

Week 1

非常手忙脚乱的第一周，因为妈妈的同事的老婆从武汉回来且一家发烧，还被拉去疾控中心隔离和一天半。

Crypto

InfantRSA:

先去查了rsa是啥，得到



里面有道例题



根据前面可知，要求解m，就照着类似的打了一遍 ⇒ gmpy2处报错了
然后得知需安装gmpy2，就去搜了后，按照教程安装了 ⇒ 但还是报错

11111

得知可在cmd处输入python来看 ⇒ 果然得到警告 ⇒ 就卸载了所有重新安装
⇒ 然后安装了wheels, gmpy2[顺便学会了用cmd]

↓

16式开始

第一遍输入的m的十进制表达，试着提交 ⇒ ×

然后不知道，就去看别的题目了，下面有一道题里有binascii这个函数，去查询的时候，想到这题会不会用到，就尝试了

```

import binascii

import gmpy2
p = gmpy2.mpz(681782737450022065655472455411)
q = gmpy2.mpz(675274897132088253519831953441)
e = gmpy2.mpz(13)
c = gmpy2.mpz(275698465082361070145173688411496311542172902608559859019841)
n = p * q
phi_n = (p-1)*(q-1)
d = gmpy2.invert(e, phi_n)
m = pow(c, d, n)
print(m)
m_hex = hex(m)[2:]
print(m_hex)
m_binary = binascii.a2b_hex(m_hex)
print(m_binary)

```

```

C:\untitled\venv\Scripts\python.exe C:/untitled/InfrantRSA.py
39062110472669388914389428064087335236334831991333245
6867616d657b74335874364f306b5f5235412121217d
b'hgame{t3Xt600k_R5A!!!}'

```

Affine

先去查询 python find 是什么用途, 然后

```

import gmpy2
TABLE = 'zxcvbnmasdfghjklqwertyuiop1234567890QWERTYUIOPASDFGHJKLZXCVBNM'
MOD = len(TABLE)
cipher = ''
for b in cipher:
    ii = cipher.find(b)
    if ii == -1:
        flag += b
    else:
        i = (2*MOD - ii) // 11
        flag += TABLE[i]
print(flag)

```

Traceback (most recent call last):
File "C:\untitled\venv\Affine1.py", line 12, in <module>
flag += TABLE[i]
TypeError: string indices must be integers
Process finished with exit code 1

一直报错, 就改成了这样 →

一个一个输入得出 flag

hgame{M4th-u5Ed-IN-cRypt0}

```

#!/usr/bin/env python3
# -*- coding: utf-8 -*-
import gmpy2
from secret import A, B, flag
assert flag.startswith('hgame{') and flag.endswith('}')

TABLE = 'zxcvbnmasdfghjklqwertyuiop1234567890QWERTYUIOPASDFGHJKLZXCVBNM'
MOD = len(TABLE)

cipher = ''
for b in flag:
    i = TABLE.find(b)
    if i == -1:
        cipher += b
    else:
        ii = (A*i + B) % MOD
        cipher += TABLE[ii]

print(cipher)
# A8I6z{xrlA J7ha vG TpH410}

```

根据对照 → 得出

由这些可知

$$\begin{aligned} (A \times 12 + B) \% 62 &= 46 & A \neq 13 \\ (A \times 11 + B) \% 62 &= 33 & \downarrow \\ (A \times 7 + B) \% 62 &= 43 & 7A + B = 167 \\ (A \times 6 + B) \% 62 &= 30 & 6A + B = 92 \\ (A \times 8 + B) \% 62 &= 0 & \downarrow \\ & & A = 75 \\ & & B = -358 \end{aligned}$$

```

1 import gmpy2
2 TABLE = 'zxcvbnmasdfghjklqwertyuiop1234567890QWERTYUIOPASDFGHJKLZXCVBNM'
3 MOD = len(TABLE)
4 ii = TABLE.find(" ")
5 for i in range(62):
6     x = (75*i - 358) % MOD
7     if x == 0:
8         print(TABLE[i])
9
10
11

