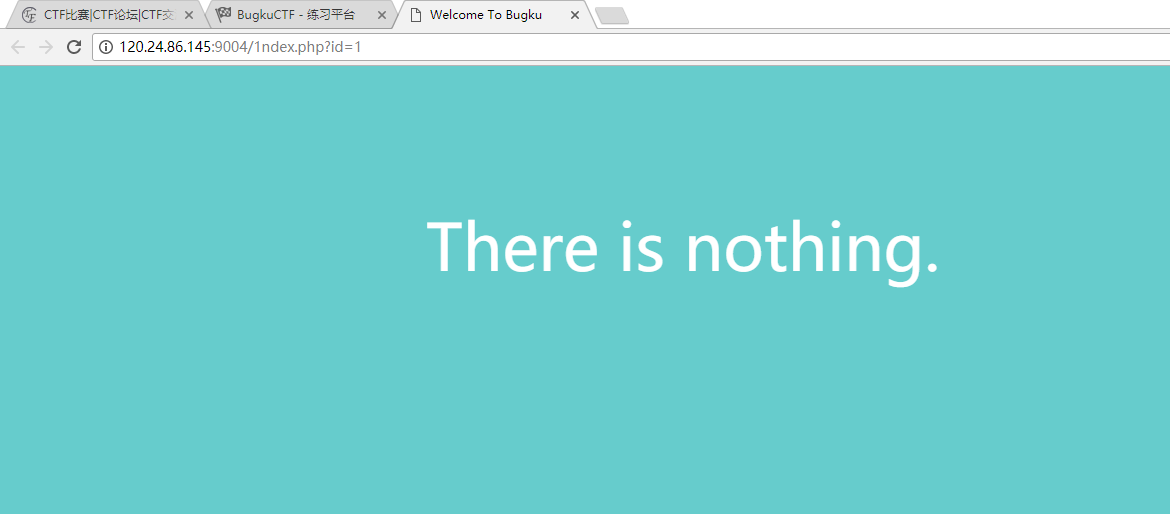
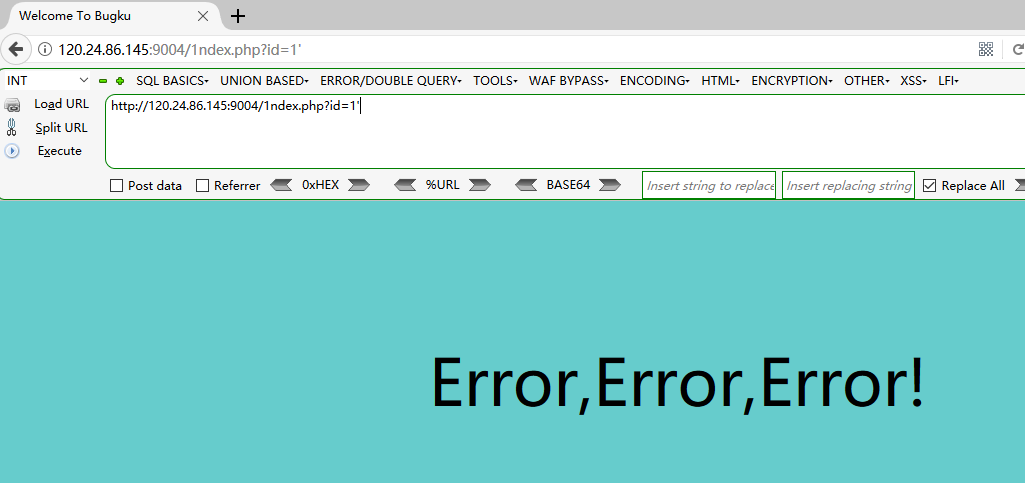
Bugku的web题目（多次）的解题



