**北京邮电大学**

**网络空间安全学院**



**数据库实验报告**

**安全性和完整性**

**姓 名 李昊伦**

**学 号 2023211595**

**班 级 2023211805**

**邮 箱 1030824397@qq.com**

**2025年5月12日**

**实验 安全性和完整性**

**1 实验内容**

**1.1 安全性部分**

授权与回收

1.在数据库中由DBA创建若干用户，权限全部选择为CONNECT（SQL Server中的db\_accessadmin角色）

2.仿照教材4.2.4 [例1]~[例10]，在DBA与这些用户之间进行授权和回收，并查看效果（4用例），注意SQL Server中登录名与用户的区别

**1.2 完整性部分**

使用SQL对数据进行完整性控制，并用实验证实，当操作违反了完整性约束条件时，系统是如何处理的

1.实体完整性(仿照[例1]、[例2]) x1

2.参照完整性(仿照[例3]) x4

3.用户定义完整性(仿照[例5]、 [例6]) x1

4.CHECK短语(仿照[例7]或[例8] 、[例9]) x1

5.CONSTRAINT子句(仿照[例10]、[例13]) x1

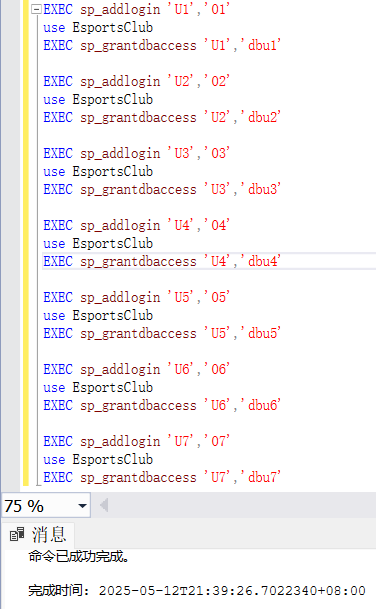
**2 实验过程**

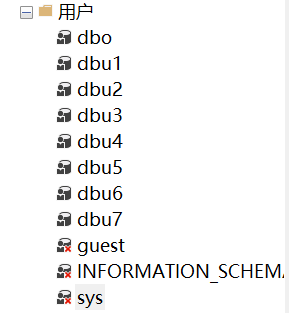
**2.1 安全性部分**

1.创建用户

建立登录帐号 U1、U2、U3、U4、U5、U6、U7 和对应的EsportsClub数据库的用户 dbu1、dbu2、dbu3、dbu4、dbu5、dbu6、dbu7。

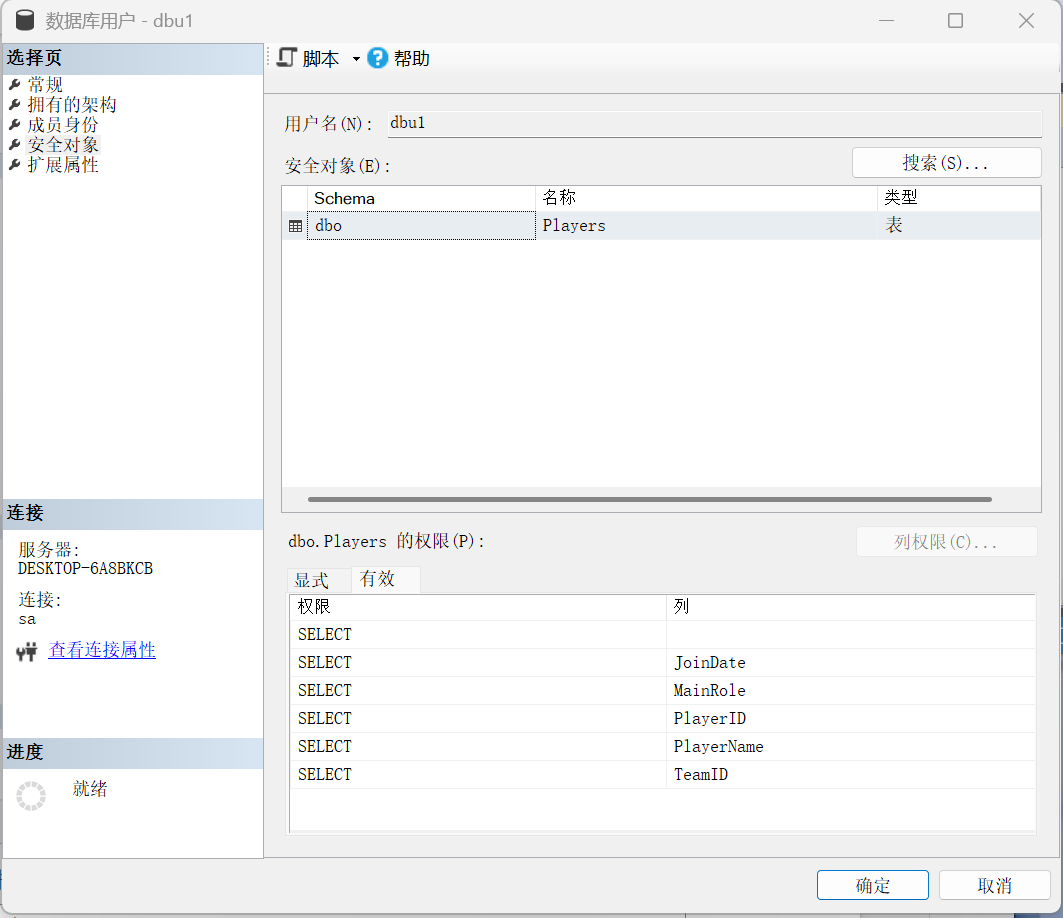
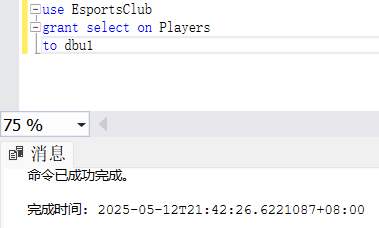
|  |
| --- |
| EXEC sp\_addlogin 'U1','01'  use EsportsClub  EXEC sp\_grantdbaccess 'U1','dbu1'    EXEC sp\_addlogin 'U2','02'  use EsportsClub  EXEC sp\_grantdbaccess 'U2','dbu2'    EXEC sp\_addlogin 'U3','03'  use EsportsClub  EXEC sp\_grantdbaccess 'U3','dbu3'    EXEC sp\_addlogin 'U4','04'  use EsportsClub  EXEC sp\_grantdbaccess 'U4','dbu4'    EXEC sp\_addlogin 'U5','05'  use EsportsClub  EXEC sp\_grantdbaccess 'U5','dbu5'    EXEC sp\_addlogin 'U6','06'  use EsportsClub  EXEC sp\_grantdbaccess 'U6','dbu6'    EXEC sp\_addlogin 'U7','07'  use EsportsClub  EXEC sp\_grantdbaccess 'U7','dbu7' |



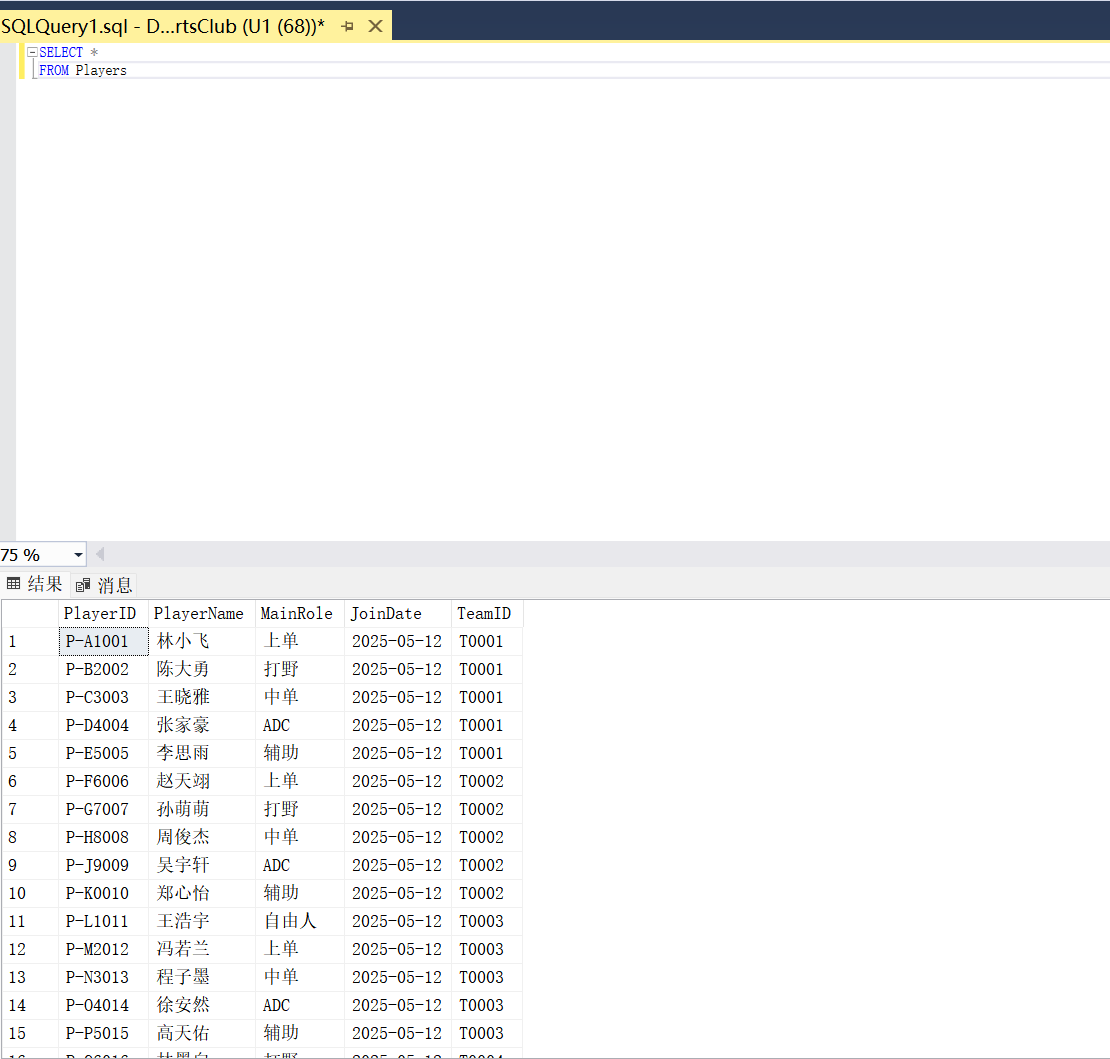
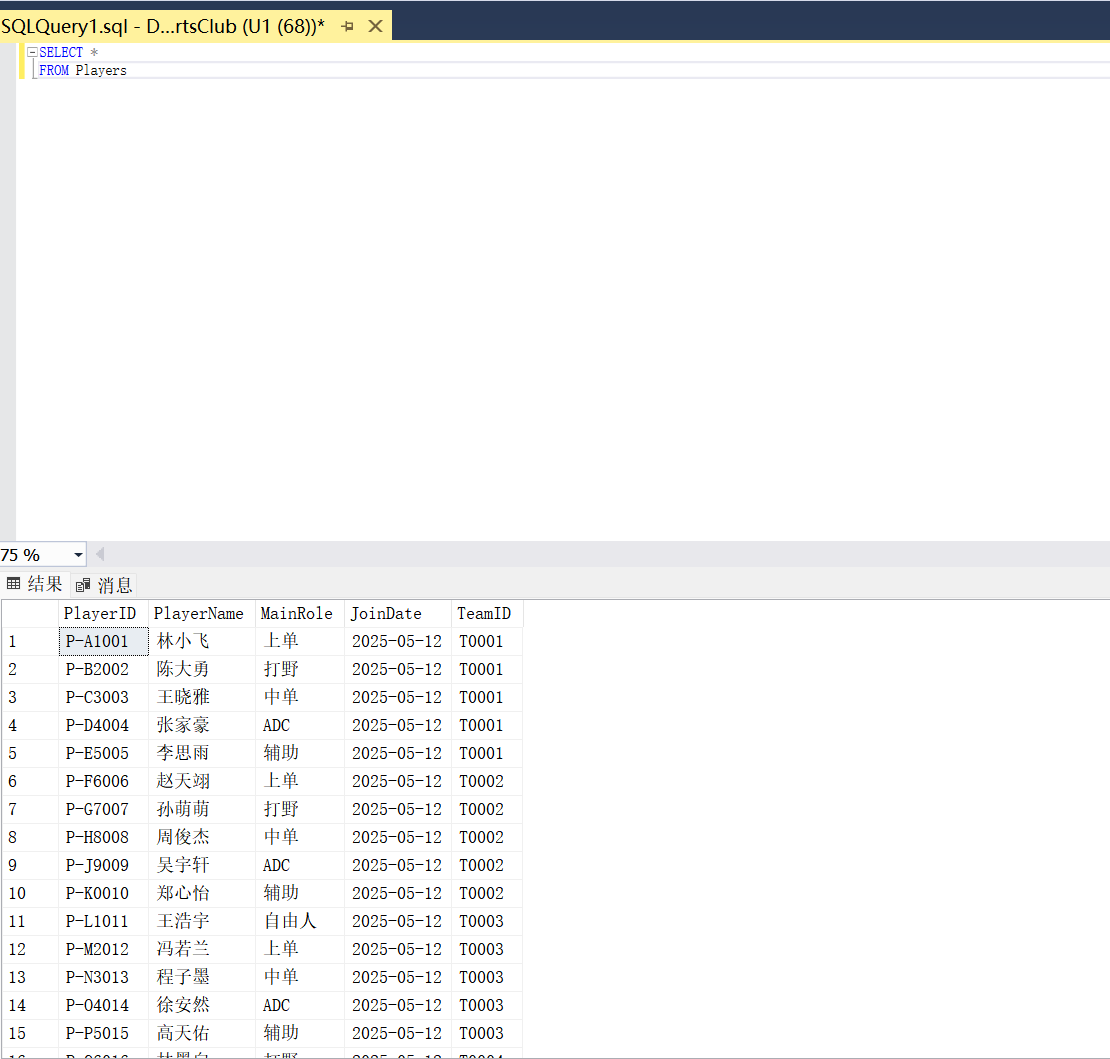


