

# 计算机安全实验

## 实验三

姓名：卢兑琬

学号：L170300901

# 实验 3：数据库用户的权限管理设计与实现

## 1. 实验目的

熟练掌握数据库（比如 MySQL）基本权限管理命令、SQL 语言以及学习数据库系统的设计、数据库用户权限管理的实现，包括特定场景下数据表创建和管理、数据库用户的创建和合理的权限分配，权限分配细化到数据库、表、列和行，或者视图。

学生自行设计应用场景（应用场景不要和实验指导书示例相同），为具体的应用需求建立数据库，比如产品销售、人口管理、医院、银行、股票、手机通信信息等的数据库。并为你所面对的应用需求进行用户分类和权限划分，要求权限设计合理，能够实现依据用户权限的分发、权限的收回，并能够成组的批量分发和收回权限。

系统要求：

- （1）系统自建操作界面，能够实现单条、批量权限的查询、分发和收回等操作。（利用数据库系统自带的界面进行演示，视为不合格）
- （2）测试权限设计的合理性。
- （3）管理操作日志。

## 2. 实验环境搭建

Windows10 64 位

MySQL8.0

## 3. 实验步骤

### 3.1 一个简单的应用场景（示例）

设想一个仓库保管系统，分有 root，老板和普通工作人员三种账户，有货品 good，成员 people 两张表。

#### 1. 用户设计

root 用户是数据库的根用户，在本次实验中，负责在初始时给老板用户授予管

理员权限，后续将无需使用。

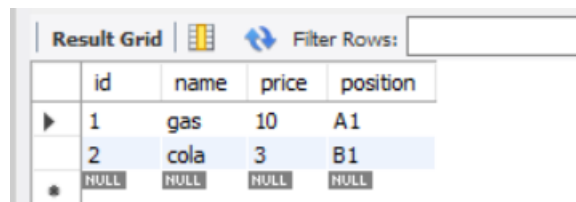
老板 boss 用户，经过 root 授予的管理员权限，可以拥有对所有表的所有四种权限（增加表项 insert、删除表项 delete、修改表项 update、查看表项 select），拥有对其他用户授予和收回权限的权限。

工作人员用户，拥有对两张表的部分权限，不可拥有对其他用户授予和撤销其权限的权限。

## 2. 表

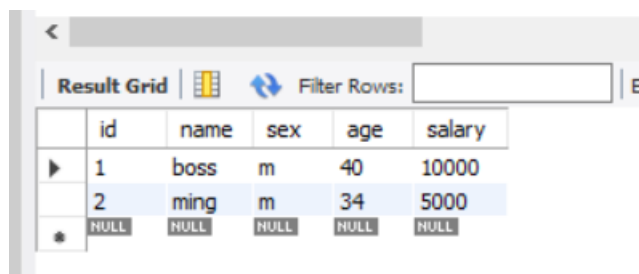
拥有两张表

货物（good）表，拥有货物序号（id），货物名称（name），货物价格（price），货物储存位置（position）四个列属性。



	id	name	price	position
▶	1	gas	10	A1
	2	cola	3	B1
✱	NULL	NULL	NULL	NULL

人员表（people），拥有人员序号（id），人员名称（name），人员性别（sex），人员年龄（age），人员薪水（salary）五个列属性。



	id	name	sex	age	salary
▶	1	boss	m	40	10000
	2	ming	m	34	5000
✱	NULL	NULL	NULL	NULL	NULL

## 3. 用户对表的权限设计

老板用户（boss）拥有对两张表的四种权限（增加表项 insert、删除表项 delete、修改表项 update、查看表项 select）。

普通用户（ming）可以拥有对 good 表：所有列的查询（select）权限，price 和 position 列的修改（update）权限，没有增加（insert）和删除（delete）权限。普通用户拥有对 people 表：id, name, sex 列的查询（select）权限，没有增加表

项 insert、删除表项 delete、修改表项 update 的权限。

### 3.2 建立数据库

创建数据库 仓库 storehouse

```
mysql> use storehouse;
Database changed
mysql> select user,host from mysql.user
-> ;
```

user	host
mysql.infoschema	localhost
mysql.session	localhost
mysql.sys	localhost
root	localhost

```
4 rows in set (0.01 sec)
```

创建的用户：boss，ming，密码分别为本身

```
mysql> rename user 'boss'@'*' to 'boss'@'localhost';
Query OK, 0 rows affected (0.01 sec)

mysql> rename user 'ming'@'*' to 'ming'@'localhost';
Query OK, 0 rows affected (0.01 sec)

mysql> select user,host from mysql.user;
```

user	host
boss	localhost
ming	localhost
mysql.infoschema	localhost
mysql.session	localhost
mysql.sys	localhost
root	localhost

```
6 rows in set (0.00 sec)
```

