Texiwus 个人赛 wp

这里是 Texiwus 的个人赛 wp，大一组 rank12，纯萌新视角

Sign in

根据题目要求去频道 copy 过来就完成了签到，认识了 flag 的形式

No copy

发现确实 copy 不了，但被{}包围着，说明是 flag！
F12 发现每一个字都被包裹着，下不去手
然后想到沉浸式阅读模式，似乎没有……
然后 ctrl+P 打开了打印机，似乎就能复制了……，复制到记事本去掉空格，提交过了
mayctf{呷呸呋呺呻呾呿咀咁咂咃咄音咇咈咉咊咋咍咎咐咑咓咔咕咖咗咘咙咚咛咜咝咞咟咠咡咢咣咤咥咦咧咨咩咪咫咬咭咮咯咰咲咳咴咵咶咷咹咺咻呙咽咾咿哂哃哅哆哇哈哊哋哌哎哏哐哑哒哓哔哕哖哗哘哙哚哛哜哝哞哟哠咔哢哤哦哧哩哪哫哬哯哰哱哳哴哵哶哷哸哹哻哼哽哾哿唀唁唂唃呗唅唆唈唉唊唋唌唍唎唏唑唒唓唔唕唖唗唘唙唚唛唝唞唟唠唡唢唣唤唥唦唧唨唩唪唫唬唭唯唰唲唳唴唵唶念唸唹唺唻唼唽唾唿啀啁啃啄啅商啇啈啉啋啌啍啎问啐啑啒启啓啕啖啖啘啙啚啛啜啝啞启啠啡啢衔啥啦啧啨啩啪啫啬啭啮啯啰啱啲啳啴啵啶啷啸啹啺啻啼啽啾啿喀喁喂喃善喅喆喇喈喉喊喋喌喍喎喏喐喑喒喓喔喕喖喗喙喛喞喟喠喡喢喣喤喥喦喨喩喪喫喬喭單喯喰营喴喵喷喸喹喺喻喼喽喾喿嗀嗁嗂嗃嗄嗅呛啬嗈嗉嗊嗋嗌嗍吗嗏嗐嗑嗒嗓嗕嗖嗗嗘嗙嗚嗛嗜嗝嗞嗟嗠嗡嗢嗣嗤嗥嗦嗧嗨嗩嗪嗫嗬嗭嗮嗰嗱嗲嗳嗴嗵哔嗷嗸嗹嗺嗻嗼嗽嗾嗿嘀嘁嘂嘃嘄嘅嘅嘆嘈嘉嘊嘋嘌喽嘎嘏嘐嘑嘒嘓呕嘕啧嘘嘙嘚嘛嘜嘝嘞嘞嘟嘠嘡嘢嘣嘤嘥嘦嘧嘨哗嘪嘫嘬嘭唠啸囍嘴哓嘶嘷呒嘹嘺嘻嘼啴嘾嘿噀噂噃噄咴噆噇噈噉噊噋噌噍噎噏噐噑噒嘘噔噕噖噗噘噙噚噛噜噝噞噟哒噡噢噣噤哝哕噧噩噪噫噬噭噮嗳噰噱哙噳喷噵噶噷吨噺噻噼噽噾噿咛嚁嚂嚃嚄嚅嚆吓嚈嚉嚊嚋哜嚍嚎嚏尝嚑嚒嚓嚔噜嚖嚗嚘啮嚚嚛嚜嚝嚞嚟嚠嚡嚢嚣嚤呖嚧咙嚩咙嚧嚪嚫嚬嚭嚯嚰嚱亸喾嚵嘤嚷嚸嚹嚺嚻嚼嚽嚾嚿啭嗫嚣囃囄冁囆囇呓囊囋囍囎囏囐嘱囒啮囔囕囖嵫嵬嵭嵮嵯嵰嵱嵲嵳嵴嵵嵶嵷嵸嵹嵺嵻嵼嵽嵾嵿嶀嶁嶂嶃崭嶅嶆岖嶈嶉嶊嶋嶌嶍嶎嶏嶐嶑嶒嶓嵚嶕嶖嶘嶙嶚嶛嶜嶝嶞嶟峤嶡峣嶣嶤嶥嶦峄峃嶩嶪嶫嶬嶭崄嶯嶰嶱嶲嶳岙嶵嶶嶷嶸嶹巂嶻嶼嶽嶾嶿巀巁巂巃巄巅巆巇巈巉巊岿巌巍巎巏巐巑巒巓巅巕巖巗巘巙巚巛懽慑懿恋懟懡懩懪懯懰懱}

