实验四 SQL 安全性

张海 3130000923

实验目的

1. 熟悉通过 SQL 保证数据安全性。

实验要求

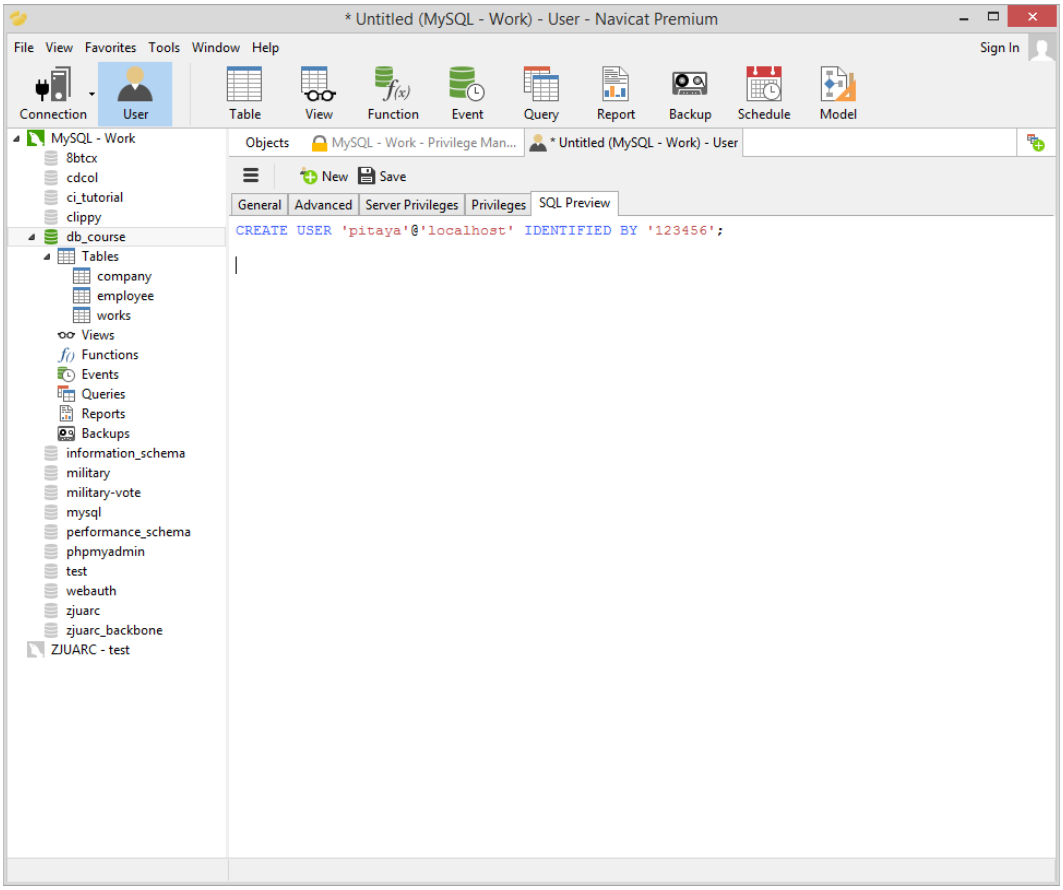
1. 建立表, 考察表的生成者拥有该表的哪些权限。
2. 使用 SQL 的 GRANT 和 REVOKE 命令对其他用户进行授权和权力回收, 考察相应的作用。
3. 建立视图, 并把该视图的查询权限授予其他用户, 考察通过视图进行权限控制的作用。
4. 完成实验报告。

