第四章作业

陈鑫蕾 22920202202877

1.什么是数据库的安全性？

数据库的安全性是指保护数据库以防止不合法使用造成的数据泄漏，更改或破坏

2.举例说明对数据库安全性产生威胁的因素

（1）非授权用户对数据库的恶意存取和破坏。例如：一些黑客或不法分子在通过特殊手段获取到用户名和用户口令后，假冒合法用户对数据库进行读取；
（2）数据库中重要或敏感的数据泄露。例如：公司职员通过自己的工资和一些推理，推断出他人的工资；
（3）安全环境的脆弱性。数据库的安全性和网络的安全性是密切相关的，不发分子可以通过监听网络中的数据来获取到数据库信息。

4.试述实现数据库安全性控制的常用方法和技术

用户身份鉴别，多层存取控制，视图机制，审计，数据加密

5.什么是数据库中的自主存取控制方法和强制存取控制方法

自助存取控制方法：用户对于不同的数据库对象有不同的存取权限，不同的用户对同一对象也有不同的权限，而且用户还可以将其拥有的存取权限转授给其他用户

强制存取控制方法：每一个数据库对象被标以一定的密级，每一个用户首于某一个级别的许可证，对于任意一个对象，只有具有合法许可证的用户才可以存取。

6. 对学生和班级使用 GRANT 语句完成以下的授权。

（1）授予用户 U1 对两个表的所有权限，并可给其他用户授权。

GRANT ALL PRIVILEGES ON TABLE 学生，班级 TO U1 WITH GRANT OPTION;

（2）授予用户 U2 对学生表具有查看权限，对家庭住址具有更新权限。

GRANT SELECT,UPDATE(家庭住址) ON TABLE 学生 TO U2;

（3）将对班级表查看的权限授予所有用户。

GRANT SELECT ON TABLE 班级 TO PUBLIC;

（4）将对学生表的查询、更新权限授予角色 R1。

GRANT SELECT,UPDATE ON TABLE 学生 ON R1;

（5）将角色 R1 授予 U1，并且 U1 可以继续授权给其他角色。

GRANT R1 TO U1 WITH GRANT OPTION;

7. 对职工、部门使用 SQL 的 GRANT 和 REVOKE 完成授权控制。

（1）用户王明对两个表都有 SELECT 权限。

GRANT SELECT ON TABLE 职工，部门 TO 王明

（2）用户李勇对两个表都有 INSERT 和 DELETE 权限。

GRANT INSERT,DELETE ON TABLE 职工，部门 TO 李勇

（3）每个职员只对自己的记录有 SELECT 权限。

GRANT SELECT ON TABLE 职工 WHEN USER()=NAME TO ALL

（4）用户刘星对职工表有 SELECT 权限，对工资字段具有更新权限。

GRANT SELECT,UPDATA(工资) ON TABLE 职工 TO 刘星

（5）用户张新具有修改这两张表的结构的权限。

GRANT ALTER ON TABLE 职工，部门 TO 张新

（6）用户周平具有对两张表的所有权限，并可以授权他人。

GRANT ALL PRIVILEGES ON TABLE 职工，部门 TO 周平 WITH GRANT OPTION

（7）用户杨兰具有每个部门职工中 SELECT 最高工资、最低工资、平均工资的权限，不能查看每个人的工资。

CREATE VIEW V_SALARY

AS

SELECT 部门.名称，MAX(工资),MIN(工资),AVG(工资)

FROM 职工，部门

WHERE 职工.部门号=部门.部门号

GROUP BY 部门号

GRANT SELECT ON VIEW V_SALARY TO 杨兰

8.对 7 中的情况撤销权限。

（1）用户王明对两个表都有 SELECT 权限。

REVOKE SELECT ON TABLE 职工，部门 FROM 王明

（2）用户李勇对两个表都有 INSERT 和 DELETE 权限。

REVOKE INSERT,DELETE ON TABLE 职工，部门 FROM 李勇

（3）每个职员只对自己的记录有 SELECT 权限。

REVOKE SELECT ON TABLE 职工 WITH USER()=NAME FROM ALL

（4）用户刘星对职工表有 SELECT 权限，对工资字段具有更新权限。

REVOKE SELECT UPDATE(工资) ON TABLE 职工 FROM 刘星

（5）用户张新具有修改这两张表的结构的权限。

REVOKE ALTER ON TABLE 职工，部门 FROM 张新

（6）用户周平具有对两张表的所有权限，并可以授权他人。

REVOKE ALL PRIVILEGES ON TABLE 职工，部门 FROM 周平 CASCADE

（7）用户杨兰具有每个部门职工中 SELECT 最高工资、最低工资、平均工资的权限，不能查看每个人的工资。

REVOKE SELECT ON VIEW V_SALARY FROM 杨兰

DROP V_SALARY

9.解释强制存取控制机制中主体、客体、敏感度标记的含义。

（1）主体是系统中的活动实体，既包括 DBMS 所管理的实际用户，也包括代表用户的各进程；

（2）客体是系统中的被动实体，受主体操纵，包括文件、基表、索引、视图等；

（3）敏感度标记被分为若干级别，例如绝密、机密、可信、公开等。主体的敏感度标记被称为许可证等级，客体的敏感度标记被称为密级。

10.举例说明强制存取控制机制是如何确定主体能否存取客体的。

规定：（1）仅当主体的许可证级别大于或等于客体的密级时，该主体才能读取相应的客体；

（2）仅当主体的许可证级别小于或者等于客体密级时，该主体才能写相应的客体。

举例：假设敏感度标记（4 = 绝密，3 = 机密，2 = 可信，1 = 公开）

S#	Message	CLASS
S1	……	2
S2	……	3
S3	……	4

假设用户 U1 和 U2 的许可证级别分别为 3 和 2，则根据规则 U1 能查得 S1 和 S2，可写入 S2 和 S3；U2 只能查得 S1，但 S1、S2、S3 都可以写入；

11. 什么是数据库的审计功能，为什么要提供审计功能？

（1）审计功能是指 DBMS 的审计模块在用户对数据库执行操作的同时把所有操作自动记录到系统的审计日志中。审计通常是很费时间和空间的，所以 DBMS 往往都将其作为可选特征，允许 DBA 根据应用对安全性的要求，灵活地打开或关闭审计功能；

（2）原因：任何系统的安全保护措施都不是完美无缺的，蓄意盗窃破坏数据的人总可能存在。利用数据库的审计功能，DBA 可以根据审计跟踪的信息，重现导致数据库现有状况的一系列事件，找出非法存取数据的人、时间和内容等。