Thin dog

虽然一开始就发现了左声道有问题，截取了出来放去讯飞识别了出来，但因为是萌新纯纯不懂

试了好几遍，突然想到是不是应该每一个都取首字母，于是可以了
以下列举了几次试验
mayctf{echoVictorechoRomeoYankee_foxtrotLimaIndiaechoRomeo_pillowNovemberOscar whiskey_IndiaRomeoSierraAlpha}

mayctf{TheYankeeCharlietangofoxtrotleftbracketechoVictorechoRomeoYankee_foxtrotLimalndiaechoRomeo_pillowNovemberOscar whiskey_IndiaRomeoSierraAlpharightBracket}

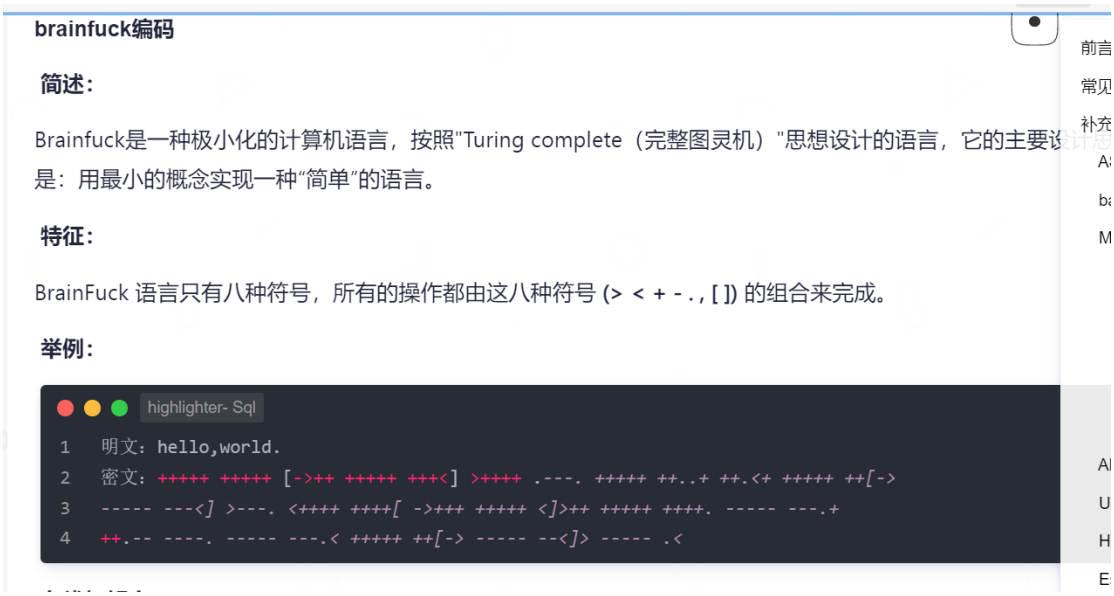
mayctf{eVeRa_fLIeR_pNOw_IRSA}

Rack your brain

打开，是佛语?
佛又曰:输蒙诃地呼阿罚佛输他耶提咩罚墀遮驮萨唵陀沙帝怛写遮呼写尼地摩舍咩那栗怛阇伊佛烁喝度醢嚧卢埵楞呼菩摩孕帝数写菩佛皤佛迦沙苏罚栗醢埵萨遮豆陀孕唵呼钵室地蒙诃无穆度羯阿佛帝舍度夜娑佛皤输孕参啰谨数墀咩谨罚那阇输他帝耶唎度谨参婆栗醢栗罚驮遮写烁伽驮阇怛唎墀夜嚧舍阿驮呼菩墀他度数墀他吉曳娑呼佛地唎楞利墀利豆数夜苏帝啰提南迦孕舍夜尼娑卢婆遮南卢阿唵嚧沙墀钵阇蒙佛曳谨萨那参呼曳阿曳参耶埵陀地呼苏无墀地度烁醢提那婆萨阇墀提参摩提诃佛遮提阇参舍豆度呼栗罚烁夜菩摩苏墀埵嚧提楞写佛地耶唵罚输钵墀罚伽唎利沙驮栗沙皤参孕孕皤参烁唎舍怛曳孕驮烁帝地利诃哆唎呼唎南室罚罚驮无驮伊婆陀遮曳阇迦阇参利豆钵室无菩吉迦啰唵钵耶俱伊他卢无喝婆唎菩啰输驮羯哆唵参婆俱伽烁遮羯帝烁沙沙南罚喝醢埵唎啰地迦萨婆婆那哆尼阿婆皤室数卢豆哆墀孕谨豆迦哆醢喝俱醢萨穆唎无谨夜卢室墀夜皤唎佛遮哆俱佛参醢他喝孕喝悉耶数俱写吉摩钵穆数烁喝夜伽豆咩尼喝曳参阿佛夜那怛曳无啰怛驮唵伊嚧萨伊皤唵埵无利写卢蒙羯佛嚧夜数南伊喝苏呼参唵舍佛伽皤栗豆菩帝蒙提南遮醢伽孕伊摩提尼羯醢羯伊那输悉皤舍孕伊陀尼提诃耶钵娑