实验平台

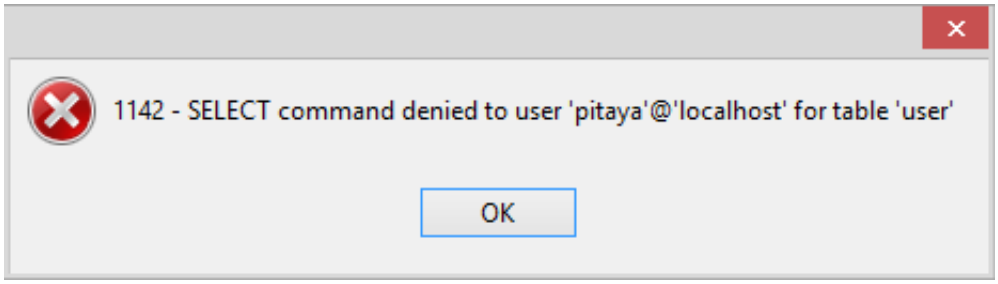
数据库管理系统：MySQL

实验过程

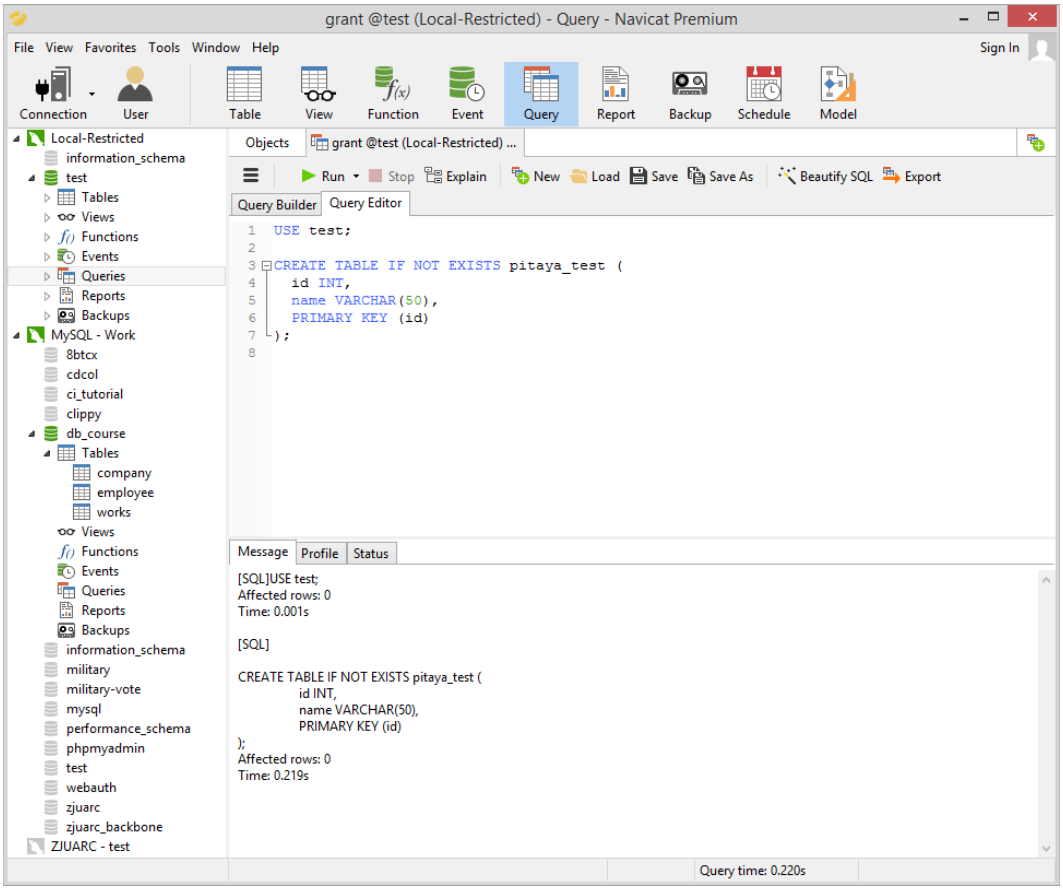
1. 新建用户，pitaya@localhost/123456, 不进行任何其他配置：



