

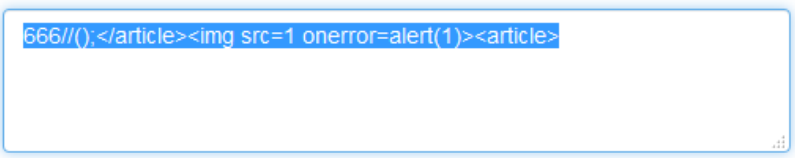
Week 2

Web

Web: xss-1

因为 script, imge, /会被代替掉, 所以

构造 666//();</article><img src=1 onerror=alert(1)><article> 【我的想法是在<article>前把 ( ) 给代替掉, 因为 replace 只执行一次】



```
666//();</article><img src=1 onerror=alert(1)><article>
```

请带着payload找fantasyqt(QQ 744399467)

Web: 最简单的 sql 题

因为存在注入点, 我想先试试万能钥匙: 2' or '1

于是



有了 flag

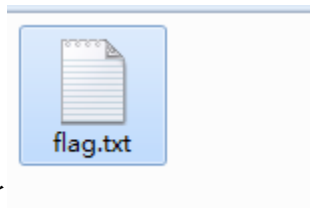


MISC:

misc-3: easy password

得到一个加密的 Zip 压缩包 于是暴力破解





答案出来了

得到 flag

Crypto

C-2 : The same simple RSA

看到是 RSA 解密的题目，我首先打开了

```
C:\Users\Administrator\Downloads\pubkey.pem - Notepad++ [Administrator]
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
pubkey.pem
1 -----BEGIN PUBLIC KEY-----
2 MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMJjauXD2OQ/+5erCQKPGqxsC/bNPXDr
3 yigb/+l/vjDdAgMBAAE=
4 -----END PUBLIC KEY-----
5
```

