|  |  |
| --- | --- |
| 第4章作业 | |
| 姓名 | 潘腾凯 |
| 学号 | 37220232203786 |
| 班级 | 01班 |

1. **什么是数据库的安全性？**

答：数据库的安全性是指保护数据库，以防不合法使用所造成的数据泄露、篡改或破坏。

1. **举例说明对数据库安全性产生威胁的因素。**

答：数据库安全性面临多种威胁，恶意攻击方面，SQL 注入攻击通过输入恶意 SQL 语句非法获取或修改数据，恶意软件会窃取数据或破坏数据库；人为因素中，内部人员可能泄露敏感信息，误操作会导致数据丢失或损坏；系统漏洞包括操作系统和数据库软件的漏洞，易被攻击者利用；网络安全问题有网络监听获取登录信息和数据，以及拒绝服务攻击使服务器瘫痪 。

1. **试述实现数据库安全性控制的常用方法和技术。**

答：主要有：

1. 用户身份检测：系统提供多种方式让用户标识自己的名字或身份。用户要使用数据库系统时，需由系统进行核对，通过鉴定后才可以使用数据库。
2. 入侵检测：用户进入数据库系统时，系统依据预先设置的检测规则实时进行入侵分析，若发现入侵情况，则实时进行处理。
3. 多层存取控制：系统提供用户权限定义和合法权限检查功能，用户只有获得某种权限，才能访问数据库中的某些数据。控制机制主要有自主存取控制和强制存取控制。
4. 视图机制：为不同的用户定义不同的视图。通过视图机制，向无权存取的用户隐藏保密的数据，从而自动对数据提供一定程度的安全保护。
5. 审计：建立审计日志，自动记录用户对数据库的所有操作并放入审计日志，审计员利用审计信息，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员、时间和内容等。
6. 存储保护：对存储的数据进行加密处理。
7. 传输加密保护： 对传输的数据加密处理，从而阻止不知道解密算法的人获知数据的内容
8. **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：自主存取中的“自主”含义是：用户可以将自己拥有的存取权限“自主”地授予别人，即用户具有一定的自主权。

强制存取控制方法：每一个数据对象被强制地标以一定的密级，每一个用户也被强制地授予某一个级别的许可证。系统规定只有具备某一许可证级别的用户才能存取某一级别的数据对象。它提供了更高程度的安全性。

**5.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。**

**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。**

**③将对“班级”表查看权限授予所有用户。**

**④将对“学生”表的查询、更新权限授予角色R1.**

**⑤将角色R1授予用户U1，并且U1可继续授权给其他角色。**

答：（1）GRANT ALL PRIVILEGES ON TABLE 学生，班级 TO UI WITH GRANT OPTION;

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

（3）GRANT SELECT ON TABLE 班级 TO PUBLIC;

（4）GRANT ROLE R1;

GRANT SELECT,UPDATE ON TABLE 学生 TO R1;

（5）GRANT R1 TO U1 WITH ADMIN OPTION;

**6.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。**

**②用户李勇对两个表有INSERT和DELETE权限。**

**③每个职工只对自己的记录有SELECT权限。**

**④用户刘星对职工表有SELECT权限，对“工资”字段具有更新权限。**

**⑤用户张新具有修改这两个表的结构的权限。**

**⑥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。**

**⑦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。**

答：(1)GRANT SELECT, UPDATE ON TABLE 职工，部门 TO 王明;

(2)GRANT INSERT, DELETE ON TABLE 职工，部门 TO 李勇;

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

(4)GRANT SELECT, UPDATE(工资) ON TABLE 职工 TO 刘星;

(5)GRANT ALTER TABLE ON TABLE 职工，部门 TO 张新;

(6)GRANT ALL PRIVILEGES ON TABLE 职工,部门 TO 周平 WITH GRANT OPTION;

(7)先创建视图

CREATE VIEW 部门工资 AS

SELECT 部门.部门号, 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.部门号

再把查询该视图的权限给杨兰

GRANT SELECT ON 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。**

答：(1)REVOKE SELECT, UPDATE ON TABLE 职工，部门 FROM 王明;

(2)REVOKE INSERT, DELETE ON TABLE 职工，部门 FROM 李勇;

(3)REVOKE SELECT ON TABLE 职工 WHEN USER() = NAME FROM ALL;

(4)REVOKE SELECT, UPDATE(工资) ON TABLE 职工 FROM 刘星;

(5)REVOKE ALTER TABLE ON TABLE 职工，部门 FROM 张新;

(6)REVOKE ALL PRIVILEGES ON TABLE 职工,部门 FROM 周平;

(7)REVOKE SELECT ON 部门工资 FROM 杨兰;

**8.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：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。

客体：是系统中的被动实体，是受主体操纵的，包括文件、基本表、索引、视图等。

敏感度标记：对于主体和客体，DBMS为它们每个实例指派一个敏感度标记。敏感度标记被分为若干级别，例如，绝密级、机密级、秘密级、公开等。主体的敏感度标记称为许可证级别，客体的则称为密级。

**9.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。**

答：

假设数据库系统的安全级别从低到高为：

Public < Confidential < Secret < TopSecret

用户与安全级别：

用户A：许可证级别为 Public

用户B：许可证级别为 Confidential

用户C：许可证级别为 Secret

用户D：许可证级别为 TopSecret

表与密级：

表 Ptable：密级为 Public

表 Ctable：密级为 Confidential

表 Stable：密级为 Secret

表 TStable：密级为 TopSecret

读取规则：

主体许可证级别 ≥ 客体密级（高级别用户可读取低密级或同级数据，但不能读取更高密级数据）

写入规则：

主体许可证级别 ≤ 客体密级（用户可写入同级或更高密级客体，但不能写入更低密级客体（防止高密级数据泄露到低密级））。

那么根据存取规则，用户D只能读取和写入Ptable；用户B可以读取Ptable和Ctable，且可以修改Ctable。

1. **什么是数据库的审计功能，为什么要提供审计功能？**

答：审计是DBMS提供的一种事后检查的安全机制，即再用户对数据库执行操作的同时，所有这些操作会被自动记录到系统的审计日志中。审计员可以根据审计日志中记录的信息，分析和重现导致数据库现状的一系列事件，找出非法存取数据的人员、时间和内容等。