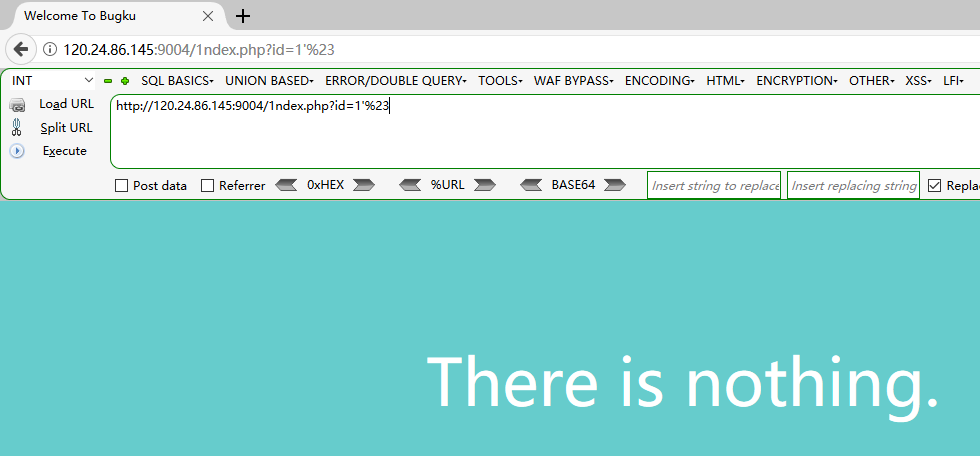
这道题目我弄了好久，最后问了朋友，然后在朋友的帮助下，将flag找到了

这里写一下解题方法，记录一下

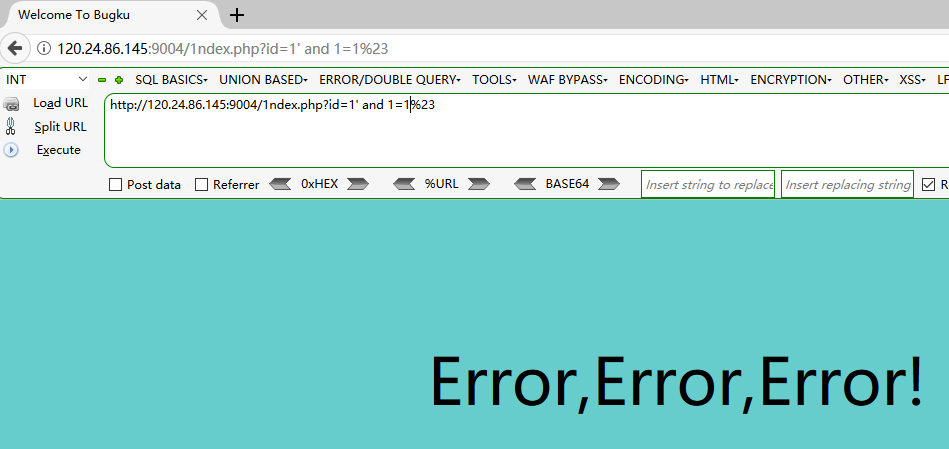
一进到这道题，看到了php?id=1，就很熟悉，很有可能是一道sql注入的题目，肯定是要试一下最简单的测试，（哪怕知道不可能是什么都没有过滤）



