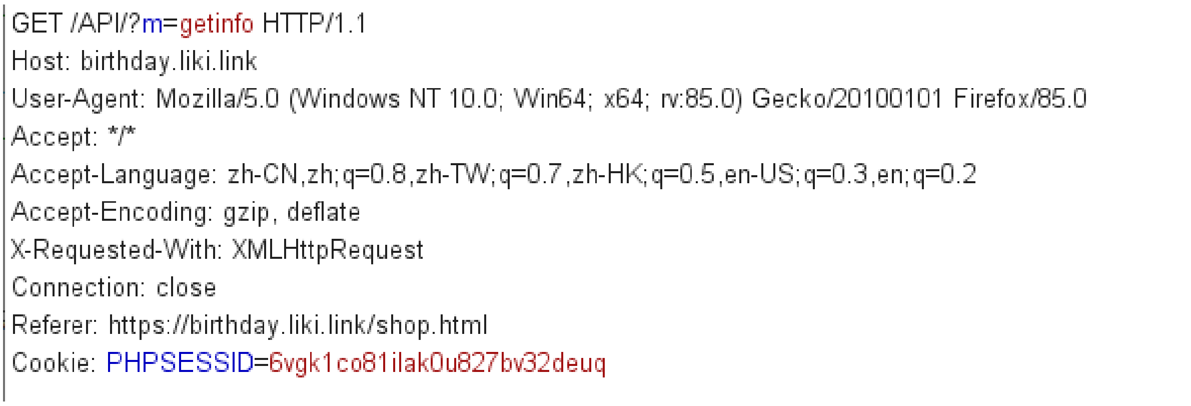
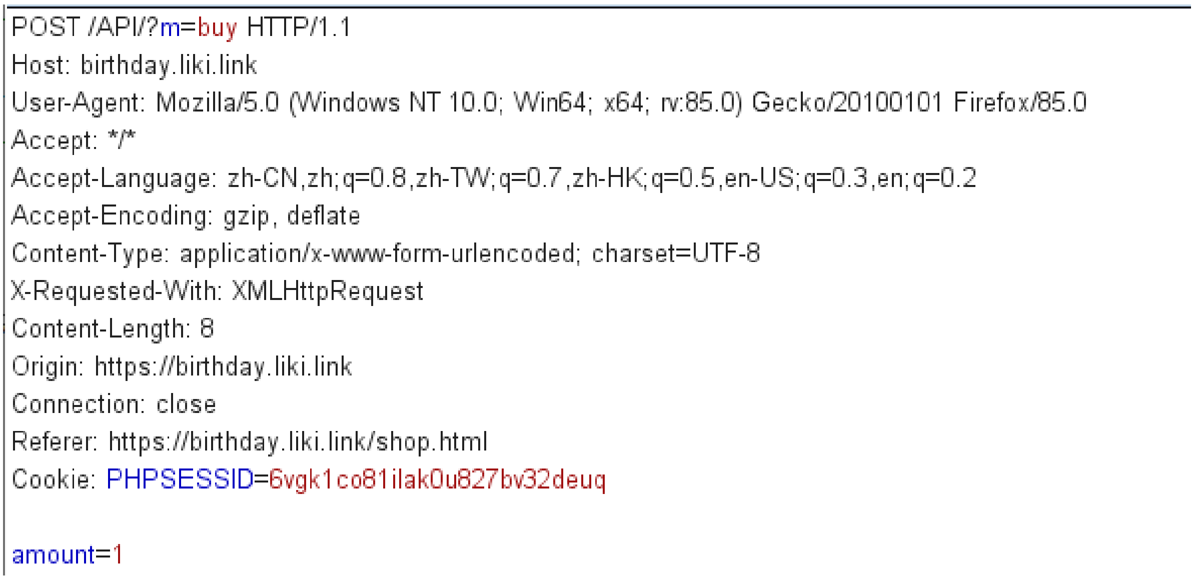
Web

