《数据库技术实验》报告

|  |  |  |
| --- | --- | --- |
| **第 六 次实验** | **日期：2022-11-01** | **得分：** |
| **学号：** | **姓名：*Steven*** | **专业：智能科学与技术** |

一、实验目的

1. 掌握管理用户和权限的SQL语句

2. 了解数据库安全性及自主存权控制机制

二、实验内容

（一）实验题

1. 创建两个用户abc和def，为他们设置密码，并以他们的身份登录系统，查看他们的权限情况。

2. 将用户abc设置超级用户，并以他的身份登录系统，查看他的权限情况。

3. 通过用户abc，设计一组权限并将这组权限授予用户def，以用户def的身份登录系统，查看他的权限情况。

（二）思考题

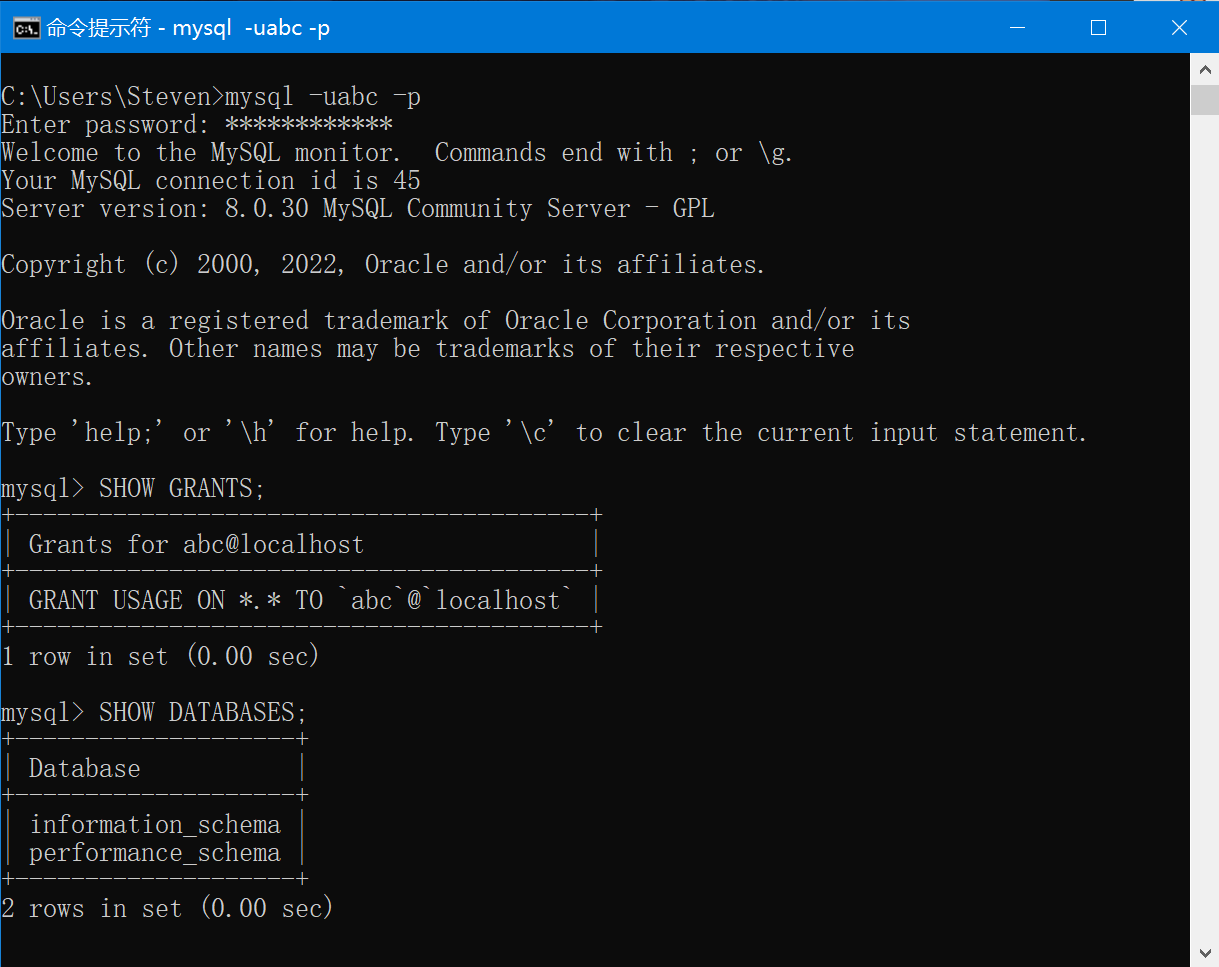
1. 自主存取控制机制的优缺点是什么

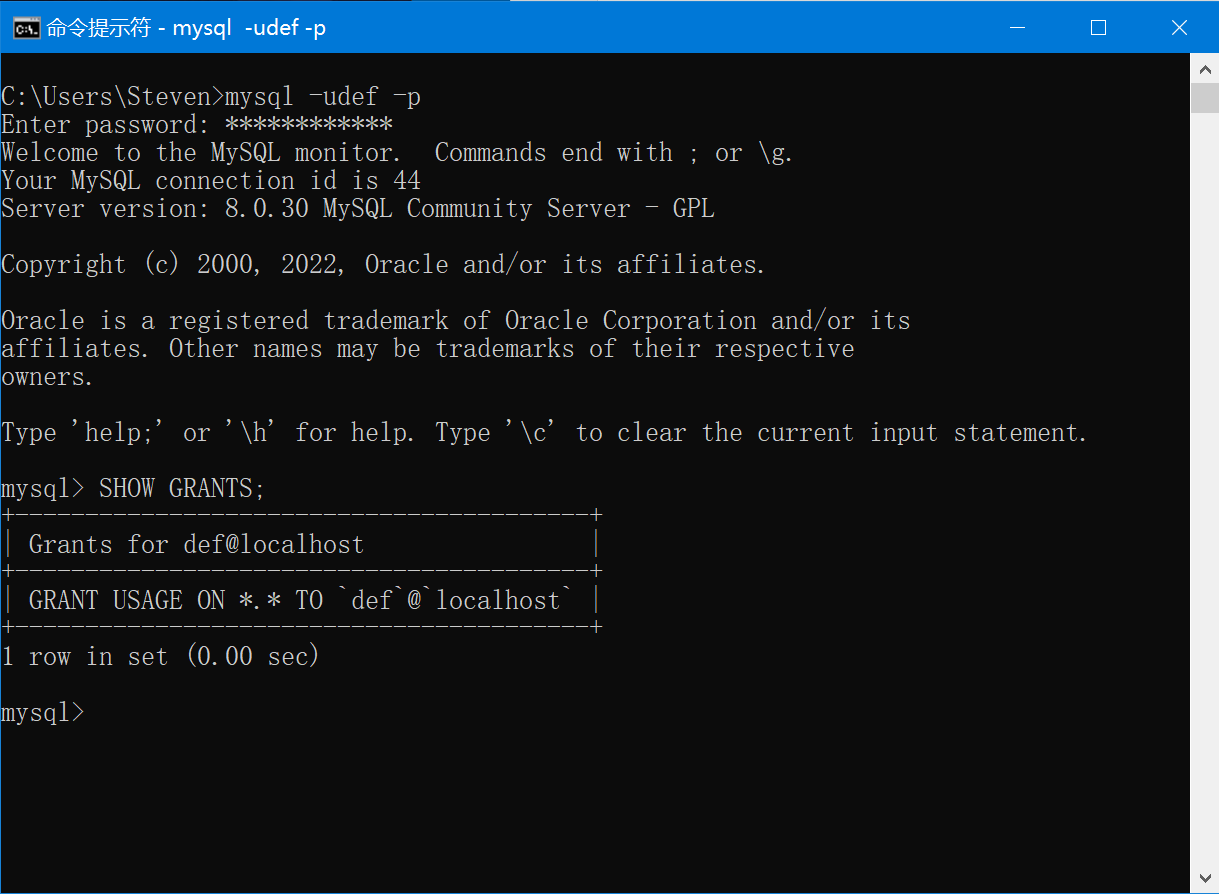
2. 视图在数据库安全性中的作用有什么

三、实验过程及实验结果

1. 创建两个用户abc和def，为他们设置密码，并以他们的身份登录系统，查看他们的权限情况。

|  |
| --- |
| -- 创建账户abc  CREATE USER 'abc'@'localhost' IDENTIFIED BY 'password\_abc';  -- 创建账户def  CREATE USER 'def'@'localhost';  SET PASSWORD FOR 'def'@'localhost'='password\_def'; |

