

# 数据库系统实验 2 实验报告

数据科学与计算机学院 计算机科学与技术 2016 级

王凯祺 16337233

2018 年 10 月 15 日

## 1 实验 2.1 自主存取控制实验

### 1.1 创建用户

创建用户 Amit, Satoshi 。

```
1 create user 'Amit'@'%' with mysql_native_password identified by '123456';  
2 create user 'Satoshi'@'%' with mysql_native_password identified by '123456';
```

我曾尝试过使用

```
1 insert into mysql.user (host, user, password) values ('%', 'Amit', password('123456'  
));
```

来添加用户，可是 mysql 总是在 password 处报错，提示 Error Code: 1064. You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '('123456'))' at line 1 。我上网查找了这个错误，发现是由于 Mysql 8.0 删除了 password 函数，遂改用 create user 语句来添加用户。

参考地址：[https://dev.mysql.com/doc/refman/8.0/en/encryption-functions.html#function\\_password](https://dev.mysql.com/doc/refman/8.0/en/encryption-functions.html#function_password)

### 1.2 创建角色并分配权限

#### 1.2.1 创建角色 instructor

```
1 create role instructor;
```

#### 1.2.2 为 instructor 角色分配权限

为 instructor 角色在 takes 表中授予 select 权限。

```
1 grant select on lab.takes to instructor;
```

### 1.2.3 将角色授予给用户/角色

将 dean 角色（未创建）授予给 Amit 。

```
1 grant dean to Amit;
```

让我意外的是，居然成功授予了角色。原来它只是创建了一条角色边。

```
1 select * from mysql.role_edges;
```

结果如下：

```
1 +-----+-----+-----+-----+-----+
2 | FROM_HOST | FROM_USER | TO_HOST | TO_USER | WITH_ADMIN_OPTION |
3 +-----+-----+-----+-----+-----+
4 | %         | dean      | %       | Amit    | N                  |
5 +-----+-----+-----+-----+-----+
6 1 row in set (0.02 sec)
```

### 1.2.4 创建角色 dean

```
1 create role dean;
```

### 1.2.5 将 instructor 角色授予给 dean

```
1 grant instructor to dean;
```

### 1.2.6 将 dean 角色授予给 Satoshi

```
1 grant dean to Satoshi;
```

## 1.3 查看验证权限

### 1.3.1 查看权限

使用 show grants 语句查看 Amit 的权限。

```
1 show grants for 'Amit'@'%' using dean;
```

结果为：

```
1 +-----+
2 | Grants for Amit@% |
3 +-----+
4 | GRANT USAGE ON *.* TO 'Amit'@'%' |
5 | GRANT SELECT ON 'lab'.'takes' TO 'Amit'@'%' |
6 | GRANT 'dean'@'%' TO 'Amit'@'%' |
7 +-----+
8 3 rows in set (0.03 sec)
```

### 1.3.2 验证授权

确认 Amit 拥有 lab.takes 的 select 授权后, 尝试使用 Amit 用户登录数据库。

使用 Amit 用户执行以下命令:

```
1 select * from takes limit 5;
```

结果如下:

```
1 ERROR 1142 (42000): SELECT command denied to user 'Amit'@'120.236.174.147' for table 'takes'
```

查阅资料后得知, 用户登录后, 没有激活角色, 需要使用 set role 语句将活动角色设置为所有授予的角色。

```
1 set role all;
2 select * from takes limit 5;
```

结果如下:

```
1 Query OK, 0 rows affected (0.02 sec)
2
3 +-----+-----+-----+-----+-----+-----+
4 | ID    | course_id | sec_id | semester | year | grade |
5 +-----+-----+-----+-----+-----+-----+
6 | 1000 | 239      | 1      | Fall     | 2006 | C      |
7 | 1000 | 319      | 1      | Spring   | 2003 | B+     |
8 | 1000 | 362      | 1      | Fall     | 2005 | B+     |
9 | 1000 | 493      | 1      | Spring   | 2010 | A-     |
10 | 1000 | 571      | 1      | Spring   | 2004 | C+     |
11 +-----+-----+-----+-----+-----+-----+
12 5 rows in set (0.02 sec)
```

### 1.3.3 收回授权

用 root 用户执行收回 instructor 对 dean 的授权。

```
1 revoke instructor from dean;
```

用 Amit 用户登录, 并使用 show grants 语句查看 Amit 的权限。

```
1 show grants for 'Amit'@'%' using dean;
```

结果为:

```
1 +-----+
2 | Grants for Amit@% |
3 +-----+
4 | GRANT USAGE ON *.* TO 'Amit'@'%' |
5 | GRANT 'dean'@'%' TO 'Amit'@'%' |
6 +-----+
7 2 rows in set (0.01 sec)
```

我们可以看到，在 lab.takes 的 select 权限已被收回。

用下面的语句测试一下是否能执行 select 操作：

```
1 set role all;  
2 select * from takes limit 5;
```

结果如下：

```
1 ERROR 1142 (42000): SELECT command denied to user 'Amit'@'120.236.174.147' for table  
  'takes'
```

## 1.4 实验总结

我明白了如何创建用户、如何授权和收回。在此过程中，我碰到了很多问题，如无法创建用户、授权后无法使用权利的问题，我均从网上搜索到原因以及解决方案，并解决了这些问题。

通过查看 mysql.user 和 mysql.role\_edges 表，我明白了授权关系是如何存储的（被授权人、授权人），也明白了为什么在未创建角色的情况下可以将角色授权给他人（只添加授权关系，不添加角色）。