实验四 数据库安全

- **实验目的**

1）熟悉通过 SQL 进行数据完整性控制的方法。
2）熟悉数据库中登录，用户，权限的概念和作用

- **实验内容**

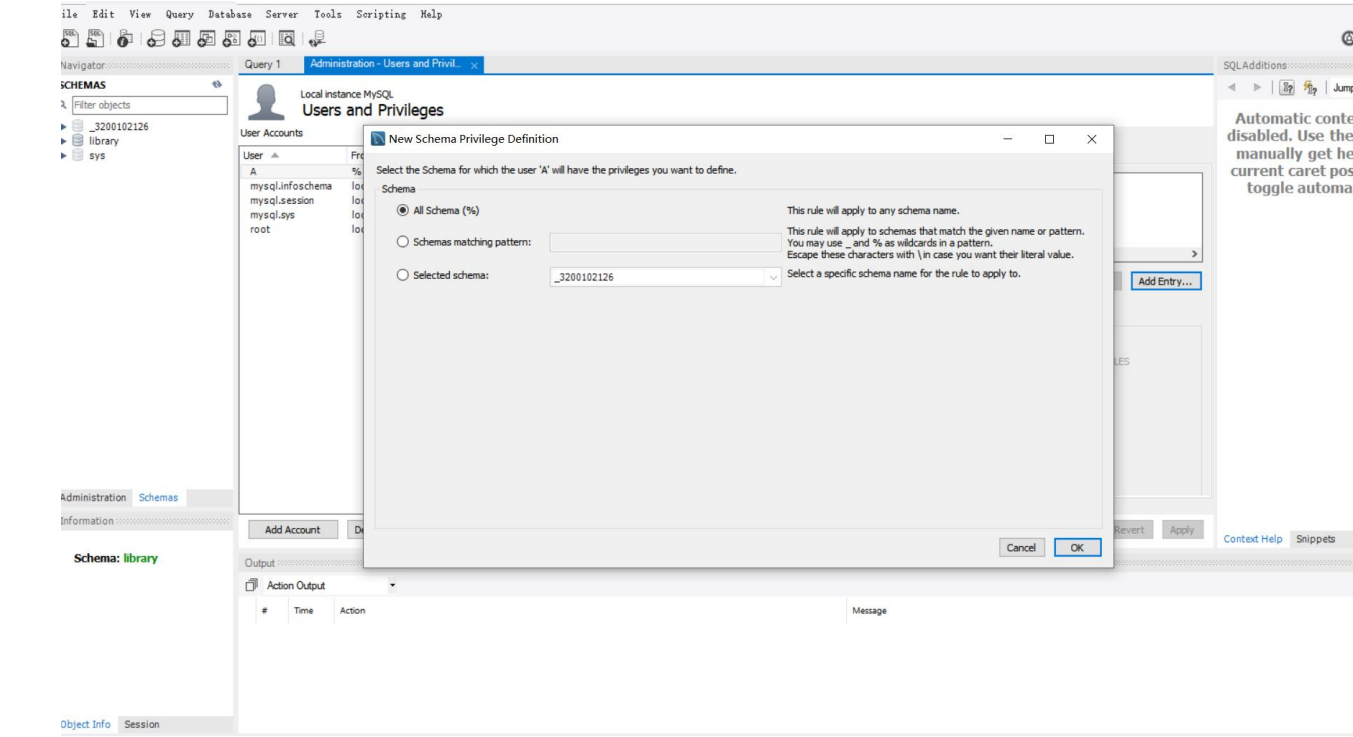
  - 建立表，考察表的生成者拥有该表的哪些权限。
  - 使用 SQL 的 grant 和 revoke 命令对其他用户进行授权和权力回收，考察相应的作用。
  - 建立视图，并把该视图的查询权限授予其他用户，考察通过视图进行权限控制的作用。
  - 建立新的角色，并为其赋予权限（create table，view，procedure 等），给用户添加角色
  - 完成实验报告。

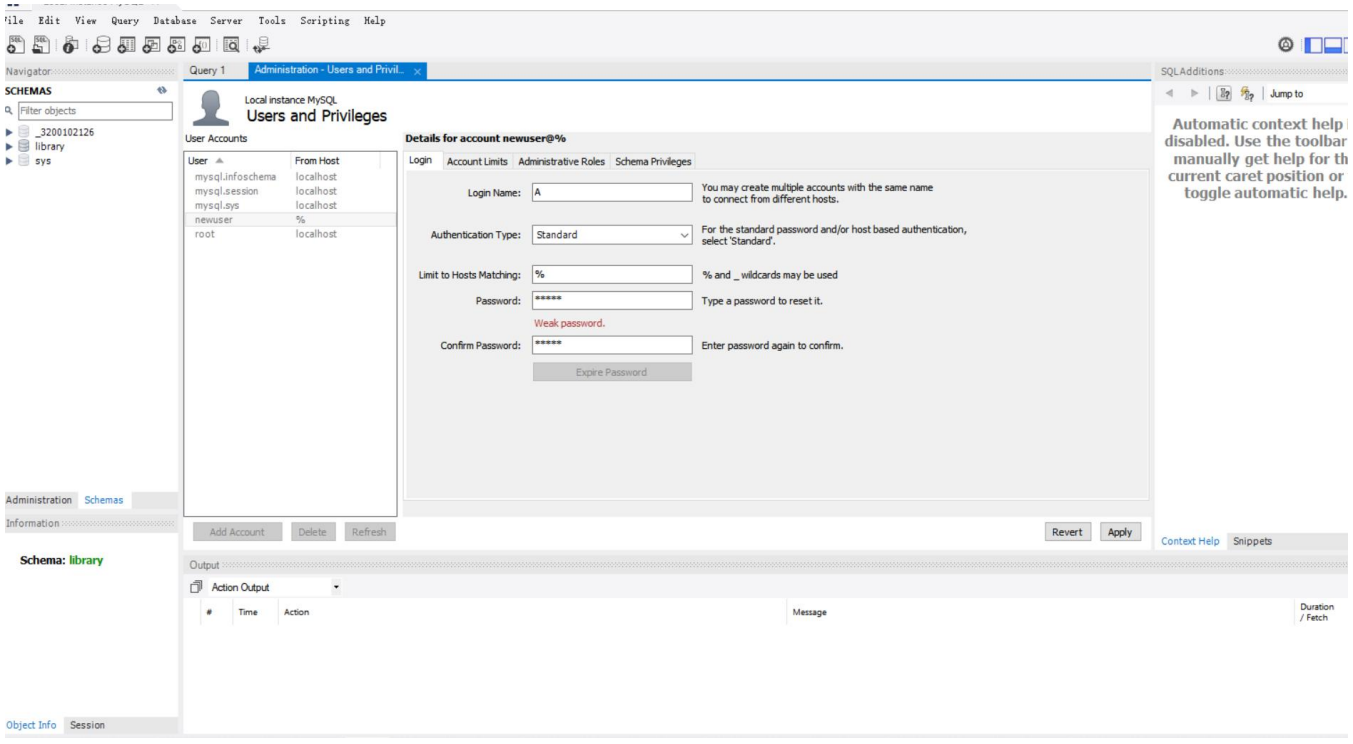
作业要求：本次作业可使用 sql 语句完成，也可直接图形化界面操作。请把实验过程截图。