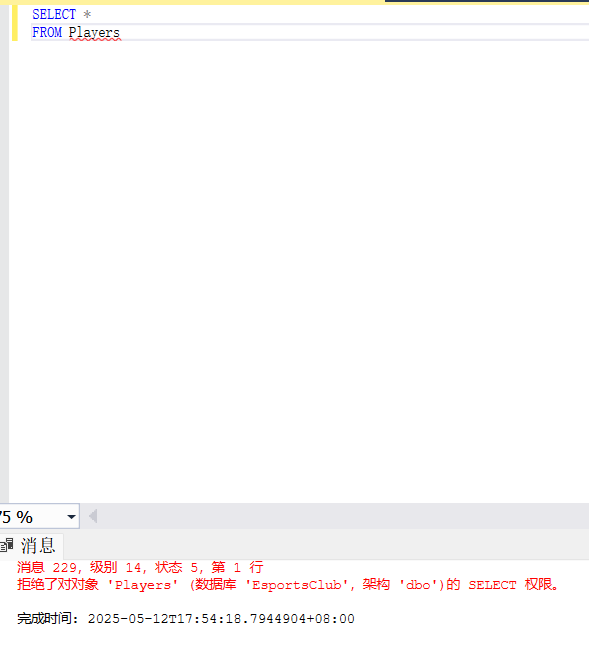
2.授权

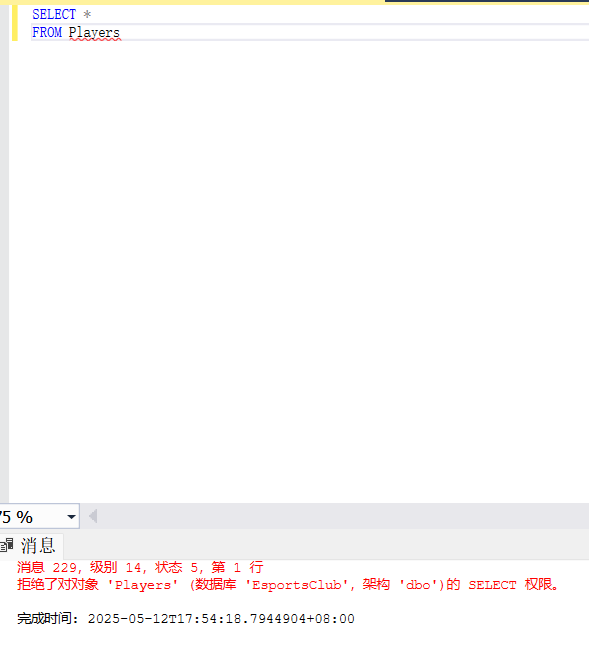
（1）把查询Players表的权限授给用户U1。



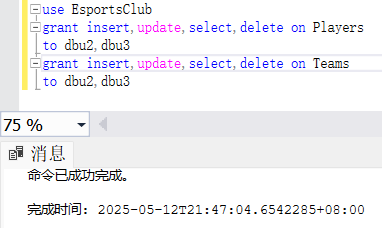
（2）对比访问结果：有权限的U1可以访问、无权限U2不可以访问

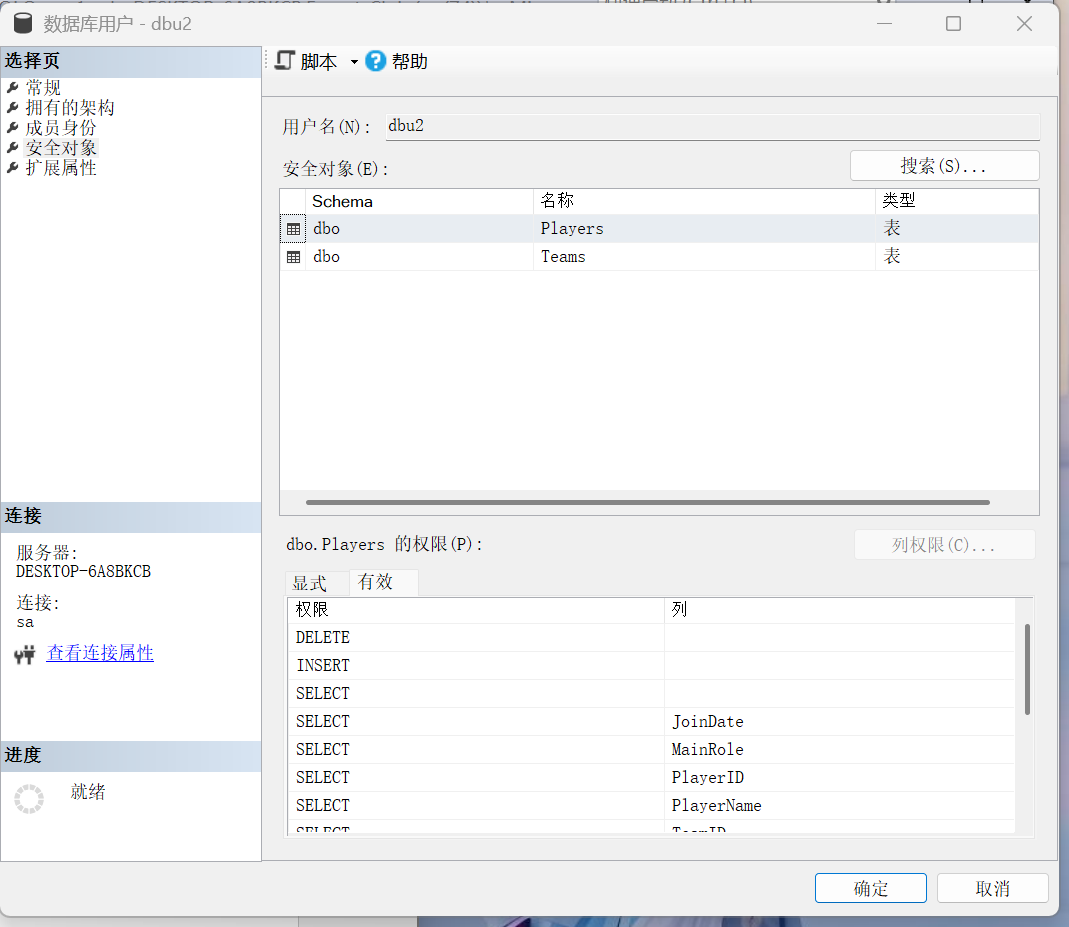


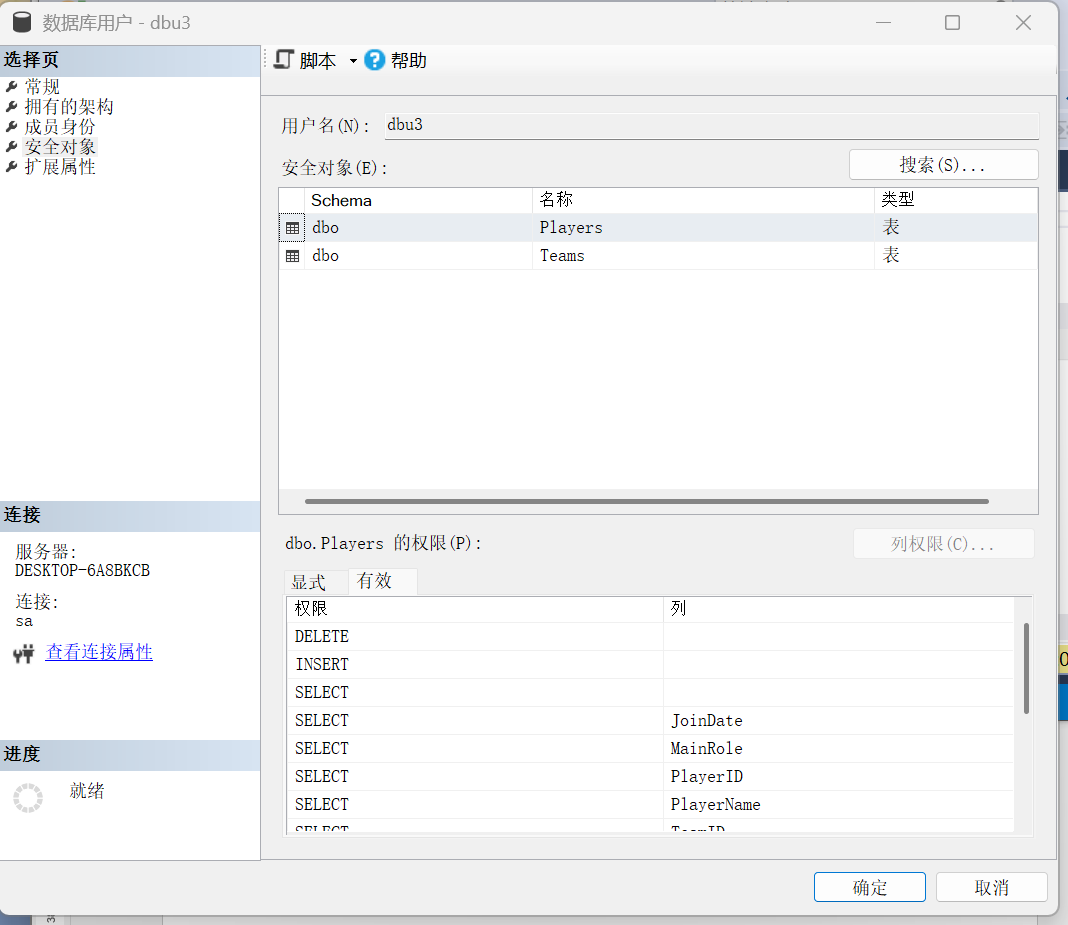




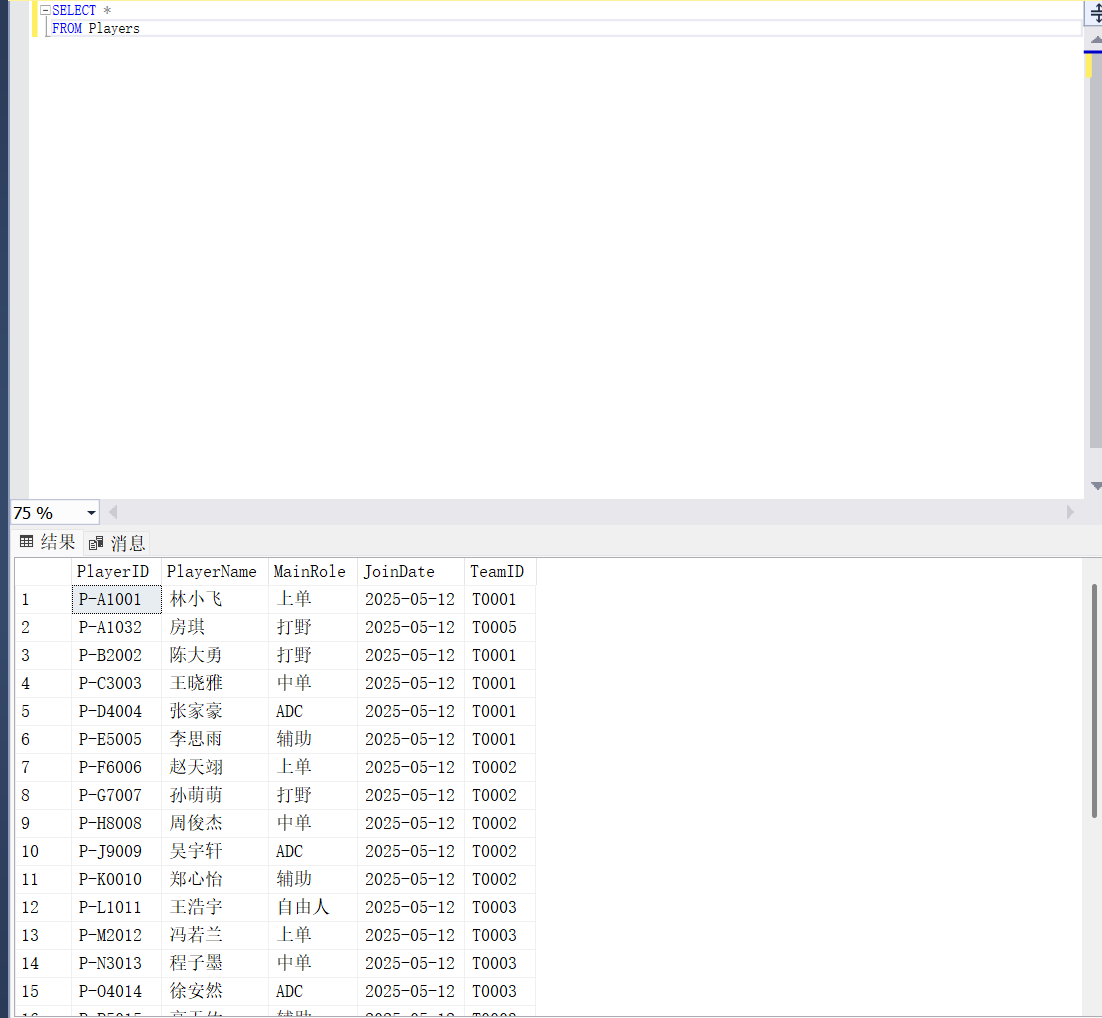
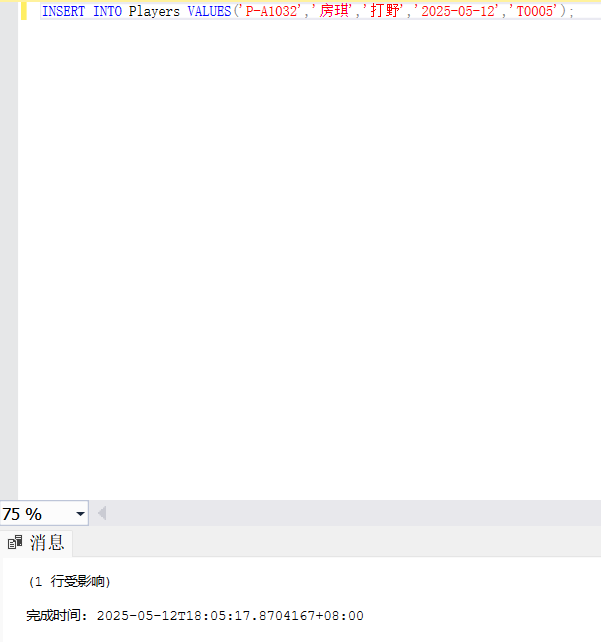
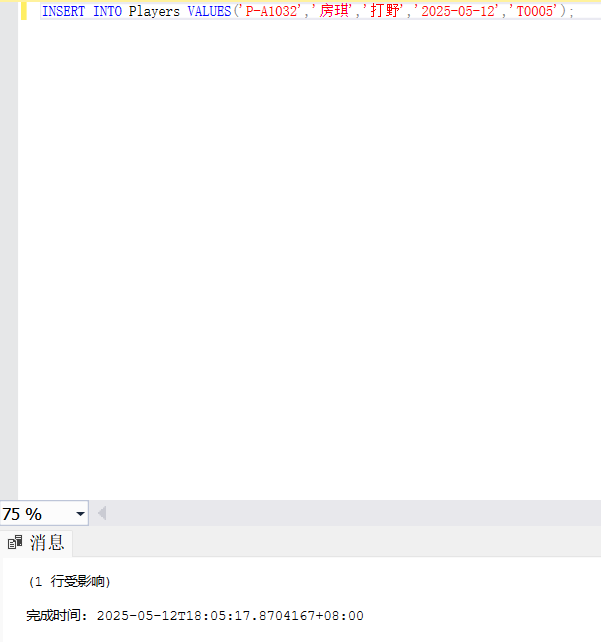
（3）把对Players表和Teams表的全部操作权限授予用户U2和U3。

