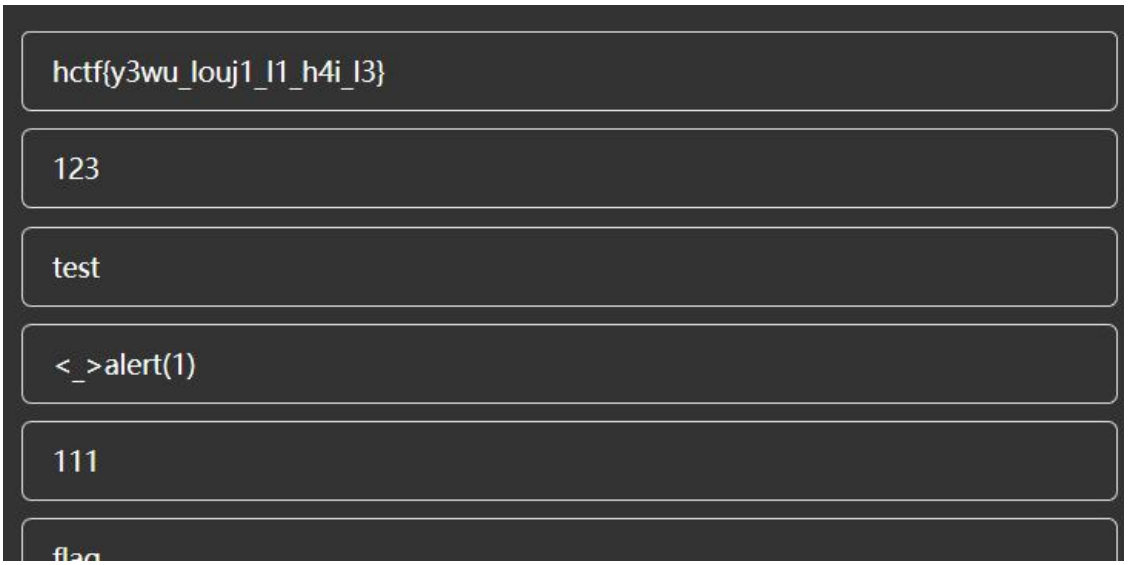
PENTEST

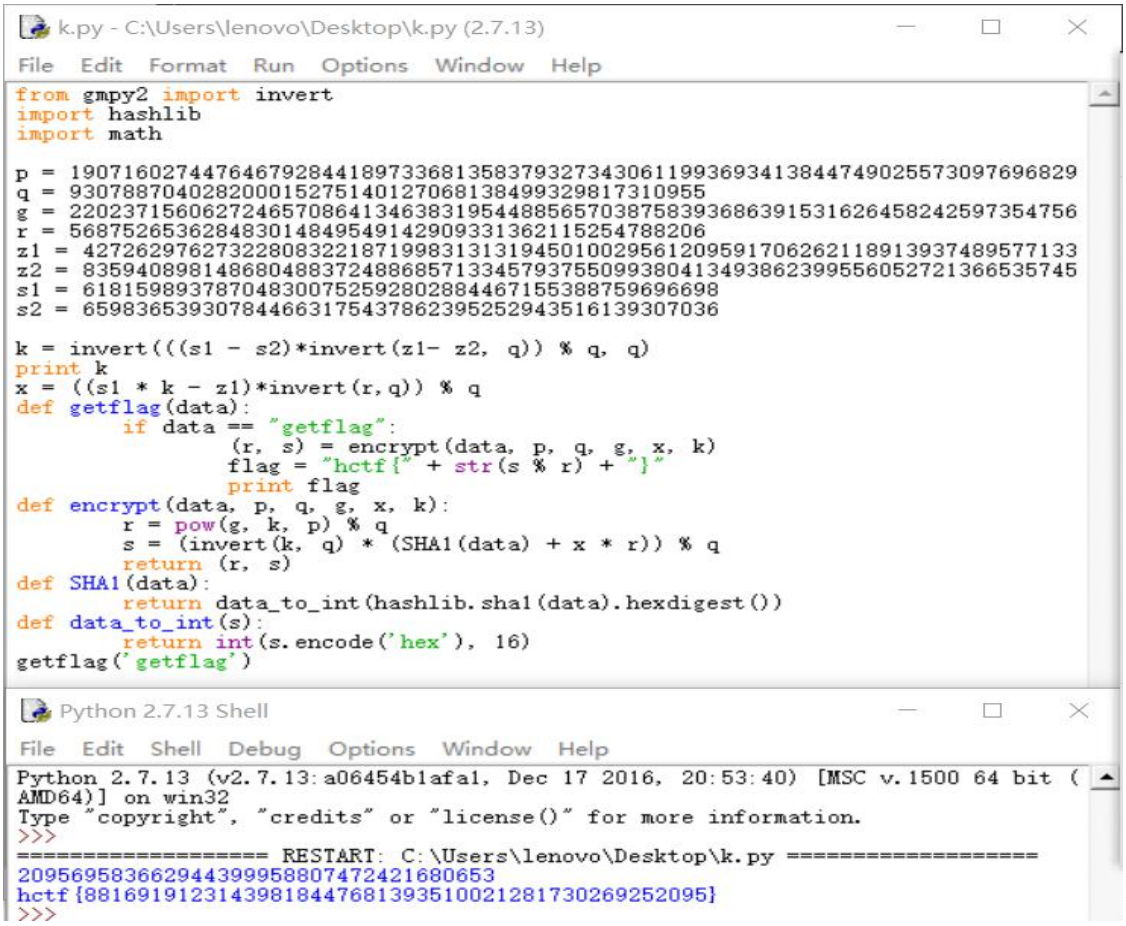
LoRexxar 的渗透之战之二

我怀疑这道题跟下一题的 hint 放反了，这道题我没有看出可以业务逻辑漏洞，而是水平越权；首先申请一个账号 ngc 密码 111111 从源码中进去得到 code，发现可以进行改密码并且在网页中不能改账号，那就在 firebug 中改为 LoRexxar，改完登录。



进击的 Crypto [4]

挺简单的数学题，看懂代码就好，写了个代码直接算出来了



进击的 Crypto [5]

E 特别小，可以用哪个中国剩余定理求密文

rsa.py - C:\Users\lenovo\Desktop\rsa.py (2.7.13)

File Edit Format Run Options Window Help

```
a2 = 45860339300158149755534876143213412903580729605395648495897585938015878234 1

a3 = 12012575342366442210994368605032582129674485327006093552902983877957202172 7

a4 = 42490059113248986304587234911515768101986190783329729114201666451272585985 1

a5 = 18557109853898405974924769550105345673703067457537813607252151469933140760 7

a6 = 19221531342713801219971420455098666365124810169512711030444063942333694562 3

a7 = 20438667185329273014541270175218359454017271737603524882205170284988617772 6

a8 = 90184064520411178679272046746492209291605099426042905723036441834512379449 1

a9 = 17978671919734595201524186618868659656036765546673883938819333911564948587 8

a10 = 85970678808124561236695949786601350586688758349242012799241627610201375826
a = []
a.append(a1)
a.append(a2)
a.append(a3)
a.append(a4)
a.append(a5)
a.append(a6)
a.append(a7)
a.append(a8)
a.append(a9)
a.append(a10)
o=[]
z=[]
X = 0
for i in range(10):
    o.append(N/n[i])
    z.append(invert(o[i],n[i]))
    X =X+ a[i]*o[i]*z[i]
X = X%N
print X
```

Ln: 74 Col: 7

n 为 n 的列表，a 为 c 的列表，N 为 n 的乘积，

最后得出十进制做 1/ 10 次方，转十六进制转字符串

16进制转字符 字符转16进制 清空结果

When e are small and same,it can be Hastad's broadcast attack.Maybe we w
{Hastad's_broadcast_attack_is_interesting}

得到 flag。