```

Affine1

C:\untitled\venv\Scripts\python.exe C:/untitled/venv/Affine1.py

e

Reorder

这题一开始以为重点是 oracle，然后搜索了甲骨文加密，然后把 oracle 字段加密方法给看了。然后搜索了 nc 47.98.192.231 25002，没有什么结果，再搜索了 47.98.192.231 25002，好像是 ip 地址的样子，但没什么进展。最后去问了学长，得到搜索 netcat。然后搜索了 net cat 用法，安装好后都试了一遍，只有

```
C:\Users\86157>nc64 -v -s 47.98.192.231 25002
47.98.192.231: inverse host lookup failed: h_errno 11004: NO_DATA
25002: inverse host lookup failed: h_errno 11004: NO_DATA
no port[s] to connect to: NO_DATA
```

结论，没做出来。

Misc

欢迎参加 Hgame

Li0tIC4uLi0tIC4tLi4gLS4tLiAtLS0tLSAtLSAuIC4uLS0uLSAtIC0tLSAuLi0tLi0gLi4tLS0gLS0tLS0gLi4tLS0gLS0tLS0gLi4tLS4tIC4uLi4gLS0uIC4tIC0tIC4uLi0t

题目中是这样的一串，根据前一天做 CRYPTO 看到的密码学，应该是 Base64 编码，解码后得到

明文:		BASE64:
<div></div>	<div>BASE64编码 ></div> <div>< BASE64解码</div>	<div>Li0tIC4uLi0tIC4tLi4gLS4tLiAtLS0tLSAtLSAuIC4uLS0uLSAtIC0tLSAuLi0tLi0gLi4tLS0gLS0tLS0gLi4tLS0gLS0tLS0gLi4tLS4tIC4uLi4gLS0uIC4tIC0tIC4uLi0t</div>

然后再运用摩斯密码

壁 纸



Pixiv@J â 卐 卐 卐
æz

根据提示，解压，获得，之后搜索 `æz` “ctf 图片”，看到

有使用 stegsolve, winhex, 还有 binwalk。先用 stegsolve 尝试, 得到这是一张正常的图片, 根据网上的改变色调也没有发生什么。然后用 winhex 打开, 可以看到最后有这样一句

flag.txt E"@=ÓÊ
 Ô E"@=ÓÊÔ Ç,œ ÓÊÔ PK Z
 v Password is picture ID.

，然后根据隐写的分类，将 50 4B 开头一直到结束的保存

为 zip 格式，得到一个压缩文件。然后去搜索了，得到

那些图片的ID怎么查

我来答

分享

举报

1个回答

#春节# 今年春节在家聚还是出去嗨?