看到了公钥，于是通过 kali 上的 openssl 跑出了

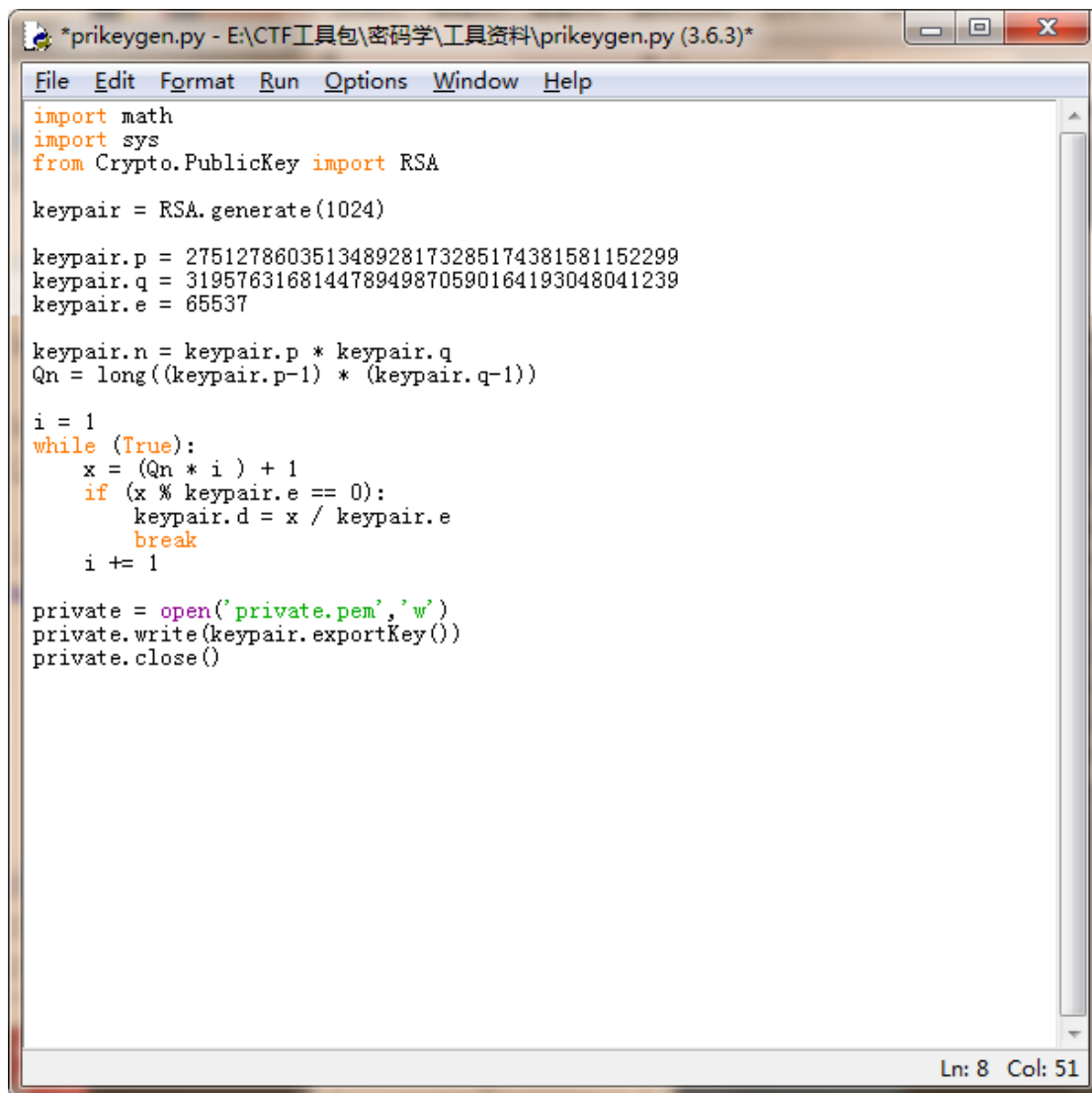
```
root@kali: ~/Desktop
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~# cd Desktop/
root@kali:~/Desktop# openssl rsa -pubin -text -modulus -in pubkey.pem
Public-Key: (256 bit)
Modulus:
 00:c2:63:6a:e5:c3:d8:e4:3f:fb:97:ab:09:02:8f:
 1a:ac:6c:0b:f6:cd:3d:70:eb:ca:28:1b:ff:e9:7f:
 be:30:dd
Exponent: 65537 (0x10001)
Modulus=C2636AE5C3D8E43FFB97AB09028F1AAC6C0BF6CD3D70EBCA281BFFE97FBE30DD
writing RSA key
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMJjauXD2OQ/+5erCQKPGqxsC/bNPXDr
yigb/+l/vjDdAgMBAAE=
-----END PUBLIC KEY-----
root@kali:~/Desktop#
```

得到模数后，再通过 msieve 跑出了 p 和 q

```
管理员: C:\Windows\system32\cmd.exe
attempting to build 36780 cycles
found 36780 cycles in 1 passes
distribution of cycle lengths:
  length 1 : 18680
  length 2 : 18100
largest cycle: 2 relations
matrix is 36332 x 36780 (5.3 MB) with weight 1084744 (29.49/col)
sparse part has weight 1084744 (29.49/col)
filtering completed in 3 passes
matrix is 26268 x 26332 (4.1 MB) with weight 860918 (32.69/col)
sparse part has weight 860918 (32.69/col)
saving the first 48 matrix rows for later
matrix includes 64 packed rows
matrix is 26220 x 26332 (2.8 MB) with weight 647257 (24.58/col)
sparse part has weight 469862 (17.84/col)
commencing Lanczos iteration
memory use: 2.8 MB
lanczos halted after 416 iterations (dim = 26215)
recovered 14 nontrivial dependencies
p39 factor: 275127860351348928173285174381581152299
p39 factor: 319576316814478949870590164193048041239
elapsed time 00:00:04

E:\CTF工具包\密码学\工具资料\msieve153_win64\msieve153>msieve153.exe 0xC2636AE5C
3D8E43FFB97AB09028F1AAC6C0BF6CD3D70EBCA281BFFE97FBE30DD -u
```

