**习题4**

1. 什么是数据库的安全性？

**答：数据库的安全性指的是对数据库中存储的数据进行保护和管理的能力，以确保数据不被未经授权的人员访问、修改、删除或泄露。**

1. 举例说明对数据库安全性产生威胁的因素

**答：1.未经授权的访问：未经授权的用户或黑客通过各种手段获取数据库系统的访问权限，可能导致敏感数据的泄露、篡改或删除；2.SQL注入攻击：黑客利用输入验证不严格的应用程序漏洞，通过构造恶意的SQL查询语句来执行非法操作，例如删除数据、获取敏感信息等；3.未加密的数据传输：在数据传输过程中，如果数据库连接未经加密，敏感数据可能会被窃听和拦截，造成数据泄露。**

1. 试述实现数据库安全性控制的常用方法和技术

**答：1.身份认证：通过用户名和密码等身份验证机制，确保只有经过授权的用户能够访问数据库系统；2.访问控制：控制用户对数据库中数据和对象的访问权限，包括对表、视图、存储过程等进行权限控制，确保用户只能执行其被授权执行的操作；3.强制访问控制：基于安全策略强制执行对数据库对象的访问控制，确保敏感数据只能被授权用户访问。**

1. 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？

**答：1.自主存取控制：在自主存取控制中，访问权限由数据所有者或管理员自主设置和管理。每个用户或用户组被赋予对数据库对象（如表、视图、存储过程等）的特定权限，包括读取、写入、修改和删除等操作；2.强制存取控制：在强制存取控制中，访问权限由系统强制执行，基于预先定义的安全策略和标签。每个用户或用户组被分配一个安全级别或标签，每个数据库对象也被标记了一个安全级别或标签，系统根据这些标签来决定用户对数据库对象的访问权限。**

1. 对下列两个关系模式：

学生（学号，姓名，年龄，性别，家庭住址，班级号）

班级（班级号，班级名，班主任，班长）

请用SQL的GRANT语句完成下列授权功能：

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;**

1. 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;**

1. 将对“班级”表查看权限授予所有用户

**GRANT SELECT ON TABLE 班级 TO PUBLIC;**

1. 将对“学生”表的查询、更新权限授予角色R1

**GRANT SELECT,UPDATE ON TABLE 学生 TO R1;**

1. 将角色R1授予用户U1，并且U1可继续授权给其他角色

**GRANT R1 TO U1 WITH ADMIN OPTION;**

1. 今有以下两个关系模式：

职工（职工号，姓名，年龄，职务，工资，部门号）

部门（部门号，名称，经理名，地址，电话号）

请用SQL的GRANT语句和REVOKE语句（加上视图机制）实现以下授权定义或存取控制功能：

1. 用户王明对两个表有SELECT权限

**GRANT SELECT ON TABLE 职工,部门 TO 王明;**

1. 用户李勇对两个表有INSERT和DELETE权限

**GRANT INSERT,DELETE ON TABLE 职工,部门 TO 李勇;**

1. 每个职工只对自己的记录有SELECT权限

**GRANT SELECT ON TABLE 职工 WHERE USER() = NAME TO ALL;**

1. 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,UPDATE(工资) ON TABLE 职工 TO 刘星;**

1. 用户张新具有修改这两个表的结构的权限

**GRANT ALTER TABLE ON TABLE 职工,部门 TO 张新;**

1. 用户周平具有对两个表的所有权限，并具有给其他用户授权的权限

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

1. 用户杨兰具有从每个部门职工中SELECT最高工资、最低工资、平均工资的权限，但不能查看每个人的工资

**首先建立一个视图，再对这个视图定义杨兰的存取权限**

**CREATE VIEW 部门工资 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 职工.部门号;**

**GRANT SELECT ON TABLE 部门工资 TO 杨兰;**

1. 针对第6题中(1)-(7)的每一种情况，撤销各用户所授予的权限
2. **REVOKE SELECT ON TABLE 职工,部门 FROM 王明;**
3. **REVOKE INSERT,DELETE ON TABLE 职工,部门 FROM 李勇;**
4. **REVOKE SELECT ON TABLE 职工 WHEN USER() = NAME FROM ALL;**
5. **REVOKE SELECT,UPDATE ON TABLE 职工 FROM 刘星;**
6. **REVOKE ALTER TABLE ON TABLE 职工,部门 FROM 张新;**
7. **REVOKE ALL PRIVILEGES ON TABLE 职工,部门FROM 周平;**
8. **REVOKE SELECT ON TABLE 部门工资 FROM 杨兰;**

**DROP VIEW 部门工资;**

1. 理解并解释强制存取控制机制中主体、客体、敏感度标记的含义

**答：主体通常指代系统中执行操作的实体，如用户、进程、程序等。主体试图访问客体（资源）或执行某种操作。在访问控制策略中，主体是拥有或请求访问权限的实体；客体是主体试图访问的资源或对象，如文件、文件夹、数据库记录等。在访问控制策略中，客体是主体尝试访问的目标，需要受到保护或限制；敏感度标记用于标识和分类客体的敏感程度或重要性。它们通常是安全策略的一部分，用于确保敏感信息只能被授权的主体访问。标记可以是分类等级、安全等级、访问控制列表（ACL）等形式。通过敏感度标记，系统可以根据不同的安全需求对客体进行分类和控制访问。**

1. 举例说明强制存取控制机制是如何确定主题能否存取客体的

**答：假设一个政府机构拥有一份包含机密级别信息的文件，并且实施了MAC机制来保护这些信息。在这个例子中：主体可以是各种实体，比如用户、程序或者进程，比如一个政府工作人员；客体是需要受到保护的资源，比如文件、数据库等，比如政府机密文件；政府机构对其文件进行了敏感度标记，指明了文件的安全级别。比如，这份机密文件被标记为"Secret"级别。**

**具体实施机制可能是这样的：系统管理员定义了访问策略，规定只有拥有"Top Secret"级别权限的主体才能够读取"Secret"级别的文件。a是政府机构的工作人员，她拥有"Top Secret"级别的权限。当a尝试访问这份机密文件时，MAC机制会检查她的权限。因为a拥有足够的权限（"Top Secret"级别），系统会允许她访问这份文件。如果另一个主体，比如普通政府职员b，尝试访问这份文件，由于他的权限不够，MAC机制会拒绝他的访问请求。**

1. 什么是数据库的审计功能，为什么要提供审计功能

**答：数据库的审计功能是一种记录和监控数据库操作的机制，用于跟踪数据库的活动并生成相关的审计日志。它可以记录诸如用户登录、数据修改、查询操作等数据库活动，并将这些信息存储在审计日志中，以供日后审查、分析和追踪。**