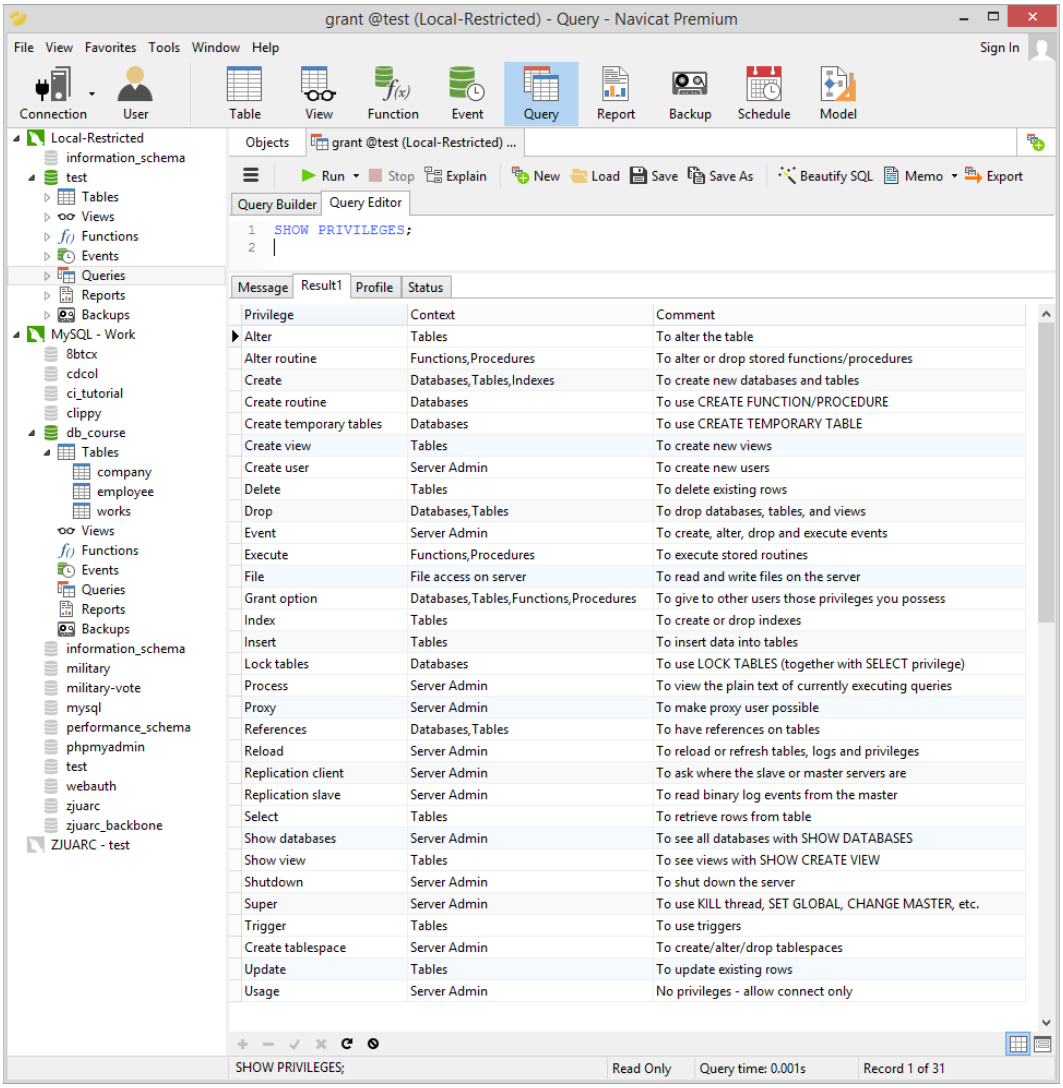
2. 尝试通过这个用户进行连接, 发现并没有足够的权限查看数据库列表：



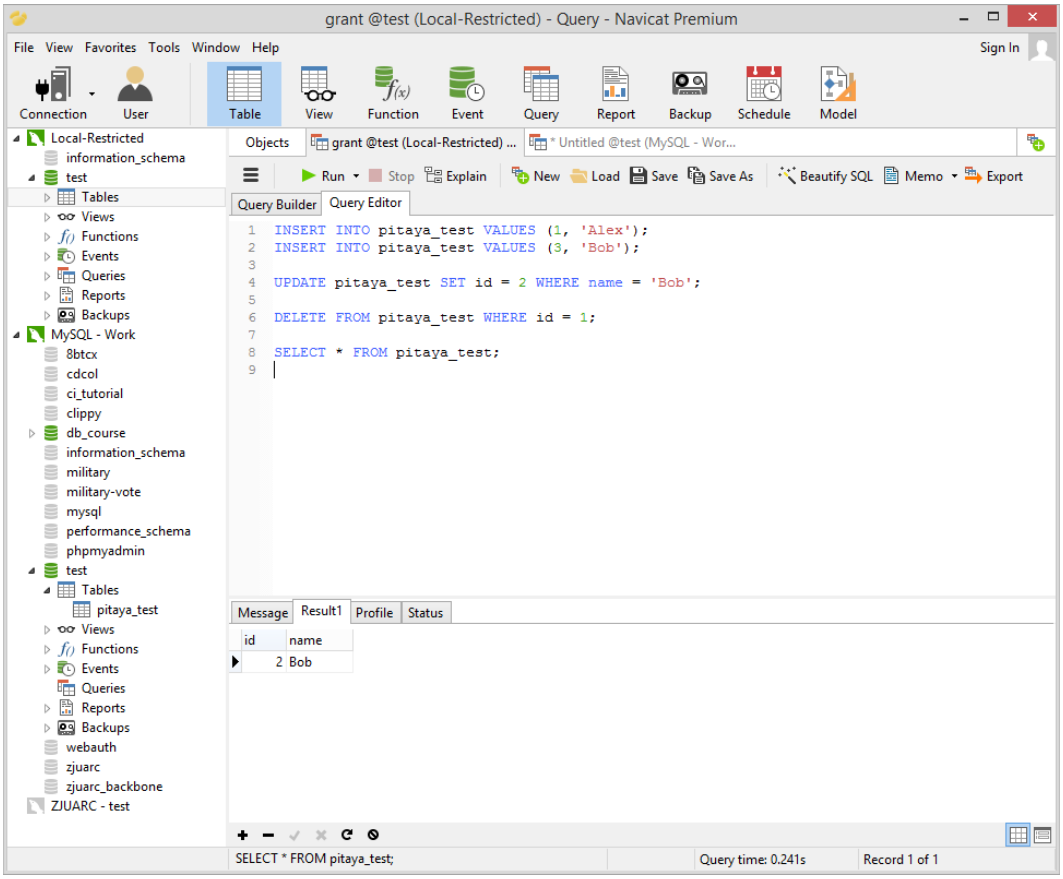