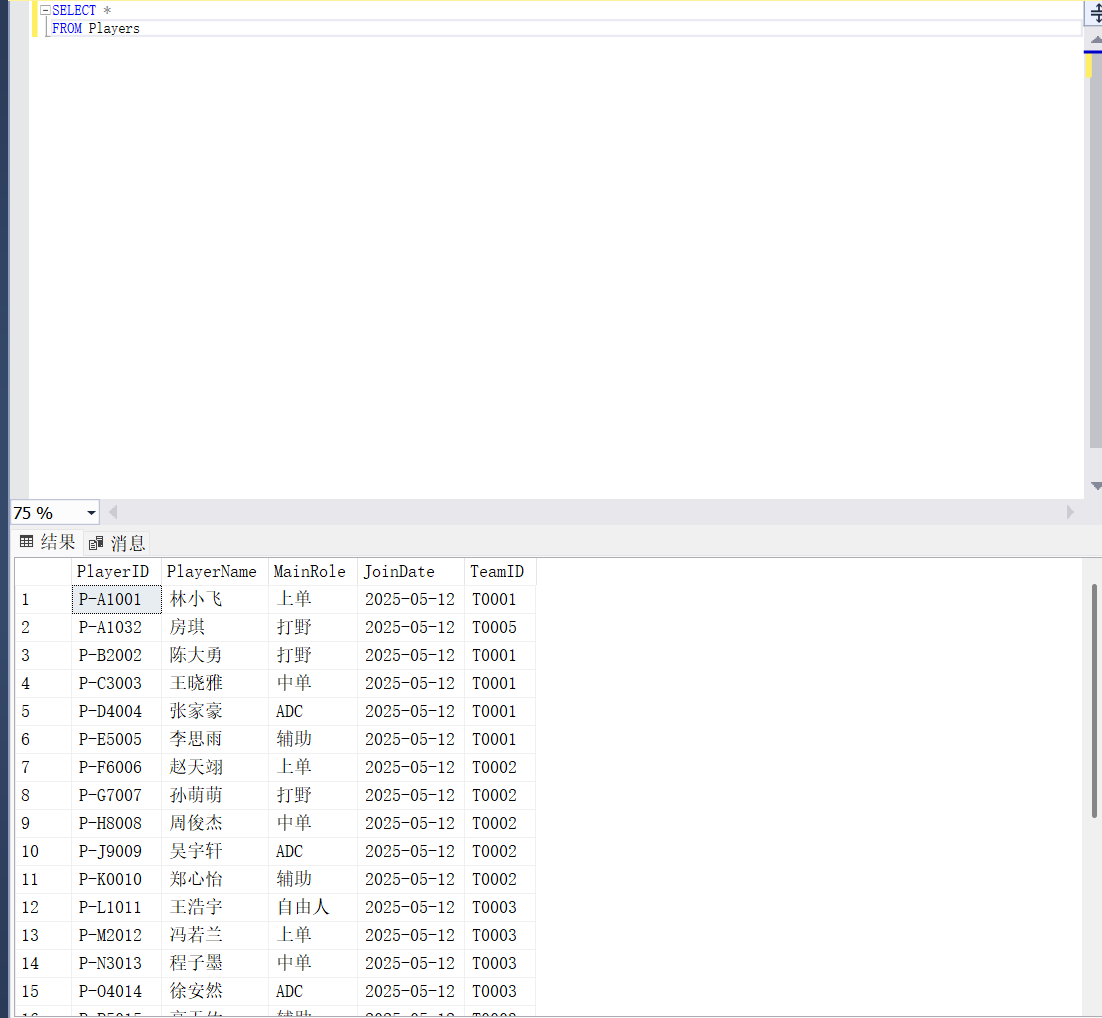






（4）此时U2插入数据，证明成功

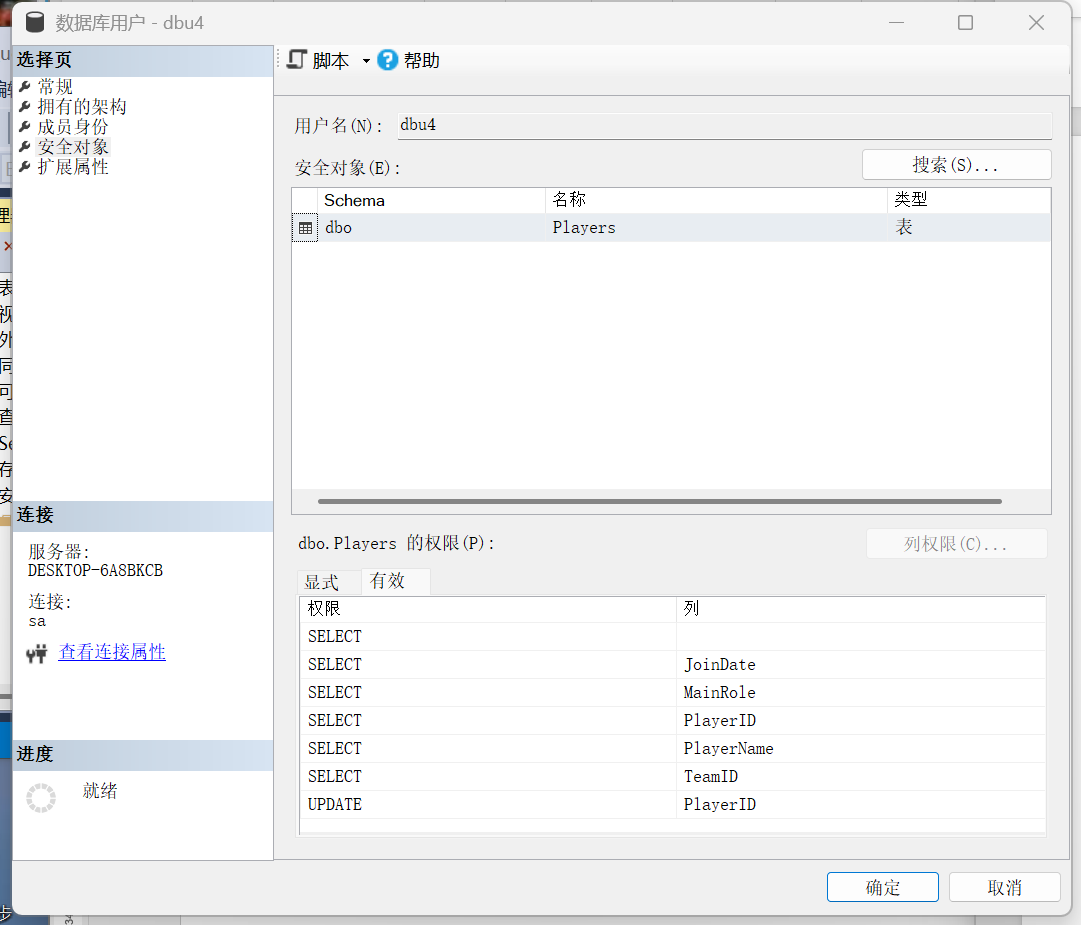
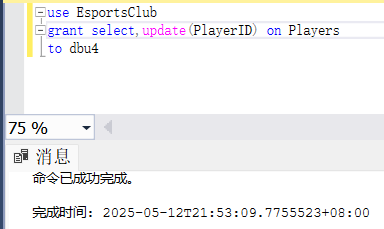




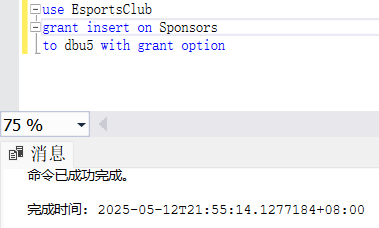
（5）把对表Sponsors的查询权限授予所有用户。

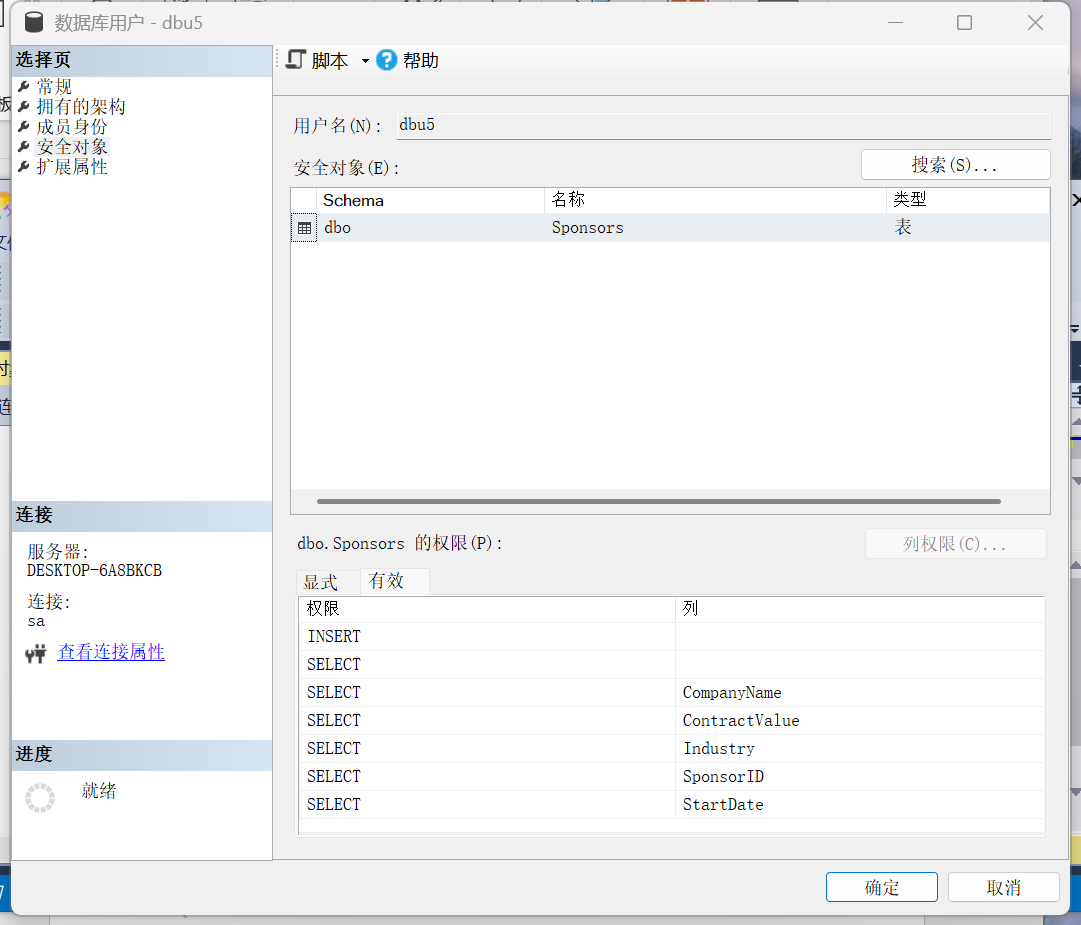


（6）把查询Players表和修改PlayerID的权限授给用户U4。

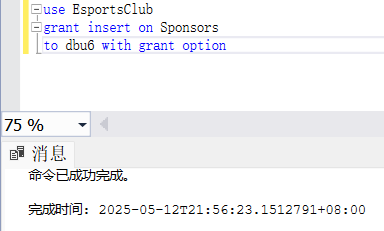


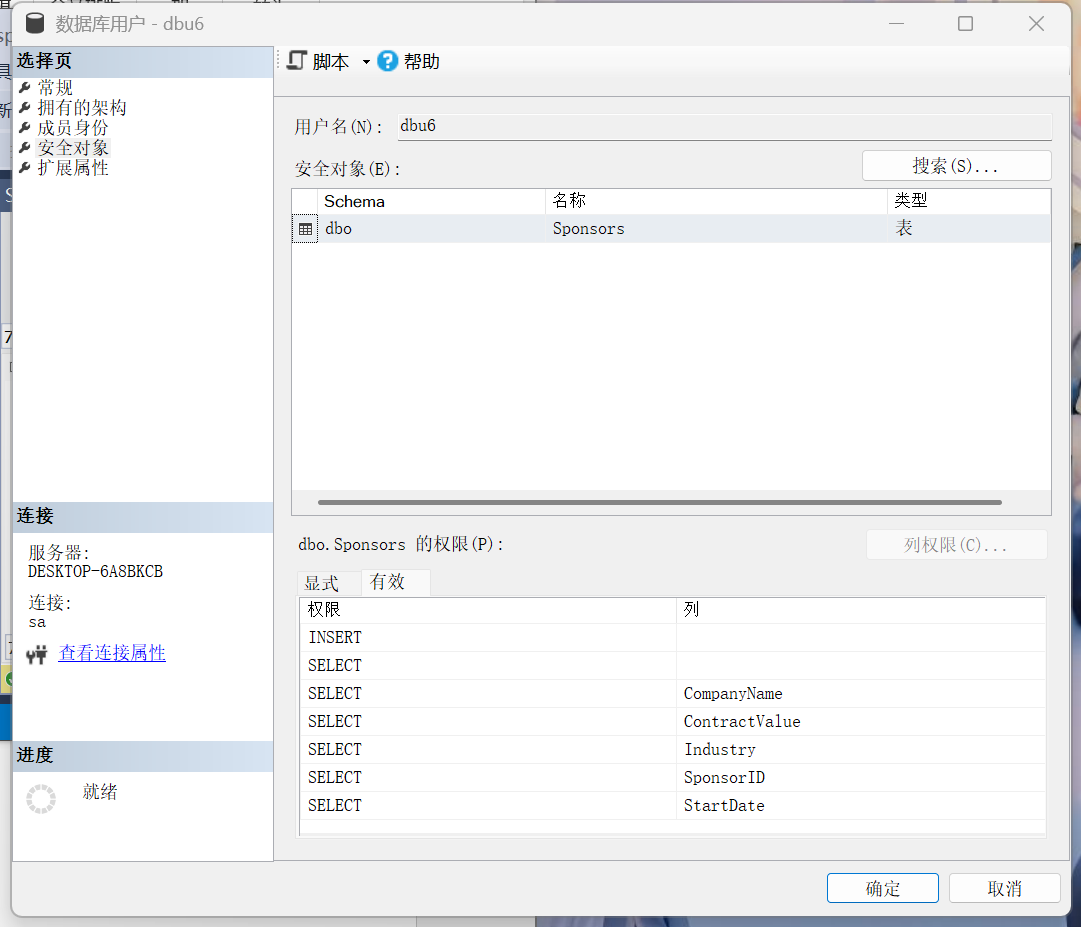
（7）把对表Sponsors的INSERT权限授予U5，并允许U5将此权限再授予其他用户。





