

# 数据库课程实验日志

学号	201726010211	姓名	陈汉轩	专业年级班级	数媒 1701
实验日期	2020. 5. 5	实验项目	安全性语言		

## 目录

数据库课程实验日志.....	1
一、实验目的 .....	1
二、实验过程&错误 .....	1
内容（一）：自主存取控制实验.....	1
内容（二）：审计实验 .....	11
三、实验重难点.....	15
四、实验心得体会 .....	15

## 一、实验目的

安全性实验包含两个实验项目(参见表 4.3)，其中 1 个为必修，1 个为选修。自主存取控制实验为设计型实验项目，审计实验为验证型实验项目。

## 二、实验过程&错误

### 内容（一）：自主存取控制实验

采用方案一：即采用 **SYSTEM** 超级用户登录数据库，完成所有权限分配工作，然后用相应用户名登陆数据库以验证权限分配正确性；

步骤 1： 创建一个管理员账号 `admin_testdb`

保存

查询创建工具

美化 SQL

代码版

toor

运行

停止

解释

1 create user 'admin\_testdb'@'localhost' IDENTIFIED BY 'admin';

信息

剖析

状态

create user 'admin\_testdb'@'localhost' IDENTIFIED BY 'admin'  
> OK  
> 时间: 0.015s

对象

\* 无标题 - 查询

\* 无标题 - 查询

编辑用户

新建用户

删除用户

权限管理员

admin@%

admin\_testdb@localhost

mysql.infoschema@localhost

mysql.session@localhost

mysql.sys@localhost

root@localhost

步骤 2: 查看 admin\_testdb 的账户权限

对象 | \* 无标题 - 查询 | \* 无标题 - 查询

保存 | 查询创建工具 | 美化 SQL | 代码段 | 文本 | 导出结果

toor | 运行 | 停止 | 解释

```
1 show grants for 'admin_testdb'@'localhost';
```

信息 | 结果 1 | 剖析 | 状态

Grants for admin\_testdb@localhost

▶ GRANT USAGE ON \*.\* TO 'admin\_testdb'@'localhost'

步骤 3: 使用 root 账户给用户 admin\_testdb 赋予权限

对象 | \* 无标题 - 查询 | \* 无标题 - 查询

保存 | 查询创建工具 | 美化 SQL | 代码段

toor | 运行 | 停止 | >>

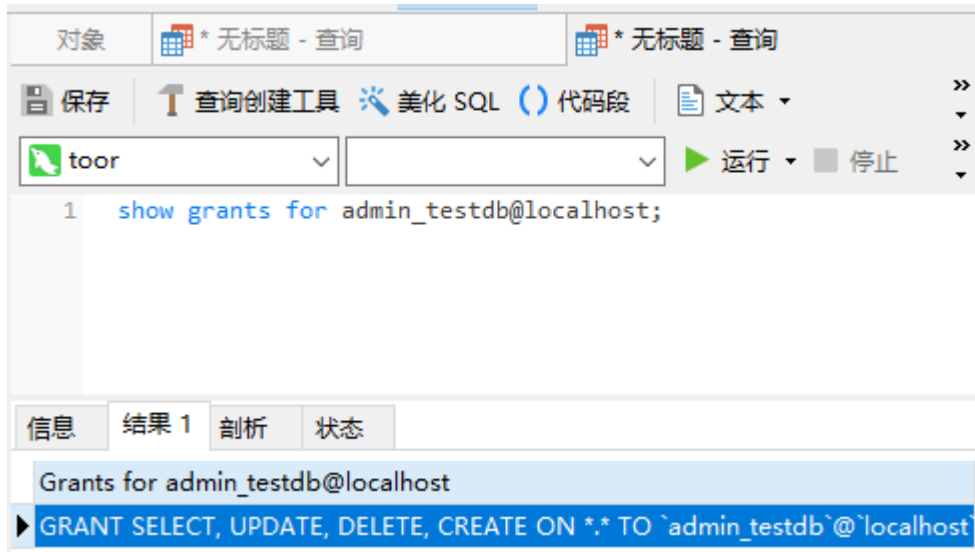
```
1 grant select, delete, update, create on *.* to 'admin_testdb'@localhost;
```

信息 | 剖析 | 状态

```
grant select, delete, update, create on *.* to 'admin_testdb'@localhost
> Affected rows: 0
> 时间: 0.011s
```