单引号出错



多加一个%23，发现不出错了

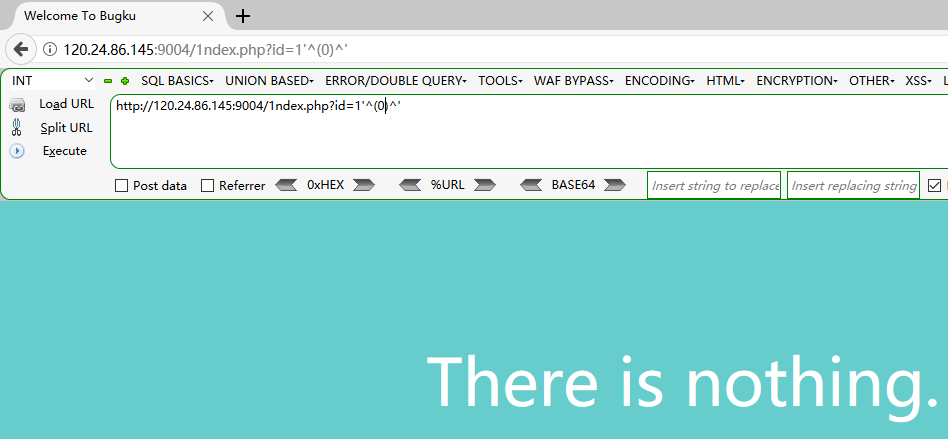


加上’ and 1=1%23

又出错了，可能是过滤了，但是不知道过滤了什么

这里有一个很好的方法知道过滤的是什么

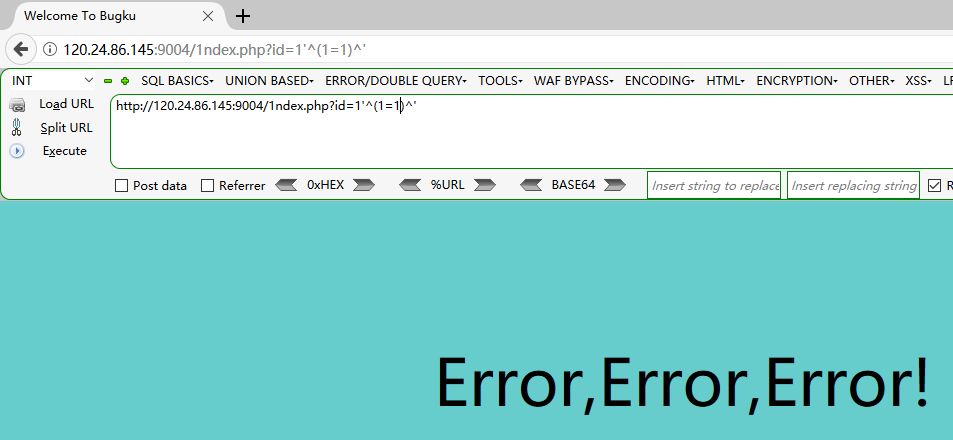
使用异或注入



在id=1后面输入 '^(0)^'

