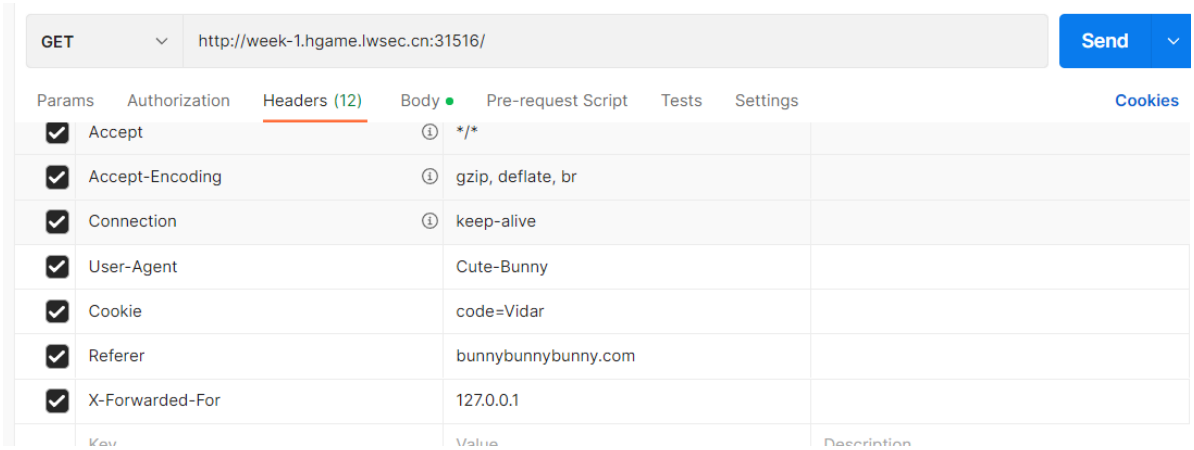
Web

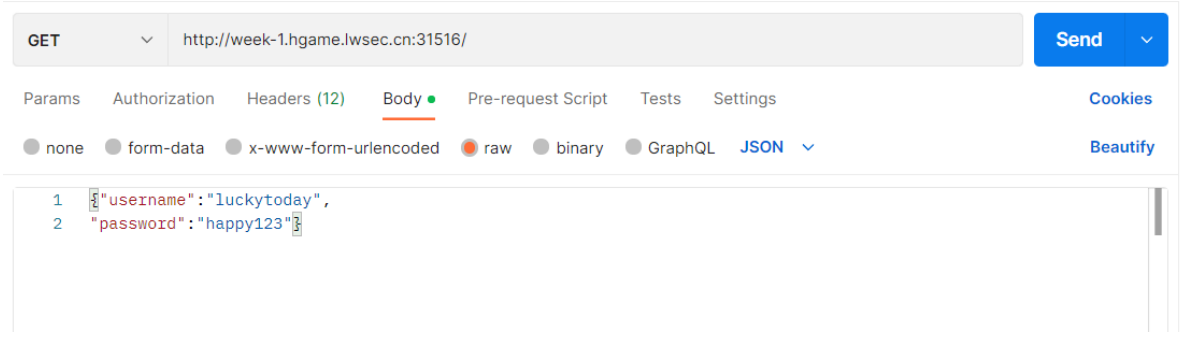
Classic Childhood Game

一个js小游戏,查看源码在Events.js的最后面发现一串字符串,十六进制转成明文base64两次即可得到flag

Become A Member



如图发送请求头即可,最后要发送json格式的用户名和密码



Guess Who I Am

根据/api/getQuestion和/api/Score以及/api/verifyAnswer页面

写脚本根据question找到id

```
#defalut列表是vidar成员的信息(太长就不放了,链接可下载)
#https://github.com/Potat0000/Vidar-Website/blob/master/src/scripts/config/member.js
```

```
url3 = 'http://week-1.hgame.lwsec.cn:32460/api/getScore'
url2 = 'http://week-1.hgame.lwsec.cn:32460/api/verifyAnswer'
url1 = 'http://week-1.hgame.lwsec.cn:32460/api/getQuestion'
cookie="session=MTY3MzA3Njk1OHxEdi1CQkFFQ18OSUFBUkFCRUFBQU9fLUNBQUlHYzNSeWFXNW5E
QTBBQzJOb1lXeHNaVzVuWlVsaOEybHVkQVFDQUdBR2MzUnlhVzVuREFnQUJuTnZiSFpsWkFOcGJuUUVB
ZOFFfPjw_jLOyVzVhq6UU5kMwAU5986JnLZt7ceOg_TM92bL"   #score=2的cookie
headers={
    "Cookie":cookie,
}

def findid(ques):    #遍历找到id
    for i in range(100):
        if(ques==default[i]['intro']):
            return default[i]['id']

while 1:
    rquestion = requests.get(url1, headers=headers)
    question = rquestion.json()['message']   #question
    print(question)
    data = {
        "id": findid(question)
    }
    answer = requests.post(url2, data=data, headers=headers)   #post id
    # print(answer.text)
    cookie = answer.headers['set-Cookie']     #找到set-cookie
    # print(cookie)
    headers = {
        "Cookie": cookie,
    }
    score = requests.get(url3, headers=headers)
    print(score.text)
```

```
{"message":97}
18级 / 会一丢丢crypto / 摸鱼
{"message":98}
18级 / 莫得灵魂的开发 / 茄粉 / 作豚 /  米厨
{"message":99}
17 级 / Web
{"message":"hgame{Guess_who_i_am^Happy_Crawler}"}
20级 / web / 想学iot
```