室蒙豆嚧利楞陀佛伊室嚧喝谨穆蒙谨室俱醢唎南摩伊唵羯孕钵诃呼地羯地穆醢墀迦嚧提豆罚唎怛咩沙呼迦遮阇那参沙佛唵烁咩怛啰室醢咩卢埵夜楞参驮娑栗醢怛无墀啰苏悉写阿娑舍阇尼蒙羯啰阿提俱埵遮南利舍菩唵啰孕嚧驮怛咩那沙摩怛怛写那醢烁怛苏南蒙地耶喝阿伽苏豆苏卢苏豆墀卢输楞尼呼阿摩南遮楞谨夜楞埵埵尼伽曳数南墀唵诃娑埵迦陀谨哆伽菩驮楞萨萨楞度墀悉楞啰曳谨悉曳婆摩写那沙烁唎羯穆谨地漫漫

于是找了一个相应的解密网站，最终找到这个
[与佛论禅加密/解密 - 一个工具箱 - 好用的在线工具都在这里！ (atoolbox.net)]
解密出来是这样
```
++++++++[>>++>++++>++++++>++++++++>++++++++++>++++++++++++>
++++++++++++++>++++++++++++++++>++++++++++++++++++>++++++++
++++++++++>++++++++++++++++++++++>++++++++++++++++++++++++
+>++++++++++++++++++++++++++++>++++++++++++++++++++++++++++>+
++++++++++++++++++++++++++++++++<<<<<<<<<<<<<<<<-]>>>>>>>>>--
-.<+.>>-------.<<++.>>-----.<<+++.>>+++++++.----.<<++.-------.>>---.<<-
-.++.--.<<<++++++.>>>>>--.<<++.>----.>----.<--
-.<<<<<++++++++++..>>>>>>---.<-.>++++++++.<<<<<...>>>>>++++++++++++.
```
然后去找 ctf 加密方式大全

CTF 常见编码及加解密（超全） - ruoli-s - 博客园 (cnblogs.com)
发现是一种叫 brainfuck 的



解密出来
Brainfuck/Ook! Obfuscation/Encoding [splitbrain.org]
mayctf{what_a_6rainf**ker666}