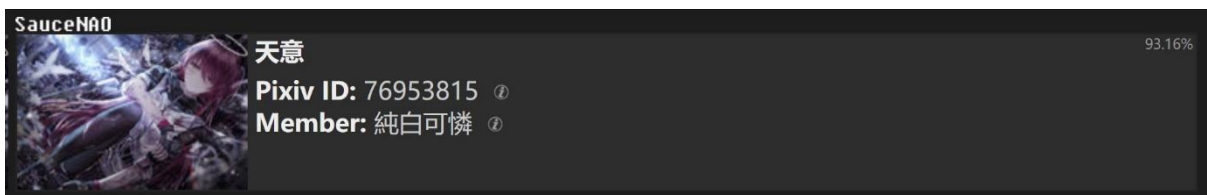
仙智慧2

2017-02-12

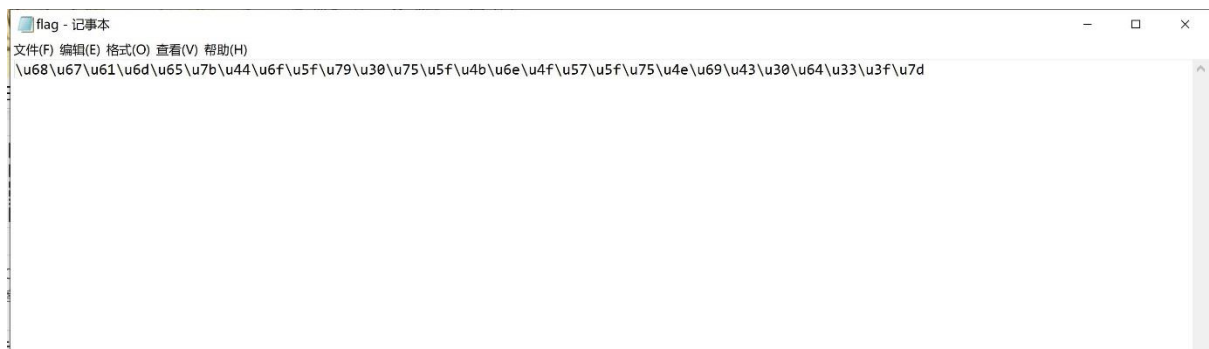
您是指pixiv（即P站的iD）吗？

如果是的话，进入下面网址，将图片上传，如果作者曾经在P站上传过这张图片，那么ID就会出现

<http://saucenao.com/index.php>



输入 ID，得到一个 flag.test,打开，得到



解码得到 flag

加密或解密字符串长度不可以超过10M

\u68\u67\u61\u6d\u65\u7b\u44\u6f\u5f\u79\u30\u75\u5f\u4b\u6e\u4f\u57\u5f\u75\u4e\u69\u43\u30\u64\u33\u3f\u7d

16进制转字符

字符转16进制

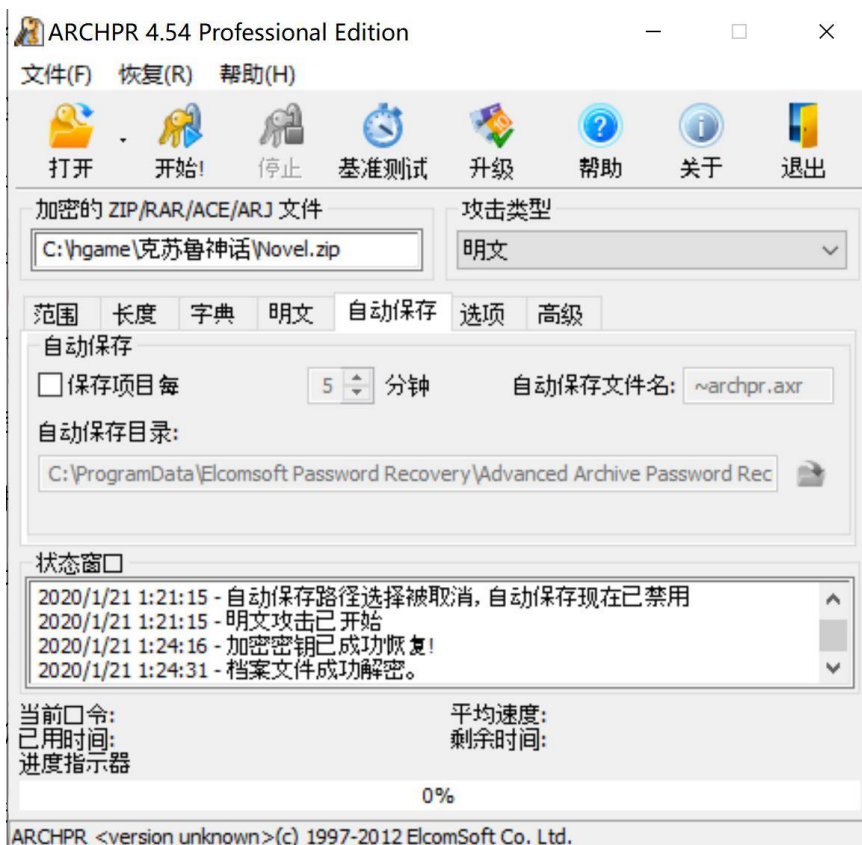
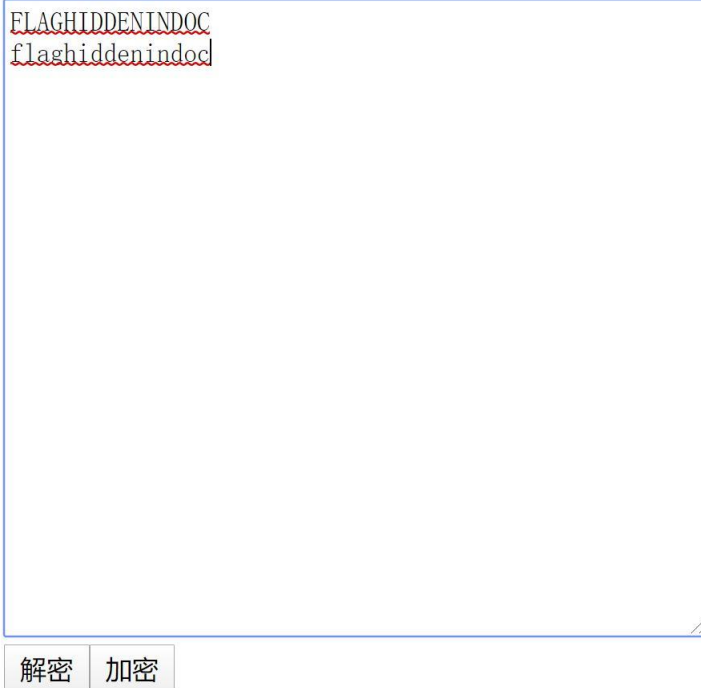
清空结果