Show Me Your Beauty

文件上传有前后端的过滤,上传jpg后抓包改为xxx.phP即可

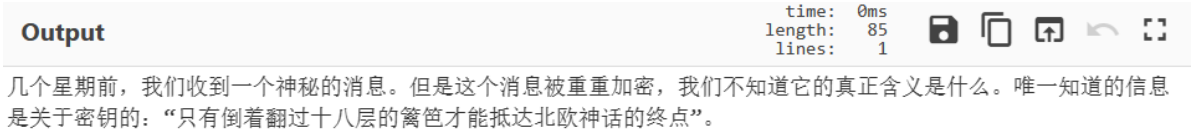
Crypto

RSA

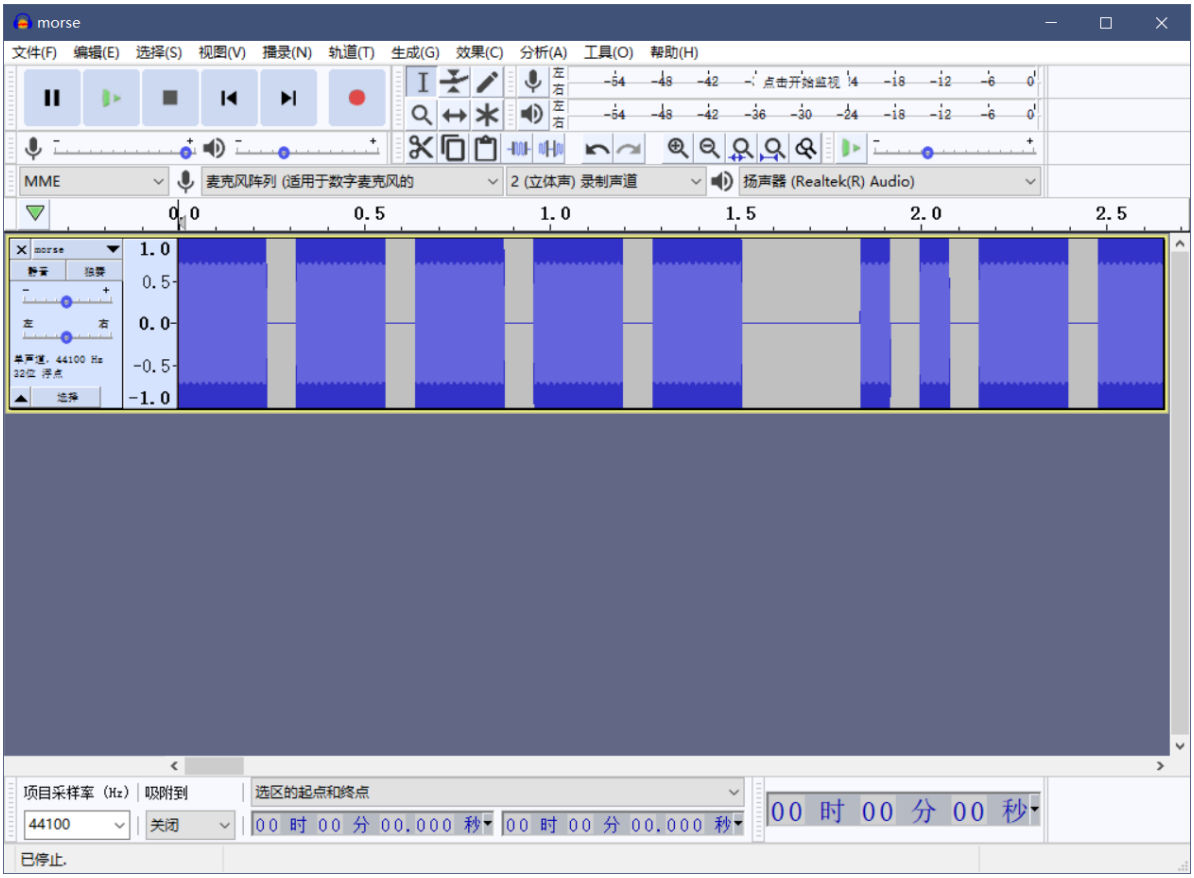
很基础的题,套公式即可,先分解N

神秘的电话

附件下载后有一个base64文本,解码后是一些提示



猜测是要逆向再18栏的栅栏解密

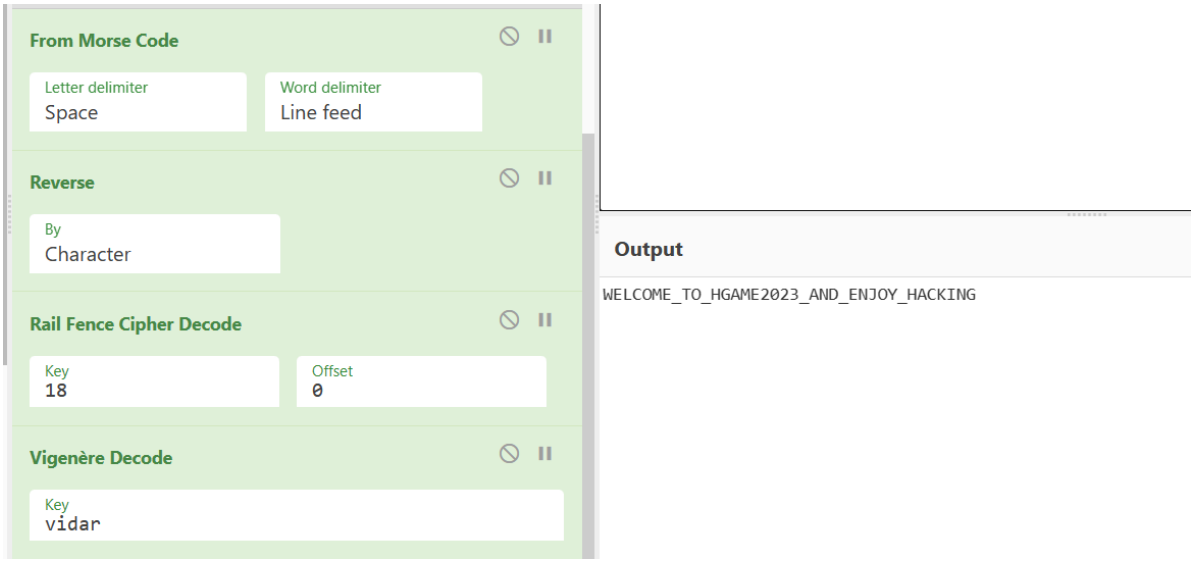