创建货品表 good

```
mysql> create table good(
  -> id int(4) not null primary key,
  -> name char(5) not null,
  -> sex char(1) not null,
  -> age int(2) not null,
  -> salary int(5) not null
  -> );
Query OK, 0 rows affected, 3 warnings (0.04 sec)

mysql> desc good
  -> ;
```

Field	Type	Null	Key	Default	Extra
id	int	NO	PRI	NULL	
name	char(5)	NO		NULL	
sex	char(1)	NO		NULL	
age	int	NO		NULL	
salary	int	NO		NULL	

5 rows in set (0.02 sec)

rename good to people

```
mysql> rename table good to people;
Query OK, 0 rows affected (0.02 sec)
```

desc good

```
mysql> desc good;
```

Field	Type	Null	Key	Default	Extra
id	int	NO	PRI	NULL	
name	char(10)	NO		NULL	
price	int	NO		NULL	
position	char(5)	NO		NULL	

4 rows in set (0.00 sec)

```
mysql> create user 'xiao'@'localhost' identified by 'xiao';
Query OK, 0 rows affected (0.01 sec)

mysql> select user,host from mysql.user;
```

user	host
boss	localhost
ming	localhost
mysql.infoschema	localhost
mysql.session	localhost
mysql.sys	localhost
root	localhost
xiao	localhost

7 rows in set (0.00 sec)

### 3.3 实验过程脚本示例

详见文档“示例脚本.txt”

## 0. 程序界面

```
Please input username and password with format [user:pswd]:
root:19260817
菜单:
1. 切换用户.
2. 查询仓库物品.
3. 向仓库添加物品.
4. 删除仓库物品.
5. 修改仓库物品.
6. 查看用户权限.
7. 授予他人权限.
8. 收回他人权限.
0. Exit退出.
```

## 1. root 给 boss 权限初始化

先用 root 用户登录

```
root:19260817
菜单:
1. 切换用户.
2. 查询仓库物品.
3. 向仓库添加物品.
4. 删除仓库物品.
5. 修改仓库物品.
6. 查看用户权限.
```

给 boss 授予 good, people 表的所有权限（四种），并且可以继承（可继承意味着 boss 可以将这些用户授予给普通员工）

```
Please input some information to grant privileges:
format: [user1,user2...:priv1,priv2...:tablename(:property_name)(:wgo)]('wgo' means 'with grant option')
Privilege hint: insert, select, update, delete...
boss:insert,select,update,delete:good:wgo
++ ~

Please input some information to grant privileges:
format: [user1,user2...:priv1,priv2...:tablename(:property_name)(:wgo)]('wgo' means 'with grant option')
Privilege hint: insert, select, update, delete...
boss:insert,select,update,delete:people:wgo
++ ~
```

查看刚才授予的权限（第 2, 3 行）

```
0. Exit退出.
6
db      |user  |table_name  |grantor      |table_priv      |column_priv      |
storehouse |boss  |good        |root@localhost|Select,Insert,Update,Delete,Grant|
storehouse |boss  |people      |root@localhost|Select,Insert,Update,Delete,Grant|
菜单:
```

## 2. 权限发放

用管理员用户 boss 身份给普通用户 ming 授予表 good 的 select 权限，授予表 good 的 price, position 列的 update 权限，授予表 people 的 id，

name, sex 项的 select 权限。并且查看权限授予结果（这里体现了权限的分发和收回设计）：

```
7
Please input some information to grant privileges:
format: [user1,user2...:priv1,priv2...:tablename(:property_name)(:wgo)]('wgo' means 'with grant option')
Privilege hint: insert, select, update, delete...
ming:update:good:price,position
菜单:
8. 收回他人权限。
0. Exit退出。
7
Please input some information to grant privileges:
format: [user1,user2...:priv1,priv2...:tablename(:property_name)(:wgo)]('wgo' means 'with grant option')
Privilege hint: insert, select, update, delete...
ming:select:people:id,name,sex
菜单:
1. 切换用户。
```

（查看刚才权限授予的结果）

```
0. Exit退出。
6
db      |user|table_name|grantor|table_priv|column_priv|
storehouse|boss|good|root@localhost|Select,Insert,Update,Delete,Grant|
storehouse|boss|people|root@localhost|Select,Insert,Update,Delete,Grant|
storehouse|ming|good|boss@localhost|Update|
storehouse|ming|people|boss@localhost|Select|
菜单:
1. 切换用户。
2. 查询仓库物品。
```