把 p 和 q 载入到 python 脚本中



```
File Edit Format Run Options Window Help
import math
import sys
from Crypto.PublicKey import RSA

keypair = RSA.generate(1024)

keypair.p = 275127860351348928173285174381581152299
keypair.q = 319576316814478949870590164193048041239
keypair.e = 65537

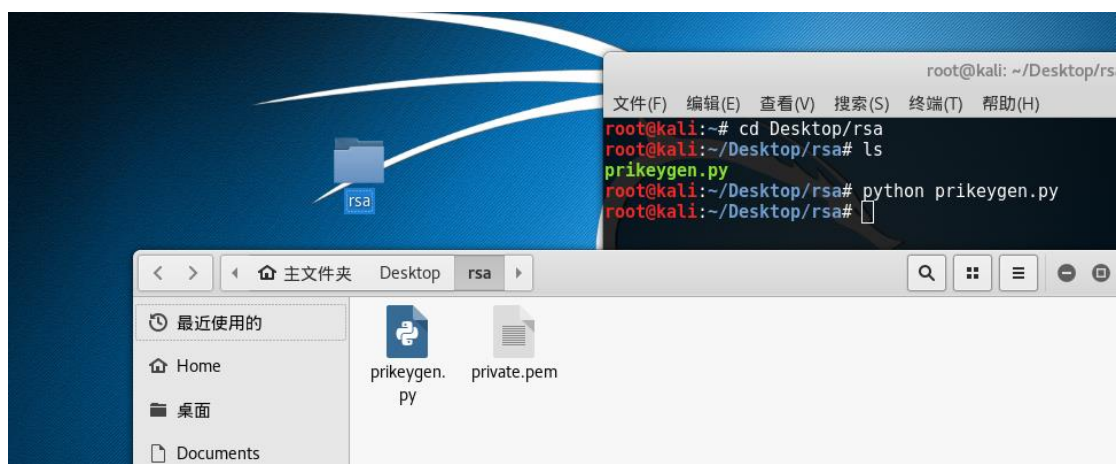
keypair.n = keypair.p * keypair.q
Qn = long((keypair.p-1) * (keypair.q-1))

i = 1
while (True):
    x = (Qn * i) + 1
    if (x % keypair.e == 0):
        keypair.d = x / keypair.e
        break
    i += 1

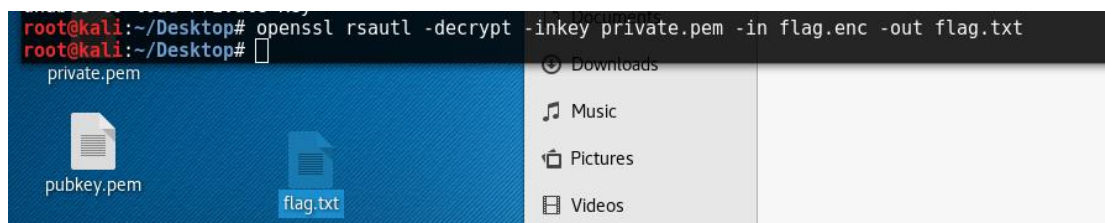
private = open('private.pem', 'w')
private.write(keypair.exportKey())
private.close()
```

Ln: 8 Col: 51

拖入到 kali 中生成所需的私钥文件



通过 openssl 解密



得到 flag

补 Week 1

Web 部分

Web-2: special number

首先看了别人的 writeup

好吧与我之前对比，之前没有搞明白

`$pattern = '/^(?=.*[0-9].*)(?=.*[a-zA-Z].*).{7,}$/';` 这串正则表达式在干啥，现在我明白是要求输入带数字和字母，且长度要大于或等于 7【由{7,}可知，“”代表了大于也可以】

之后是 `$b = json_decode($key);` 这个函数，我先前并没有明白，一直按照网上的说法按照数组在输入。好吧，现在知道了“数组==字符串”是不会成立的。

看了 wp 最后是用科学计数法解出来的。

总结：要多尝试，不能在一颗树上吊死。。同时要充分理解函数的作用，以及给的提示。

Misc-3: pacp1

我在解题时先想到的是追踪流来找 flag，追踪了 http 流和 tcp 流都没用【追踪 http 流时发现好多 flag，都不知道是哪个】，还看到一些黑色的数据包【意味着损坏？】以为是要修复，就放弃了。

看了 wp 后，好吧，要通过过滤 http 后，找到一个叫 flag.php 的，然后追踪 http 流，搜搜 hgame 就找到 flag。

总结：要多尝试几个关键词，找有提示的信息。