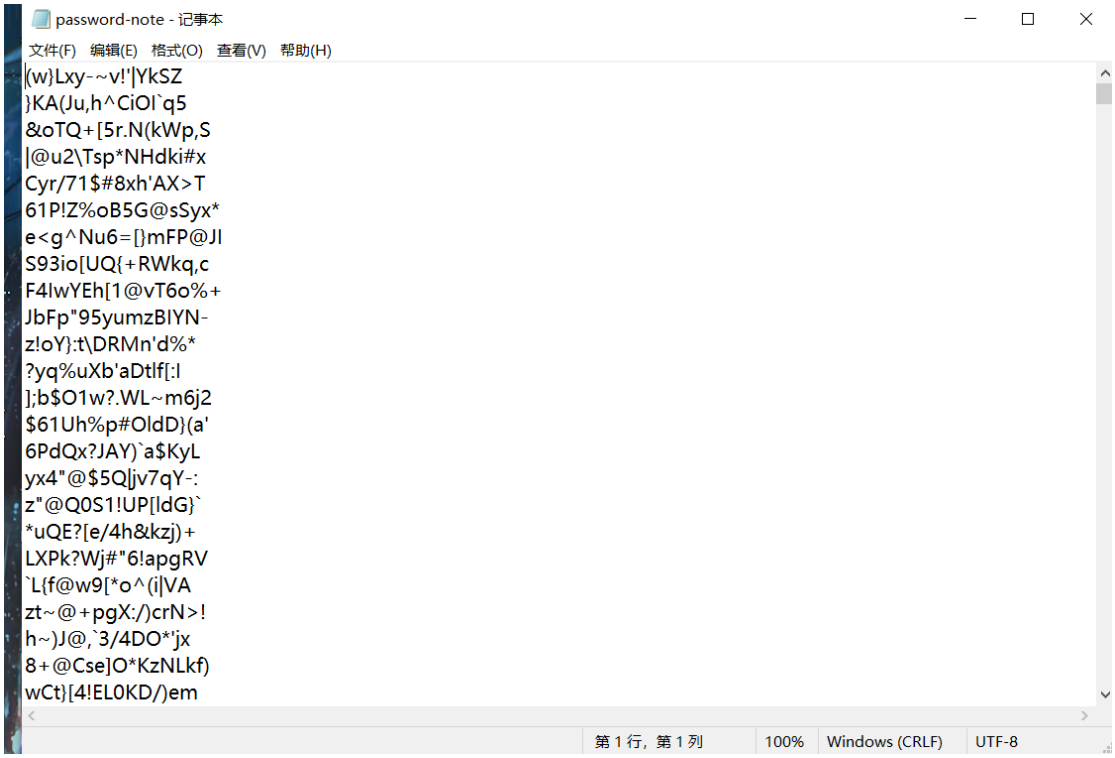
照题目那样做就行了，关注公众号发送消息即可

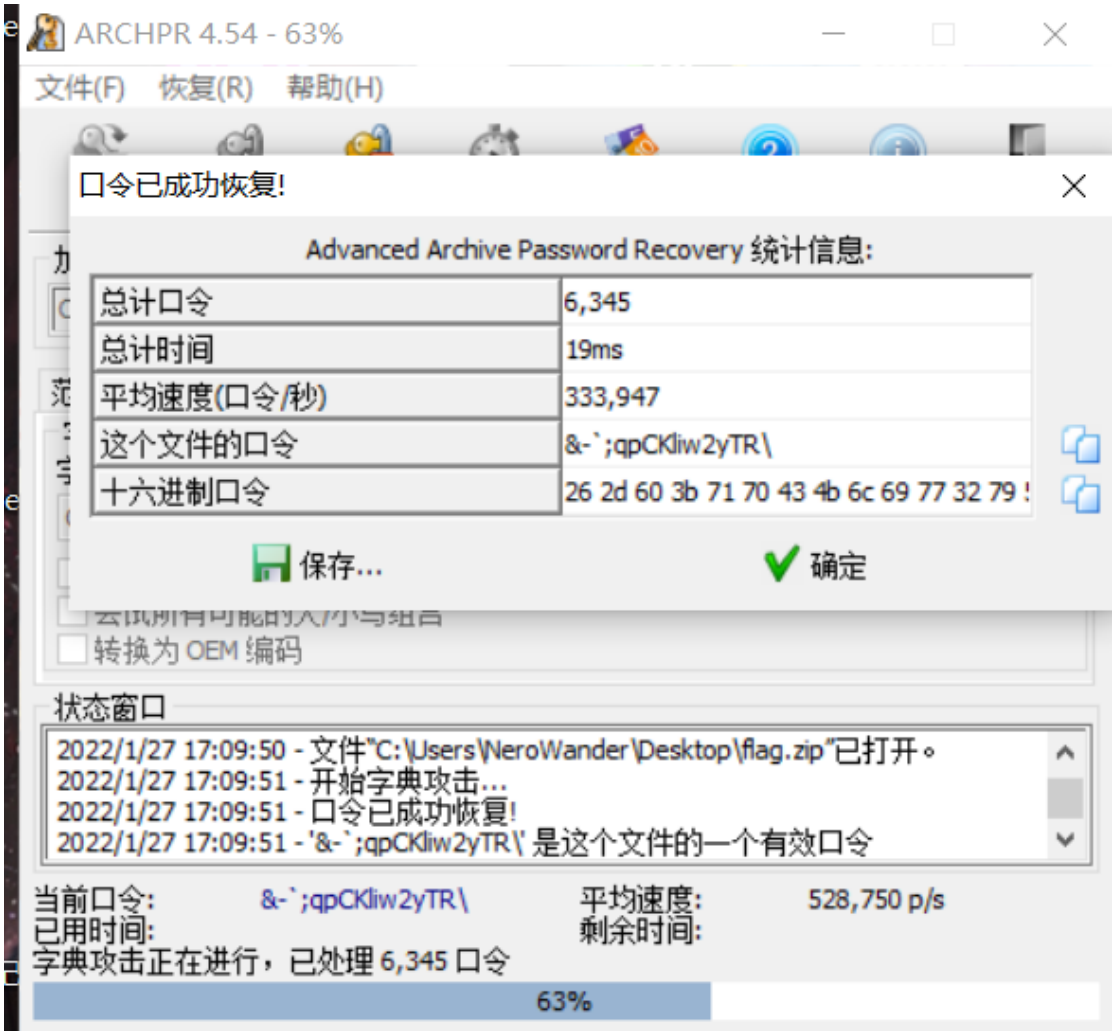
这个压缩包有点麻烦

打开压缩包，发现第一道的密码是弱纯数字类型口令

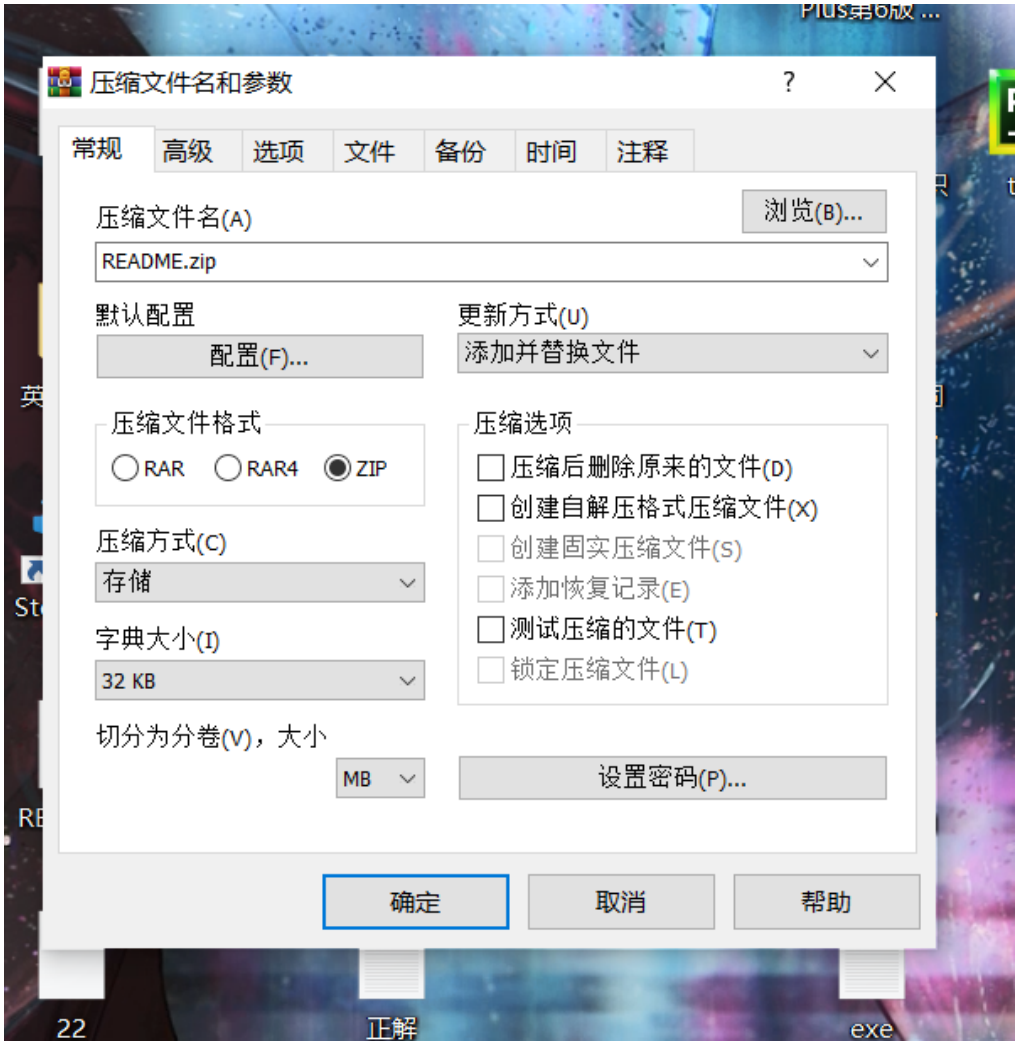