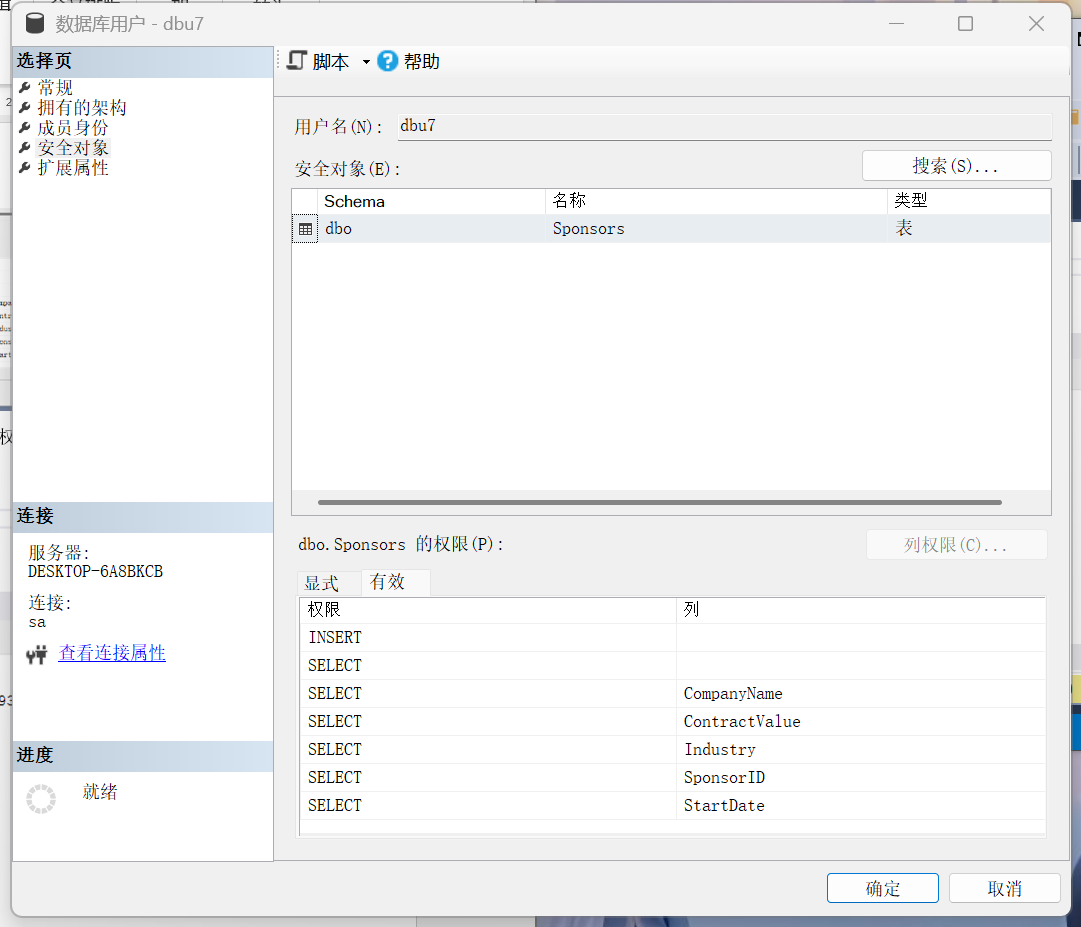
（8）用户U5将对表Sponsors的INSERT权限授予U6,并允许将权限转授给其他用户。



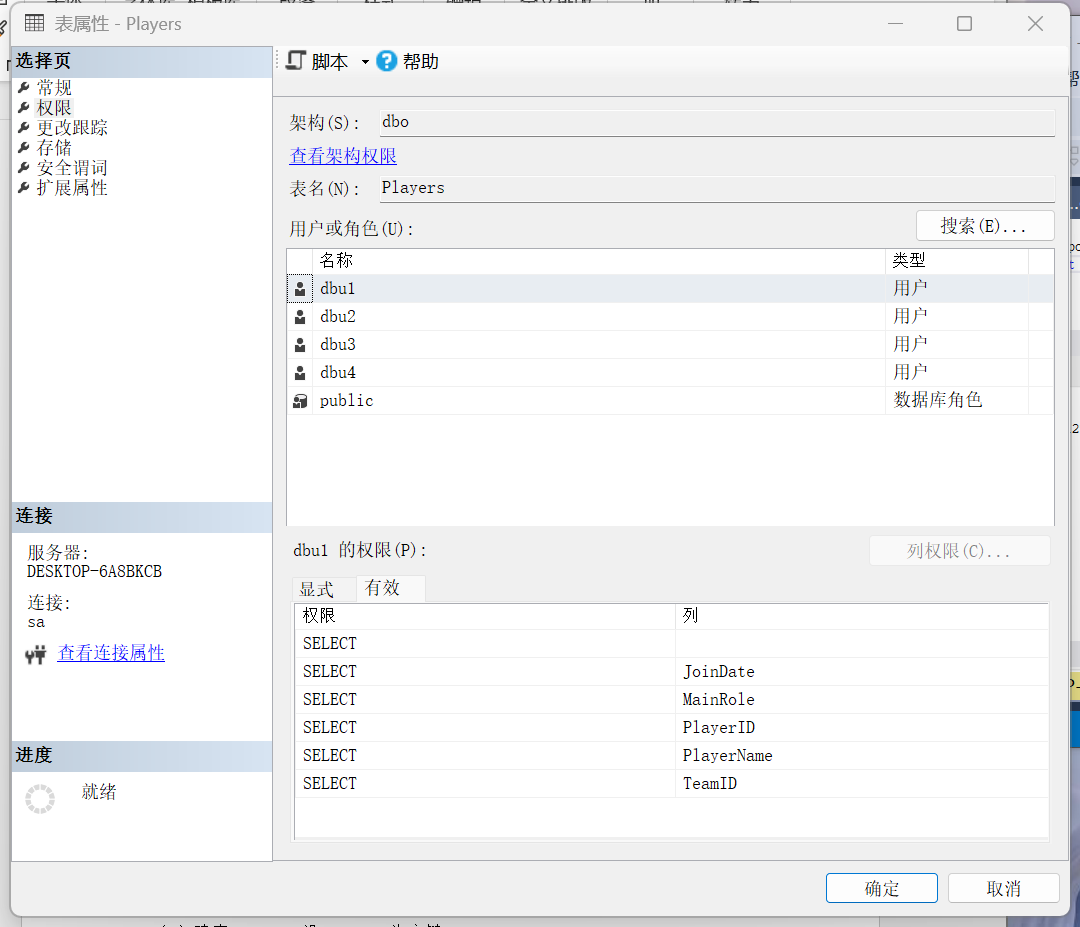


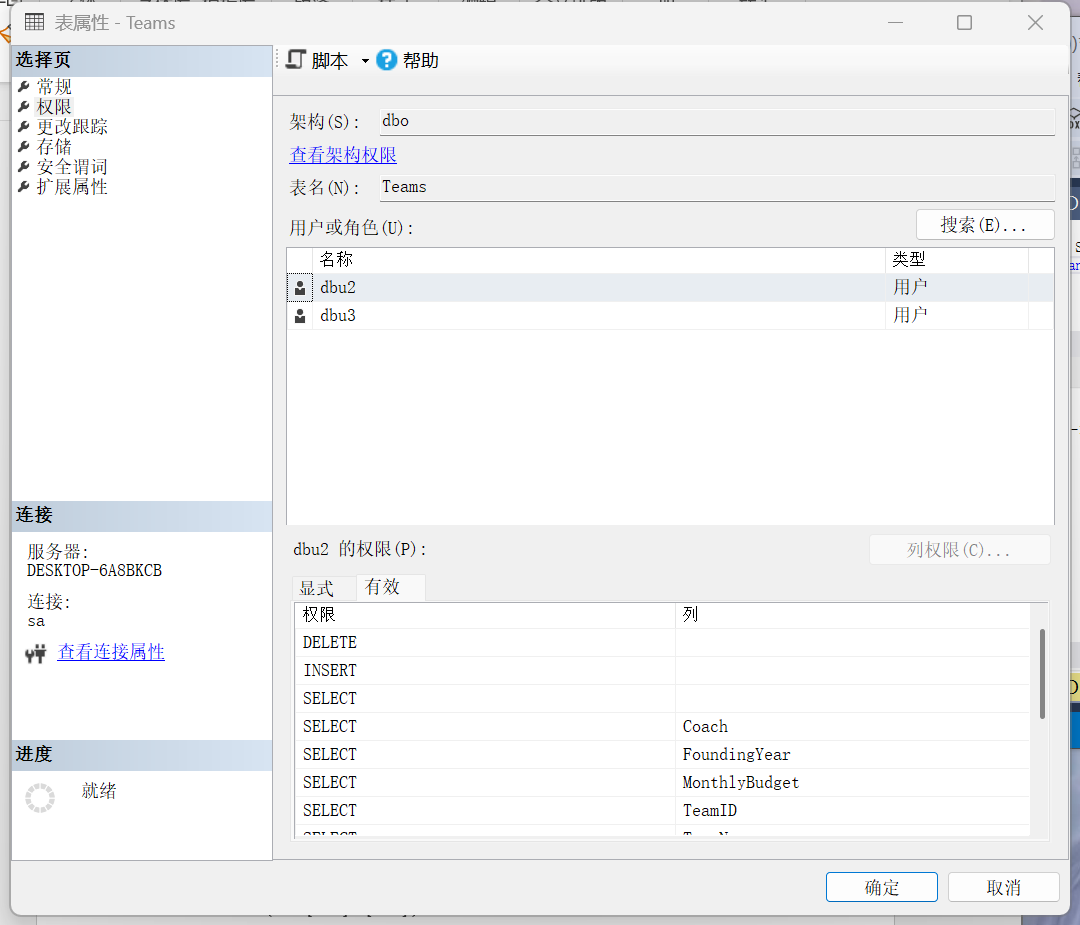
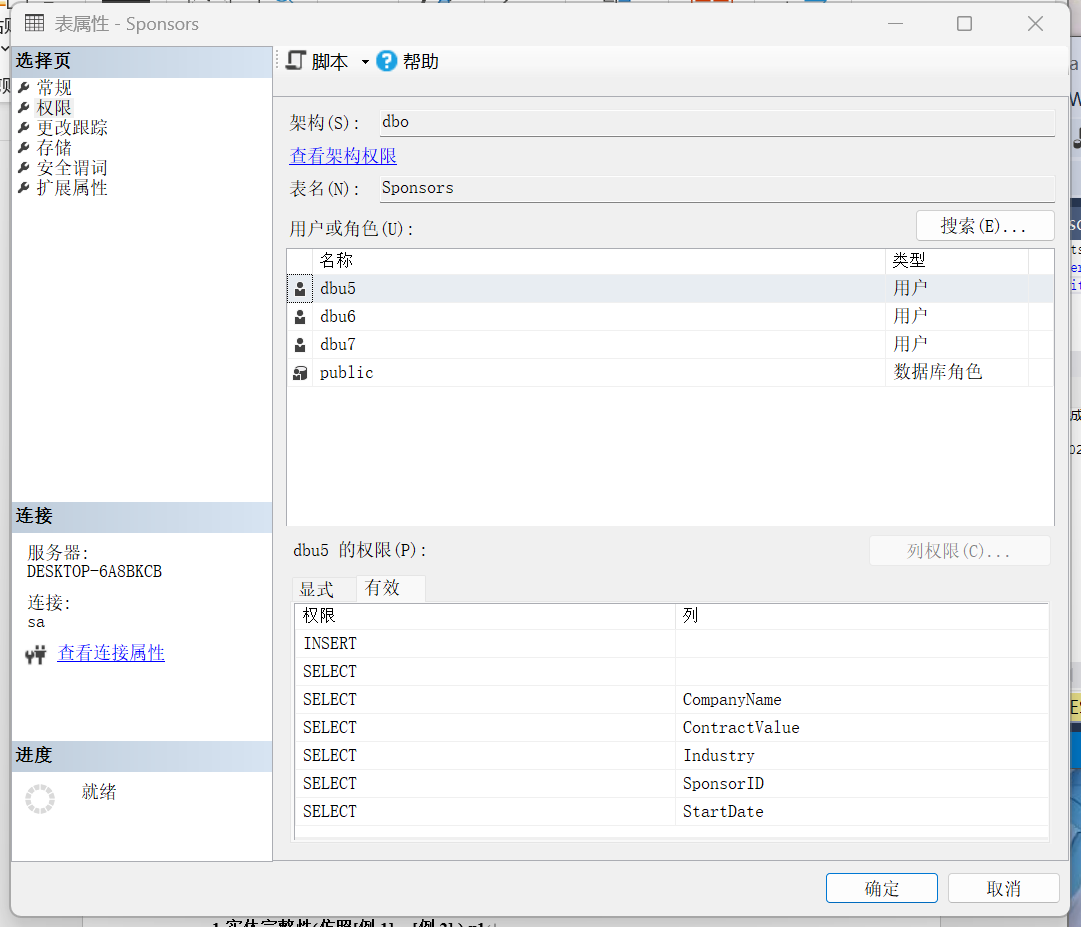
（9）用户U6将对表Sponsors的INSERT权限授予U7。