赋予的权限为: select,delete,update,create

步骤 4: 再次查看 admin\_testdb 的权限



步骤 5: 登录 admin\_testdb 账户验证权限

MySQL - 新建连接

常规高级数据库SSLSSHHTTP

  
Navicat

  
数据库

连接名:

admin\_testdb

主机:

localhost

端口:

3306

用户名:

admin\_testdb

密码:

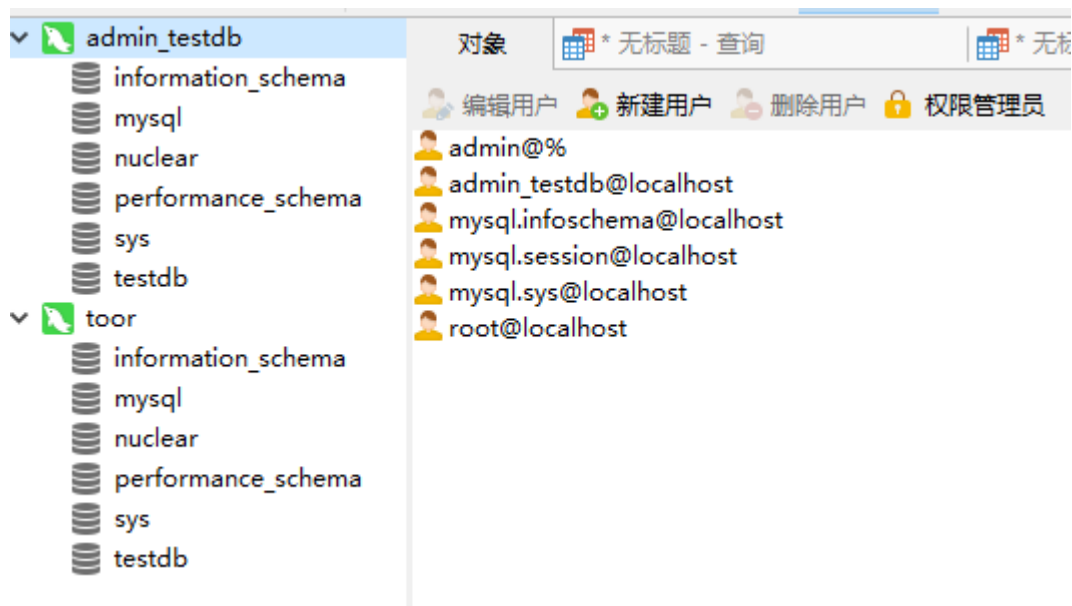
•••••

☒ 保存密码

测试连接

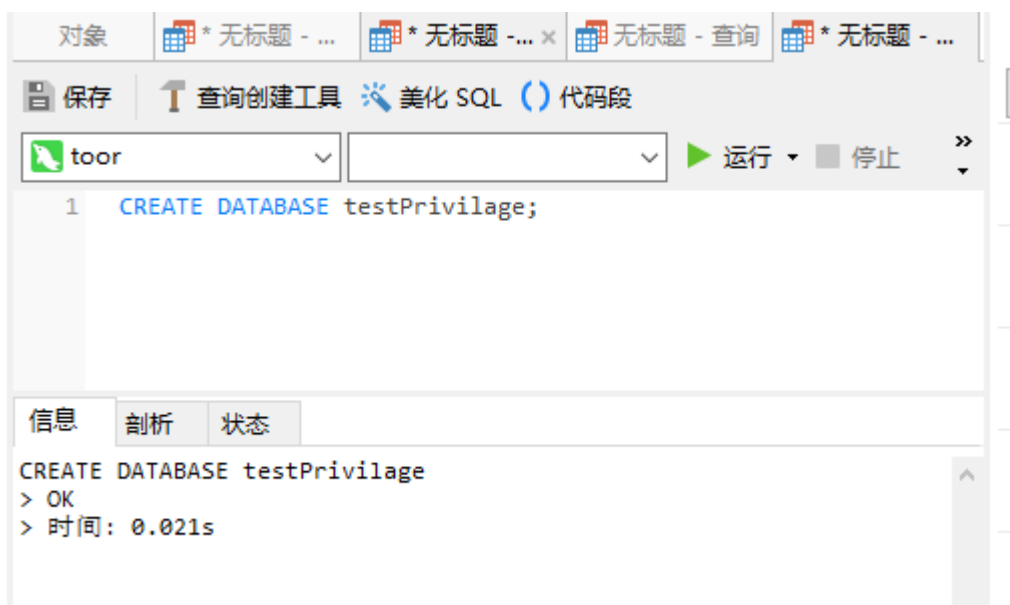
确定

取消



现在 root 和 admin\_testdb 同时连接到了数据库。

步骤 6: 使用 root 账户创建一个新的数据库。



步骤 7: 使用 admin 账户尝试 drop 这个账户。



可以看到请求被拒绝，之前没有给 `drop` 权限所以这里无法使用 `drop`。


步骤 8: 验证给 `admin` 账户分配的权限

information_schema	开始事务	文本	筛选
mysql	num	id	
nuclear	42	0	
performance_schema	42	1	
sys	42	2	
testdb	42	3	
表	42	4	
course	42	5	
dept	42	6	
dept_age	42	7	
sc	42	8	
student	42	9	
test_index	42	10	
视图	42	11	
函数	42	12	
查询	42	13	
备份	42	14	
testprivilage	42	15	
toor	42	16	
information_schema	42	17	
mysql	42	18	
nuclear	42	19	
performance_schema	42	20	
sys			
testdb			

删除 test\_index 表中的 id=0 的数据：



 保存

 查询创建工具


 美化 SQL


 代码段

 admin\_testdb

 testdb

 运行

 停止

 解释

```
1 delete from test_index where id=0;
```

信息

剖析

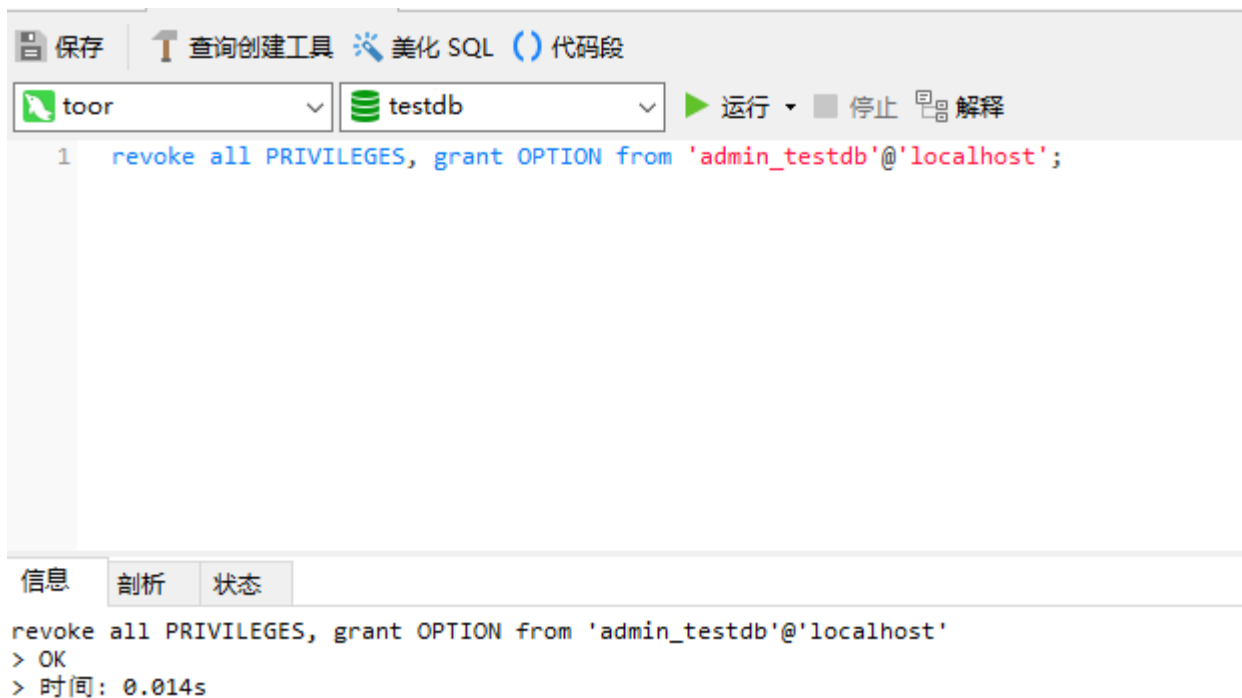
状态

```
delete from test_index where id=0
> Affected rows: 1
> 时间: 0.17s
```