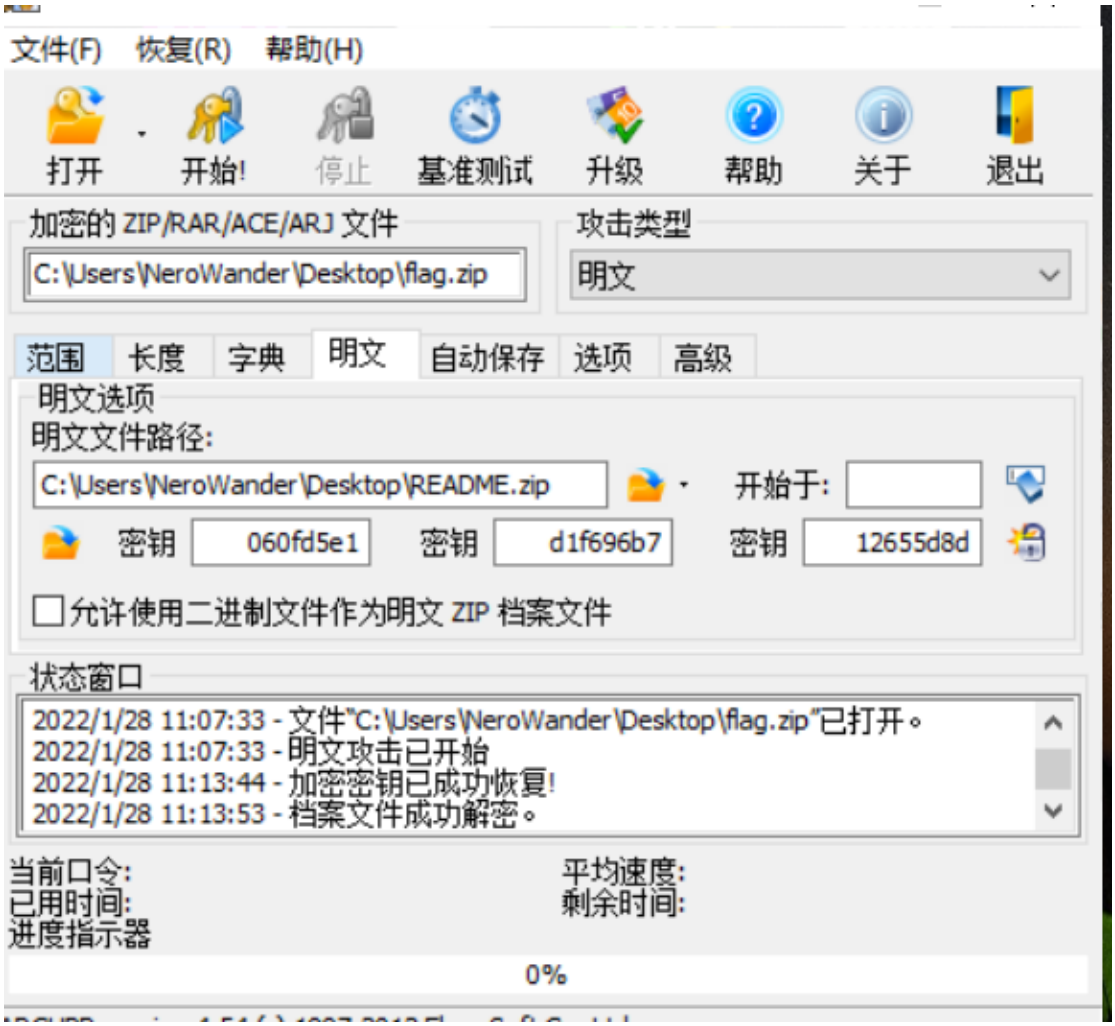
打开之后，发现一个密码本，根据密码本解密





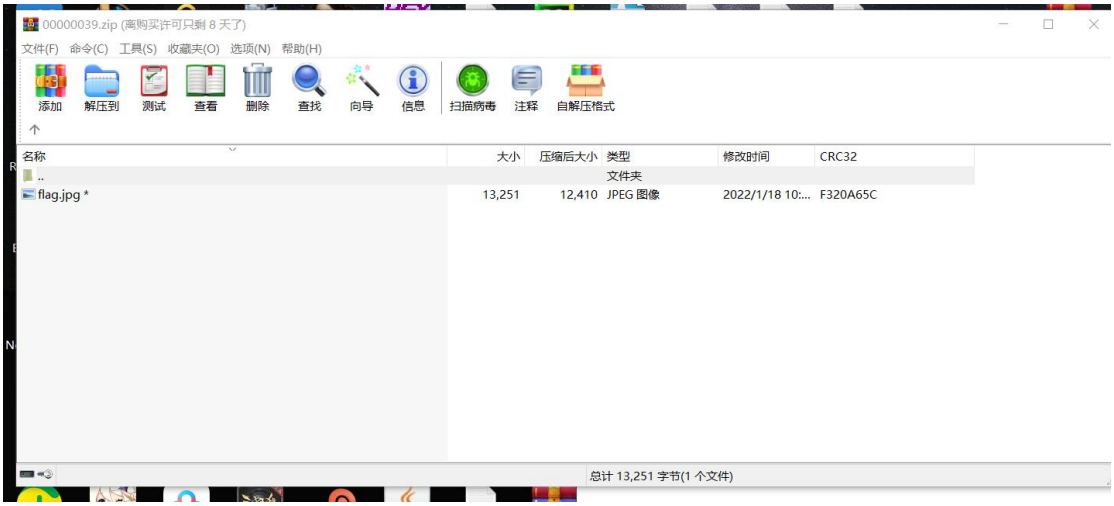
其中的已经解开的 readme 当中提示压缩包需要以“储存”的方式保存文件，然后将第二个压缩包里的 readme 分出来，运用明文攻击，得到第三道的密码