hgame{Do_y0u_KnOW_uNiC0d3?}

克鲁苏神话

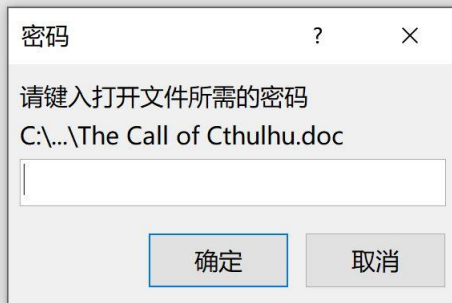
根据提示，用 7zip 解压得到然后打开记事本，解密得到这个，同时发现.zip 中还有一个一样的文件，根据做壁纸那道题搜到的应

Bugku|培根密码加解密



 Novel_decrypted	2020/1/21 1:24	ZIP 压缩文件	26 KB
 The Call of Cthulhu	2020/1/11 0:22	Microsoft Word ...	28 KB

该使用明文攻击，然后就得到一个不加密的压缩包，解压得到文档，打开，提示需要密码，输入 FLAGHDDENINDOC ， 打 开 ， 再 搜 索 了 文 档 隐 写 ， 得 到



更改文档内容在屏幕上的显示方式和在打印时的显示方式。

页面显示选项

- ☒ 在页面视图中显示页面间空白(W) ①
- ☒ 显示突出显示标记(H) ①
- ☒ 悬停时显示文档工具提示(L)

始终在屏幕上显示这些格式标记

- ☐ 制表符(T) →
- ☐ 空格(S) ...
- ☒ 段落标记(M) ↵
- ☒ 隐藏文字(D) abc
- ☐ 可选连字符(Y) ~
- ☒ 对象位置(C) ⚓
- ☐ 可选分隔符(O) ¶
- ☐ 显示所有格式标记(A)

Flag。

签到题 proplus

这道题一开始尝试，没有解除来，去询问了得到要把三行（包括空格行）一起看，（一开始把所有空格去掉了），就根据要求先是栅栏密码，再是凯撒密码，得到

Rdjxfwxjfmkn z,ts wntzi xtjrwm xsfjt jm ywt rtntwhf f y h jnsxf qjFjf jnb rg fiyykwtbsnkm tm xa jsdwqjfmkjy
wlviHtqzqsGsffyyjjyyntf yssm xfjypnyihjn.