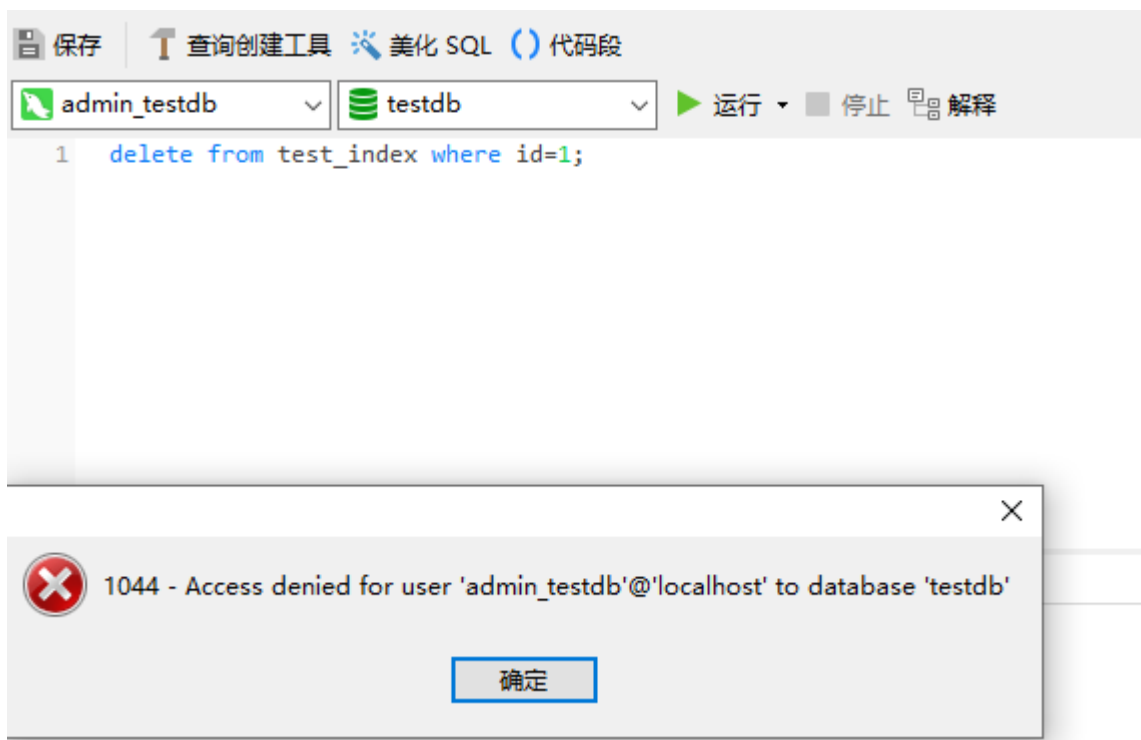
可以看到数据已经丢失:

连接	新建查询	表	视图	函数	用户
admin_testdb		对象	* 无标题 - 查询	* 无标题 -	
information_schema		开始事务	文本	筛选	排序
mysql		num	id		
nuclear		42	1		
performance_schema		42	2		
sys		42	3		
testdb		42	4		
表		42	5		
course		42	6		
dept		42	7		
dept_age		42	8		
sc		42	9		
student		42	10		
test_index		42	11		
视图		42	12		
函数		42	13		
查询		42	14		
备份		42	15		
testprivilege		42	16		
toor		42	17		
information_schema		42	18		
mysql		42	19		
nuclear		42	20		
performance_schema		42	21		
sys		42	22		
testdb		42	23		
表					
视图					
函数					