Liki的生日礼物

作为小白，在学长没有给公告提示这是条件竞争，我是根本没有思路的。百度之后大致知道了原理。

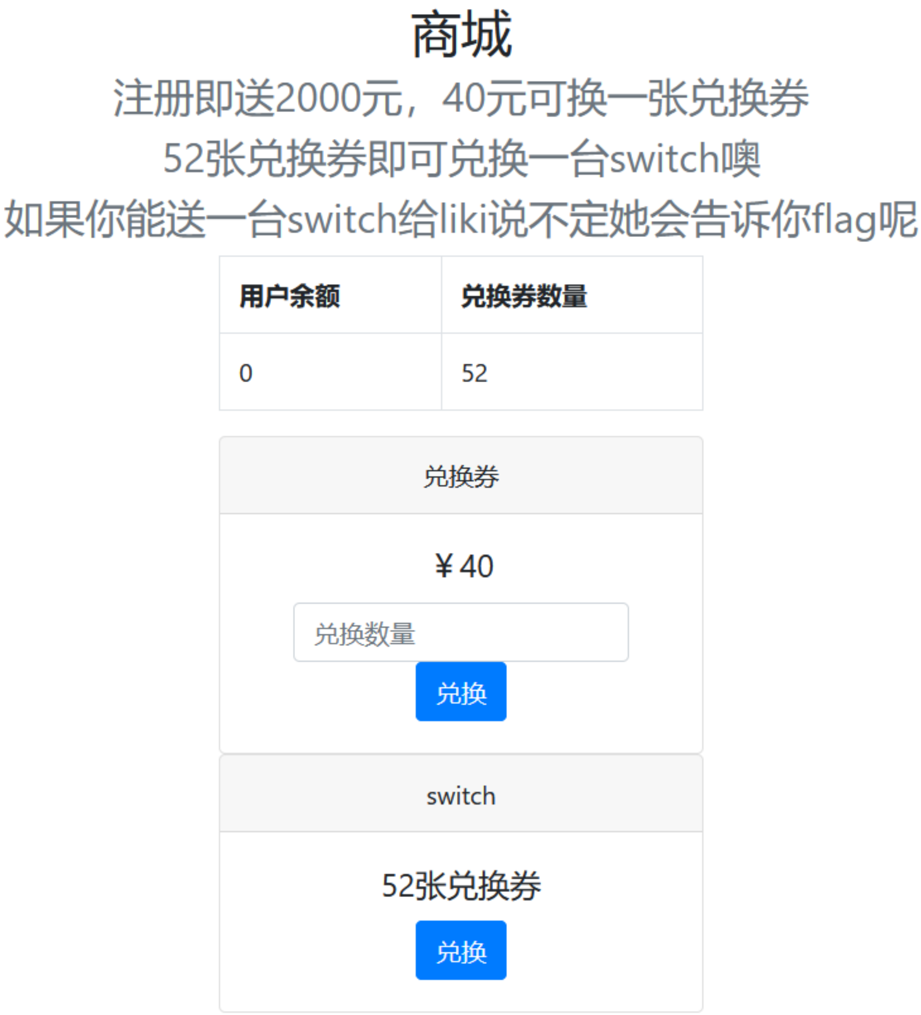


```
GET /API/?m=getinfo HTTP/1.1
Host: birthday.liki.link
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer: https://birthday.liki.link/shop.html
Cookie: PHPSESSID=6vgk1co81ilak0u827bv32deuq
```



```
POST /API/?m=buy HTTP/1.1
Host: birthday.liki.link
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 8
Origin: https://birthday.liki.link
Connection: close
Referer: https://birthday.liki.link/shop.html
Cookie: PHPSESSID=6vgk1co81ilak0u827bv32deuq

amount=1
```