JRFV.IYFZVRUAGMAI

每组字数 3

加密

解密

Rfsd djfwx qfyjw fx mj kfhji ymj knwnsl xvxzi, Htqtsjq Fzwjqnfst Gzjsinf bfx yt wjrjrgjw ymfy inxyfsy fkyjwstts bmjs
mnx kfyjmw yttp mnr yt inxhtajw nhj.

JFARZGFVMVRAJUIY

第6次解密:many years later as he faced the firing squad, colonel aureliano buendia was to remember
that distant afternoon when his father took him to discover ice.

eavmubaoqhmvepdt

打开压缩包, 得到一个.text,然后根据之前看到过这个密码, 解密得到, 看到有 base32, 再用其解密

```
data:text;base32,NFLEET2S04YEW3HN5AUCQKBJZJVK2CFKVTUCQKBKFIUCQK
BIVCUGQKZIFAUCRCPINCW6S2BIFAU6V2VNRCVCVSSGRXE6MTBKM3DIRK0053UIMZ
PGB3DOV3ZINJV00CHMNCTQ33LMJFXEQKPHBQSW3CBKNLC6MRTIFAUIKZVMM4WIK
BIRVWQ2FIF3UCY2NIFIUCK2ZIFTUCOCBIZCECSKBKBDUCSKBMZGUCUKBJ5AUI2D
HIFAUQN2ZJU2GKL3WNIXWINBQM5CTANJZ0ZHG2YLYLJQW6L2KMIYXGM3YJMYFIVR
WK52G25LNMFGYMYKZF5GFUMKRHF3TMY2WLBQXC4DNOVLV04KQPFLTSYSOHBXIRJ
RMVWHEWTSOBWCWBSNVIHSMTEKVIIGT30IZLDE4LRLJZGY3DRNI4GY5SXPJTEK4S
SJZMHAYJSME3FU4LMHFGUODUNZLEIM2EOB4FMZDROFWWCNK2MFXS6STCGFZTG6C
LGBKFMNSXORWVK3LBOBTGCWJPJRNDUJZ043GGVSYMFYXA3LVK5LXCUDZK44WETR
YKN2EKMLFNRZFU4TQNVYVQMTNKB4TEZCWJ5FU66BRNRXHON2OJRXGVLVOR5HGTC
```

Text to Ook!

Text to short Ook!

Ook! to Text

Text to Brainfuck

Brainfuck to Text

然后看到有很多=号,
和大小写字母, 再用
BASE64 解密, 有个 png
文件, 保存打开是一个
二维码。


```
4UhlPWpzKmu36Ftav3JmnXrvxaGUNanMqe6foe2qfUna9at/1oYQlmfypzq+h3aptafrFm3/mthCGV9KnOq63dom1p/smbd+q+FIdDnwKckeeYOMAT6HPe
UJM/cAYZAn+OekuSZO8AQ6HPcU5I8cwcYAn2Oe0qSZ+4AQ6DPcU9J8swdYAj0Oe4pSZ65AwyBPsc9Jckzd4Ah0Oe4pyR55g4wBPoc95Qkz9wBhIDUZ
zLug+6Yp2s3xvfZnTRVWHWfbybgOefSh3Njnd9JUYdV9JuM65NGHckuf3UIThVX3mYzrkEcfyi19didNFvbdZzKuQx59KLf02Z00VVh1n8m4Dnn0odzSZ3f
SVGHVfSbjOuTRh3JLn91JU4VV95mM65BHH8otfXYnTRVW3WcyrkMefSi39NmdNFVYdZ/JuA559KHc0qcjaSqpg3IfYNrr1n+XE+4EQ3iQupDuA0x73frvc
sKdYAgPUhfSfYBpr1v/XU64EwzhQepCug8w7XXrv8sJd4lhPEhdSPcBpr1u/Xc54U4whAepC+k+wLTxrf8uJ9wJhvAgdSHdB5j2uvXf5YQ7wRAepC6k+wD
TXrf+u5xwJxjCg9SFdB9g2uvWf5cT7kRqCLc8pWZKunt01ebo85qc3YWd8JSaKXEskKM2R5/X5Owu7ISn1EyJY4EctTn6vCZnd2EnPKVmShwL5KjN0ec1
ObsLO+EpNVPIWCBHbY4+r8nZXdgJT6mZEscCOWpz9HINzu7CTnhKzZQ4FshRm6PPa3J2F3bCU2qmxLFAjtocfV6Ts7uwE55SMYWOBLU5ujzmpzdh
Z3wJlopSyQozZHn9fk3P4SAI4HQwCADxgCAHzAEADgA4YAA8BwBAD4gCEAwAcMAQA+YAgA8AFDAIAP/wAFo0hUZrh1mAAAAABJR5ErkJggg==
```

