Hgame-Writeup Week2

WEB

ID40 从0开始LFI之0

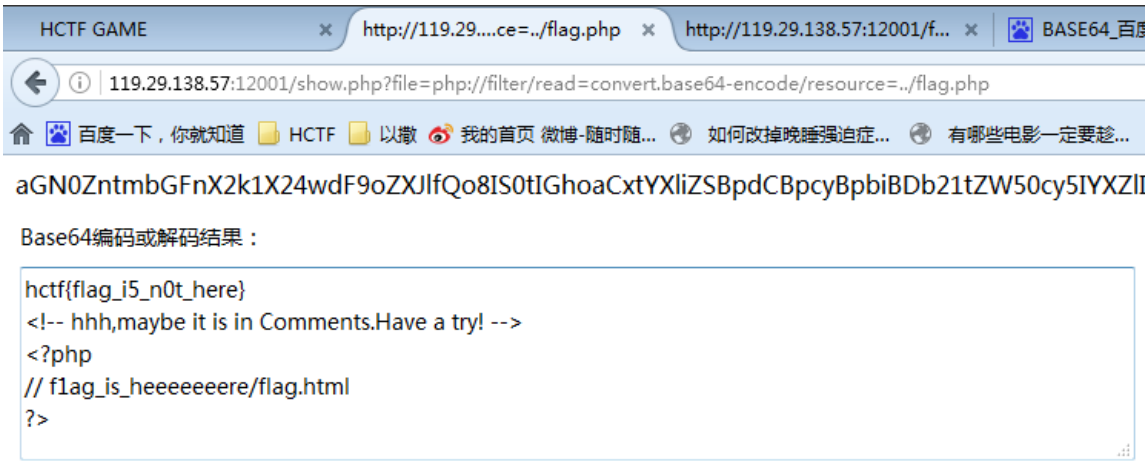
> 送分题 flag在../flag.php http://119.29.138.57:12000/

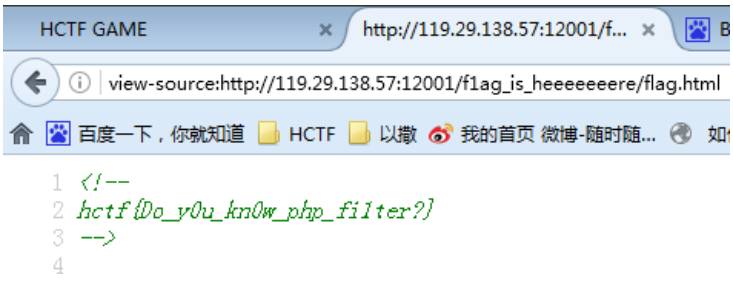
查看html源代码发现有文件包含漏洞 ?file=../flag.php 得到flag

ID41 从0开始LFI之1

> flag在哪呢? http://119.29.138.57:12001/

同样文件包含漏洞，但是flag.php里没有flag，利用 ?file=php://filter/read=convert.base64-encode/resource=../flag.php查看base64加密后的php源代码，解密后得到flag.html地址，得到flag

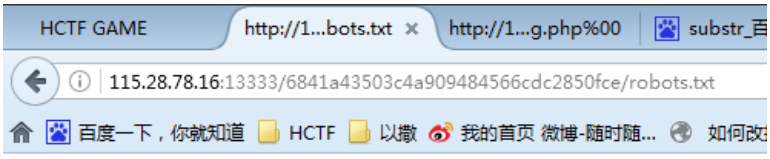




ID43 Explorer的图包

> LoRexxar一直念念不忘Explorer的图包，一气之下Explorer把图放在了服务器上，当LoRexxar又需要的时候可以自己去下。
> 115.28.78.16:13333/6841a43503c4a909484566cdc2850fce/

查看robots.txt，发现好东西，利用文件下载漏洞下载，发现虽然文件名是对的，内容是index.php的，估计有过滤，绕过去就行了



PENTEST

ID45 我是最简单的渗透题

网上查了很多万能密码，啥也没管一个一个试过去就登陆成功了

后来回头看了一下万能密码原理，用的是SQL注入

CRYPTO

ID34 密码学教室进阶（五）

不多说了，贴上代码，先去http://www.factordb.com/分解n，然后根据p,q,e算出d，解出明文

```
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:
        raise Exception('modular inverse does not exist')
    else:
        return x % m
p=input("p=")
q=input("q=")
e=input("e=")
c=input("c=")
d=modinv(e,(p-1)*(q-1))
m=pow(c,d,p*q)
print m
```

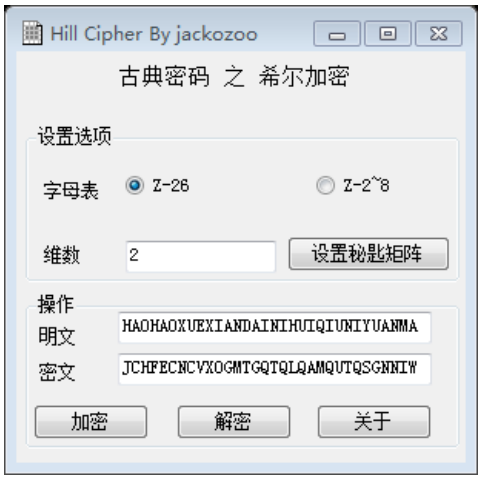
ID55 进击的 Crypto [0]

http://www.factordb.com/发现无法分解，给了多个n，但是e相同，在网上看到过例题，是寻找不同n之间的公因数，随后解出p,q，代码如下

```
def gcd(a, b):
   if a < b:
     a, b = b, a
   while b != 0:
     temp = a % b
     a = b
     b = temp
   return a
n1=input("n1=")
n2=input("n2=")
print gcd(n1,n2)
```