3. 使用 test 数据库, 建立数据表：



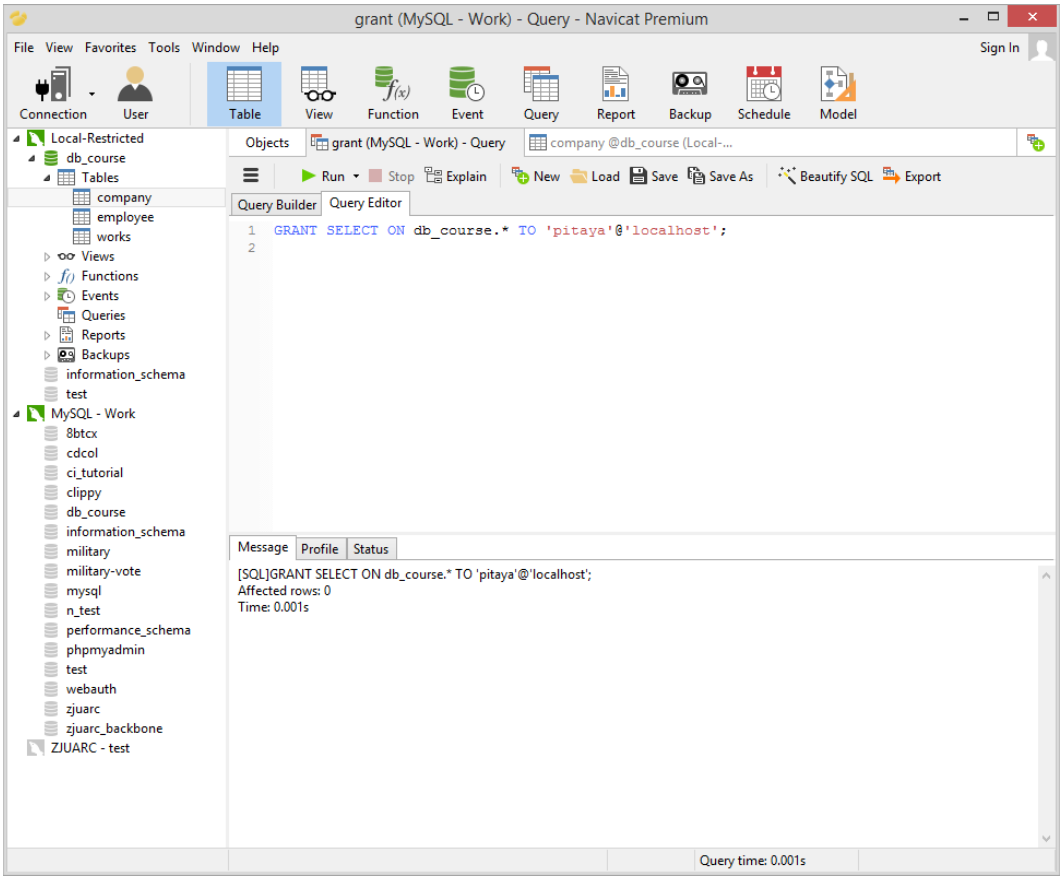
4. 查看该用户所有的权限, 可见其包括查找, 插入, 修改, 删除均可以进行操作, 并且有这个数据库及以下所有上下文的授权 (GRANT) 命令：