发现不出错，那就将0换成1=1

如果出错，那就是成功了

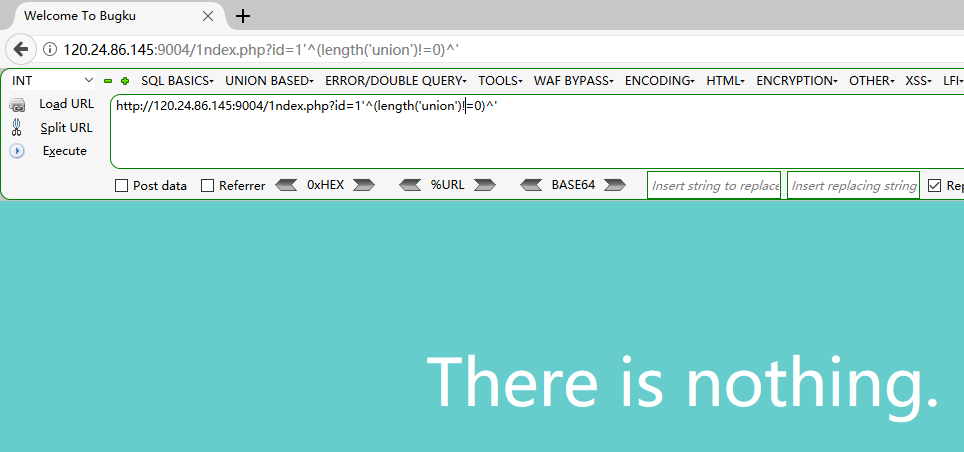


通过验证是可以的

也就是说，如果括号里面的判断是假的，那么页面就会显示正确

那么同理，如果我修改里面的内容为length(‘union’)!=0

如果页面显示正确，那就证明length(‘union’)是等于0的，也就是union被过滤了



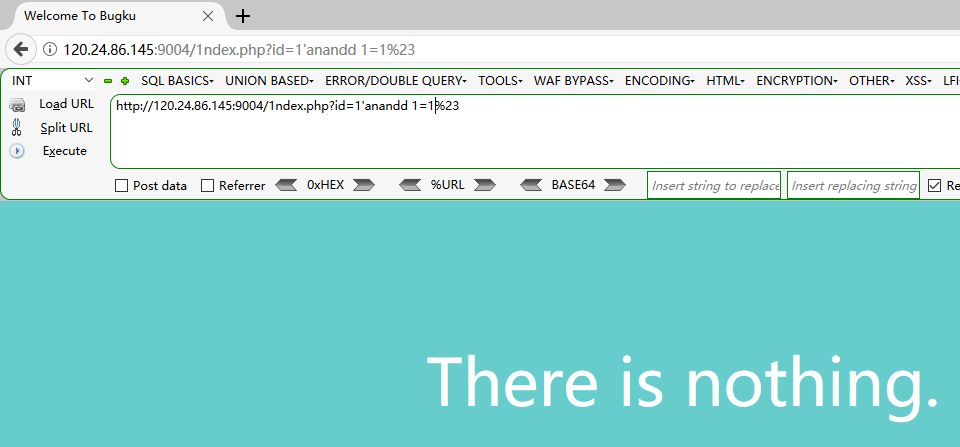
发现确实是这样，那就可以在这里进行判断，看看到底那些函数被过滤了

最后发现union,select,or,and被过滤了

limit,from没有被过滤

尝试绕过过滤，既然union这些都是被过滤掉了

那构造ununionion 一旦union被过滤，删除了，那剩下来的还是union，这样就可以起到作用了

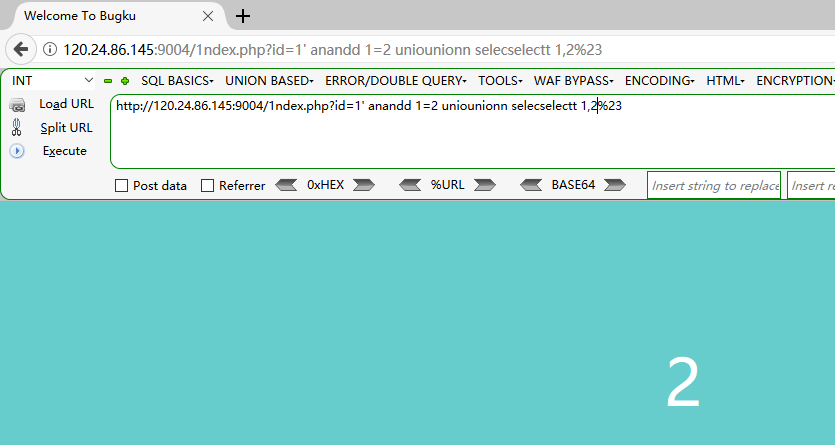


经过测试，用那个方法，确实可以

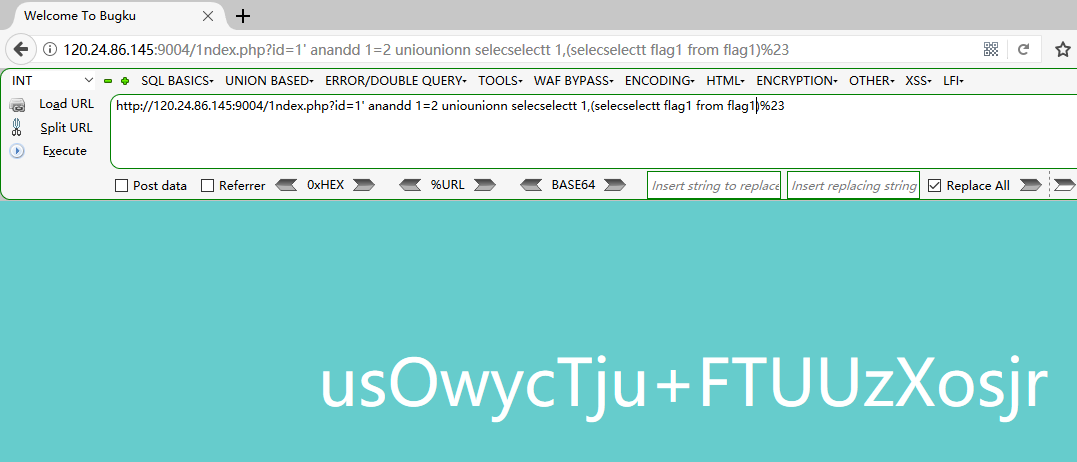
最终的payload为

http://120.24.86.145:9004/1ndex.php?id=1' anandd 1=2 uniounionn selecselectt 1,2%23