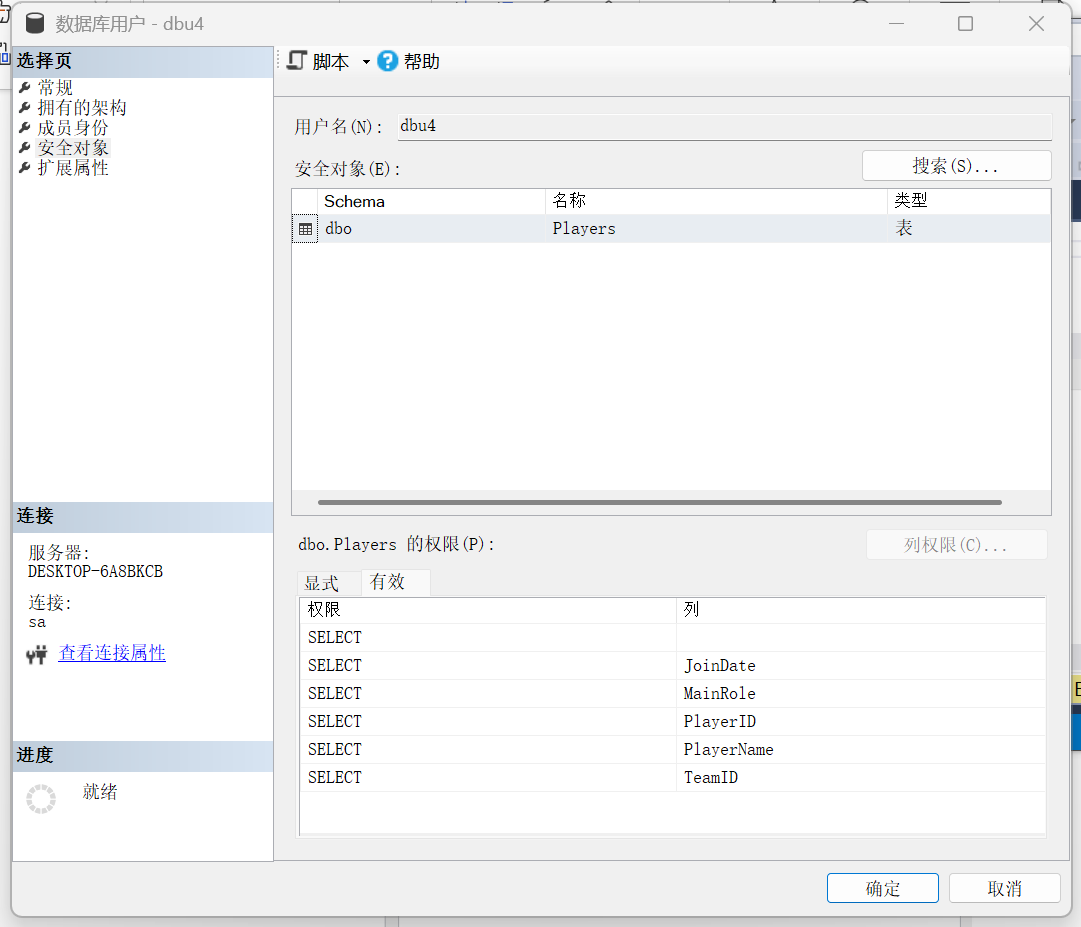
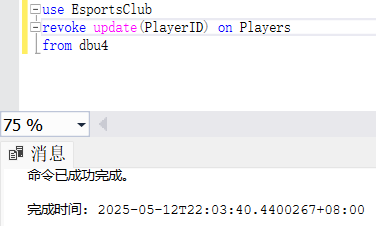
（10）最终效果