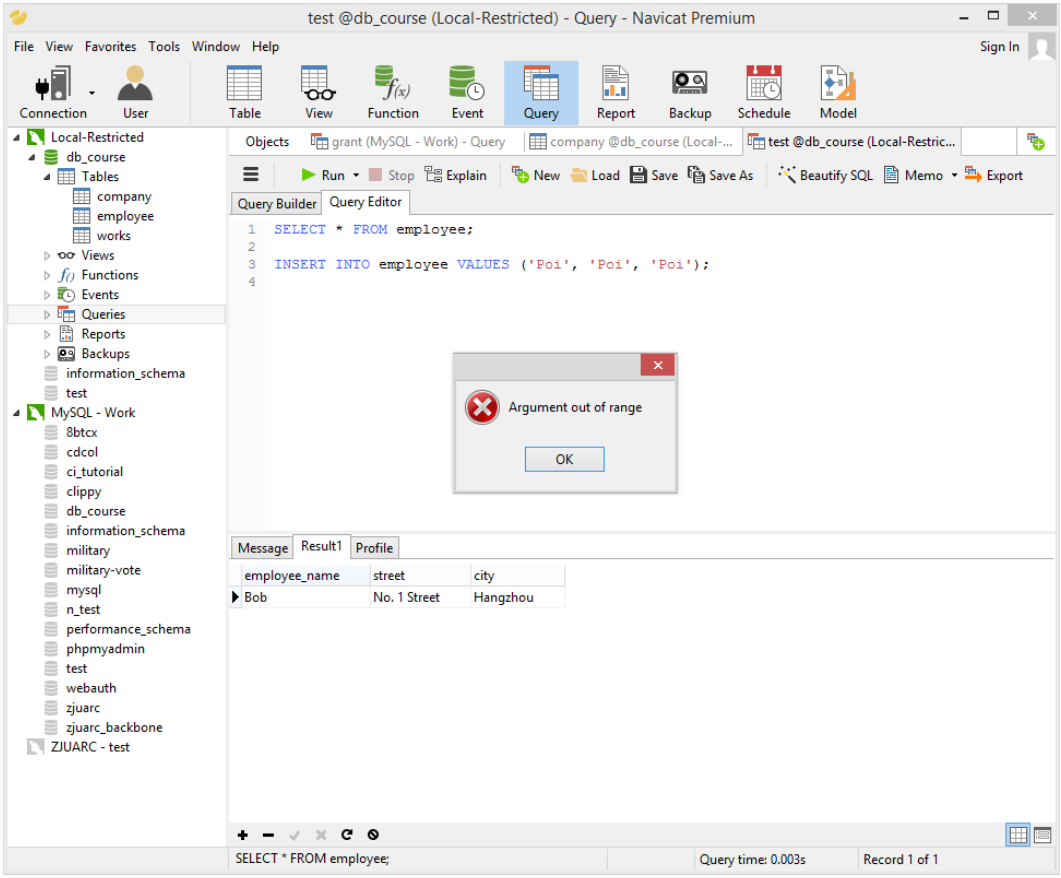
5. 测试发现所有的插入、修改、删除与查询都可以正常地实现：



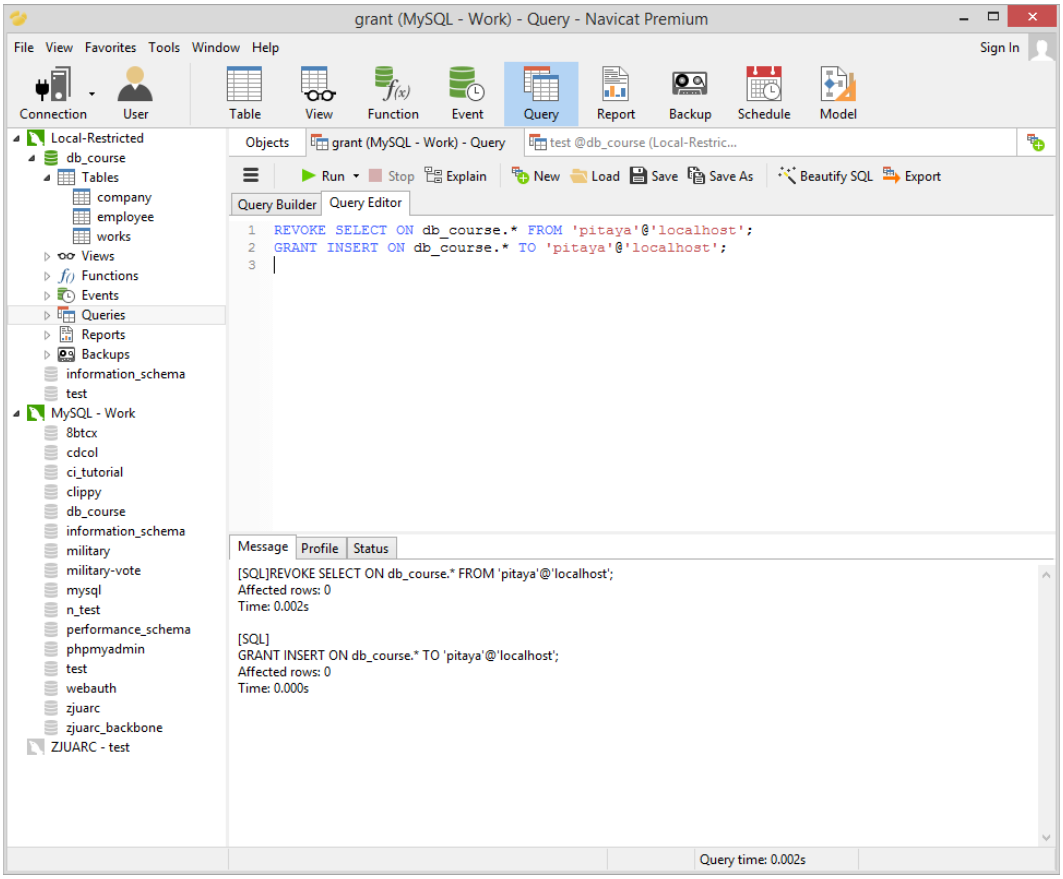
6. 使用 root 用户给予其查看 db_course 数据库中所有表的权限：



