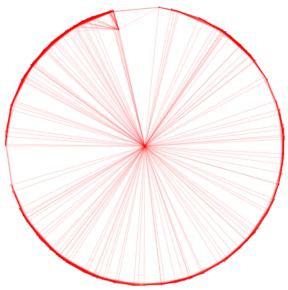
# 超级菜的wp

## web

- sign_in
  会按f12就行（x
- typing train
  看了源码之后没啥思路，感觉只能跑6666次看看再说（？，，但我不会写python脚本。然后尝试去速通爬虫库，参考了一些blog，勉强凑出来了，能跑出来flag。
  requests-html

```
from requests_html import HTMLSession
  sesstion=HTMLSession()
  r=session.get("http://124.220.41.254:20002/index.php?start")
  t=r.html.find("h1",first=True)
  m=t.text
for i in range(6666):
  r=session.get("http://124.220.41.254:20002/index.php?input="+m)
  t=r.html.find("h1",first=True)
  m=t.text
print(r.html.html)
```

- find it
  看了看源码没啥思路，看做出来的人也比较少，本来不打算做了(x 但是看了频道的hint，就去仔细找了找，观察了一下每张网页的文字，觉得这张比较可疑。



哼，你想要的东西就在这里

就去找了一下，在css文件中翻了一下，就发现了hhh

- sheep
  （游戏还挺好玩的hhh）一开始就没有玩通关的想法，依旧先按f12看源码，在game.js里找

到一个fetch.php，访问后发现"Please use **hack browser**"，面向google学习后用burpsuite抓包后用repeater修改了请求头，发现还有一层，关键词：**admin,cookie**.依旧面向goole学习，修改了请求头的cookie，但没有成功，，，我以为是方法的问题，开始往其他方向想，花了好久但是没有成功，最后还是求助了学长，呃呃原来是我不小心打了空格，，，好吧，顺利进入下一层，按照提示把"GET"改成了"POST"，然后就拿到了flag .

## Misc

- sign_in
  手速题hhh，频道里发了flag
- rack your brain
  与佛论禅和brainfuck的解密
- thin dog
  第一遍听的时候只知道左声道藏了点东西，但我英语不好orz，听不出来是啥，听了几遍就放弃了。最后看到大群群友说是无线电（）乐，感谢群友拓宽了我的知识面，然后对着字母表一个一个听。100分到手（
- wingman
  搜了下图片里的adrienne's pet shop ,谷歌出来的第一个是美国orlando的universal studio，图片长得也很像，直接给了我先入为主的印象，把地点限制在了美国，然后麻了，试的每个坐标都是错的，而且orlando没有海底捞，放弃。后来封榜的那几个小时没啥可做的就回来观察了一下图片，发现里面大部分人都是亚洲人，开始意识到自己的方向应该是错了...决定再试一下北京和日本，然后再结合law和海底捞，试了几个大学，成功，是日本的大阪大学。

## Reverse Engineering

- hello_net
  呃呃放进IDA里面flag就出来了（

## Crypto

- baby rsa
  一个e多组nc，搜了下buuctf的rsa5和这个题很像，是低密度指数广播攻击，就直接开始搜buuctf的wp了，但是网上的脚本真的很让人绝望，试了五六个都跑不通也修不好，开始反思自己为啥还不会写脚本:(
  找了找终于翻到了一个能跑的，虽然开始报了错。reduce函数是py2的，py3需要调用functools库，然后成功的跑了出来。
  https://blog.csdn.net/qq_38154820/article/details/110102864

```
from gmpy2 import*
from Crypto.Util.number import*
from functools import*
```

```
#39组nc
n = [N0,N1,N2,,N38]
c = [c0,c1,c2,,c38]
def CRT(a,n):
    sum = 0
    N = reduce(lambda x,y:x*y,n)   # ni 的乘积,N=n1*n2*n3
    for n_i, a_i in zip(n,a):    # zip()将对象打包成元组
        N_i = N // n_i           #Mi=M/ni
        sum += a_i*N_i*invert(N_i,n_i)   #sum=C1M1y1+C2M2y2+C3M3y3
    return sum % N
x = CRT(c,n)
m = iroot(x,e)[0]           #开e次方根
print(hex(m))               #数值转字符串
```

## Pwn

- get_my_number
  呃呃也只会签到题捏。用整数溢出绕过第一个if，比如输入2147483649，溢出后变成-2147483648+1=-2147483647，小于1000满足第一个if，而sizeof的返回值的类型是size_t类型，会将值转换成无符号进行比较，因此2147483647满足第二个if，得到shell，ls查看，find .-name flag查找，得到路径/temp/flag ，得到flag啦。

  *by noir*