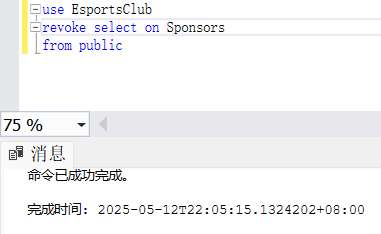


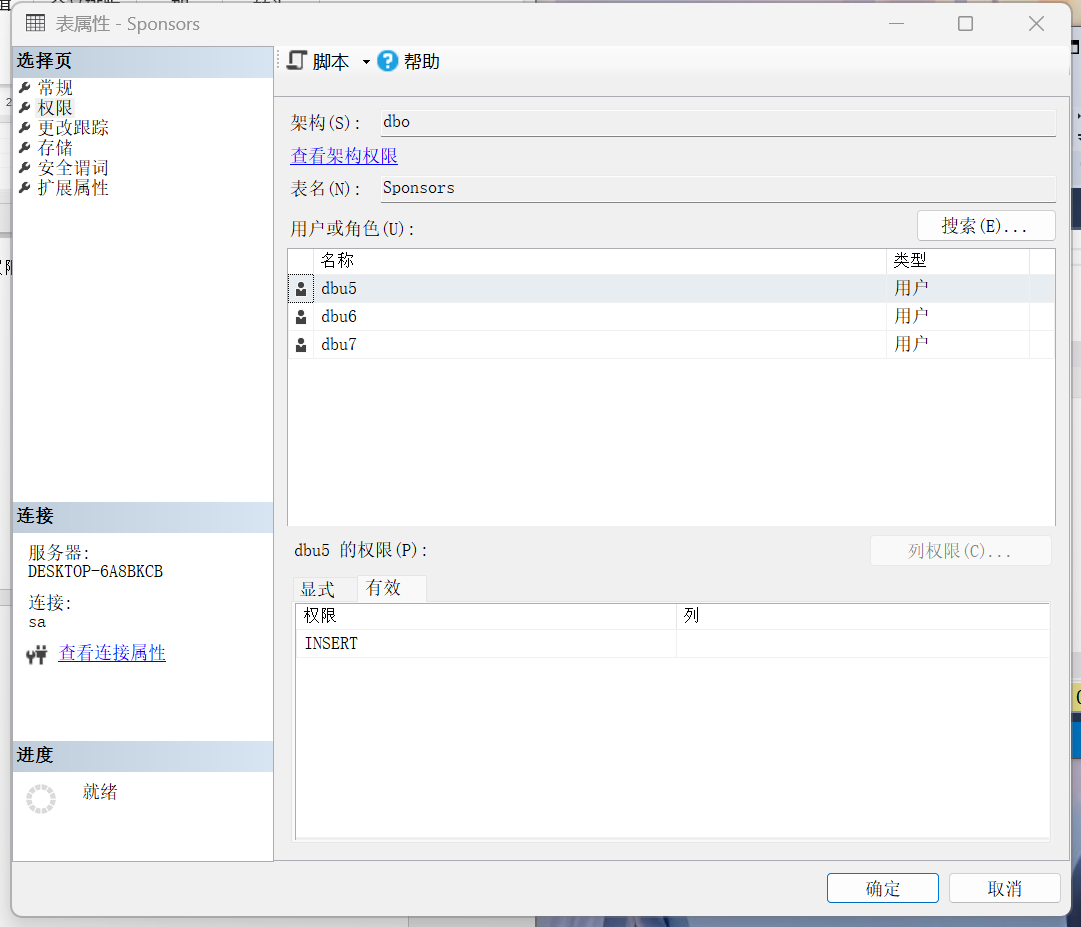
3.回收

（1）收回用户U4修改Players表PlayerID的权限。



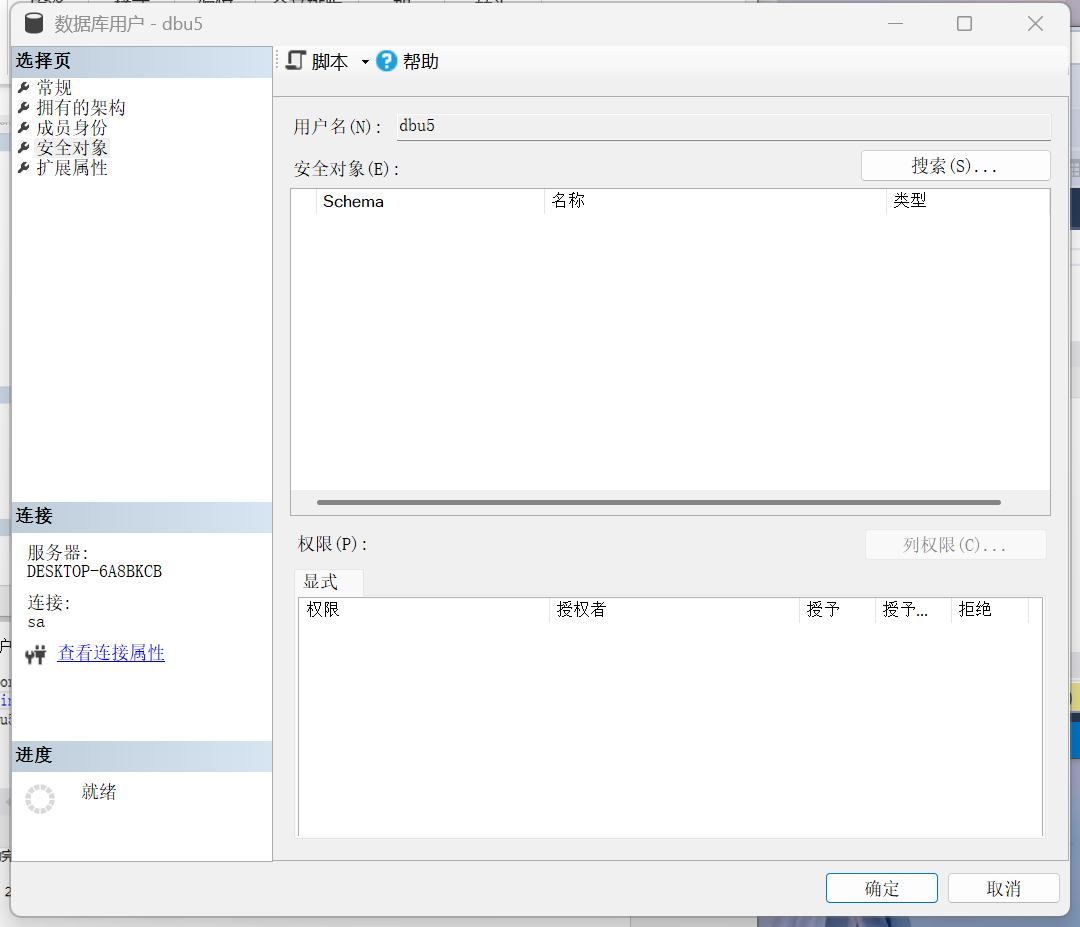
（2）收回所有用户对表Sponsors的查询权限。



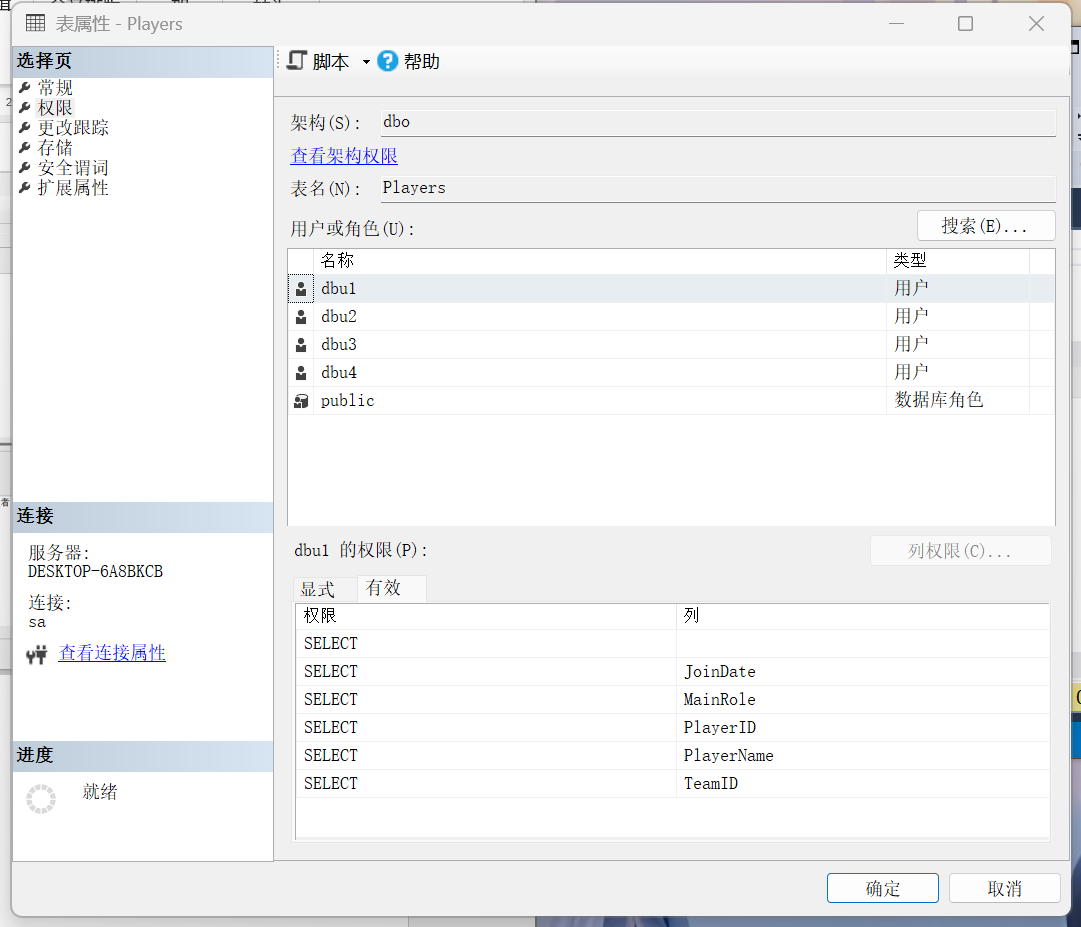