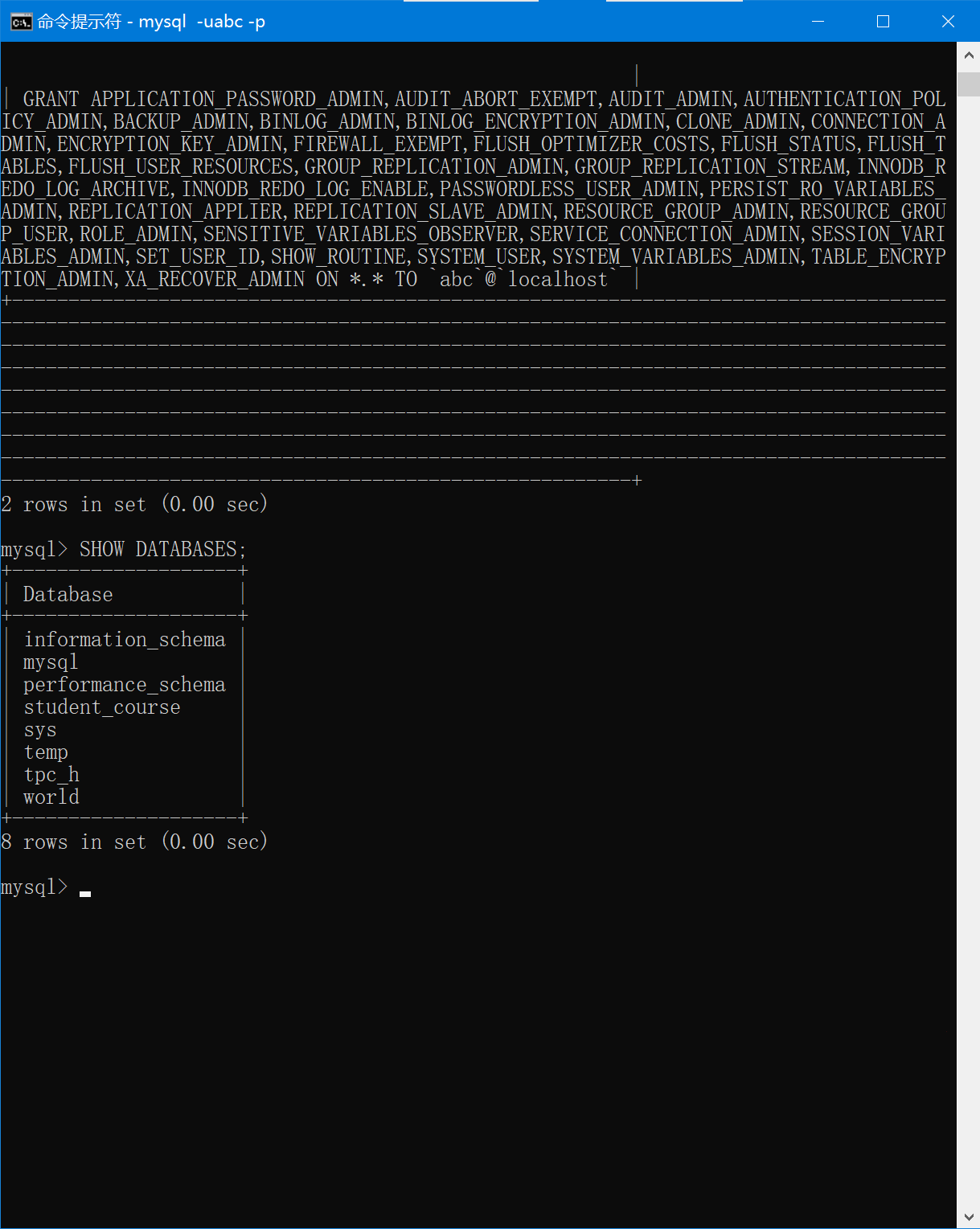




登录abc和def账户，发现abc和def对所有的数据库有USAGE权限，即登录连接的权限，除此之外没有其他的权限，在可见的Database中也只有两个默认架构可见。

