**实验4 数据库中角色和授权**

**1140320206 霍峻杰**

**一、实验目的：**

熟练掌握MySQL基本权限管理命令、SQL语言以及学习数据库系统的设计、数据库用户权限设定的实现，包括特定场景下地数据表创建和管理、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。

**二、实验步骤：**

**2.1 实验场景**

1. 顾客（顾客号，姓名，性别，联系方式）

2. 库管（库管号，姓名，性别，联系方式，工资）

3. 商品（商品号，单价，生产日期,库存）

4. 顾客商品关系（顾客号，商品号，花销，日期）

5. 库管商品关系（库管号，商品号，入库量，日期）

**2.2 建立数据库**

参考下面附录中的建库建表代码

**2.2 创建新用户**

创建三个用户： admin, custom, wareOperator

CREATE USER 'admin'@'localhost' IDENTIFIED BY '';

CREATE USER 'custom'@'%' IDENTIFIED BY '';

CREATE USER 'wareOperator'@'%' IDENTIFIED BY '';

**2.3 权限设计**

admin:

nearly all(select, insert,update, delete,alter)

custom:

select customer(all),

update customer（cname,cgender,ctel）

wareOperator:

select wareOperator(all),

update wareOperator(wname,wgender,wtel)

select goods(all),

w\_g(select,delete,insert,update),

update goods(storage)

**2.4 权限语句**

**admin:**

grant select, insert, update, delete,alter on mall2.\* to admin@'localhost';

**custom:**

grant select on mall2.customer to 'custom'@'%';

grant update(cname,cgender,ctel) on mall2.customer to 'custom'@'%';

**wareOperator:**

grant select on mall2.wareOperator to 'wareOperator'@'%';

grant update(wname,wgender,wtel) on mall2.wareOperator to 'wareOperator'@'%';

grant select on mall2.goods to 'wareOperator'@'%';

grant select,insert,update,delete on mall2.w\_g to 'wareOperator'@'%';

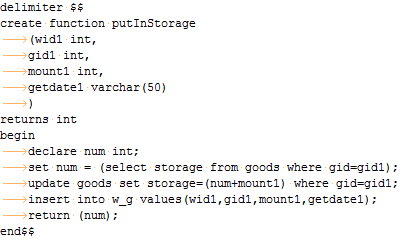
grant update(storage) on mall2.goods to 'wareOperator'@'%';

**三、sql函数：**

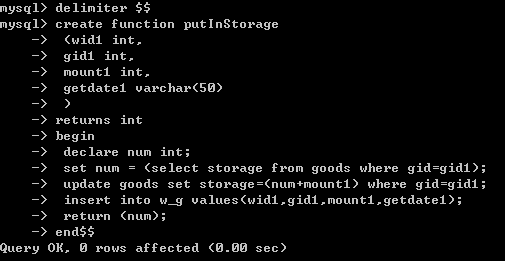
这里需要补充一个东西，因为要在指定用户，而不是root运行函数，所以需要将执行权限execute赋给指定用户，这里选择赋给admin用户。



函数声明：



函数声明正确：



函数使用结果：

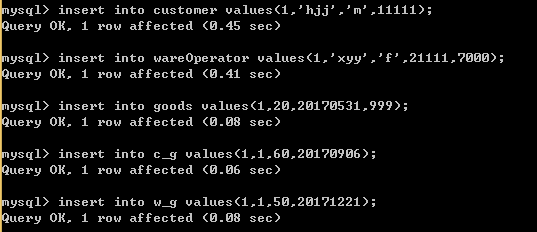


正确的把新到货的数量加入到了库存信息中。

**四、实验结果：**

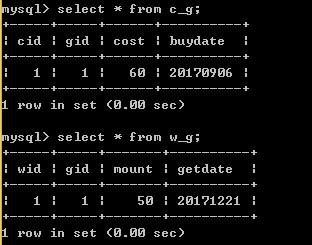
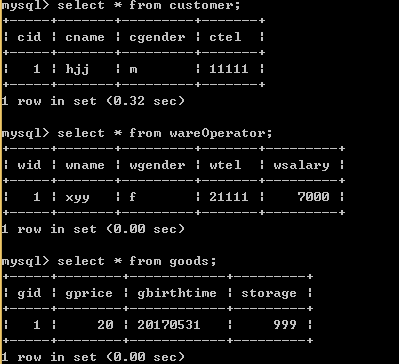
1. 当前为admin在localhost登陆（admin需要限制主机，不能从其他地点用admin用户名登陆数据库，保证安全）