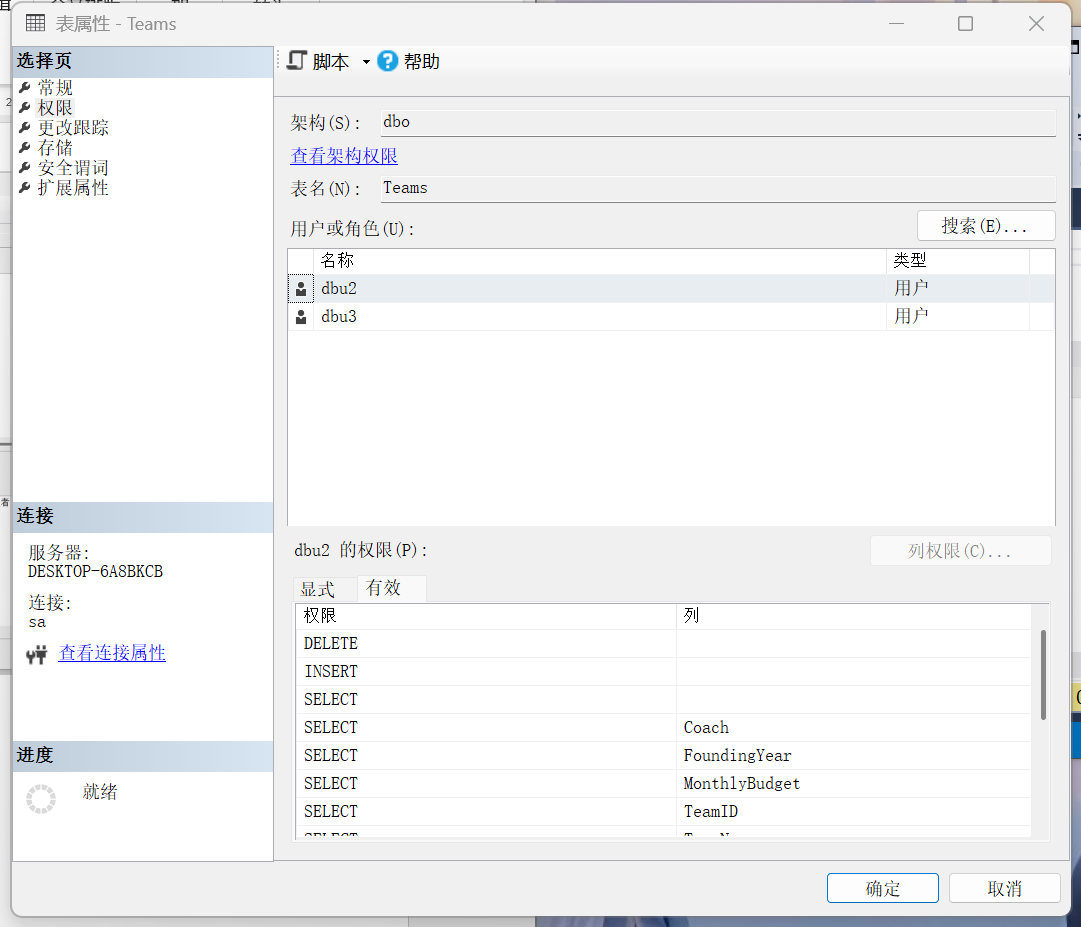
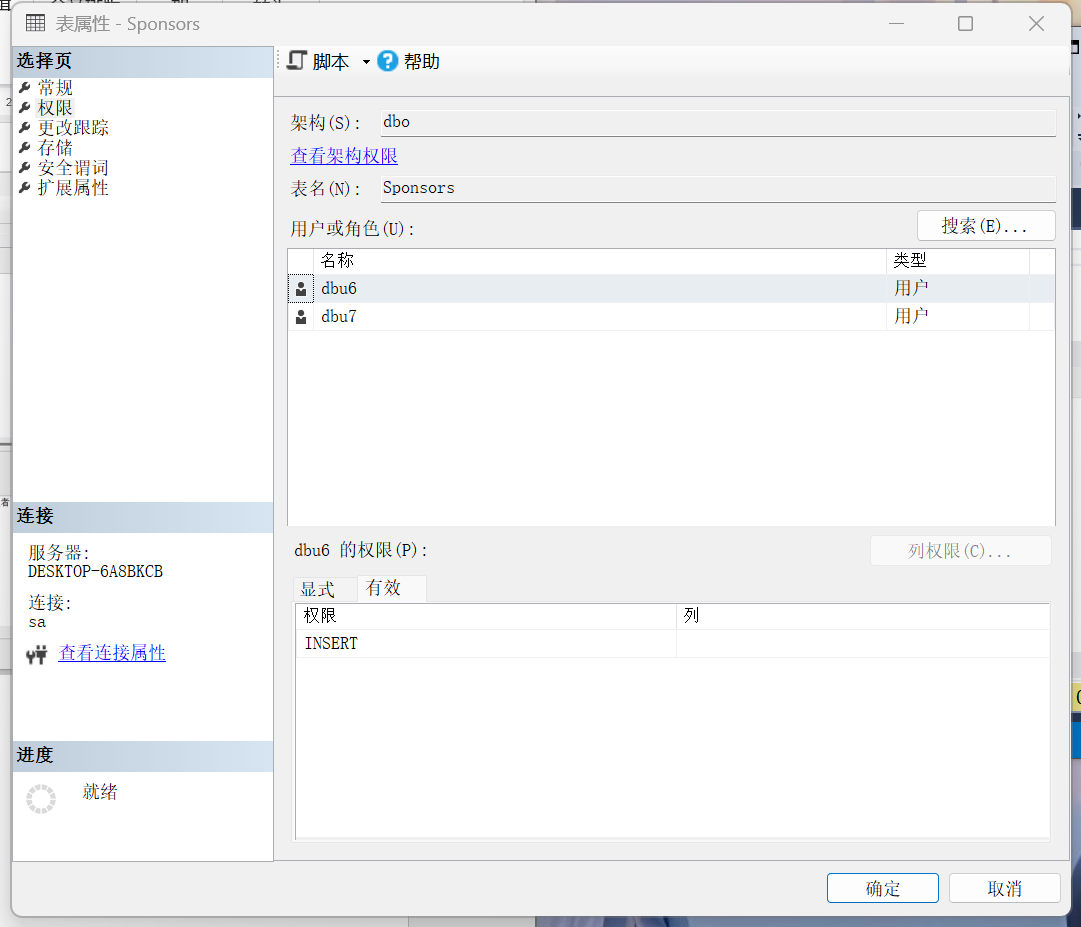
（3）收回用户U5对Sponsors表的INSERT权限。





（4）最终效果



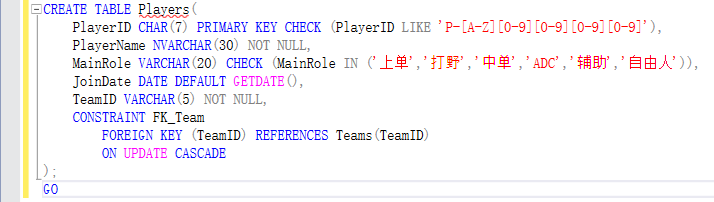


**2.2 完整性部分**

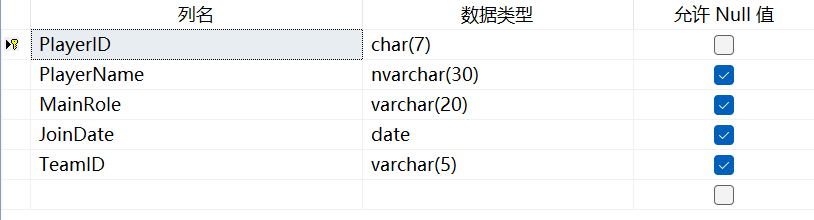
使用SQL对数据进行完整性控制，并用实验证实，当操作违反了完整性约束条件时，系统是如何处理的

