

实验4 SQL安全性

实验目的：

1.熟悉通过SQL进行数据完整性控制的方法。

实验平台：

1.数据库管理系统：MySQL

实验内容和要求：

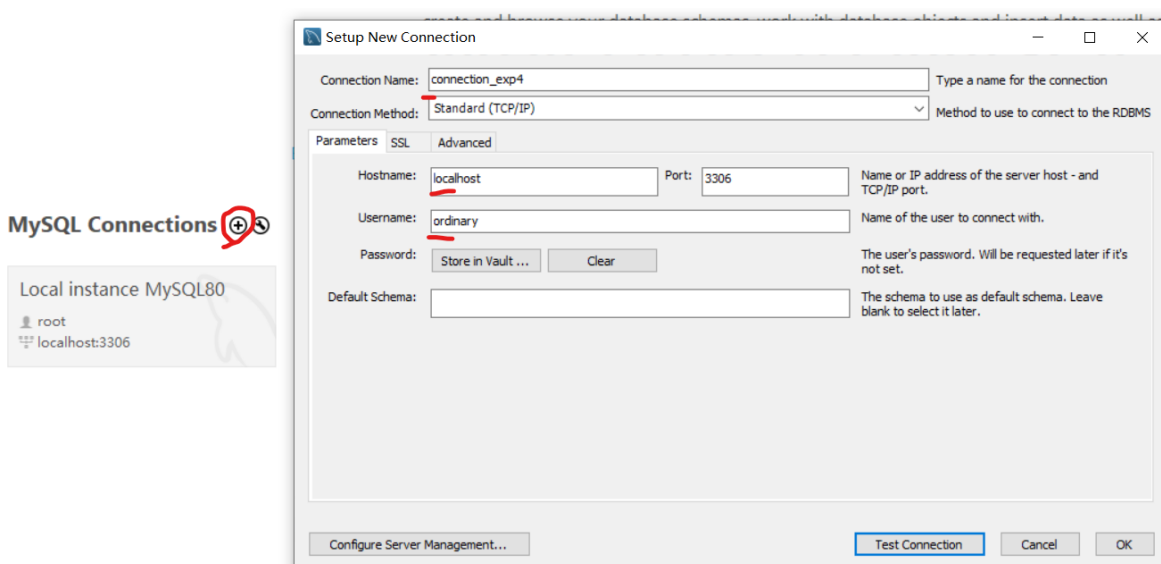
- 1.建立表，考察表的生成者拥有该表的哪些权限。
- 2.使用SQL的grant和revoke命令对其他用户进行授权和权力回收，考察相应的作用。
- 3.建立视图，并把该视图的查询权限授予其他用户，考察通过视图进行权限控制的作用。

实验过程：

1. 建立普通用户并连接。

```
1 #利用root用户建立普通用户，在root连接中执行如下代码
2 #语法: CREATE USER <user_name>@<host_name> identified BY
   <password>;
3 CREATE USER 'ordinary'@'localhost' IDENTIFIED BY '000000';
```

连接



从左边空空如也的schema界面就可以看出新建的普通用户无法访问root的数据库。



回到root用户的连接页面，为该普通用户授权。

- 1 #语法: GRANT priv_type ON [object_type] TO user;
- 2 GRANT select ON testyh.department TO 'ordinary'@'localhost';
- 3 #将数据库testyh的department表的选择权限向普通用户开放。

查看ordinary@localhost的权限

- 1 show grants for 'ordinary'@'localhost';#可用root查询也可用普通用户自身

	Grants for ordinary@localhost
▶	GRANT USAGE ON *.* TO `ordinary`@`localhost`
	GRANT SELECT ON `testyh`.`department` TO `ordinary`@`localhost`

查看一下哪些用户有哪些在表department上的权限：

```
1 | select * from mysql.tables_priv where table_name='department';#  
只能用root查询
```

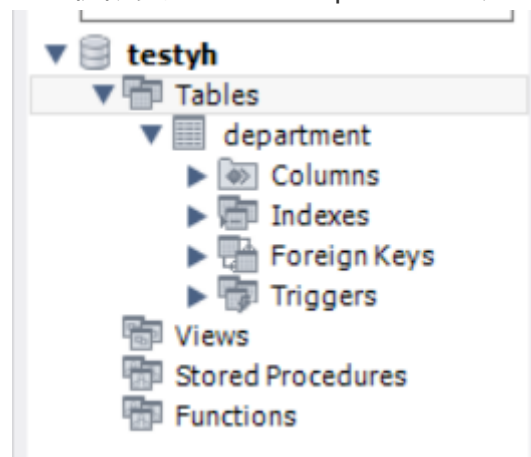
	Host	Db	User	Table_name	Grantor	Timestamp	Table_priv	Column_priv
▶	localhost	testyh	ordinary	department	root@localhost	2022-04-05 22:29:01	Select	
*	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