ID42 密码学教室进阶（六）

一开始手工算的，没做出来，后来网上找了个解密工具，成功了



RE

ID48 re从零开始的逆向之旅：Gold Miner

蹭了一道RE题，纯属玩出来的

MISC

ID39 explore的奇怪番外2

百度了工作量证明，根据nc后的反应，是要求我给出一个长度为100的字符串，且该字符串使用sha256加密后的前六位与它给我的相同，贴上我的

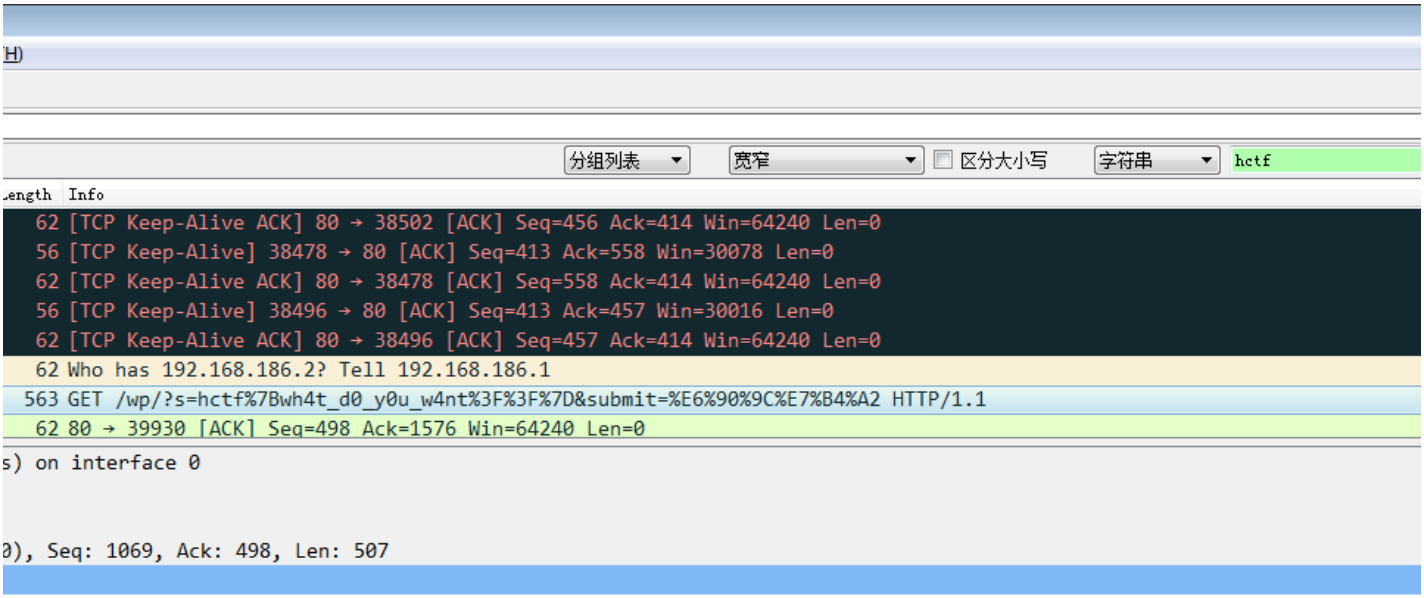
socket

```
import socket
import time
import hashlib

sha = hashlib.sha256()
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(('121.42.25.113', 20001))
k = sock.recv(1024)
print k
k = sock.recv(1024)
print k
from random import Random
def random_str(randomlength):...
def sha256(check):
    text = ''
    for a in range(0,127):
        for b in range(0,127):
            for c in range(0,127):
                for d in range(0,127):
                    list=["0"]*96+[chr(a),chr(b),chr(c),chr(d)]
                    text=''.join(list)
                    sha = hashlib.sha256()
                    sha.update(text)
                    #print sha.hexdigest()[0:6],a,b,c,d
                    if(sha.hexdigest()[0:6]==check):

    return text
ppp=raw_input()
text0=sha256(ppp)
print text0
sock.send(text0 + "\n")
k = sock.recv(1024)
print k
k = sock.recv(1024)
print k
```

Remove redundant parentheses more... (Ctrl+F1)

ID61 我是一个有格调的misc题目

摸索了一下wireshark的用法，使用过滤器查找hctf，得到flag



```
H)

分组列表  宽窄  区分大小写  字符串  hctf
ength  Info
  62 [TCP Keep-Alive ACK] 80 → 38502 [ACK] Seq=456 Ack=414 Win=64240 Len=0
  56 [TCP Keep-Alive] 38478 → 80 [ACK] Seq=413 Ack=558 Win=30078 Len=0
  62 [TCP Keep-Alive ACK] 80 → 38478 [ACK] Seq=558 Ack=414 Win=64240 Len=0
  56 [TCP Keep-Alive] 38496 → 80 [ACK] Seq=413 Ack=457 Win=30016 Len=0
  62 [TCP Keep-Alive ACK] 80 → 38496 [ACK] Seq=457 Ack=414 Win=64240 Len=0
  62 Who has 192.168.186.2? Tell 192.168.186.1
 563 GET /wp/?s=hctf%7Bwh4t_d0_y0u_w4nt%3F%3F%7D&submit=%E6%90%9C%E7%B4%A2 HTTP/1.1
  62 80 → 39930 [ACK] Seq=498 Ack=1576 Win=64240 Len=0
s) on interface 0


0), Seq: 1069, Ack: 498, Len: 507
```