bp抓包，分别把这两个请求丢到intruder中，根据原理，post请求数要比get请求数大，所以分别设置线程为30，5。最后刚好买到52张。



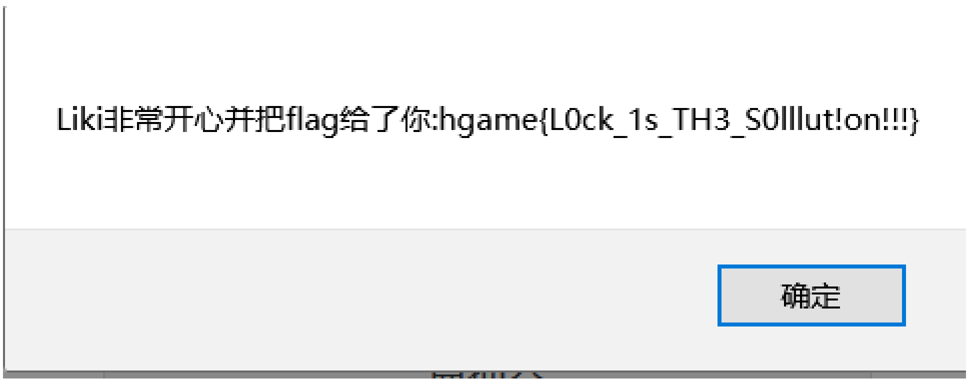
商城

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
0	52



Liki非常开心并把flag给了你:hgame{L0ck_1s_TH3_S0lllut!on!!!}

Crypto

WhitegiveRSA

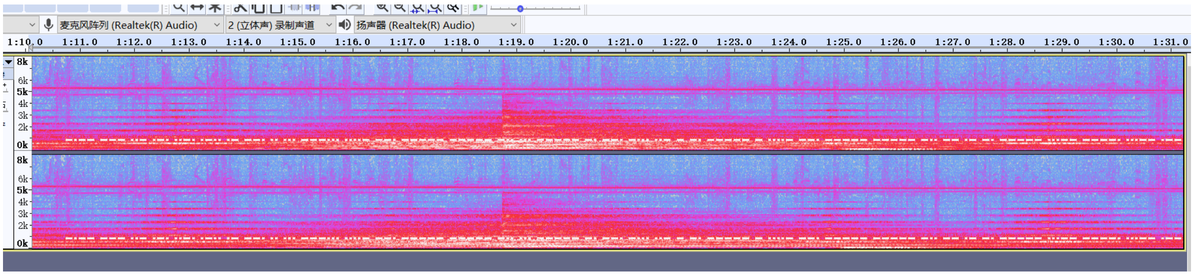
```
import libnum
from Crypto.Util.number import long_to_bytes

c = 747831491353896780365654517748216624798517769637260742155527
n = 882564595536224140639625987659416029426239230804614613279163
e = 65537
q = 857504083339712752489993810777
p = 1029224947942998075080348647219

d = libnum.invmod(e, (p - 1) * (q - 1))
m = pow(c, d, n)
string = long_to_bytes(m)
print(string)
```