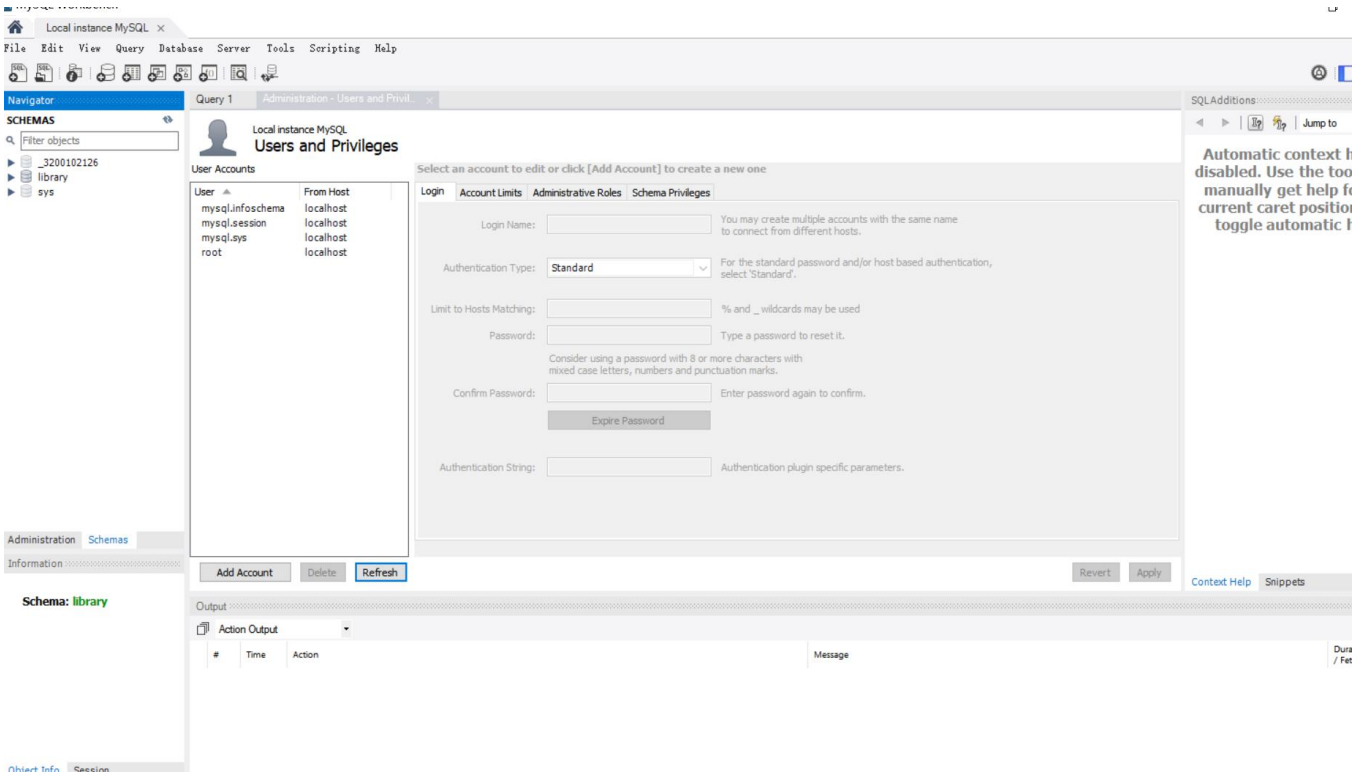
参考资料：
https://www.cnblogs.com/keme/p/10288168.html
https://www.cnblogs.com/xiao-lan-mao/p/6875423.html