2. 将用户abc设置超级用户，并以他的身份登录系统，查看他的权限情况。

|  |
| --- |
| GRANT ALL PRIVILEGES ON \*.\* TO 'abc'@'localhost' WITH GRANT OPTION; |

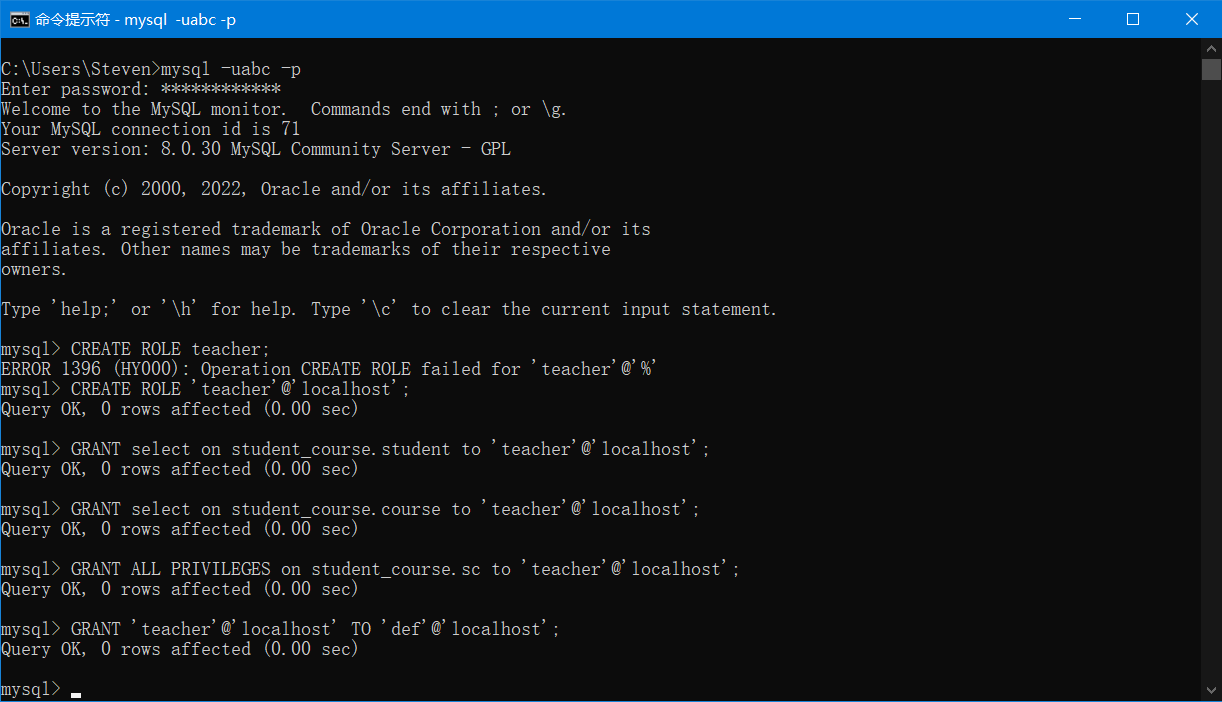


授权后发现，abc有了全部权限，同时也能查看到所有的database。

3. 通过用户abc，设计一组权限并将这组权限授予用户def，以用户def的身份登录系统，查看他的权限情况。

假设def为教务老师，则其应当只能查看student\_course.student，student\_course.course可以修改student\_course.sc。这一组权限可以通过role统一分配。