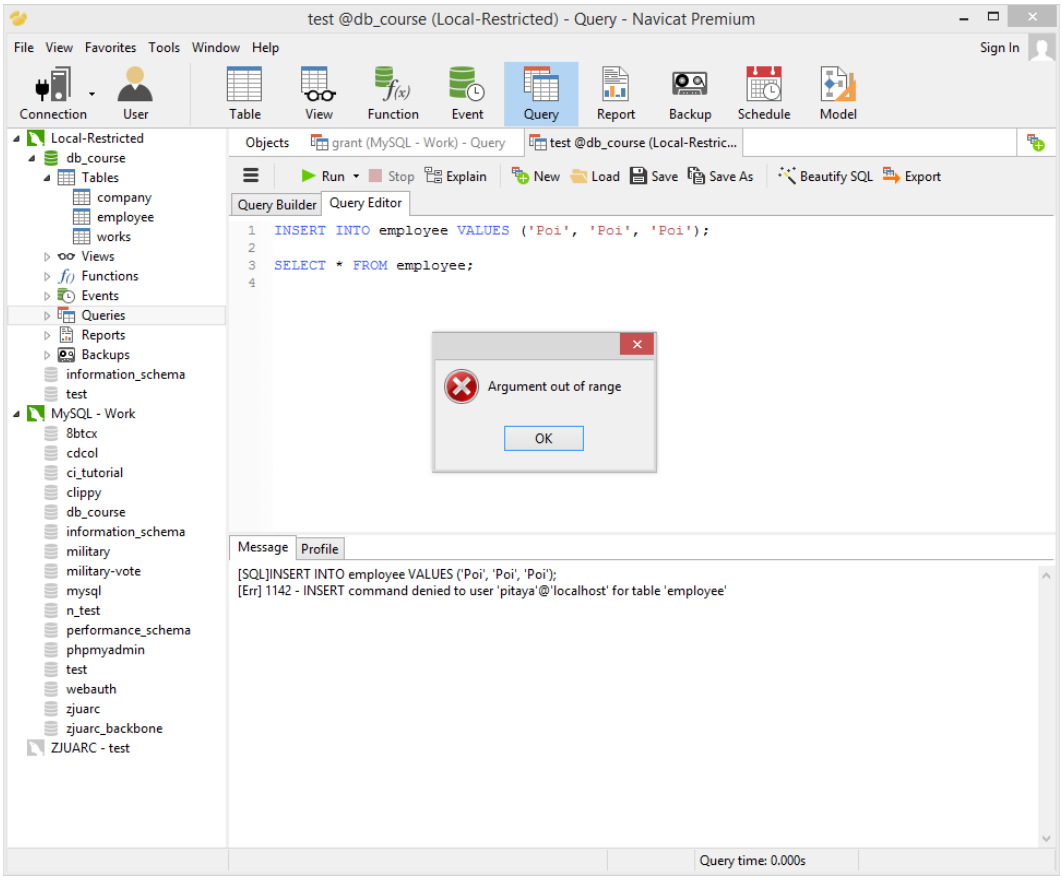
7. 现在 pitaya 用户对于其中的表, 可以查询但是无法插入：