Sheep

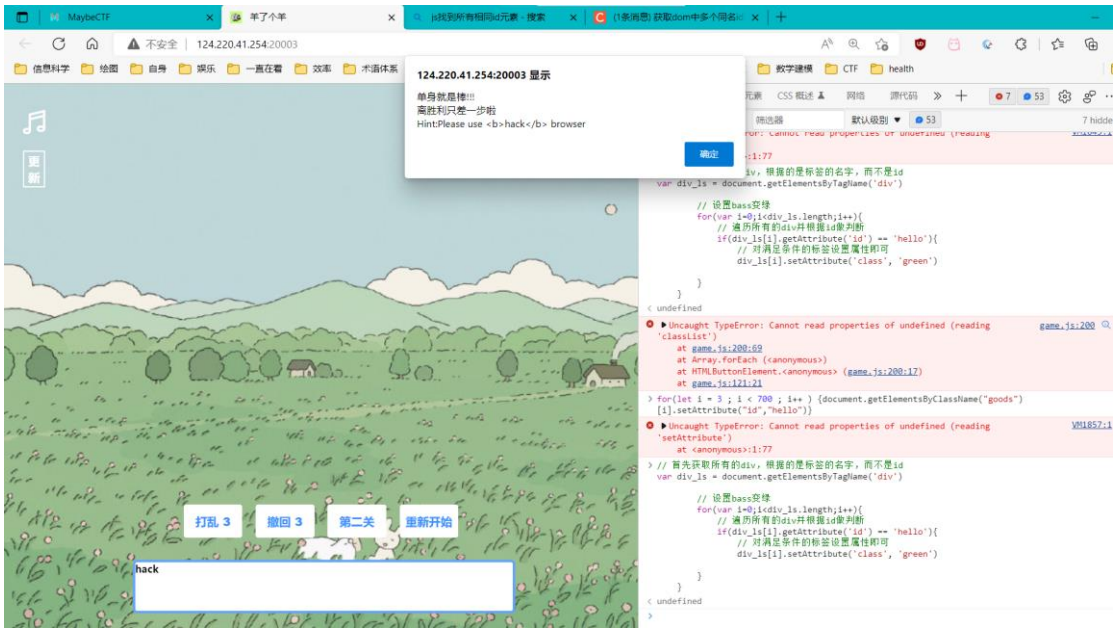
玩了十几分钟，意识到确实不能好好玩，右上角是剩余的卡片数量
接着就在 F12 里面捣鼓，发现了这些卡片能直接 delete，但几百次，delete 完之后，超时了
呜呜呜
幸好之前做过全栈项目，还有一点点 js 记忆，最后试出来 js 确实可行

1.先放置在控制台
```
for(let i = 3 ; i < 700 ; i++ )
{document.getElementsByClassName("goods")[i].setAttribute("id","hello")}
```
2.点击第二关
3.Enter
4.粘贴一下的代码，把 class 改掉，卡片就没了
```
// 首先获取所有的 div，根据的是标签的名字，而不是 id
var div_ls = document.getElementsByTagName('div')
        // 设置 bass 变绿
        for(var i=0;i<div_ls.length;i++){
            // 遍历所有的 div 并根据 id 做判断
            if(div_ls[i].getAttribute('id') == 'hello'){
                // 对满足条件的标签设置属性即可
                div_ls[i].setAttribute('class', 'green')
```

```
        }
    }
```