编码源格式: ☒ 文本 ☐ HEX

解码结果:

自动识别

中文编码方式:

UTF-8

编码

解码

```
3A A7 ED 3E BB 93 A6 0A EB EA F3 16 C6 1F 4A E8
DE 62 08 18 C2 48 C6 1F 4A E8 DE 62 08 18 C2 48
C6 1F 4A E8 DE 62 08 18 C2 48 C6 1F 4A E8 DE 62
08 18 C2 48 C6 1F 4A E8 DE 62 08 18 C2 48 C6 1F
4A E8 DE 62 08 18 C2 48 C6 1F 4A E8 DE 62 08 18
C2 48 C6 1F 4A E8 DE 62 08 18 C2 48 C6 1F 4A E8
DE 8E 37 84 64 1C 83 4A 35 34 35 DD 75 25 6B A1
04 43 28 04 43 A8 03 43 A8 01 43 28 04 43 A8 03
43 A8 01 43 28 04 43 A8 03 43 A8 01 43 28 04 43
A8 03 43 A8 01 43 28 04 43 A8 03 43 A8 01 43 28
```

插件名: 【Png】.Png Image 【确认】

附加信息:

Size: 260x260

另存为: png文件

当前编码: 【Hex】

插件总数: 12, 识别耗时: 1ms



扫一扫得到 FLAG

每日推荐

看到题目去搜索了.pcapng，得知要用 wireshark 打开，下载安装完成后，打开，得到

Capture1.pcapng

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
1	0.000000	fe80::3016:7e4c:4f7...	ff02::1:ff00:2222	ICMPv6	86	Neighbor Solicitation for fe80::250:56ff:fec0:2222 from 00:50:56:c0:00:08
2	1.000021	fe80::3016:7e4c:4f7...	ff02::1:ff00:2222	ICMPv6	86	Neighbor Solicitation for fe80::250:56ff:fec0:2222 from 00:50:56:c0:00:08
3	2.098279	192.168.146.132	114.114.114.114	DNS	75	Standard query 0x95c4 A www.gstatic.com
4	2.121295	192.168.146.132	114.114.114.114	DNS	89	Standard query 0xa935 A clientservices.googleapis.com
5	2.121296	192.168.146.132	114.114.114.114	DNS	79	Standard query 0x0d3c A clients2.google.com
6	2.155248	114.114.114.114	192.168.146.132	DNS	139	Standard query response 0x95c4 A www.gstatic.com A 203.208.50.56 A 203.208.50.55 A 203.208.50.54
7	2.175517	114.114.114.114	192.168.146.132	DNS	119	Standard query response 0x0d3c A clients2.google.com CNAME clients1.google.com A 172.217.14.110
8	2.179274	114.114.114.114	192.168.146.132	DNS	153	Standard query response 0xa935 A clientservices.googleapis.com A 203.208.39.239 A 203.208.39.238
9	2.181660	192.168.146.132	203.208.39.239	TCP	66	50106 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
10	2.182117	192.168.146.132	172.217.160.78	TCP	66	50107 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
11	2.182718	192.168.146.132	203.208.50.56	TCP	66	50108 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
12	2.183144	192.168.146.132	203.208.50.56	TCP	66	50109 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
13	2.184516	192.168.146.132	114.114.114.114	DNS	79	Standard query 0xfe16 A accounts.google.com
14	2.185034	192.168.146.132	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

