## sql防注入

cursor.execute("select user,pass from tb7 where user=%s and pass=%s",(user,passwd))

如果使用 cursor.execute("select \* from %s”,tablename)此处会报错

print(cursor.mogrify("select \* from %s”,tablename))会发现是

select \* from ‘table’,多了引号

solution：”select \* from “+table

## mysql存储过程

之前没有理解

存储过程是一组sql保存在数据库中，类似一个函数，存在数据库中，主要是数据处理，随时可以被用户调用

CREATE PROCEDURE `select\_students\_by\_name`(

in \_name varchar(225), -- 输入参数

out \_city varchar(225), -- 输出参数

inout \_age int(11) -- 输入输出参数

)

BEGIN

SELECT city from students where name = \_name and age = \_age into \_city;

END;;