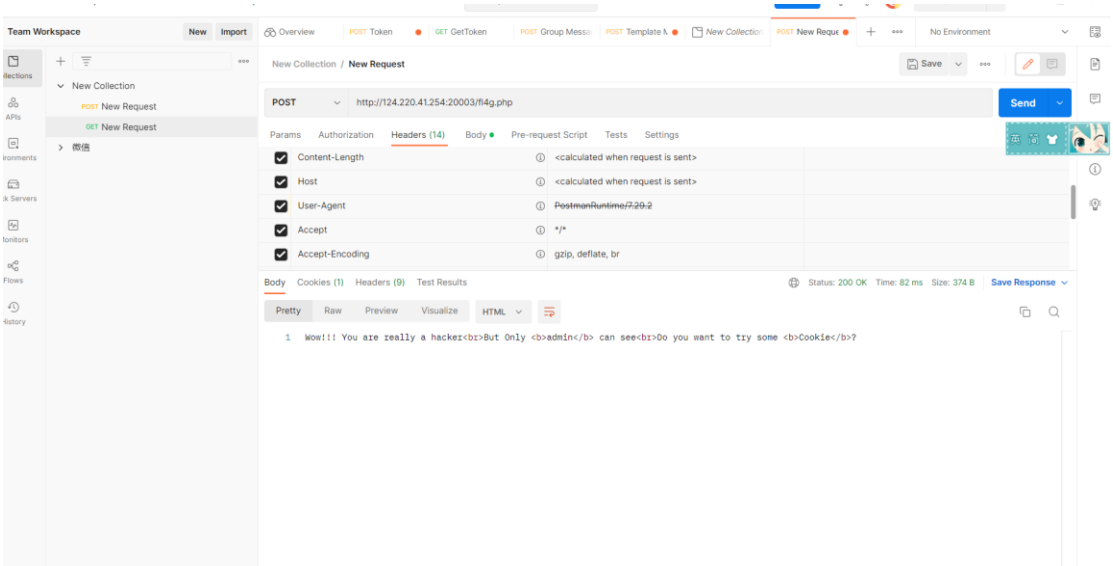
5.Enter

快速点三个，出现了

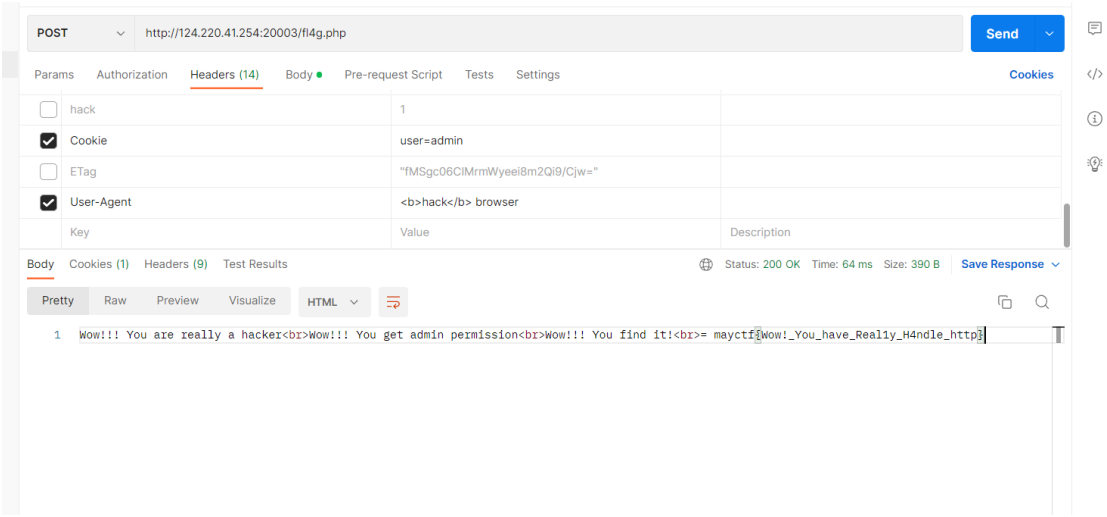


这是啥子？把hack放进里面不行呀

于是就沉默了一个下午，中间问了学长，学长回复“搜索常用请求头学习”，最后搜到一个实例改 User-agent 伪造浏览器，才知道这个题目也是一个道理



继续按照说它说的，修改 cookie 的 user



答案出现了

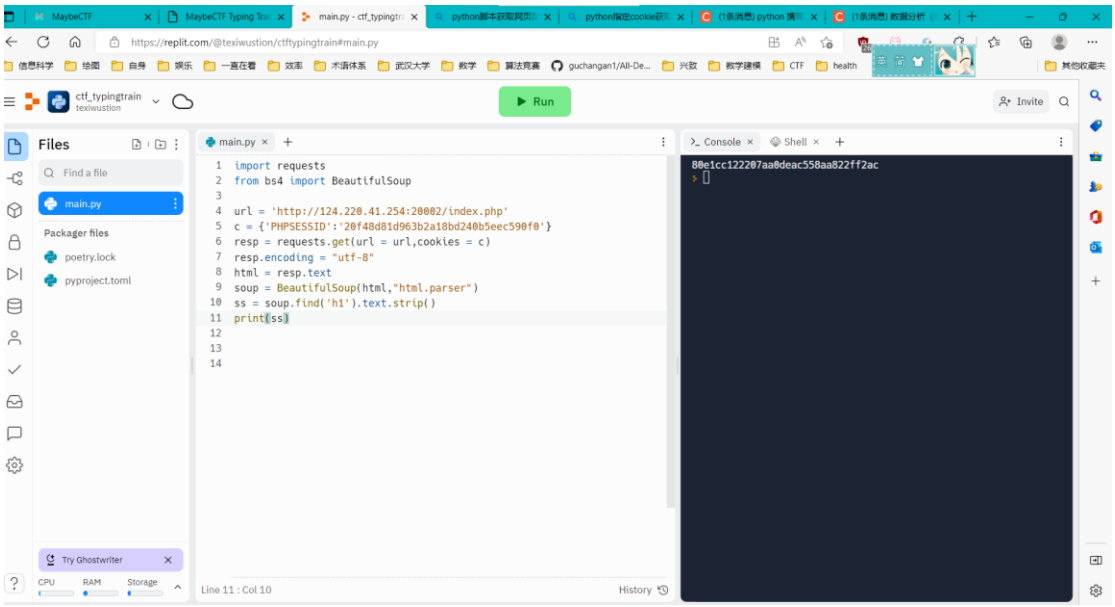
Hello net

一开始运行，怎么百度，怎么输入指令也没用
后来想起了网上看到的一句话，万物皆文件，想起了 010editor 这是在试图解密某 shojo2.rar 文件时在网上看见的一个 16 进制编辑软件
后来打开了 010editor 一看，就在里面