### 3. 批量权限的查询，插入，删除，修改

管理员用户 boss 向 good 表中添加商品 gass, colaa

```
6. 查看用户权限。
7. 授予他人权限。
8. 收回他人权限。
0. Exit退出。
3
Please input table name:
good
Please input values with format [id,'name',price,'position']:
3,'gass',9,'A2'
菜单:
4
Please input table name:
good
Please input the item's name that you want to delete:
4,'colaa',6,'A2'
java.sql.SQLException: You have an error in your SQL syntax; check the manual that corresponds to your MySQL ser
菜单:
1. 切换用户。
2. 查询仓库物品。
3. 向仓库添加物品。
4. 删除仓库物品。
5. 修改仓库物品。
```

管理员用户 boss 查看所有员工（people 表）的信息

```
Please input table name and properties with format 'tablename:property1,property2...':
people:id,name,sex,age,salary
id      name    sex    age    salary
1       boss    m      40     21000
2       ming    m      30     2000
菜单:
```

切换到普通用户 ming，查看所有员工（people 表）的信息（只能查看 id, name, sex）

```
2
Please input table name and properties with format 'tablename:property1,property2...':
people:id,name,sex
id      name    sex
1       boss    m
2       ming    m
菜单：
```

普通用户 ming 可以修改 good 表的价格和位置，但是不能修改 id, name（修改商品 gas 的价格至 88）

```
0. Exit退出.
5
Please input table name:
good
Please input the item's name, aim property and the new value that you want to modify:
format: [name,property,value](if value is a number) or [name,property,'value'](if value is a string)
gas,price,88
菜单：

2
Please input table name and properties with format 'tablename:property1,property2...':
good:id,name,price
id      name    price
1       gas     88
2       cola    3
3       gass    9
4       colaa   6
菜单：
```

（修改商品 gas 的名称至 gass，会出现错误）

```
8. 收回他人权限.
0. Exit退出.
5
Please input table name:
good
Please input the item's name, aim property and the new value that you want to modify:
format: [name,property,value](if value is a number) or [name,property,'value'](if value is a string)
gas,name,gass
java.sql.SQLException: UPDATE command denied to user 'ming'@'localhost' for column 'name' in table 'good'
菜单：
1. 切换用户.
2. 查询仓库精品.
```

## 4. 批量权限的收回

管理员用户 boss 收回普通用户 ming 的对表 people 的 select 权限



```

0. Exit退出。
8
Please input some information to revoke privileges:
format: [user1,user2...:priv1,priv2...:tablename
Privilege hint: insert, select, update, delete...
ming:select:people
菜单:
1. 切换用户。
2. 查询仓库物品。
3. 向仓库添加物品。
4. 删除仓库物品。
5. 修改仓库物品。
6. 查看用户权限。
7. 授予他人权限。
8. 收回他人权限。
0. Exit退出。
6
db      |user|table_name|grantor|table_priv|column_priv
java.sql.SQLException: SELECT command denied to user 'boss'@'localhost' for table 'tables_priv'
菜单:
1. 切换用户。
2. 查询仓库物品。
3. 向仓库添加物品。
4. 删除仓库物品。
5. 修改仓库物品。
6. 查看用户权限。
7. 授予他人权限。
8. 收回他人权限。
0. Exit退出。
1
Please input username and password with format [ user:pswd ]':
root:19268817
Change user succeed! Current user: [root]
菜单:
1. 切换用户。

```

查看 select 权限收回是否成功（下表中，ming 用户没有了对 people 的 select 权限）

```

5. 修改仓库物品。
6. 查看用户权限。
7. 授予他人权限。
8. 收回他人权限。
0. Exit退出。
6
db      |user|table_name|grantor|table_priv|column_priv
storehouse|boss|good|root@localhost|Select,Insert,Update,Delete,Grant|
storehouse|boss|people|root@localhost|Select,Insert,Update,Delete,Grant|
storehouse|ming|good|boss@localhost|Select|Update
菜单:
1. 切换用户。
2. 查询仓库物品。

```

## 4. 实验总结和反思

通过本次实验，我初步掌握了数据库 MySQL 基本权限管理命令、SQL 语言的使用，并且设计了一个简单的应用场景下的数据表创建和管理、数据库用户的创建和权限划分、分发和收回策略。这也提示我们，在数据库的设计中，需要更多考虑权限的分配问题，以免出现数据库安全问题。