还有个音频附件,应该是摩斯密码

----- ..--- ..--- ...-- . ..--.- .--. .-. .. .. -... .-.. -.-- ..--.- ..--.- .... --- -. .-- .- ..--.- .--- -- --. ....

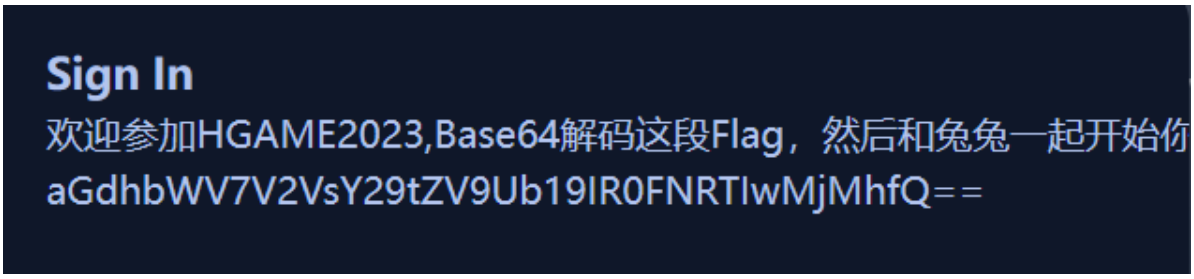
..--.- ..-. --. -.- -.-. --.- .- --- --.- - -- ..-. .-.

