实验4 SQL 安全性

实验目的：

熟悉通过SQL进行数据完整性控制的方法。

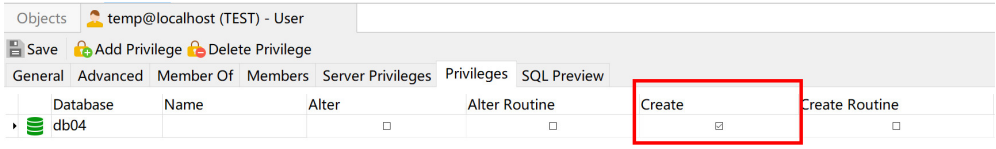
实验平台：

1. 操作系统： Windows 10
2. 数据库管理系统：MySQL 8.0.28

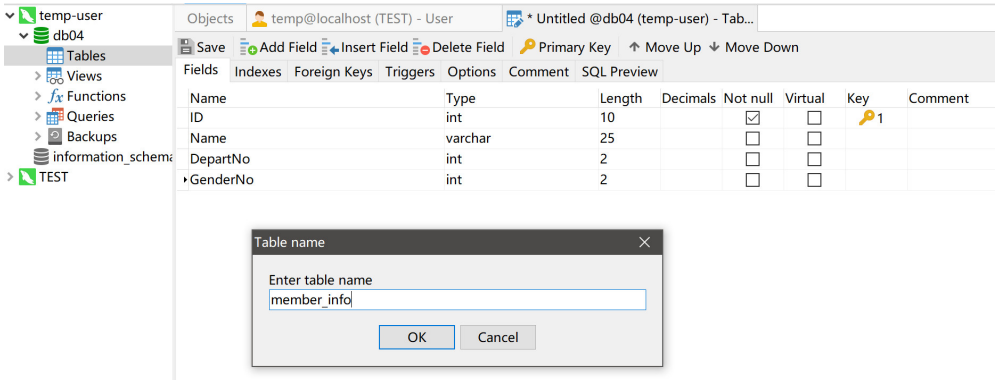
实验内容和要求：

1. 建立表，考察表的生成者拥有该表的哪些权限。

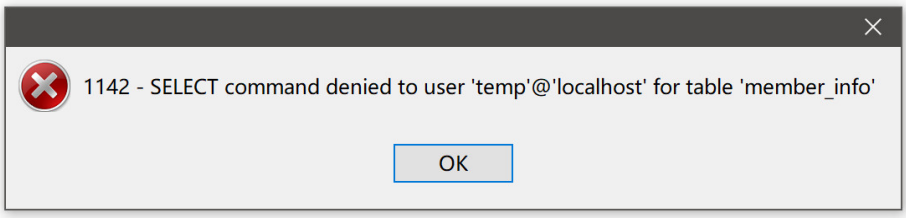
   在locoalhost用户组下新建用户temp，赋予其对数据库db04的CREATEA权限，如图：

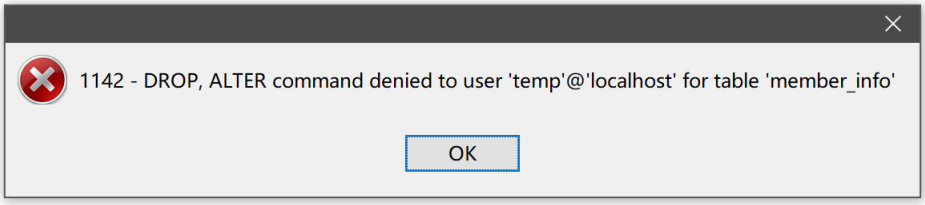


   在数据库db04下新建表 member_info，其字段信息如下：



   由于root只授予用户temp在数据库db04下新建数据表的权限，故表的创建者对该表不具备任何编辑、查看及删除的权限（非常奇怪）。部分操作截图如下：





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。

本次实验以SELECT权限为例。

在 temp 用户被授权查询表 member_info 前：

```
1 SELECT *
2 FROM   member_info;
```

BEFORE

Message Status

```
SELECT *
FROM   member_info
> 1142 - SELECT command denied to user 'temp'@'localhost' for table 'member_info'
> Time: 0s
```