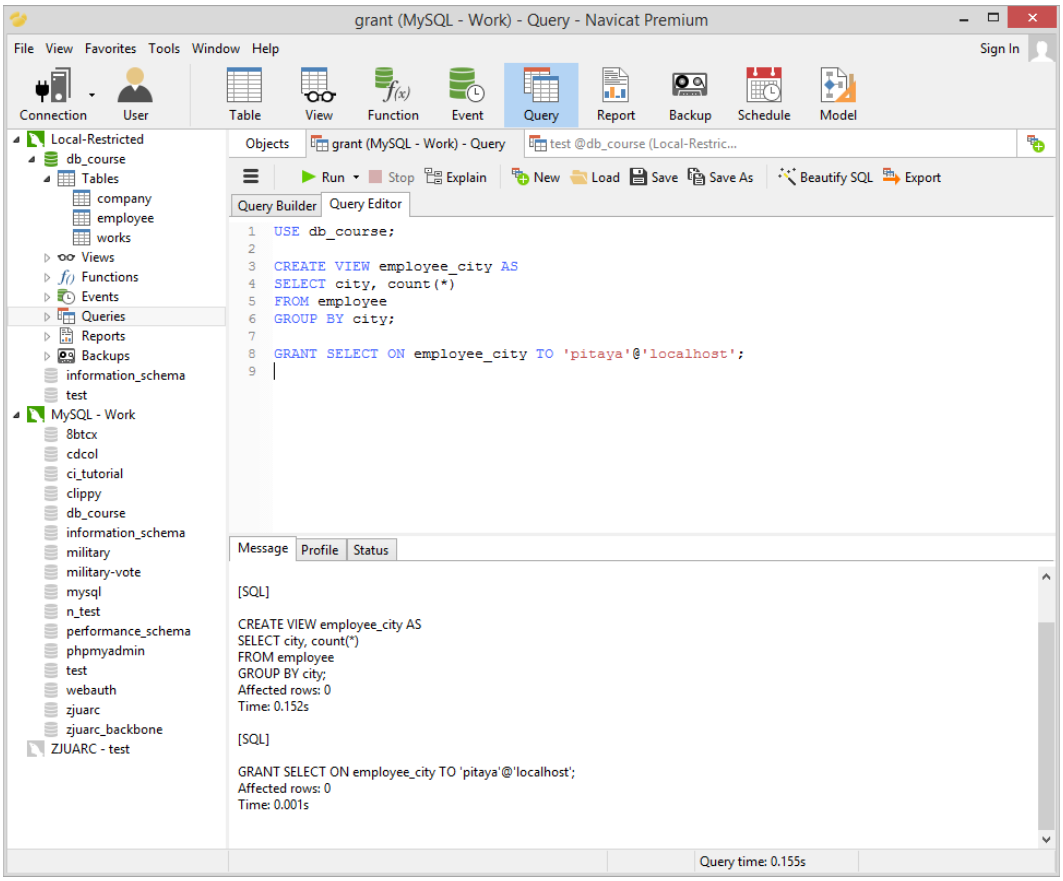
8. 现在给予 pitaya 用户插入的权限, 但是收回查询的权限, 再进行一次测试：