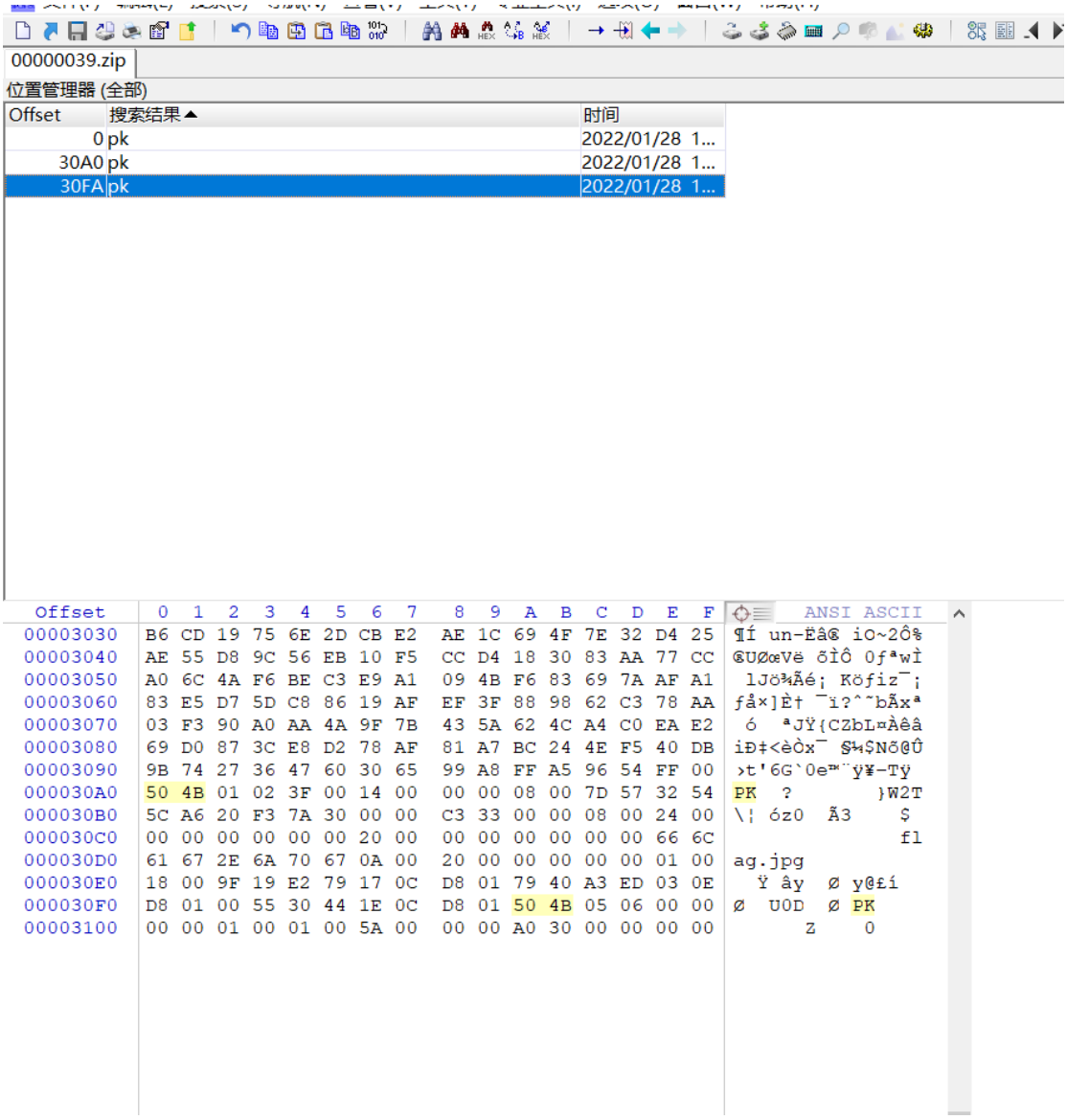

压缩文件名和参数
常规
高级
选项
文件
备份
时间
注释
压缩文件名(A)
浏览(B)...
README.zip
默认配置
配置(F)...
更新方式(U)
添加并替换文件
压缩文件格式
RAR
RAR4
ZIP
压缩选项
压缩后删除原来的文件(D)
创建自解压格式压缩文件(X)
创建固实压缩文件(S)
添加恢复记录(E)
测试压缩的文件(T)
锁定压缩文件(L)
压缩方式(C)
存储
字典大小(I)
32 KB
切分为分卷(V)，大小
MB
设置密码(P)...
确定
取消
帮助



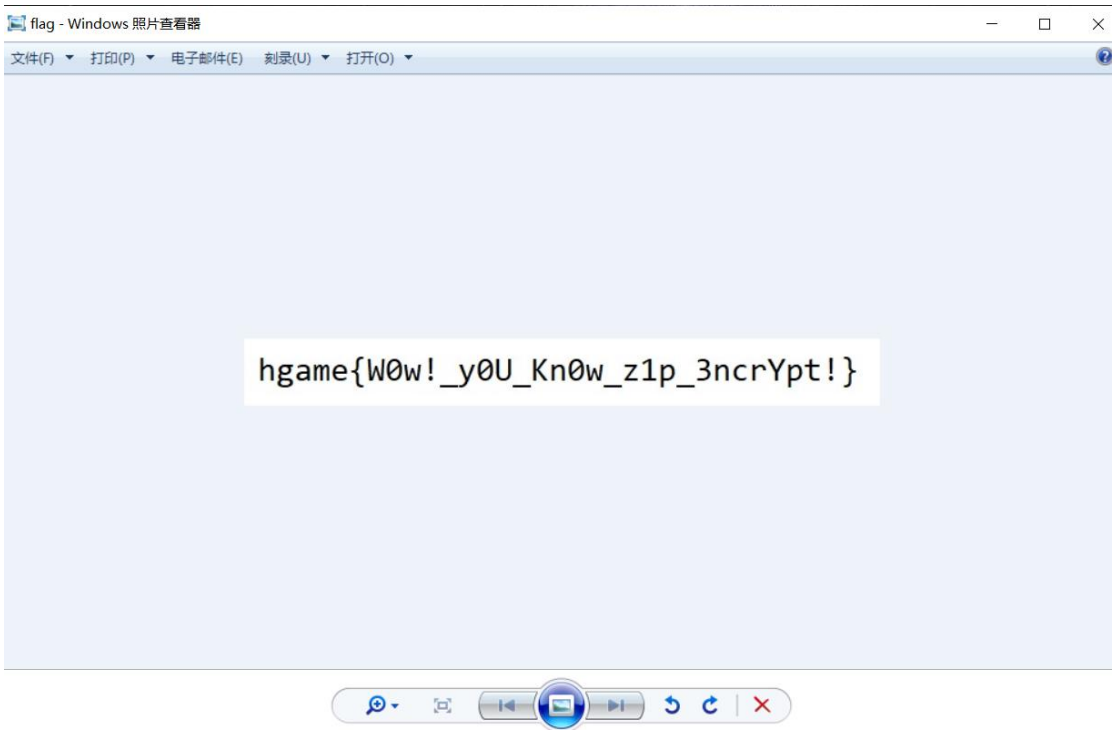
打开图片，没有什么线索，猜测图片里可能藏了文件，用 foremost 将图片分解