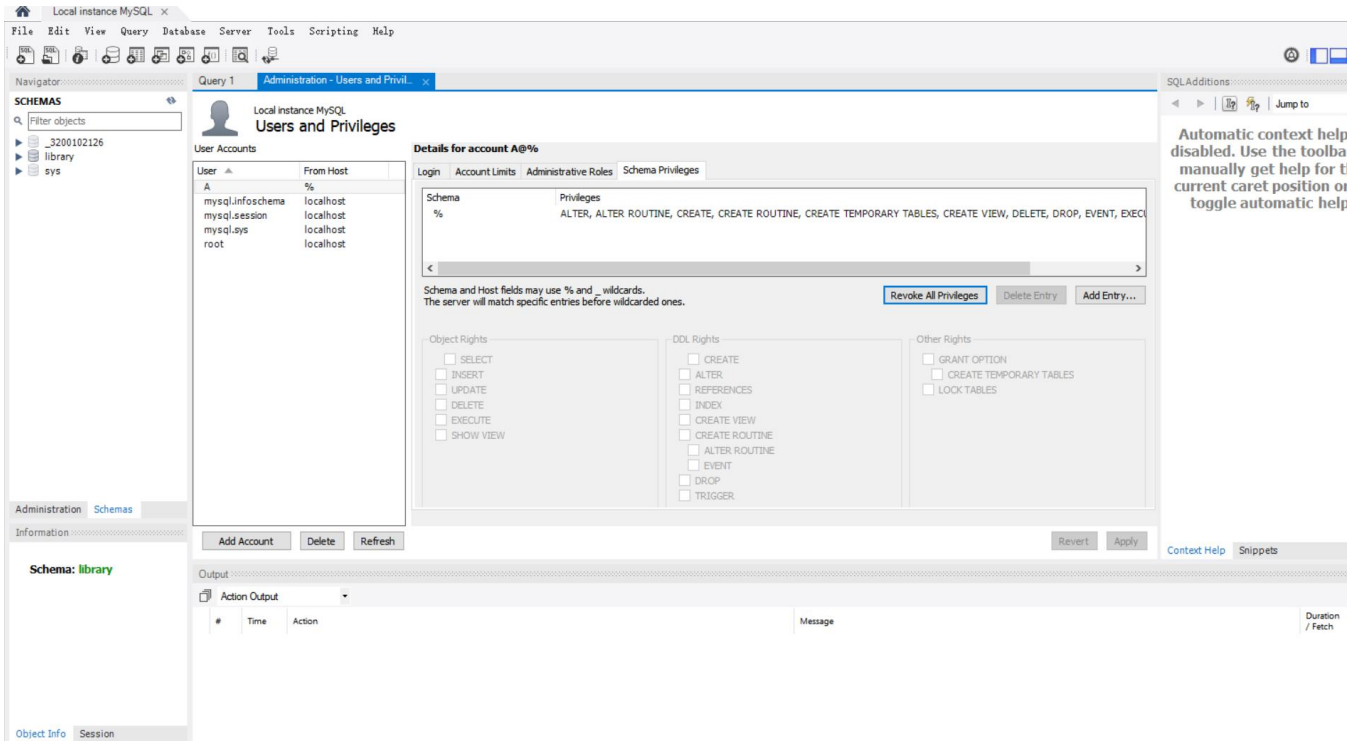
- **实验步骤**

1. 基于上一次实验的 library 数据库的 book 表。先用 root 账户登录，创建一个账户 A，并授予 A 在 library 数据库上的“All”和“grant option”权限。