还是一个回显的



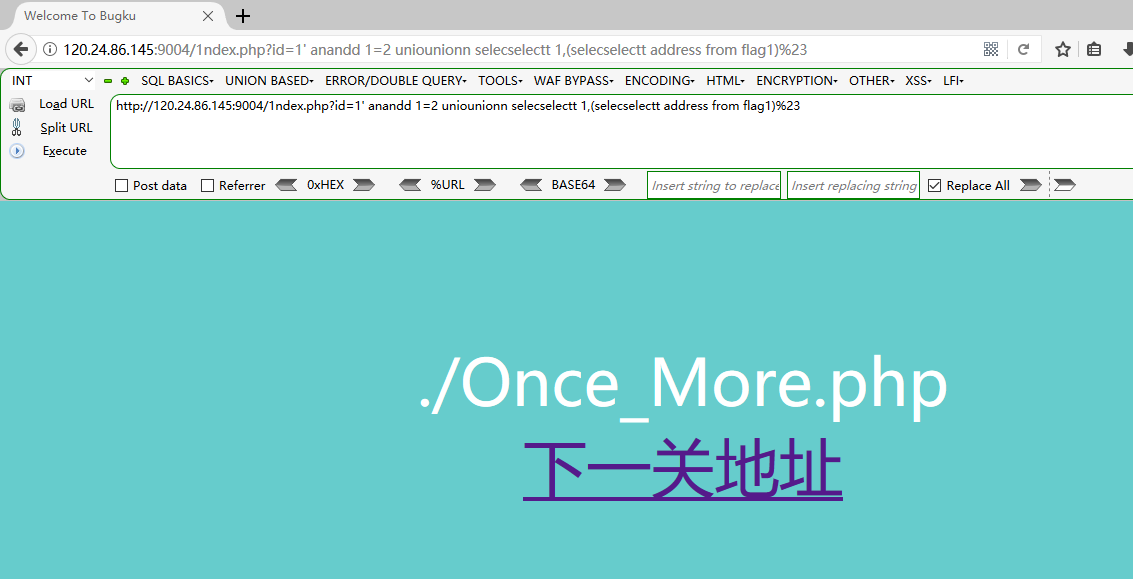
然后测试，找到了一个表为flag1，列名为flag1



出来一串不知道是什么东西的数据

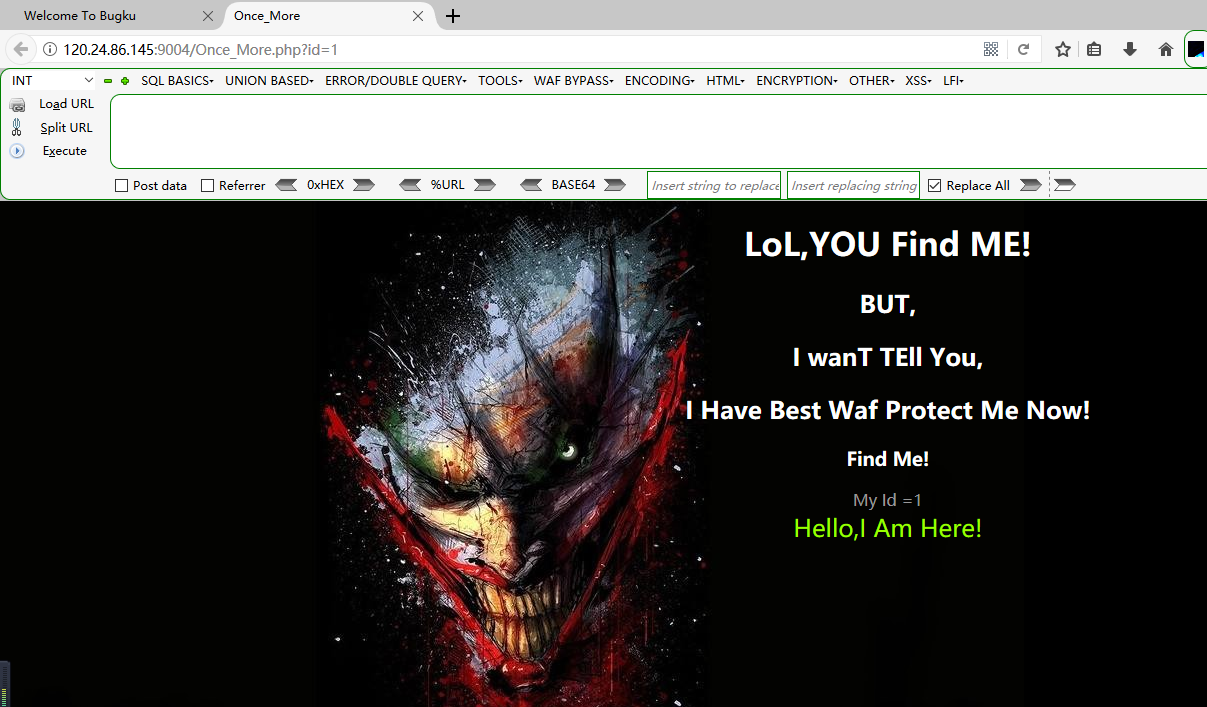
然后就继续查找，因为提示说有2个flag，那就是还有一个

最后在address这个列里面找到一个网址

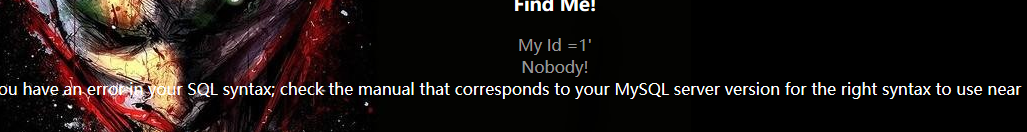


点击进去发现

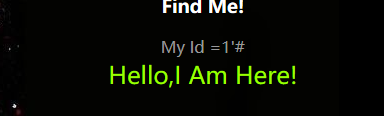
这道题还没有做完，前面的只是为了找这个链接……



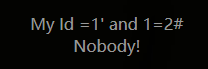
这里还是一个考注入，那就常规测试一下，加上单引号



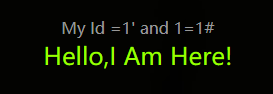
出现报错，还是最常见的报错，那就是要%23注析掉了



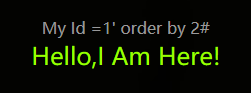
然后继续测试其他的



1=2出错

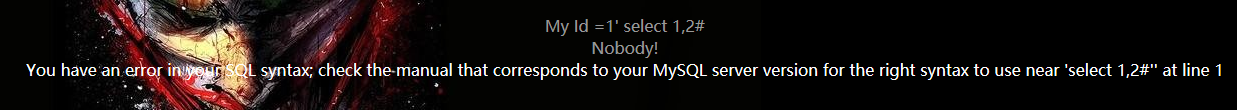