这图片又是加密的……但是已经没有任何线索了，联想到伪加密,修改 09 为 00 即可



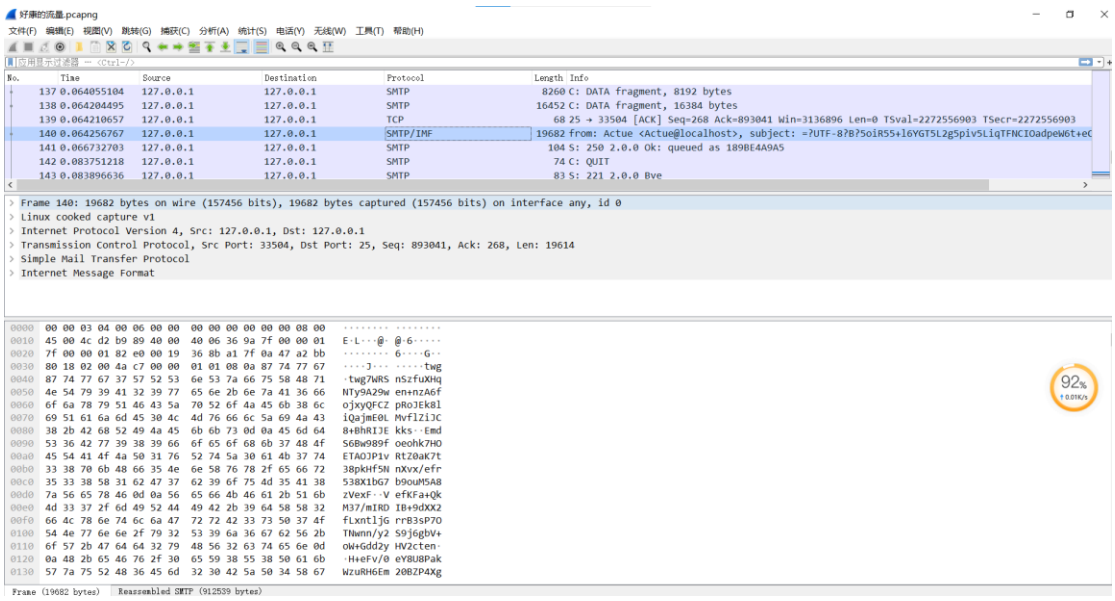

00000039.zip
位置管理器 (全部)
Offset 搜索结果 时间
0 pk 2022/01/28 1...
30A0 pk 2022/01/28 1...
30FA pk 2022/01/28 1...
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F ANSI ASCII
00003030 B6 CD 19 75 6E 2D CB E2 AE 1C 69 4F 7E 32 D4 25
00003040 AE 55 D8 9C 56 EB 10 F5 CC D4 18 30 83 AA 77 CC
00003050 A0 6C 4A F6 BE C3 E9 A1 09 4B F6 83 69 7A AF A1
00003060 83 E5 D7 5D C8 86 19 AF EF 3F 88 98 62 C3 78 AA
00003070 03 F3 90 A0 AA 4A 9F 7B 43 5A 62 4C A4 C0 EA E2
00003080 69 D0 87 3C E8 D2 78 AF 81 A7 BC 24 4E F5 40 DB
00003090 9B 74 27 36 47 60 30 65 99 A8 FF A5 96 54 FF 00
000030A0 50 4B 01 02 3F 00 14 00 00 00 08 00 7D 57 32 54
000030B0 5C A6 20 F3 7A 30 00 00 C3 33 00 00 08 00 24 00
000030C0 00 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C
000030D0 61 67 2E 6A 70 67 0A 00 20 00 00 00 00 00 01 00
000030E0 18 00 9F 19 E2 79 17 0C D8 01 79 40 A3 ED 03 0E
000030F0 D8 01 00 55 30 44 1E 0C D8 01 50 4B 05 06 00 00
00003100 00 00 01 00 01 00 5A 00 00 00 A0 30 00 00 00 00

打开图片，得到 flag



好康的流量

附件是一个流量包，发现里面可能包含了某种文件



将其导出，是一个邮件，打开邮件，发现图片

Wireshark · 导出 · IMF 对象列表

文本过滤器：

Content Type: All Content-Types

分组	主机名	内容类型	大小	文件名
140	Actue@localhost	EML file	912kB	=?UTF-8?B?5oiR55+l6YGT5L2g5piv5LiqTFNCIOadpeW6t+e