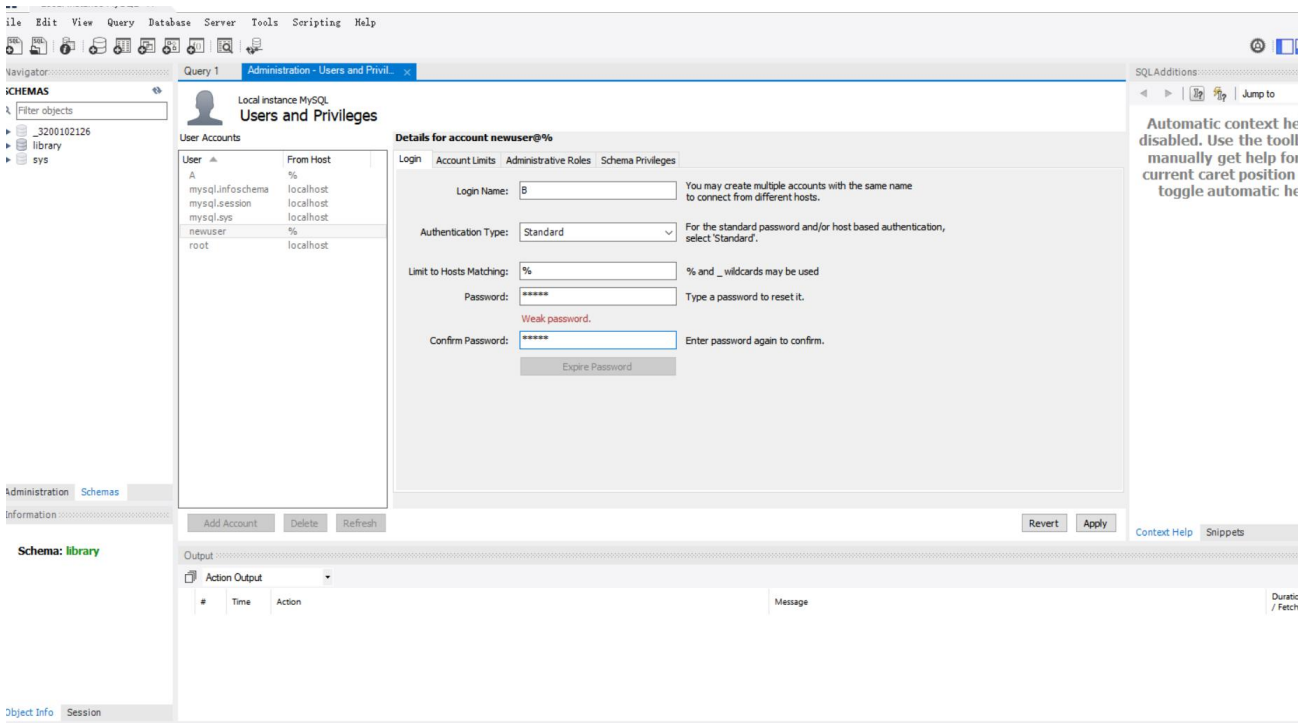

File Edit View Query Database Server Tools Scripting Help
Navigator
SCHEMAS
Filter objects
_3200102126
library
sys
Query 1
Administration - Users and Privil...
Local instance MySQL
Users and Privileges
User Accounts
User
A
mysql.infoschema
mysql.session
mysql.sys
root
New Schema Privilege Definition
Select the Schema for which the user 'A' will have the privileges you want to define.
Schema
All Schema (%)
This rule will apply to any schema name.
Schemas matching pattern:
This rule will apply to schemas that match the given name or pattern.
You may use _ and % as wildcards in a pattern.
Escape these characters with \ in case you want their literal value.
Selected schema:
_3200102126
Select a specific schema name for the rule to apply to.
Cancel
OK
Add Account
Add Entry...
Revert
Apply
Administration
Schemas
Information
Schema: library
Object Info
Session
Output
Action Output
#
Time
Action
Message
SQLAdditions
Automatic conte
disabled. Use the
manually get he
current caret pos
toggle automa
Context Help
Snippets

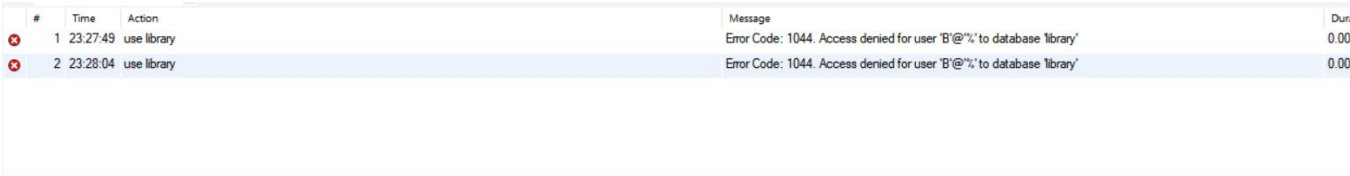

File Edit View Query Database Server Tools Scripting Help
Navigator
SCHEMAS
Filter objects
_3200102126
library
sys
Query 1
Administration - Users and Privil...
Local instance MySQL
Users and Privileges
User Accounts
User
From Host
mysql.infoschema
localhost
mysql.session
localhost
mysql.sys
localhost
newuser
%
root
localhost
Details for account newuser@%
Login
Account Limits
Administrative Roles
Schema Privileges
Login Name:
A
You may create multiple accounts with the same name
to connect from different hosts.
Authentication Type:
Standard
For the standard password and/or host based authentication,
select 'Standard'.
Limit to Hosts Matching:
%
% and _ wildcards may be used
Password:
Type a password to reset it.
Weak password.
Confirm Password:
Enter password again to confirm.
Expire Password
Add Account
Delete
Refresh
Revert
Apply
Administration
Schemas
Information
Schema: library
Object Info
Session
Output
Action Output
#
Time
Action
Message
Duration / Fetch
SQLAdditions
Jump to
Automatic context help
disabled. Use the toolbar
manually get help for th
current caret position or
toggle automatic help.
Context Help
Snippets





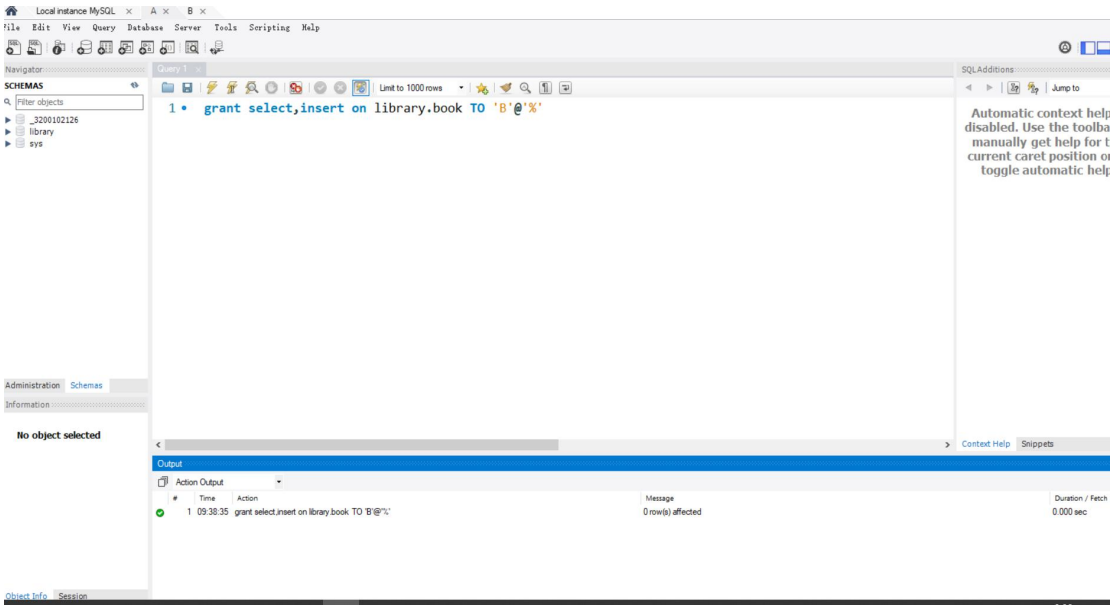
2. 创建 B，不授予权限。以账户 B 登录，测试 B 能否对 book 表进行 CRUD（增、删、改、查）操作。