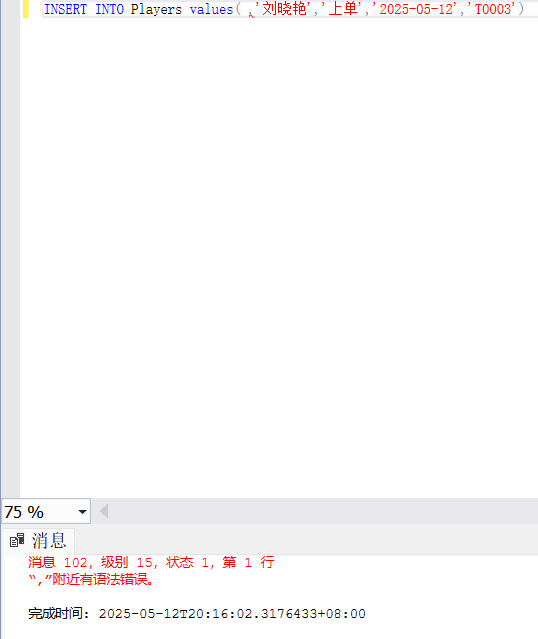
**1.实体完整性(仿照[例1]、[例2] ) x1**

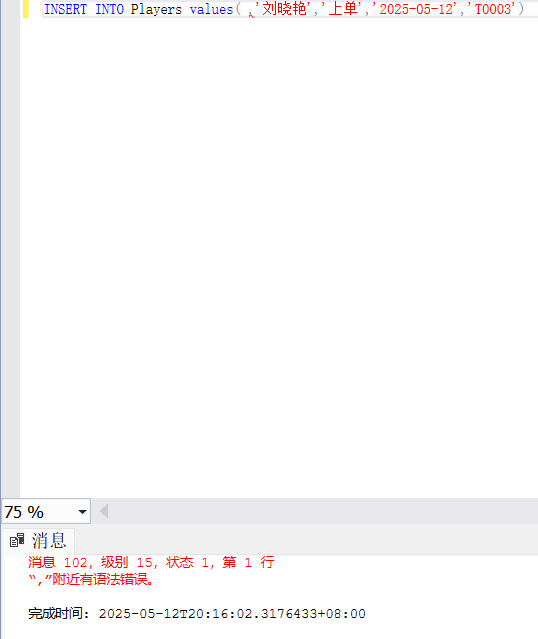
（1）建表Players，设PlayerID为主键



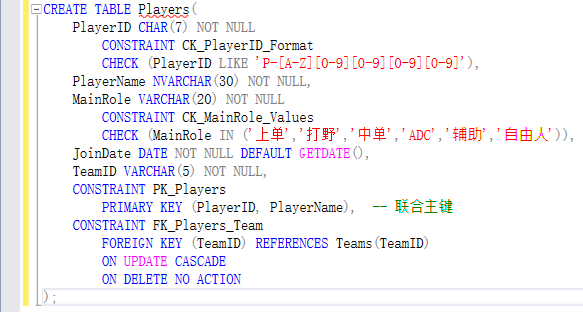
（2）已知Players表中各元素属性

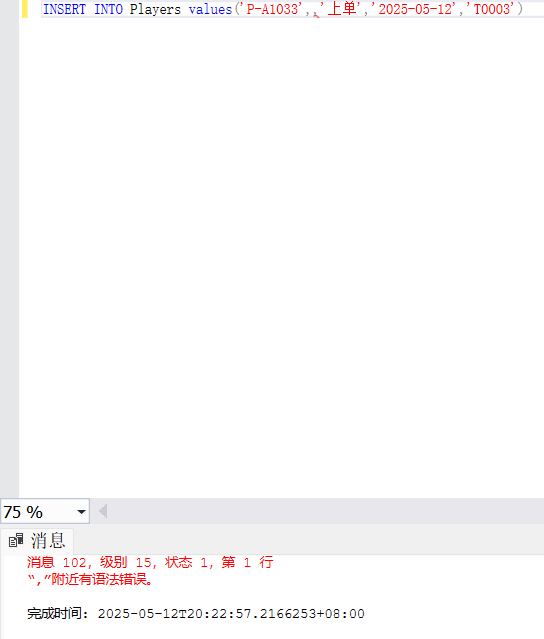


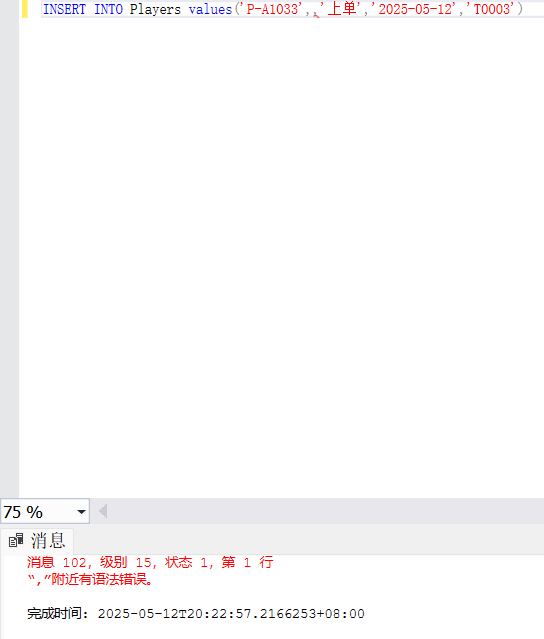
（3）可以看到主键为空会报错



（4）如果设置PlayerID和PlayerName两个主键

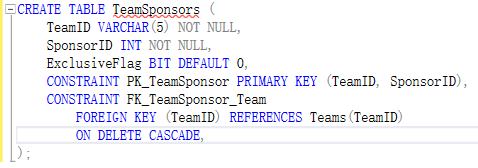


（5）则只有当两个主键都不为空时才能执行，否则会报错

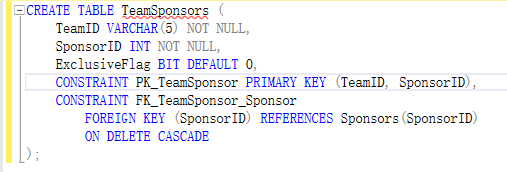


**2.参照完整性(仿照[例3]) x4**

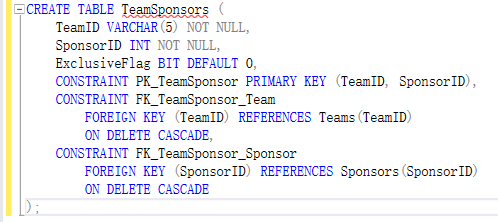
（1）设置TeamSponsors的主码TeamID参照Teams的主码



（2）设置TeamSponsors的主码SponsorsID参照Sponsors的主码



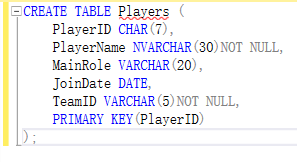
（3）设置TeamSponsors的主码TeamID参照Teams的主码同时主码SponsorsID参照Sponsors的主码

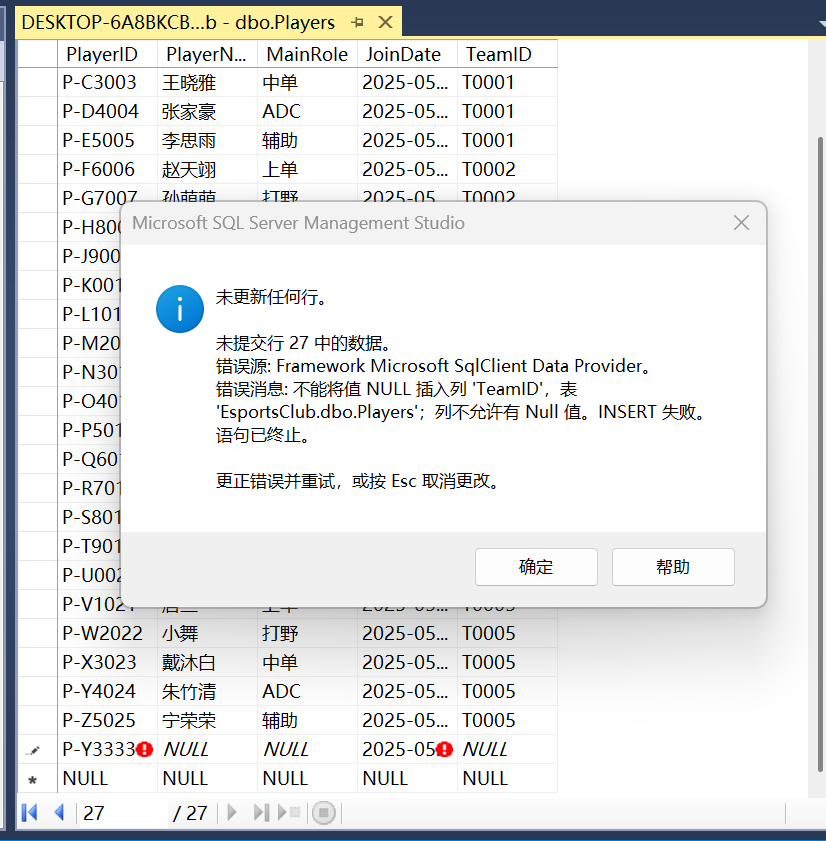


****

**3.用户定义完整性(仿照[例5]、[例6]) x1**

设置PlayerName、TeamID不为空



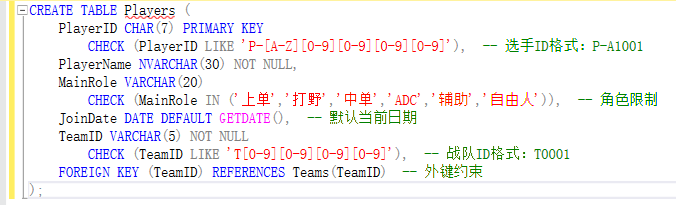
****

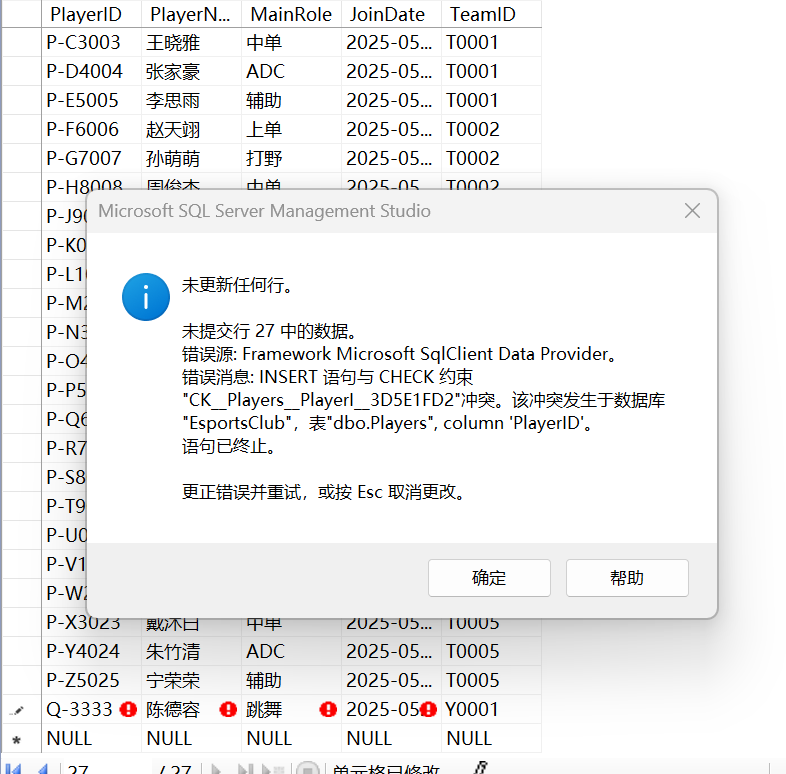
**4.CHECK短语(仿照[例7]或[例8]、[例9]) x1**

（1）设置PlayerID格式必须为​：P-[A-Z][0-9][0-9][0-9][0-9]（如 P-A1001）

（2）设置TeamID格式必须为​：T[0-9][0-9][0-9][0-9]（如 T0001）

（3）设置MainRole必须为限定角色，为指定的6种类型之一



****

**5.CONSTRAINT子句(仿照[例10]、[例13]) x1**

让TeamID字段的值只能在T0001到T0010之间