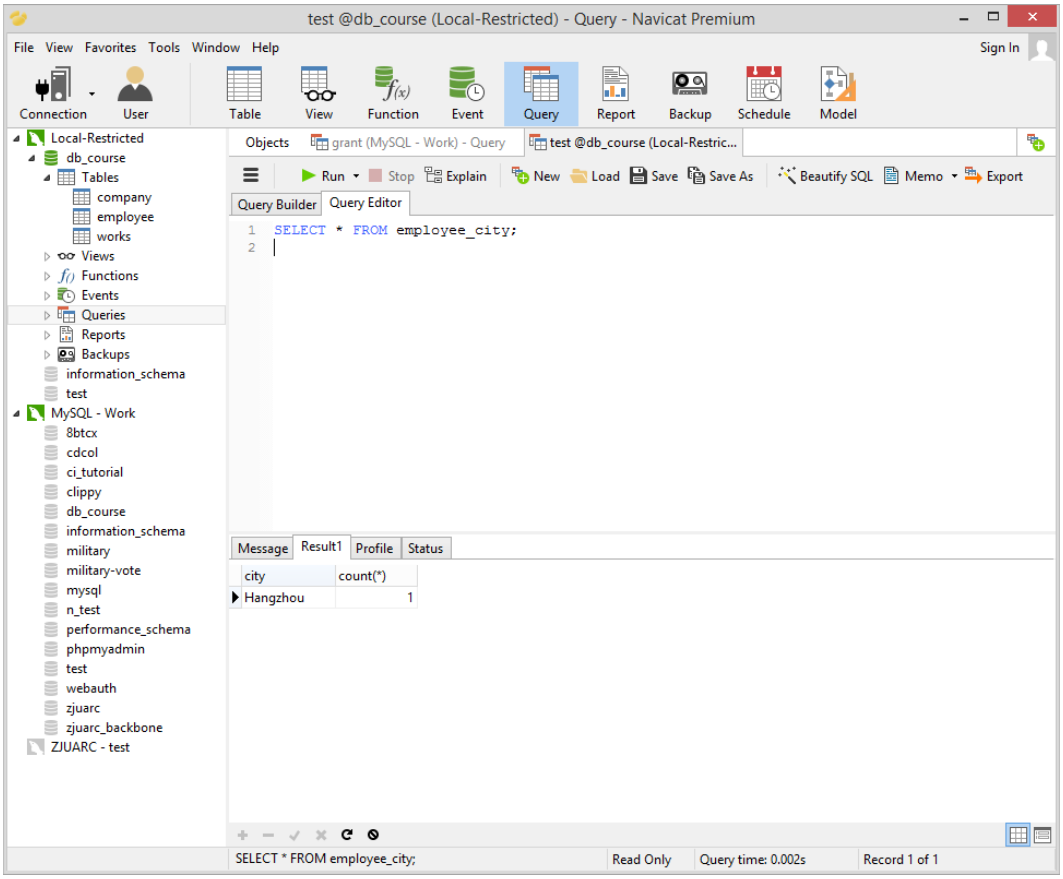
9. 可见即使没有查询权限还是可以进行正常的插入：



0. 以 root 用户新建一个 view, 并给予 pitaya 用户查询权限：



1. pitaya 用户即使没有对应 employee 表的权限, 依旧可以可以查看这个 view, 但是无法修改：



实验心得

1. 用户权限是关乎到一个数据库安全的最重要部分, 使用 SQL 管理权限可以高效准确地进行权限查询和管理, 并且在数据库系统的配合下达到一种比较高的安全性。
2. 视图的灵活运用有助于提高整个数据库的安全性, 通过只展示希望展示出来的局部信息来保护全局的重要信息。