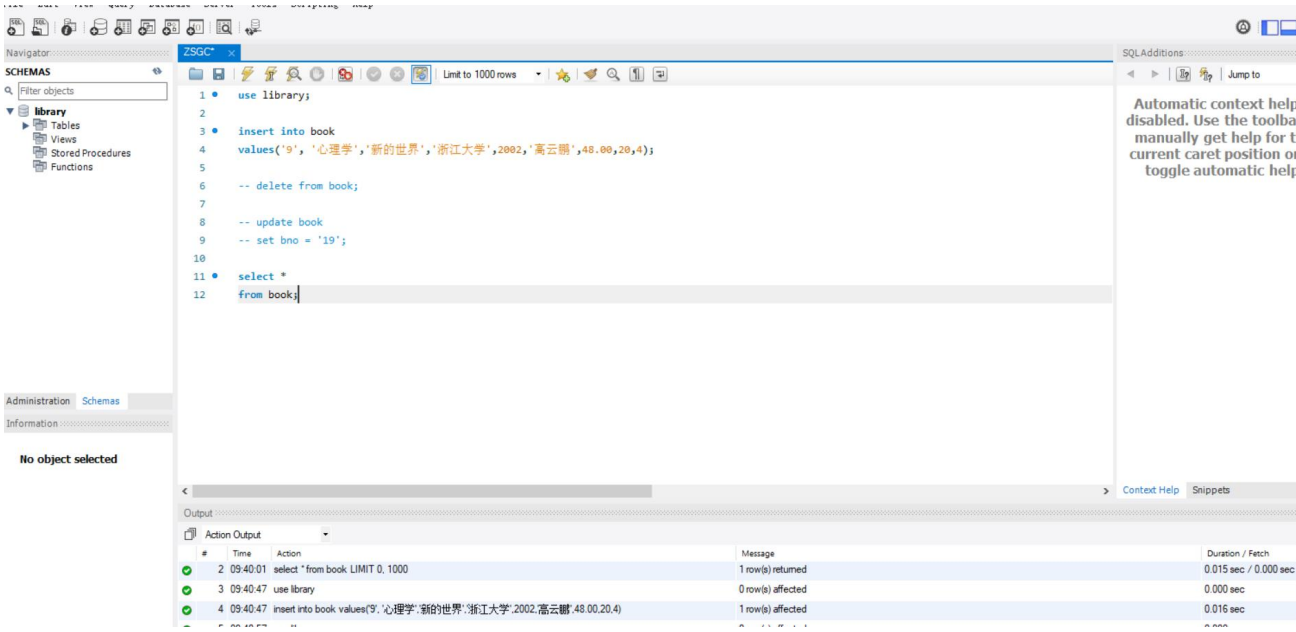


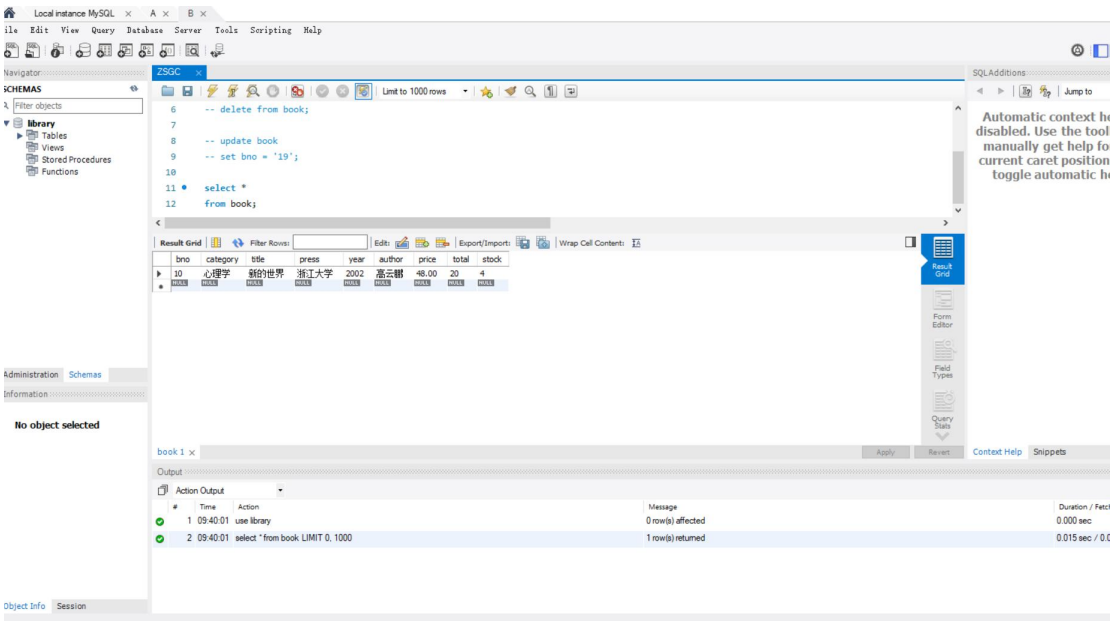
无法进行任何操作

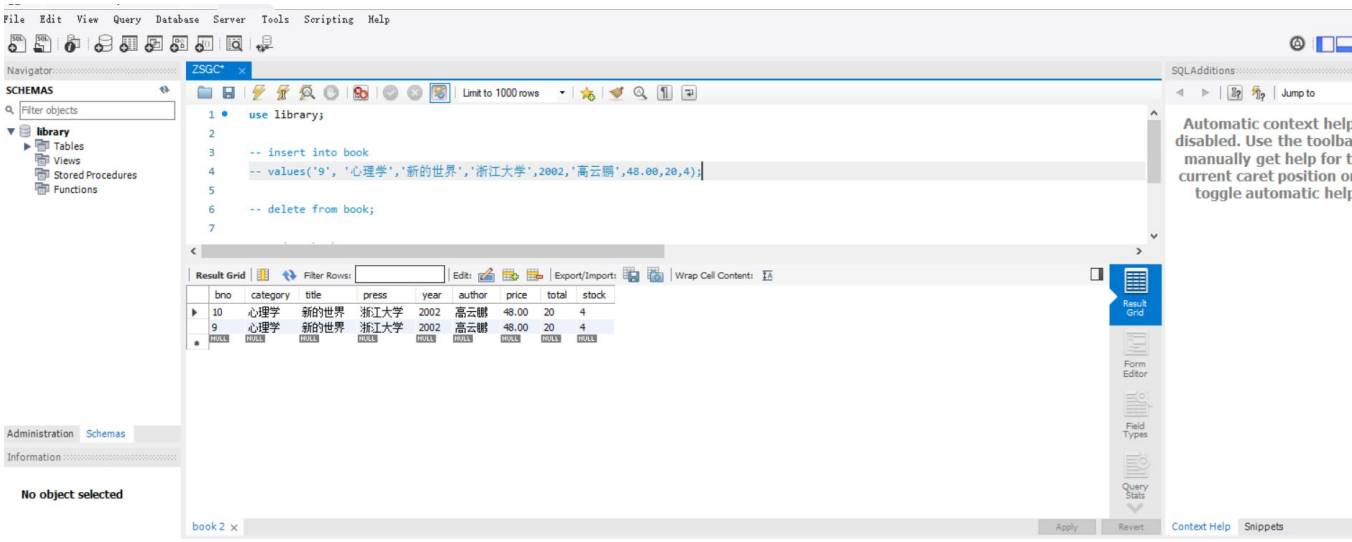
3. 用 A 登录，利用 grant 语句赋给 B 对于 Book 表的查询和插入的权限。