使用无敌的 root 账户授予 temp 用户表 member_info 的查询权限：

TEST mysql Run

```
1 GRANT SELECT ON db04.member_info
2 TO    'temp'@'localhost';
```

Message Profile Status

```
GRANT SELECT ON db04.member_info
TO    'temp'@'localhost'
> OK
> Time: 0.006s
```

再次使用 temp 用户对表 member_info 进行 SELECT 操作，成功：

temp-user db04 Run Stop

```
1 SELECT *
2 FROM   member_info;
```

AFTER

Message Result 1 Profile Status

ID	Name	DepartNo	GenderNo
1	Sam	1	1
2	Tina	4	2
3	Mike	1	1
4	Anya	2	2

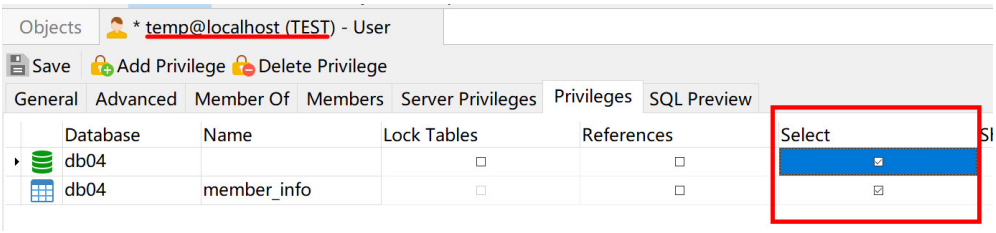
但对于未授权查询的表 gender_info 查询操作依然被拒绝：

```
1 SELECT *
2 FROM   gener_info;
```

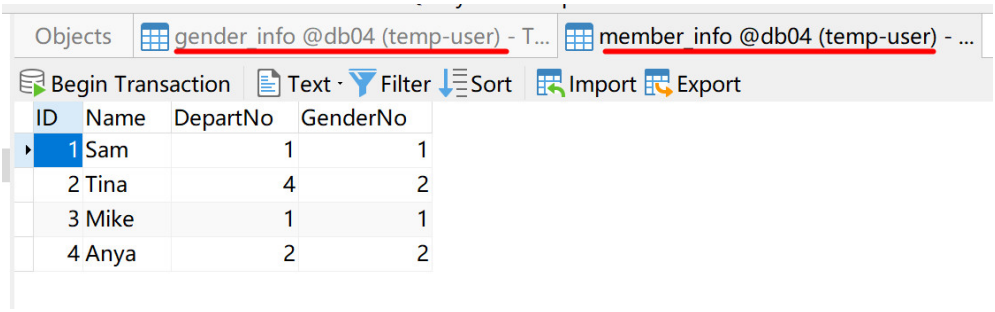
Message | Status

```
SELECT *
FROM   gener_info
> 1142 - SELECT command denied to user 'temp'@'localhost' for table 'gener_info'
> Time: 0s
```