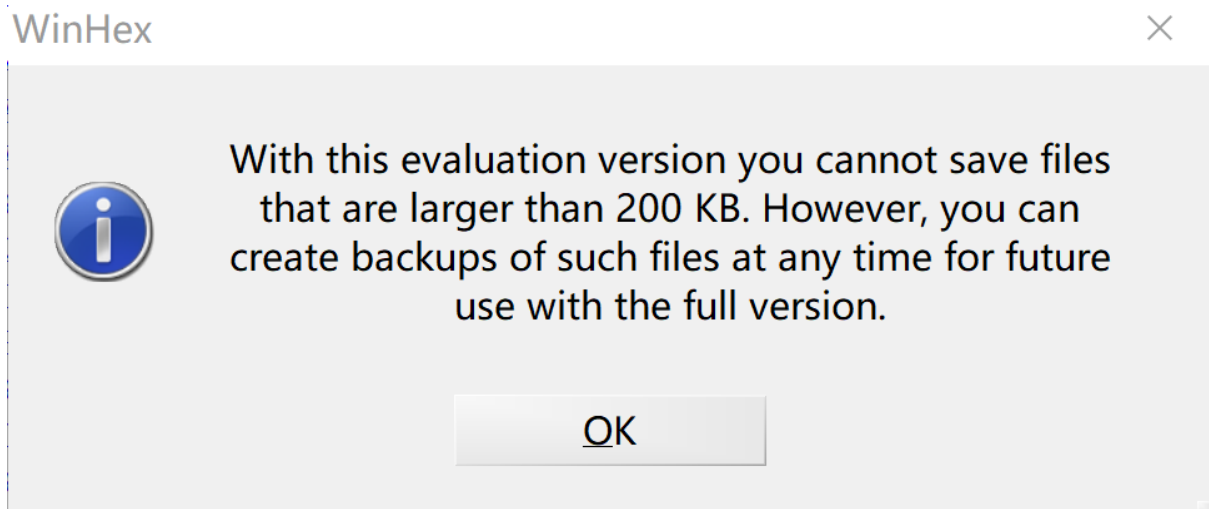
便去搜了如何使用 wireshark，根据搜索到的，

3048	28.449637	192.168.146.132	192.168.146.1	HTTP	790	POST /wp-admin/async-upload.php HTTP/1.1 (application/x-zip-compressed)
------	-----------	-----------------	---------------	------	-----	---

找到这个，发现上传了一个 song.zip，然后

50 4b 03 04 14 00 01 00

看到开头也对的上，就保存为 zip 格式后用 winhex 打开，删去不要的部分，保存，却一直跳出来



就觉得方向错误，然后就导出了 http 对象，并全部保存，发现里面有 png 图片和 gif，就想到做前面的题的时候看到有更改 png 宽和高的，就用 winhex 打开尝试了，但不可以，然后就把保存下来

...nb!"

的文件打开看了，就看到一个.txt 里有，就...还是没解出来。等到昨天晚上 8 点结束后，去问了学长，发现要用破解版的 winhex，下载后，成功得到

async-upload 2020/1/23 20:40 ZIP 压缩文件 8,096 KB

总结一下 week1，好像花在下载各种软件上的时间更多，再加上肺炎的袭击，web 和 pwn 的题还没看过，就出新题了（谁让你菜呢），不过得知了截止前碰到问题也是可以问哒，（觉得…不能问来着），其实在疾控中心想着 writeup 交不上就在群里喊：“我被关着！”