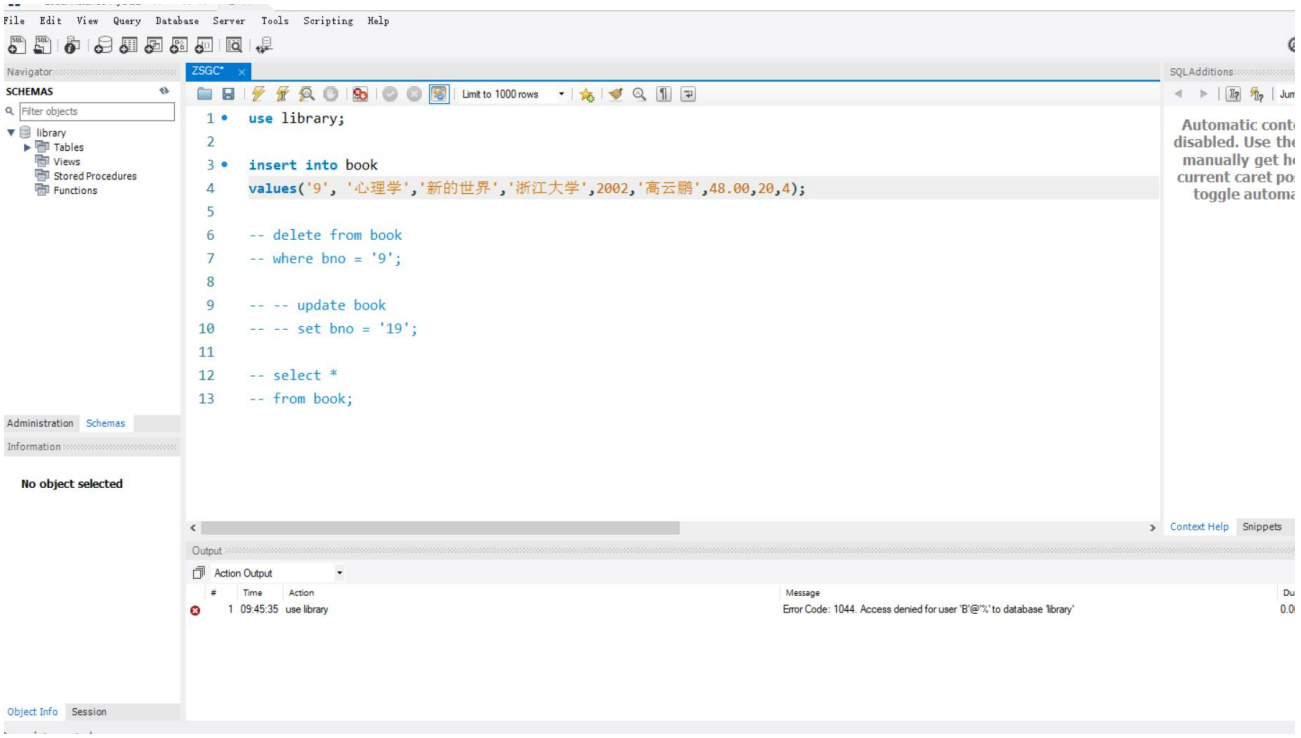
4. 用 B 登录测试是否具有相应的权限。

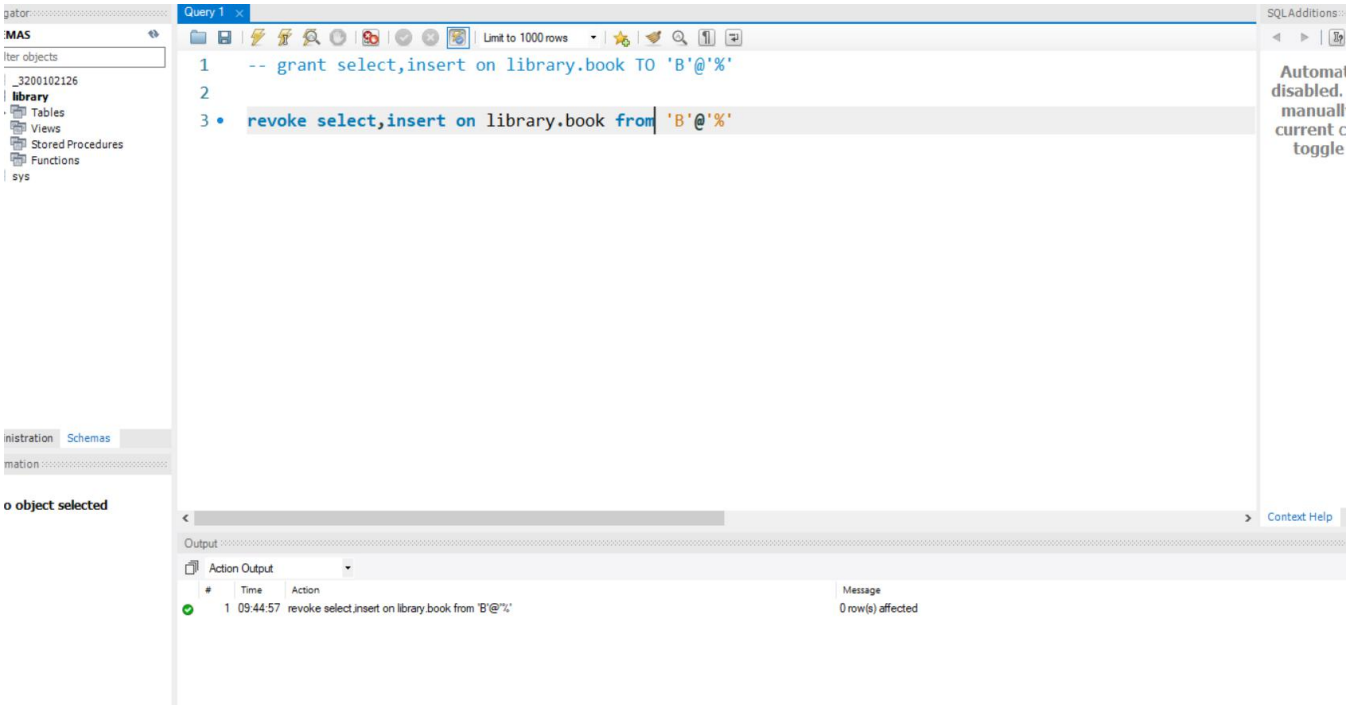

use library;
insert into book
values('9', '心理学','新的世界','浙江大学',2002,'高云鹏',48.00,20,4);
-- delete from book;
-- update book
-- set bno = '19';
select *
from book;
No object selected
1 row(s) returned