Save | Save All | Preview | Close | Help

邮件

我知道你是个LSB 来康点涩图

Actue <Actue@localhost>

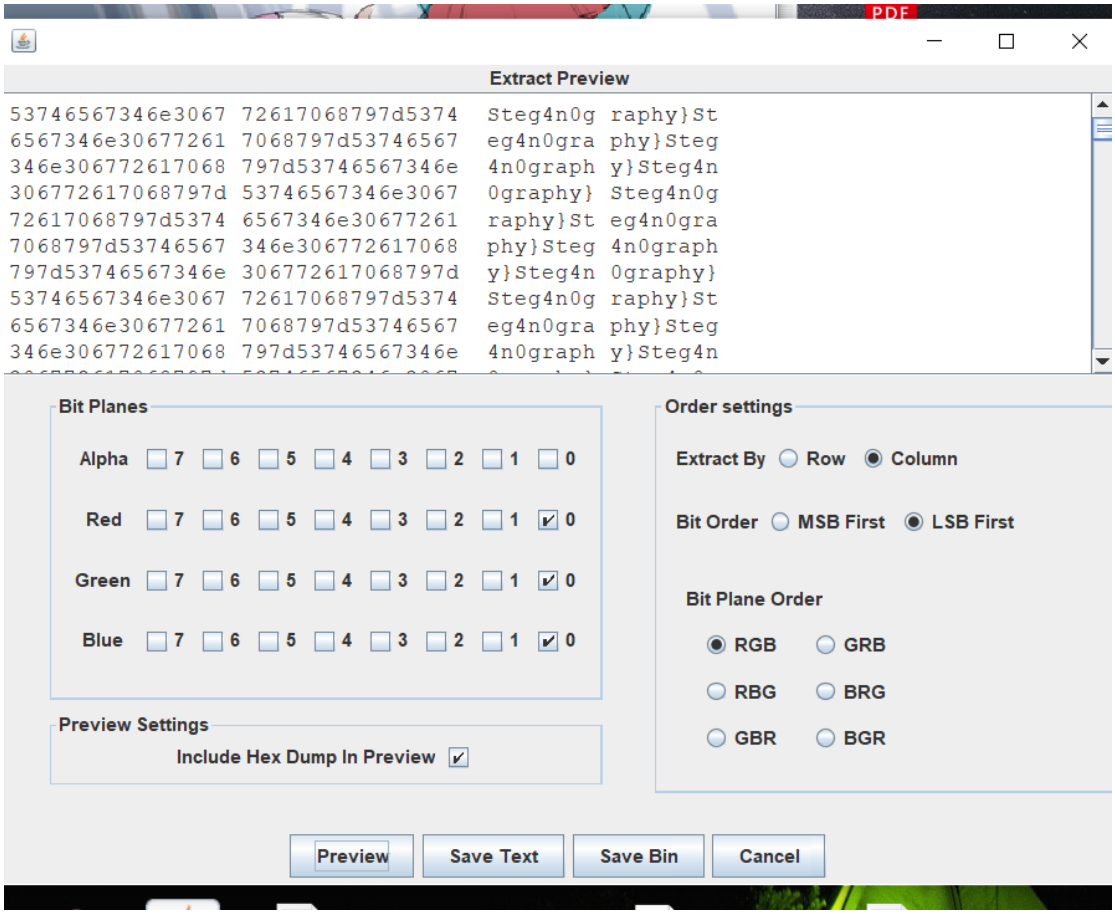
2022/1/18 21:49

收件人: dinner_card@localhost

用 stegsolve 分析，发现一份条形码

只有 flag 的前半部分，此时发现了新的线索

再用 stegsolve 的 lsb 分析一下，发现后半部分的 flag



群星（其实是幽灵东京）

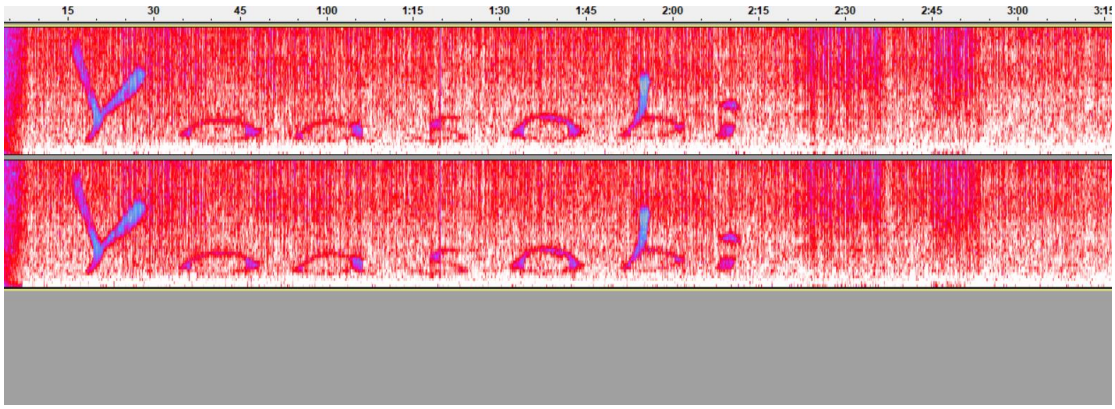
打开发现歌曲文件内有暗示

属性	值
说明	
标题	
副标题	
分级	☆☆☆☆☆
媒体	
参与创作的艺术家	why not try try SilentEye
唱片集	
年	
#	
流派	
时长	00:03:30
音频	
比特率	1536kbps
来源	
创建媒体日期	
版权	
内容	
家长分级	
父级分级原因	
文件	