hgame{w0w~yOU_kNoW+R5@!}

MISC

Telegraph：1601 6639 3459 3134 0892

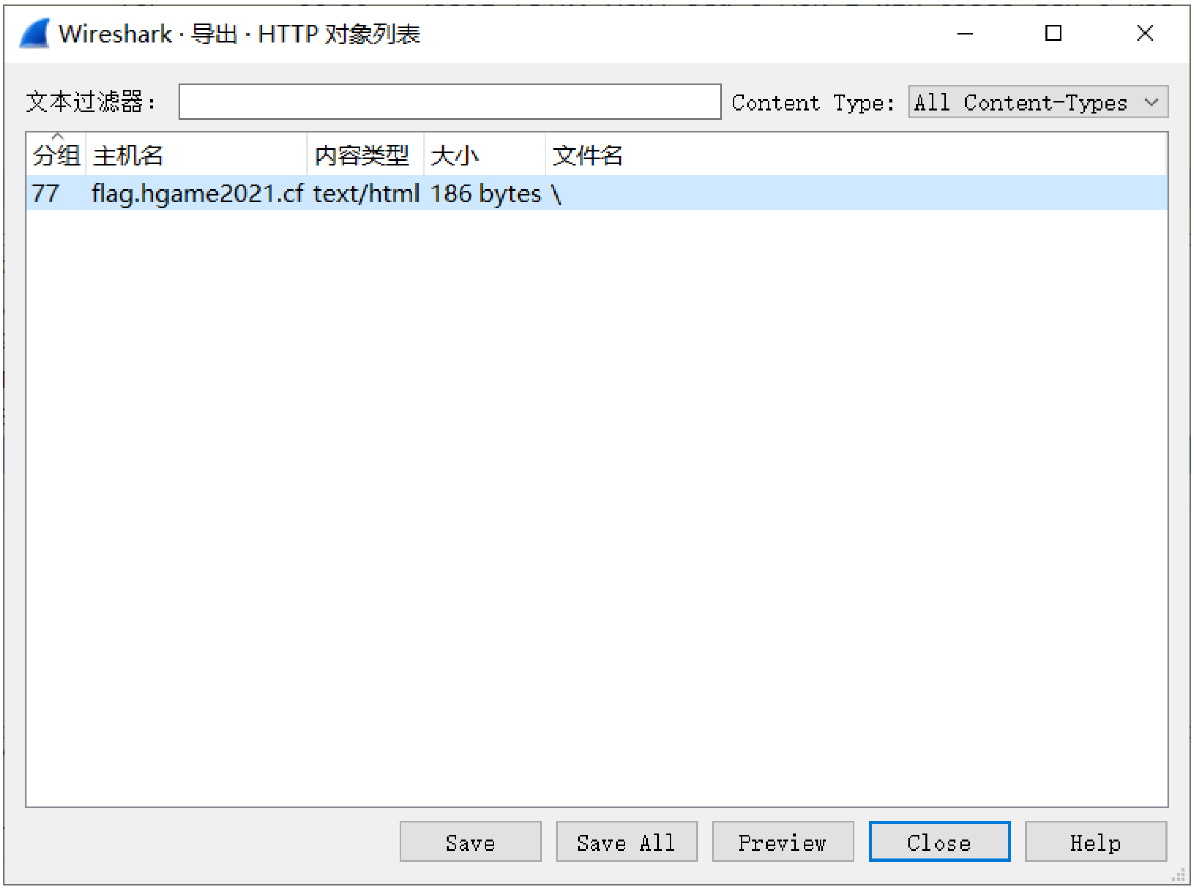
点开链接是一段音频，直接下载，用Audacity打开后，从头开始听，发现从1分10秒到1分35秒是一段摩斯电码，将它用频谱图显示，然后就发现：



```
-.-- --- ..- .-. ..-. .-.. .- --. .. ... ---... ....- --. ----- ----- -.. ... ----- -. --. -... ..- - -. ----- - ....- --. ----- ----- -.. -- .- -. ----- ...-- ----. ...-- .---- ----- -.- ..

YOUR FLAG IS:4G00DS0NGBUTN0T4G00DMAN039310KI
```

然后根据题目提示flag的格式，写出flag：hgame{4G00DS0NGBUTN0T4G00DMAN039310KI}

DNS



Wireshark · 导出 · HTTP 对象列表
文本过滤器：
Content Type: All Content-Types
Save
Save All
Preview
Close
Help

分组	主机名	内容类型	大小	文件名
77	flag.hgame2021.cf	text/html	186 bytes	\

选择导出对象http，发现有一个txt文件，保存后打开：

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

根据提示百度SPF后，根据网上的操作，最后得到flag：

```
C:\Users\Lenovo>nslookup
默认服务器:  localhost
Address:  192.168.1.1

> set type=txt
> flag.hgame2021.cf
服务器:  localhost
Address:  192.168.1.1

非权威应答:
flag.hgame2021.cf       text =

        "hgame{D0main_N4me_5ystem}"
>
```