0 row(s) affected
0.015 sec / 0.000 sec
0.000 sec
0.016 sec

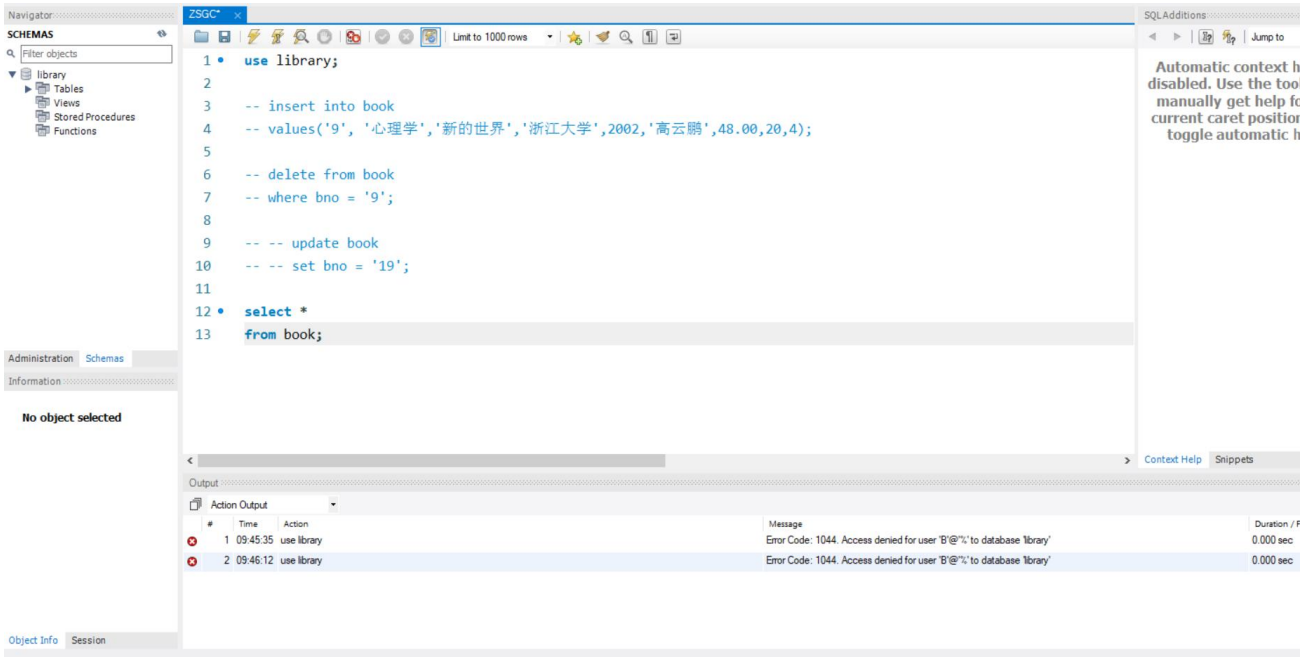

No object selected
0 row(s) affected
1 row(s) returned
0.000 sec
0.015 sec


use library;
-- insert into book
-- values('9', '心理学','新的世界','浙江大学',2002,'高云鹏',48.00,20,4);
-- delete from book;
No object selected