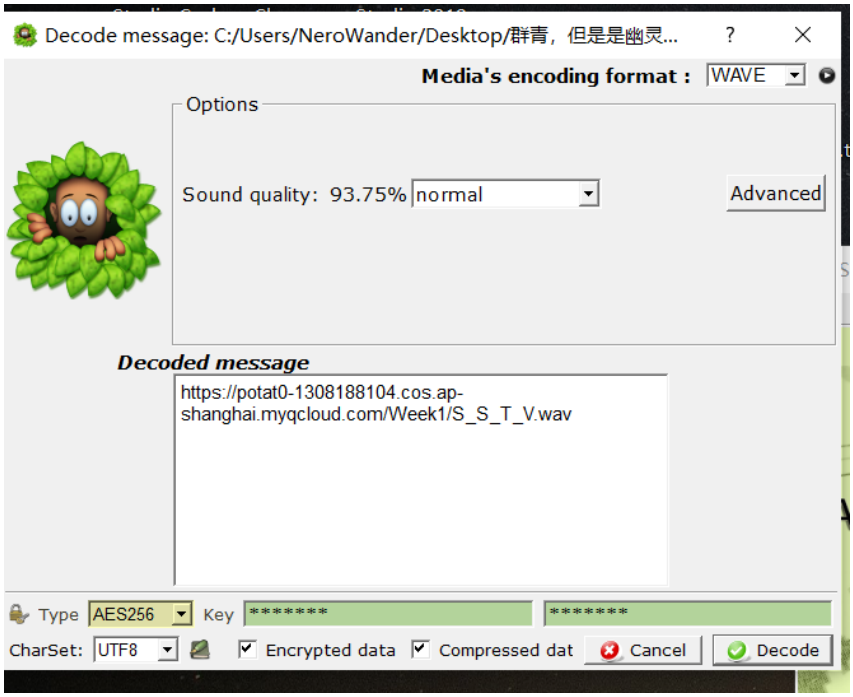
删除属性和个人信息

使用 silenteye

并用 audacity 分析歌曲，发现一串字符，猜测是密钥



解密后打开另外一个网址



发现是 sstv 的形式

可以用手机的 robot36 监听

得到一个二维码

扫二维码，得出 flag

PWN

test*your*nc

最入门的，利用爆破脚本，直接调试即可

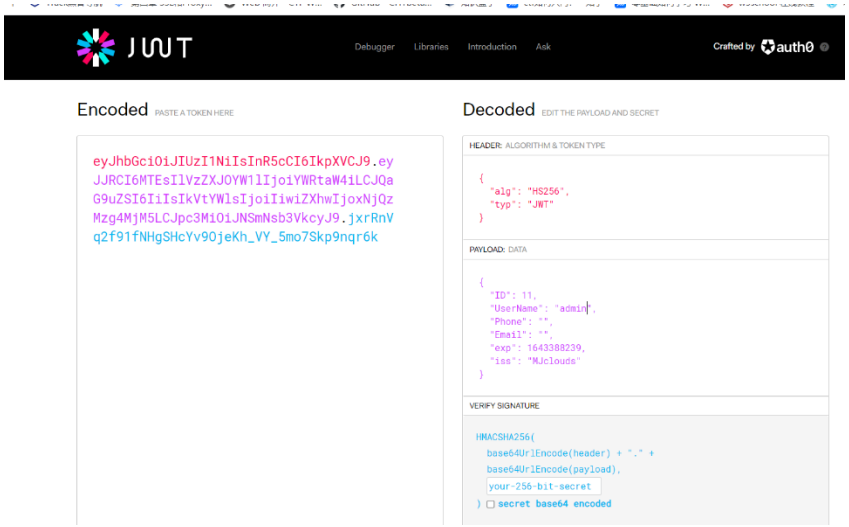
WEB

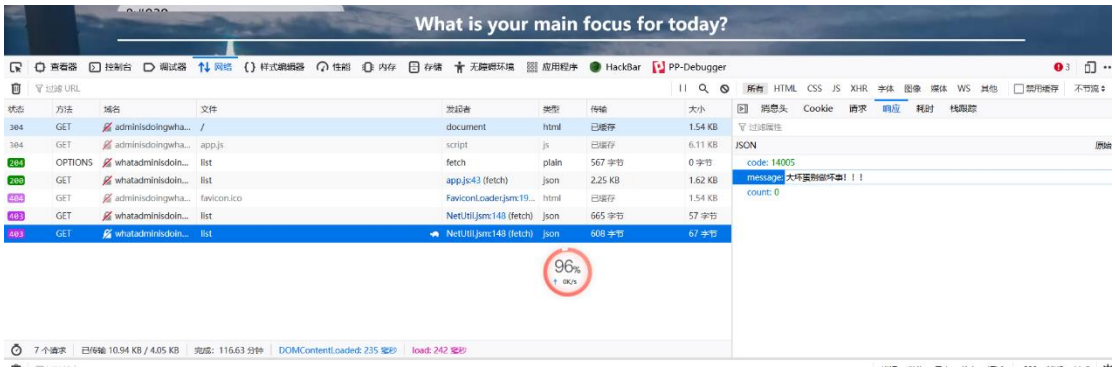
easy_auth

题目提示我们不要爆破，那就只能思考别的方法

结合群里发的学习资料可以得出应该利用 jwt token 的方法通过认证

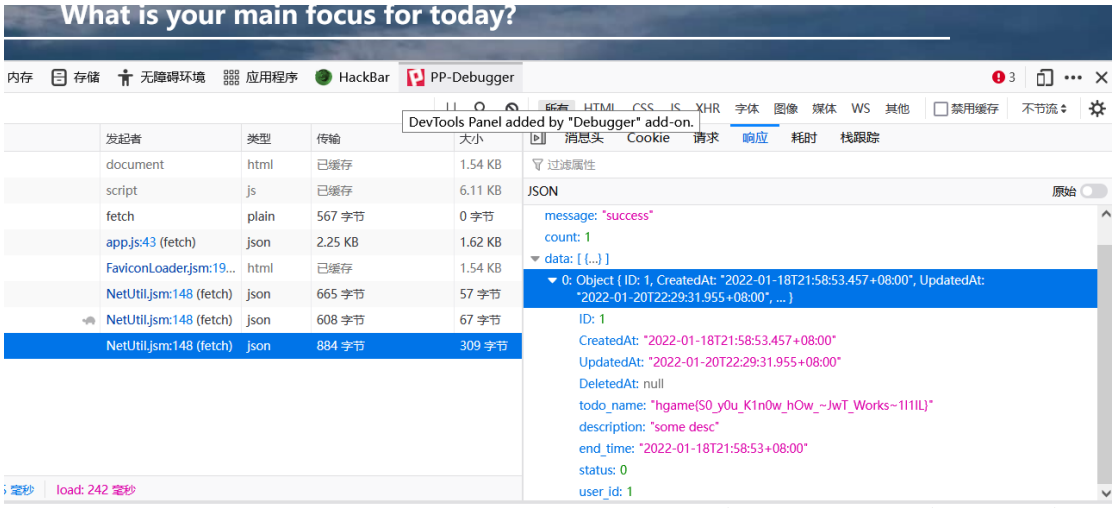
伪造 jwt token，username 修改为"admin"，发现并没有成功





