Week2----writeup

写这周的 wp 非常轻松(因为只写出了一道题，其他都是半成品，没拿到 flag)。尽管只写出了一道题，但是在写其他的过程中也学到了好多，总的来说，这周过得挺充实的。

Crypto

WritegiveRSA

一看到题目，字如其名，白给分的题目。在一个网站上将 n 分解了为 p 和 q，接下来用脚本进行解密，一开始用 gmpy2 来解密，python 一直报错，后来用 libnum 成功解密，获得了 flag。解密脚本如下：

```
import libnum
n = 882564595536224140639625987659416029426239230804614613279163
e = 65537
c = 747831491353896780365654517748216624798517769637260742155527
p = 857504083339712752489993810777
q = 1029224947942998075080348647219
phi=(p-1)*(q-1)
d=libnum.modular.invmod(e,phi)
m=libnum.n2s(pow(c,d,n))
print(m)
```