步骤 9: 回收权限



步骤 10: admin 账户再次尝试删除操作



访问被拒绝。

## 内容（二）：审计实验

网上的插件都是基于 5.7 版本的，由于我使用的是最新版 8.21 所以不是使用插件，而是使用 mysql8.x 提供的 general log 来实现审计功能。

mysql 本身并没有操作审计的功能，需要采用 general log 方法记录 sql 操作。

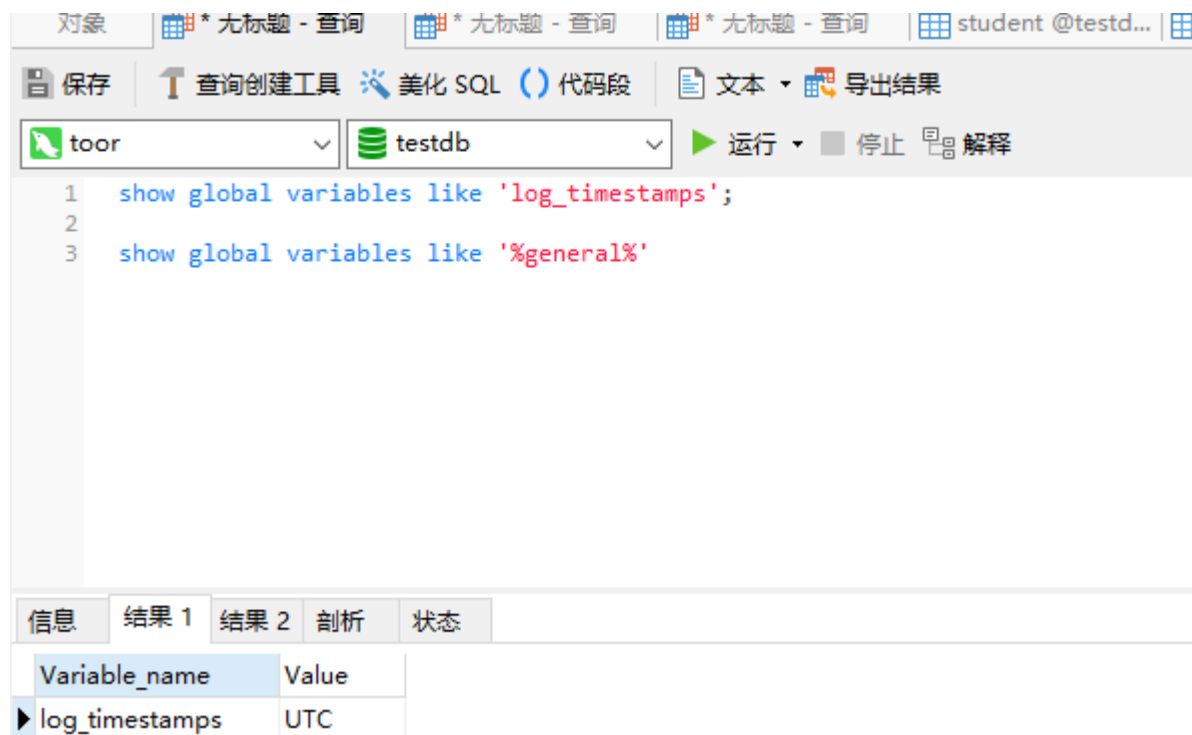
但是开启它有以下几个缺点

无论 sql 有无语法错误，只要执行了就会记录，导致记录大量无用信息，后期的筛选有难度。

sql 并发量很大时，log 的记录会对 io 造成一定的印象，是数据库效率降低。

日志文件很容易快速膨胀，不妥善处理会对磁盘空间造成一定影响。

步骤 1：查询审计配置情况



The screenshot shows a MySQL query tool interface. The top toolbar includes buttons for '保存' (Save), '查询创建工具' (Query Creation Tool), '美化 SQL' (Format SQL), '代码段' (Code Snippets), '文本' (Text), and '导出结果' (Export Results). Below the toolbar, there are dropdown menus for '对象' (Object) set to 'toor' and '数据库' (Database) set to 'testdb'. The main query area contains the following SQL commands:

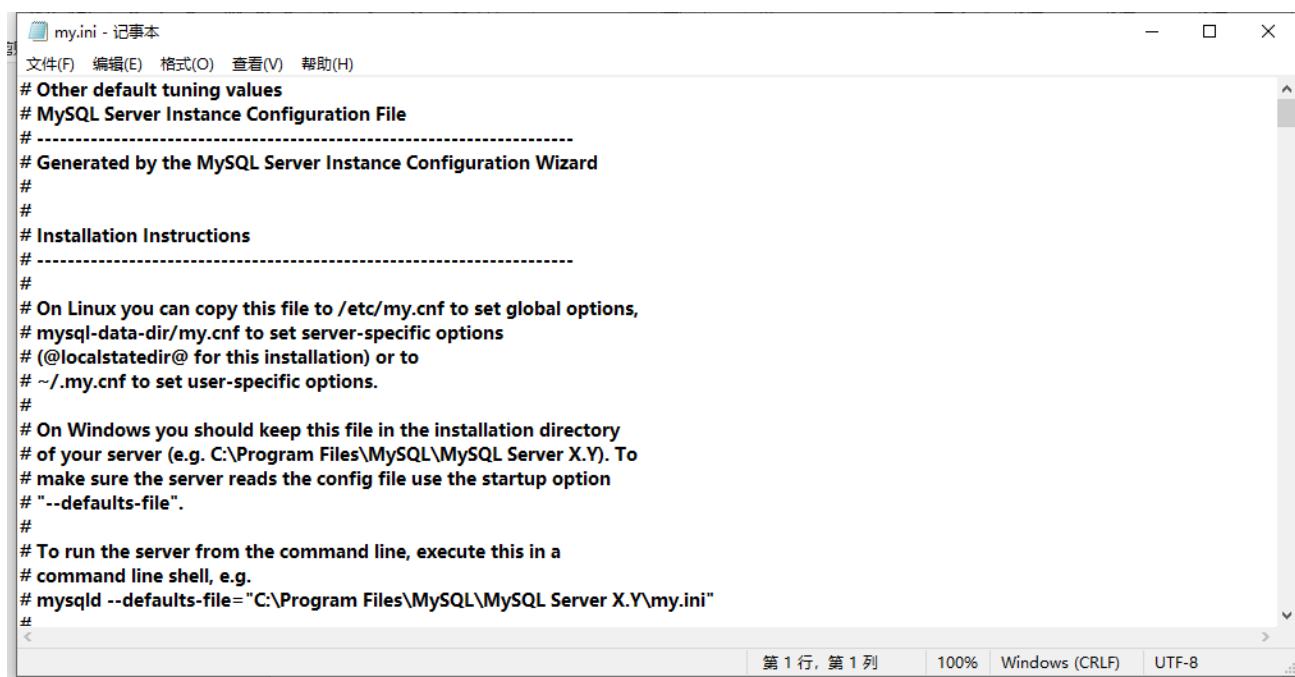
```
1 show global variables like 'log_timestamps';
2
3 show global variables like '%general%'
```

At the bottom, there is a tabbed interface with '信息' (Info), '结果 1' (Result 1), '结果 2' (Result 2), '剖析' (Analyze), and '状态' (Status). The '结果 1' tab is active, displaying a table with the following data:

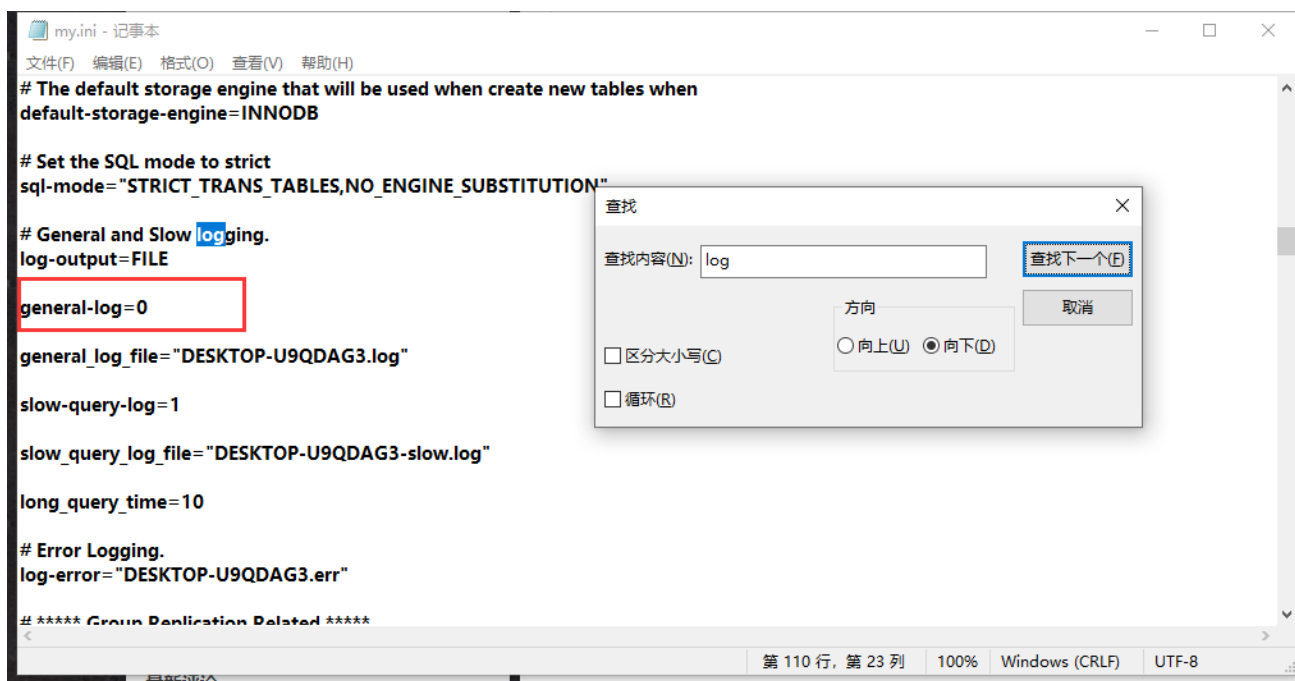
Variable_name	Value
log_timestamps	UTC

步骤 2：找到 mysql 的配置文件路径

```
C:\Program Files\MySQL\MySQL Server 8.0\bin\mysql.exe"
"--defaults-file=C:\ProgramData\MySQL\MySQL Server 8.0\my.ini
```



### 步骤 3: 修改配置文件



可以看到目前 log 没有打开。

### 步骤 4: 修改配置文件，打开审计功能。

```
my.ini - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

# The default authentication plugin to be used when connecting to the server
default_authentication_plugin=caching_sha2_password