和出题人交流了一下，得出 id=1 和密钥即为空的结论（照应了题目名称）

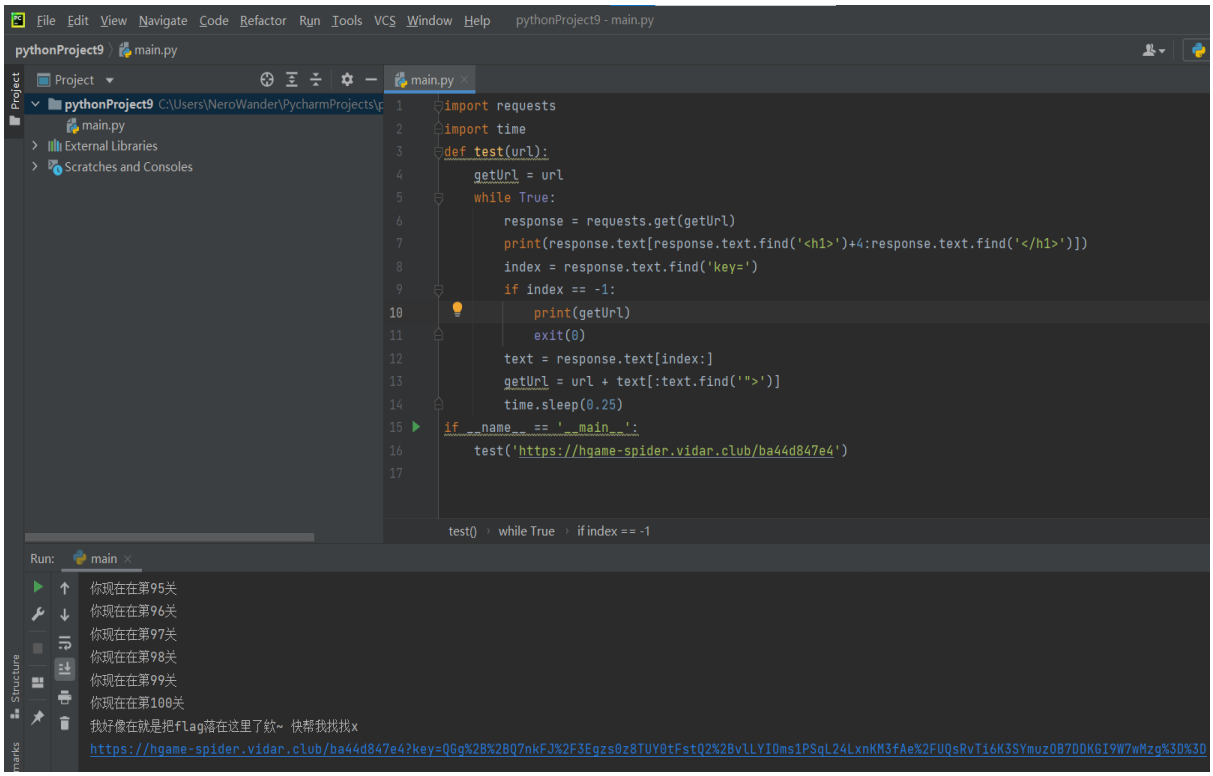
修改请求，在响应信息里看看，找到 flag



蛛蛛...嘿嘿♥我的蛛蛛

点 100 次，或者写个脚本

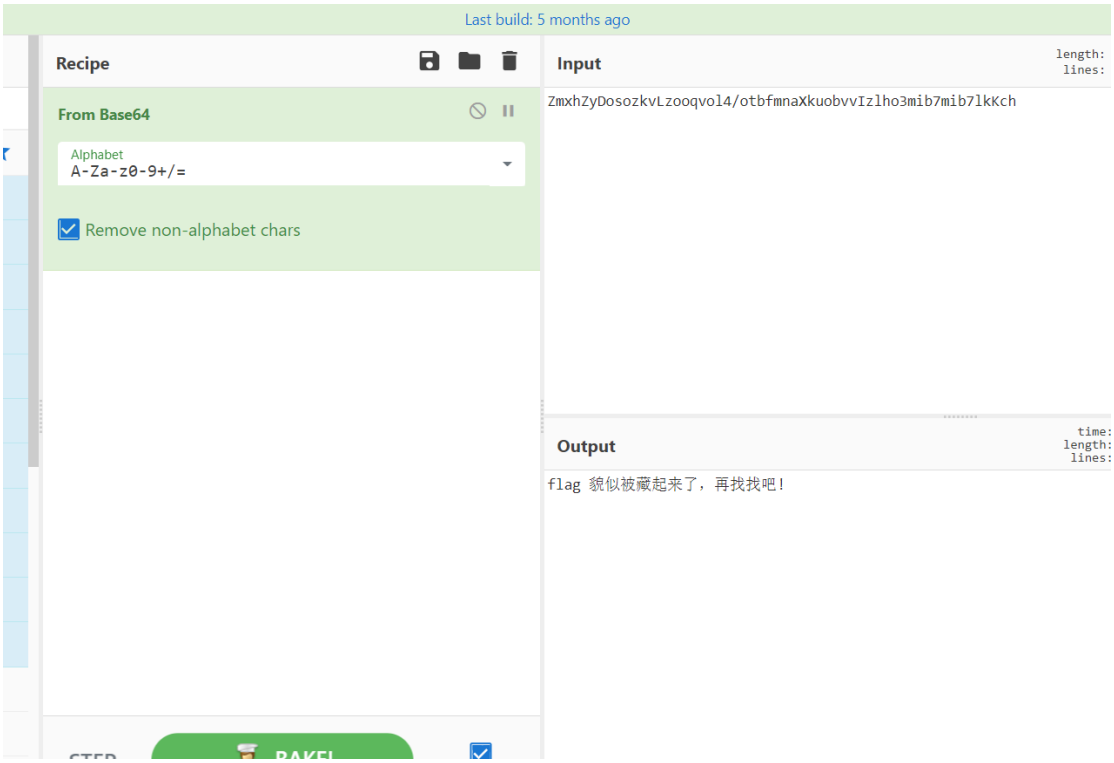
脚本如下



Tetris plus

首先要明白这是不可能拿到 3000 分的，在其 js 文件里发现一串 base64 编码

解码如下



之后又发现了注释里有关键信息

考虑到是 jsfuck 编码，在 console 里直接输入即可

Fujiwara Tofu Shop