后来卡在北欧神话这个hint上,经出题人提示后发现是密钥vidar



Misc

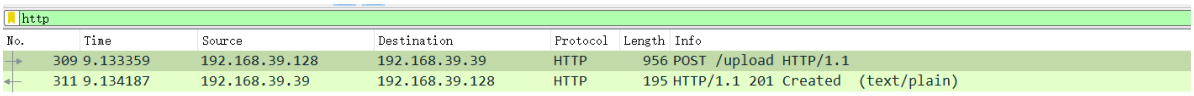
Sign In



签到,base64

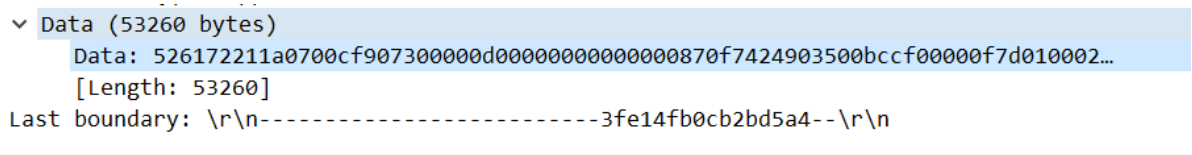
Where am I

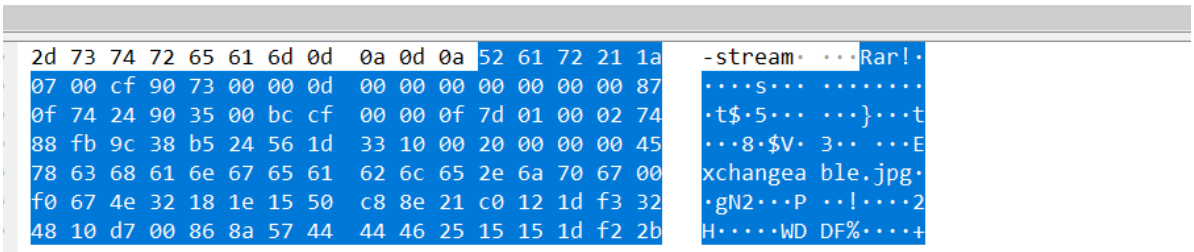
过滤http发现两个包

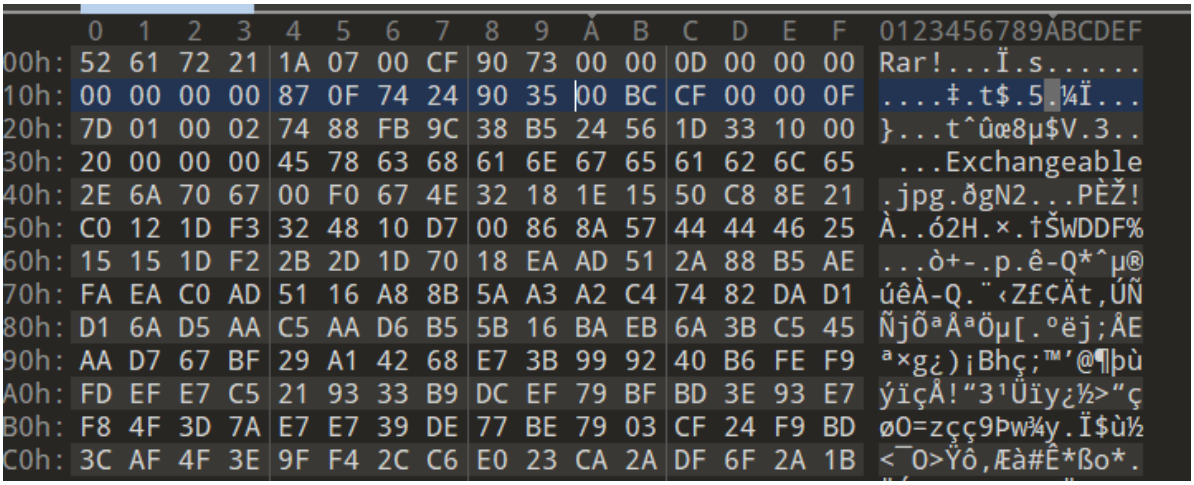


No.	Time	Source	Destination	Protocol	Length	Info
309	9.133359	192.168.39.128	192.168.39.39	HTTP	956	POST /upload HTTP/1.1
311	9.134187	192.168.39.39	192.168.39.128	HTTP	195	HTTP/1.1 201 Created (text/plain)