# The default storage engine that will be used when create new tables when
default-storage-engine=INNODB

# Set the SQL mode to strict
sql-mode="STRICT_TRANS_TABLES,NO_ENGINE_SUBSTITUTION"

# General and Slow logging.
log-output=FILE

# general-log=0
general-log=1

# general_log_file="DESKTOP-U9QDAG3.log"
general_log_file="C:/Users/Administrator/Desktop/DESKTOP-U9QDAG3.log"

slow-query-log=1

slow_query_log_file="DESKTOP-U9QDAG3-slow.log"

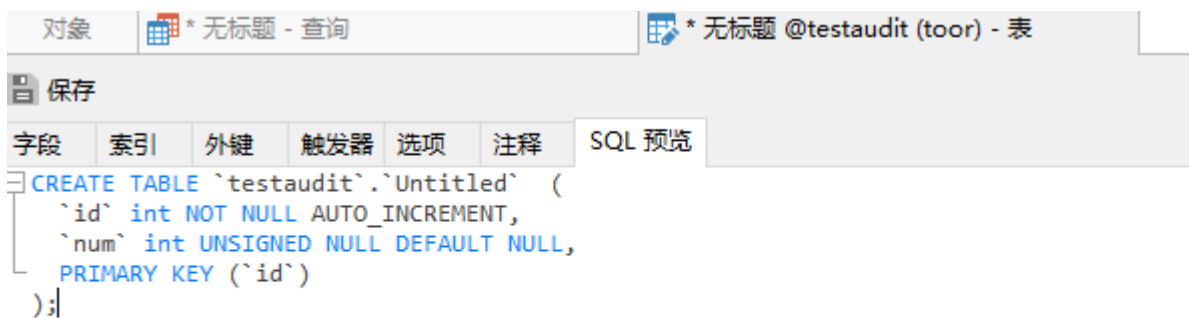
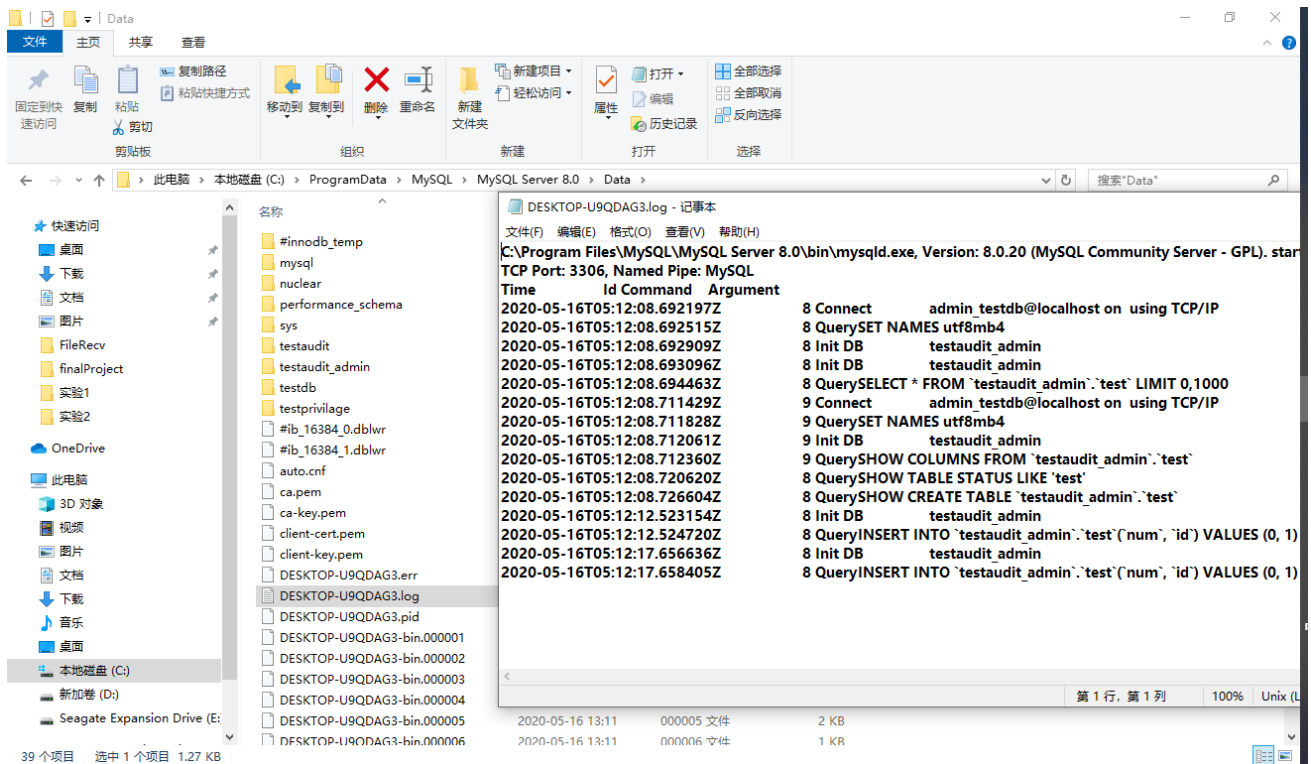
long_query_time=10

第 117 行, 第 50 列 100% Windows (CRLF) UTF-8
```