1=1正常



Order by 2也正常

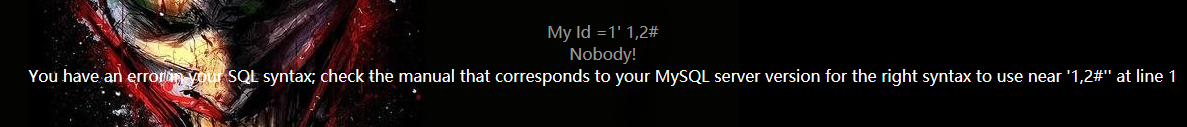
一切都好顺利



' union select 1,2%23

出现了过滤，把union过滤了

用之前的方法绕过

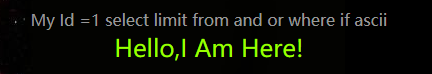


' uniunionon select 1,2%23

发现把select也吃掉了

那就测试一下看看还有那些函数被过滤了

直接在id后面输入函数就可以知道，因为有回显我们输入的数据



id=1 union select limit from and or where if sleep substr ascii

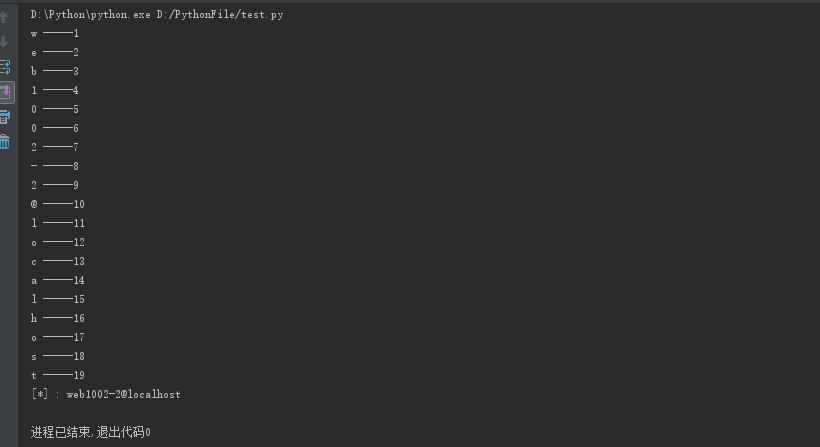
发现 union sleep substr被过滤了

那就是不能回显，substr也不能用了

我这里用了一个不常用的函数locate()

直接判断查出来的数据里面有那些字符，然后将它们按顺序排序





完整代码在我的GitHub里面有

https://github.com/niechaojun/Duoci