利用普通用户查询department表。

```
1 | use testyh;  
2 | select * from department;
```

	dept_name	building	budget
▶	Finance	Painter	120000.00
	History	Painter	50000.00
	Music	Packard	80000.00
	Physics	Watson	50000.00
*	NULL	NULL	NULL

从侧边栏的变化也可看出权限变化。有了department表但仍无student表。



收回权限

```
1 | #语法: REVOKE priv_type ON [object_type] FROM user  
2 | REVOKE select ON testyh.department FROM 'ordinary'@'localhost';
```

再次从普通用户处查询，出现错误信息。

22:40:29 select * from department LIMIT 0, 1000 Error Code: 1142. SELECT command denied to user 'ordinary'@'localhost' for table 'department' 0.000 sec

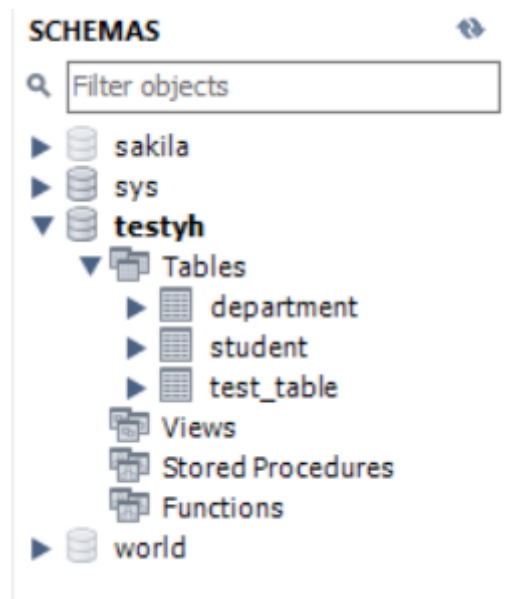
2. 建立表，考察表的生成者拥有该表的哪些权限。

```

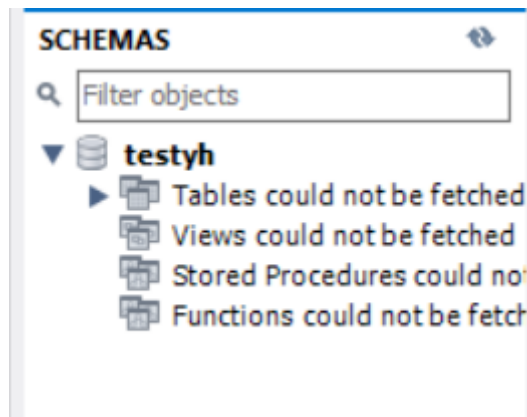
1  #为普通用户授予建表的权限
2  GRANT create ON testyh.* TO 'ordinary'@'localhost';
3  #利用普通用户建立新表 test_table.
4  use testyh;
5  create table test_table(
6      id      char(8),
7      name    varchar(10),
8      primary key(id)
9  );

```

在root用户界面刷新后发现确实多了一个表。



在普通用户的界面连表的名字都无法看到，说明普通用户只有建立的权限，其余的选择、更新权限一概没有。



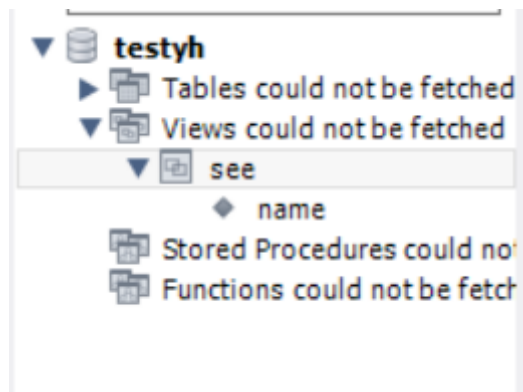
3. 授权与回收，参见步骤1.
4. 建立视图，并把该视图的查询权限授予其他用户，考察通过视图进行权限控制的作用。

```

1  #建立视图
2  create view see
3  as
4  select name from student where dept_name = 'Music';
5
6  #授予普通用户对视图查询的权限
7  GRANT select ON testyh.see TO 'ordinary'@'localhost';
8
9  #利用普通用户查询视图
10 select * from see;
11

```

授权结果：



查询结果：

	name
▶	Garze
	Chriso