1. 首先登录abc，创建一个ROLE teacher，为其分配权限，最后将teacher分配给def。

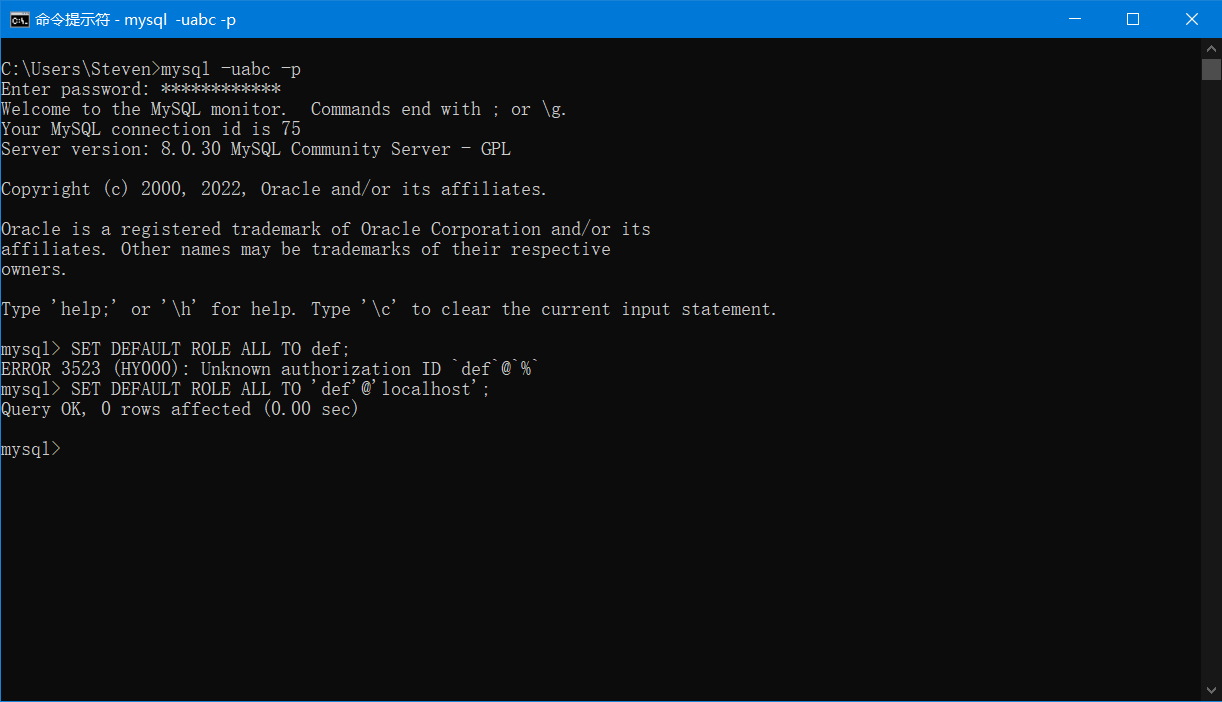


1. 然后登录def，却发现只是被授予了teacher，并没有实际对student\_course库的权限。

文本

描述已自动生成

1. 经查，才知道还需要将def这个用户激活才可获取teacher对应的权限，于是又回到abc账户，使用 SET DEFAULT ROLE ALL TO，激活def



1. 此时，def账户有了其应有的权限。

文本

描述已自动生成

(权限查看，将ROLE teacher实际拥有的权限赋给了def)

文本

中度可信度描述已自动生成

(权限测试)

四、思考题

1. 自主存取控制机制的优缺点是什么

优点：用户权限可以灵活地进行授权、收回，能够通过授权机制有效地控制其他用户对敏感数据的存取。

缺点：可能存在数据的“无意泄露” ，因为这种机制仅仅通过对数据的存取权限来进行安全控制，数据本身并无安全性标记。

2. 视图在数据库安全性中的作用有什么

视图有助于限制对特定用户的数据访问，通过视图向用户分配部分数据的查看权限，有利于保护敏感数据。

此外，视图本身是个虚表，并不与真实存储的数据相关联。创建只读视图后，视图的使用者只能查看无法修改，进而保护了数据。