一开始让我们先去一趟“秋名山”

在 referer 中添加网址

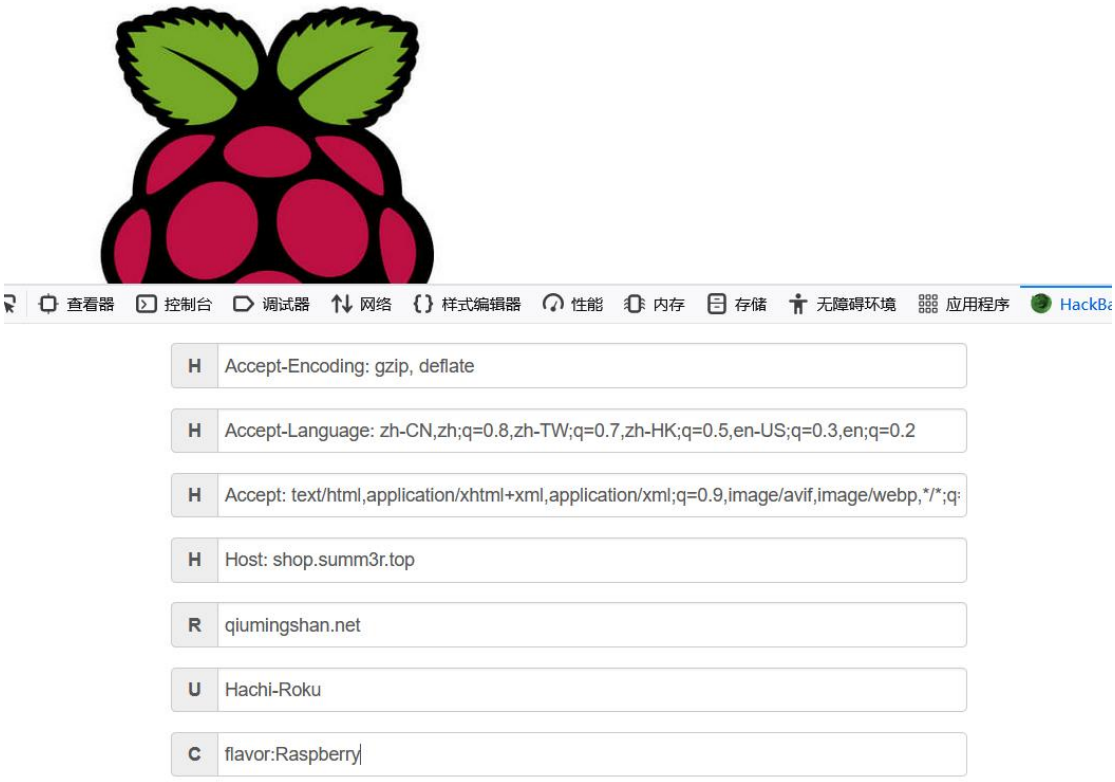
想成为车神，你需要先去一趟秋名山（qiumingshan.net）

接着让我们用 ae86 的通行证

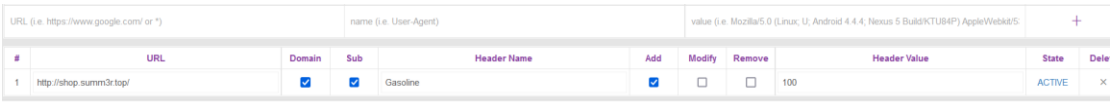
在 user-agent 里添加通行证信息

然后提示我们要在 cookie 当中添加树莓味的甜饼

按照提示操作



还要加满油



接下来是内网 ip 登录

发现 x-forward-for 没有生效

改用 x-real-ip，得到 flag

hgame{I_bOught_4_S3xy_swlmSu1t}