这里发现了rar文件的十六进制码,提取出来

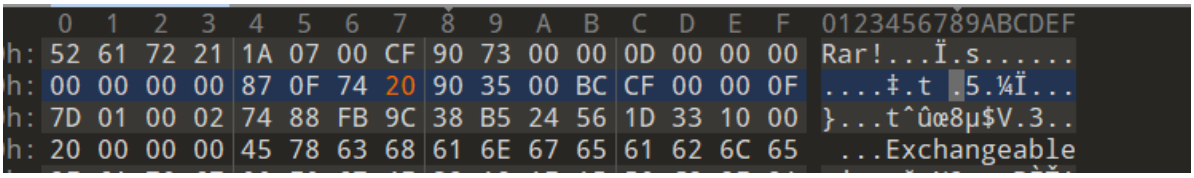






```
    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
00h: 52 61 72 21 1A 07 00 CF 90 73 00 00 0D 00 00 00 Rar!...Ï.s......
10h: 00 00 00 00 87 0F 74 24 90 35 00 BC CF 00 00 0F ....‡.t$.5.¼Ï...
20h: 7D 01 00 02 74 88 FB 9C 38 B5 24 56 1D 33 10 00 }...tˆûœ8µ$V.3..
30h: 20 00 00 00 45 78 63 68 61 6E 67 65 61 62 6C 65  ...Exchangeable
40h: 2E 6A 70 67 00 F0 67 4E 32 18 1E 15 50 C8 8E 21 .jpg.ðgN2...PÈŽ!
50h: C0 12 1D F3 32 48 10 D7 00 86 8A 57 44 44 46 25 À..ó2H.×.†ŠWDDF%
60h: 15 15 1D F2 2B 2D 1D 70 18 EA AD 51 2A 88 B5 AE ...ò+-.p.ê-Q*ˆµ®
70h: FA EA C0 AD 51 16 A8 8B 5A A3 A2 C4 74 82 DA D1 úêÀ-Q.¨‹Z£¢Ät‚ÚÑ
80h: D1 6A D5 AA C5 AA D6 B5 5B 16 BA EB 6A 3B C5 45 ÑjÕªÅªÖµ[.ºëj;ÅE
90h: AA D7 67 BF 29 A1 42 68 E7 3B 99 92 40 B6 FE F9 ª×g¿)¡Bhç;™'@¶þù
A0h: FD EF E7 C5 21 93 33 B9 DC EF 79 BF BD 3E 93 E7 ýïçÅ!"3¹Üïy¿½>"ç
B0h: F8 4F 3D 7A E7 E7 39 DE 77 BE 79 03 CF 24 F9 BD øO=zççŞw¾y.Ï$ù½
C0h: 3C AF 4F 3E 9F F4 2C C6 E0 23 CA 2A DF 6F 2A 1B <¯O>Ÿô,Æà#Ê*ßo*.
```

发现打不开提示文件头损坏,结合压缩包名字fake.rar,想到伪加密



```
    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
h: 52 61 72 21 1A 07 00 CF 90 73 00 00 0D 00 00 00 Rar!...Ï.s......
h: 00 00 00 00 87 0F 74 20 90 35 00 BC CF 00 00 0F ....‡.t .5.¼Ï...
h: 7D 01 00 02 74 88 FB 9C 38 B5 24 56 1D 33 10 00 }...tˆûœ8µ$V.3..
h: 20 00 00 00 45 78 63 68 61 6E 67 65 61 62 6C 65  ...Exchangeable
```

将第24字节改成0即可打开

里面是一张图片,有经纬度信息

神秘的海报

stegsolve查看图片发现有LSB隐写有一半flag,且给出了一个下载音乐附件的网站,提示是steghide隐写,stegseek一把梭爆出密码是123456,两个flag合起来即可

e99p1ant_want_girlfriend

修改图片宽高即可,一把梭