（1）Insert



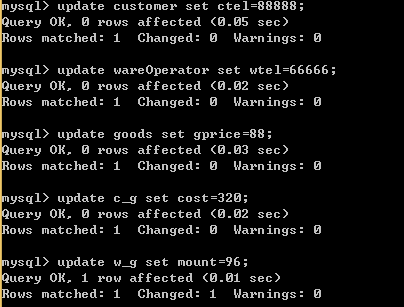
每个表都可以insert

（2）Select



每张表都可以select

(3)update



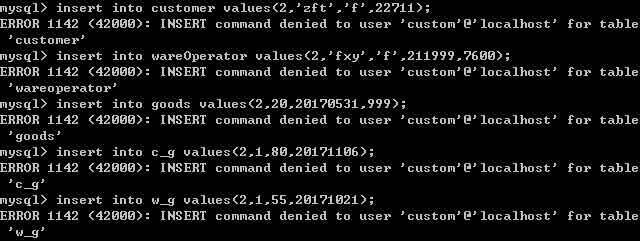
每张表都可以修改

（4）delete和alter都可以成功使用，这里就不再重复截图

2. 当前为custom在localhost登陆

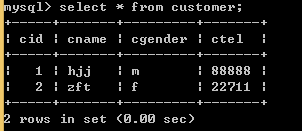
因为custom可以从任意主机访问（我设置的%），所以这里可以被访问。

（1）insert



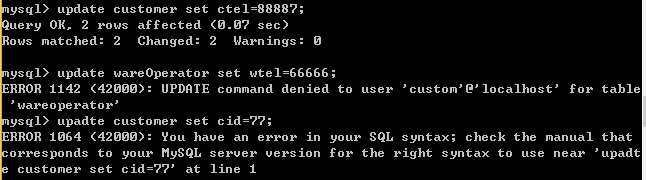
一个都不能insert，并不会给顾客任何插入权限。

(2)select



只能查询出customer的信息，其他的不能查询

(3)update

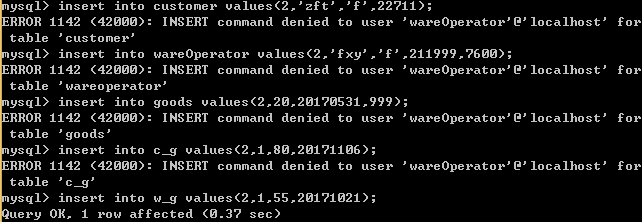


只能对customer的cname,cgender,ctel修改，不能对其他表，或对customer的cid修改。

（4）delete，alter什么的都不能进行，没有付给custom那么多的权限。

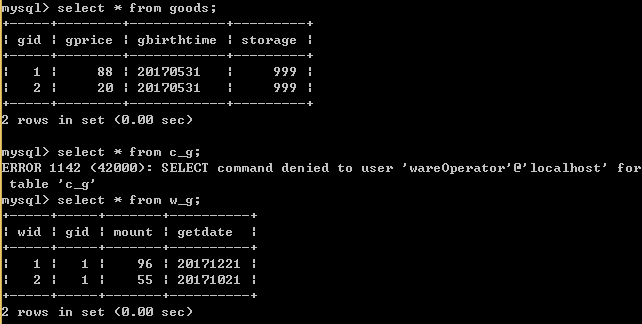
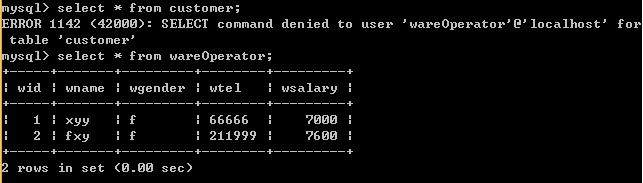
3. 当前为wareOperator在localhost登陆

（1）insert



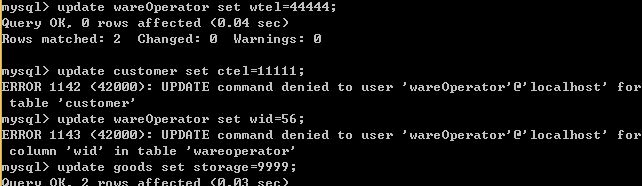
只有insert w\_g表的权限，因为库管有权添加物流信息。

(2)select



只能查询库管信息，商品信息，和物流信息。

(3)update



可以修改自己的信息和商品库存，其他不能修改。

(4)delete等都不能进行，没有相应权限。

**五、实验体会：**

这次实验的收获还是非常大的，其实在学习这门课之前，我也经常使用mysql数据库，但是从来没有考虑过安全权限的问题，甚至根本不知道mysql直接提供这种权限设置，在学习了本课程后，我发现了一篇安全的新大陆，mysql可以细粒度到列来进行权限的控制，会使自己的数据库变得更加的安全。

这次实验，我还了解到了mysql可以自己定义一些函数，虽然一开始函数总是出错，但是经过改进，最终我的入库函数好用了。在这其中，也掌握了删除函数等相关的函数操作语句。

总体来说，这次实验效果非常的好。

纵观整个系统安全实验，我觉得使我获益匪浅，这些实验都非常的有趣且有用，使我在安全方面懂得了更多，这些实验非常的棒！

**六、附录**

create table customer(

cid int,

cname varchar(50),

cgender varchar(10),

ctel varchar(20),

PRIMARY KEY (cid)

);

create table wareOperator(

wid int,

wname varchar(50),

wgender varchar(10),

wtel varchar(20),

wsalary int,

PRIMARY KEY (wid)

);

create table goods(

gid int,

gprice int,

gbirthtime varchar(50),

storage int,

PRIMARY KEY (gid)

);

create table c\_g(

cid int,

gid int,

cost int,

buydate varchar(50),

PRIMARY KEY (cid,gid)

);

create table w\_g(

wid int,

gid int,

mount int,

getdate varchar(50),

PRIMARY KEY (wid,gid)

);