步骤 5: 重新启动 mysql 服务

服务					
MySQL80					
<a href="#">停止</a> 此服务 <a href="#">暂停</a> 此服务 <a href="#">重新启动</a> 此服务					
名称	描述	状态	启动类型	登录为	
Microsoft Passport	为用...		手动(触发...	本地系统	
Microsoft Passport Cont...	管理...	正在...	手动(触发...	本地服务	
Microsoft Software Shad...	管理...		手动	本地系统	
Microsoft Storage Space...	Micr...		手动	网络服务	
Microsoft Store 安装服务	为 M...	正在...	手动	本地系统	
Microsoft Windows SMS ...	根据...		手动(触发...	本地服务	
MS-MPI Launch Service	Servi...		禁用	本地系统	
MySQL80		正在...	自动	网络服务	
Net.Tcp Port Sharing Ser...	提供...		禁用	本地服务	
Netlogon	为用...		手动	本地系统	
Network Connected Devi...	网络...		手动(触发...	本地服务	
Network Connection Bro...	允许 ...	正在...	手动(触发...	本地系统	
Network Connections	管理...	正在...	手动	本地系统	
Network Connectivity Ass...	提供 ...		手动(触发...	本地系统	
Network Information Ma...			手动	本地系统	

步骤 5: 查看 log 日志，确定开启了审计功能



可以看到，审计服务开启成功。

### 三、实验重难点

如何创建用户并管理用户权限，如何在 MySQL 中使用审计功能。

### 四、实验心得体会

学习了如何创立用户以及 SQL 授权语句，收回授权语句和查看授权，授权传递如何制作一个审计功能。