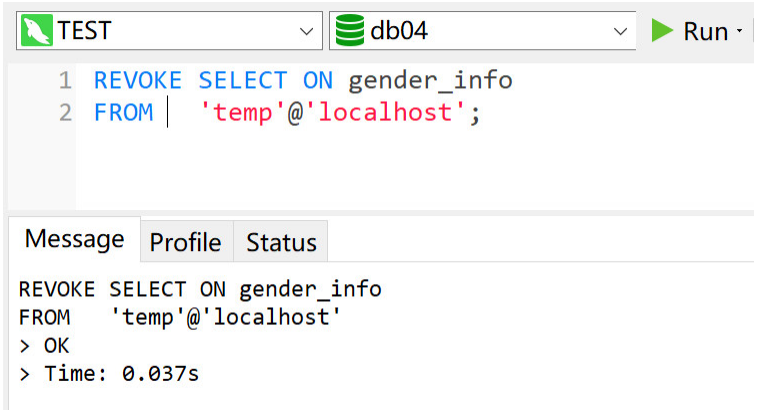
使用 root账户授予 temp 查询数据库 db04 下所有数据表的权限：

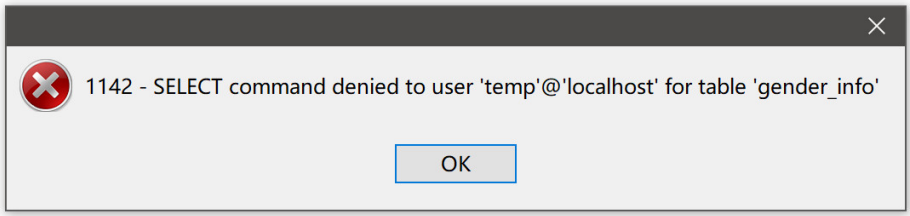


保存修改后，使用 temp账户对数据库 db04 下的表 member_info 与 gender_info 进行查询，成功：



通过 root 账户回收 temp 账户对表 gender_info 的查询权限，再次使用 temp 权限对表 gender_info 进行查询，查询失败：





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。

TEST db04 Run Stop Explain

```
1 CREATE VIEW v_member AS
2 SELECT member_info.ID, member_info.Name, gender_info.Gender
3 FROM member_info, gender_info
4 WHERE member_info.GenderNo = gender_info.GenderNo;
```

在 Navicat 中建立名为 v_member 的视图，结果如下：

Objects v_member @db04 (TEST) - View

Begin Transaction Text Filter Sort

ID	Name	Gender
1	Sam	Male
2	Tina	Female
3	Mike	Male
4	Anya	Female

使用 root 账户为 temp 账户授予对视图 v_member 的查询权限：

Objects * Untitled - Query

Save Query Builder Beautify SQL Code Snippet

TEST mysql Run Stop Explain

```
1 GRANT SELECT ON db04.v_member
2 TO    'temp'@'localhost';
```

使用 temp 账户对视图 v_member 进行选择操作，操作成功，结果如下：

temp-user db04 Run Stop Explain

```
1 SELECT *
2 FROM   v_member
3 WHERE  Gender = 'Female';
```

Message Result 1 Profile Status

ID	Name	Gender
2	Tina	Female
4	Anya	Female

使用 temp 账户对视图 v_member 进行 DELETE/INSERT/UPDATE，操作失败：

```sql
DELETE FROM v_member
WHERE  ID = 1;
```

Message Status

```
DELETE FROM v_member
WHERE  ID = 1
> 1142 - DELETE command denied to user 'temp'@'localhost' for table 'v_member'
> Time: 0s
```

```sql
INSERT INTO v_member
VALUES (5, 'Robe', 'Male');
```

Message Status

```
INSERT INTO v_member
VALUES (5, 'Robe', 'Male')
> 1142 - INSERT command denied to user 'temp'@'localhost' for table 'v_member'
> Time: 0s
```

```sql
UPDATE v_member
SET    ID = 5
WHERE  Name = 'Anya';
```

Message Status

```
UPDATE v_member
SET    ID = 5
WHERE  Name = 'Anya'
> 1142 - UPDATE command denied to user 'temp'@'localhost' for table 'v_member'
> Time: 0s
```

对数据源表 member_info / gender_info 的操作也被拒绝：

```sql
SELECT *
FROM   member_info, gender_info;
```

Message Status

```
SELECT *
FROM   member_info, gender_info
> 1142 - SELECT command denied to user 'temp'@'localhost' for table 'member_info'
> Time: 0s
```

实验心得：

- 终于用上了 Navicat 的图形化界面，感到十分快乐。
- 实验期间曾通过 Navicat User 选项下的 Privilege 表格对 check box 直接进行勾选，从而实现对用户进行授权。但通过此途径授予的权限似乎并不支持通过 Revoke 指令进行移除。
- 表格的查询结果不是实时更新的，在通过 GRANT 命令为用户授权后，只有对 table_priv 表格进行刷新后，才能显示最新的用户权限列表。
- 但是 temp 用户作为表 member_info 的创建者，table_priv 表格中始终没有显示其对于表格 member_info的权限，好奇怪（temp 用户仅拥有对数据库 db04 的 CREATE 权限）。