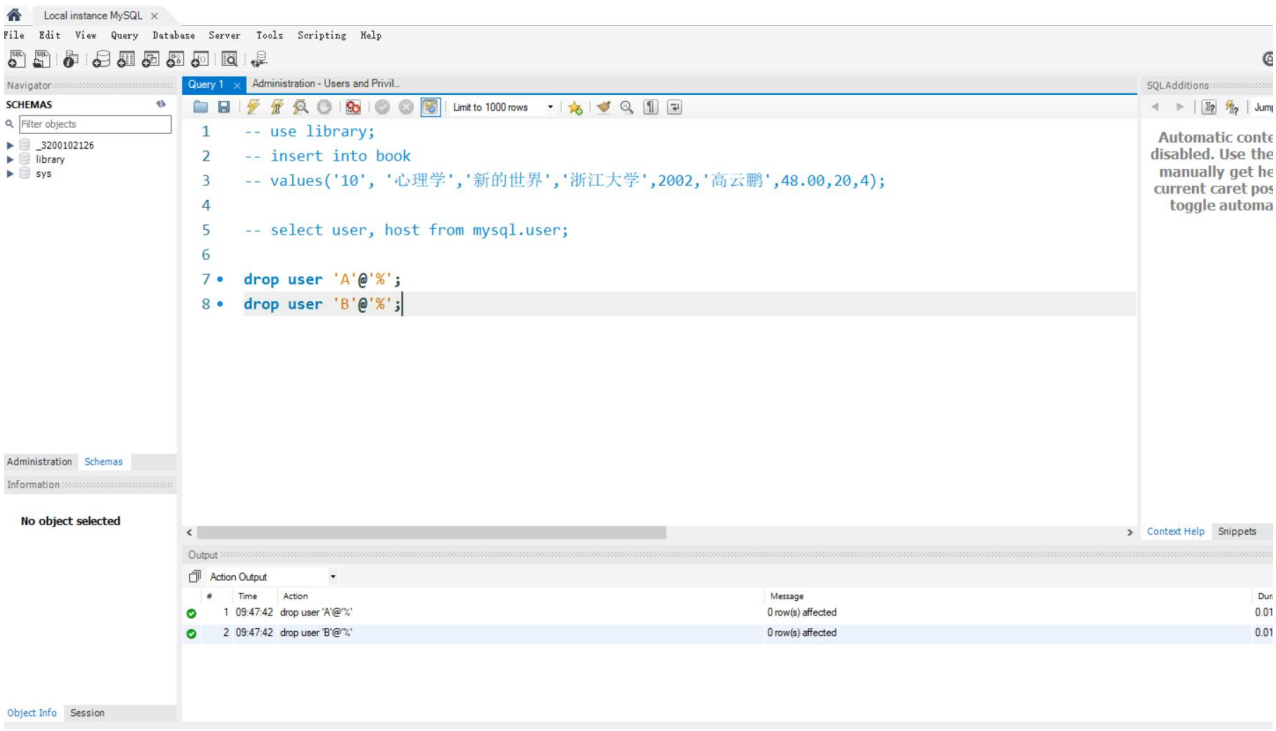
5. 用 A 登录，利用 revoke 语句收回 B 的 book 表的操作权限，再登录 B 测试 B 是否有相应权限。


File Edit View Query Database Server Tools Scripting Help
Navigator
SCHEMAS
Filter objects
library
Tables
Views
Stored Procedures
Functions
ZSGC*
Limit to 1000 rows
1 use library;
3 insert into book
4 values('9', '心理学','新的世界','浙江大学',2002,'高云鹏',48.00,20,4);
6 -- delete from book
7 -- where bno = '9';
9 -- -- update book
10 -- -- set bno = '19';
12 -- select *
13 -- from book;
SQL Additions
Automatic cont
disabled. Use the
manually get h
current caret po
toggle automa
Administration Schemas
Information
No object selected
Context Help Snippets
Output
Action Output
Time Action Message
1 09:45:35 use library Error Code: 1044. Access denied for user 'B'@'%' to database 'library'
Object Info Session


Query 1
Limit to 1000 rows
1 -- grant select,insert on library.book TO 'B'@'%'
3 revoke select,insert on library.book from 'B'@'%'
SQL Additions
Automat
disabled.
manuall
current c
toggle
_3200102126
library
Tables
Views
Stored Procedures
Functions
sys
Schemas
o object selected
Context Help
Output
Action Output
Time Action Message
1 09:44:57 revoke select,insert on library.book from 'B'@'%' 0 row(s) affected



6. 用 root 登录数据库，删除账户 A 和账户 B。



7. 实验总结及思考

本次实验主要是进行用户权限相关的操作，用户权限在数据库中是一个非常重要的部分，涉及到数据库的安全问题，对于不同用户给与不同的权限也是一个非常现实的问题。Mysql 对权限的划分主要是从全部，数据库，表几个层级进行划分的，在数据库和表中又有不同的操作权限，比如在给表进行权限管理的时候就需要注明究竟是哪些操作（select, insert, update, delete 等），同时也需要注明是

对哪些数据库的权限。当然仅仅是实验中的一系列操作还是不够的，在进行权限分配的时候还有更多需要细化的地方。