Mayctf{I_Think_NET_1S_S1mpler_Than_NATIVE!}

Typing train

题目说要输入 6666 次正确的结果，那就按照它说的
1.一开始使用 js，在控制台三行过一个，但每次过就刷新，意识到不太行
let t = document.getElementsByClassName("typing")[0].textContent　//js 获取元素内文本
document.getElementsByName("input")[0].value = t //js 修改文本框内容
document.getElementsByTagName("form")[0].submit() //js 提交表单
2.然后想到了 python 脚本，毕竟以前试过用 python 爬取 b 站评论区
Get 文本



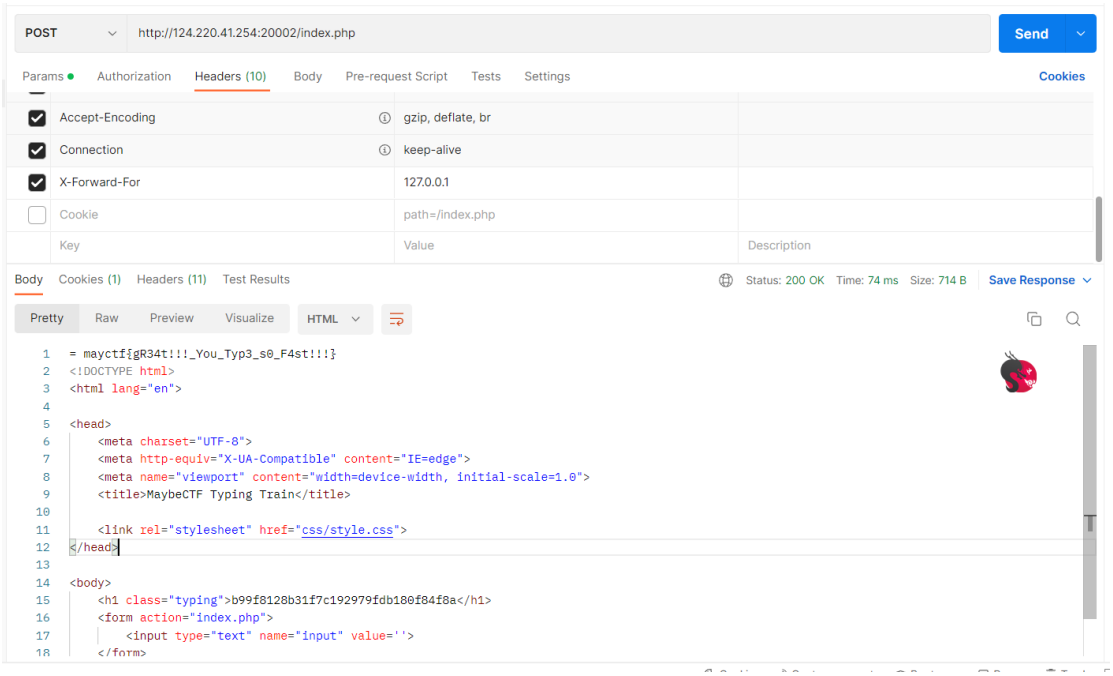
3.在网上的 editor，效率是真慢，后来换到了本地执行
4.中途上了三节课，断断续续的，课上也在试

试验了 5 个小时左右，最终的脚本

```
import requests
import lxml
from bs4 import BeautifulSoup

txt = '232a8ea482565574de8d1109e01f62d9' #这就是下一个的输入
c = {'PHPSESSID':'27bbbba70a199fbf4eed98d57923ffa7'} #postman 中的 cookies
url =''
data={}
res=''
html=''
for _ in range(6770):
    url = 'http://124.220.41.254:20002/index.php?input='+txt
    res = requests.post(url=url,data=data,cookies = c)
    html = res.text
    soup = BeautifulSoup(html,"lxml")
    txt = soup.find('h1').text.strip()
    print(f"{_}:{txt}")
```

最后一访问看见了



Ps：反正整个过程接近 collapse，最后一访问，才发现答案已经出来了