**数据库作业 第4章**

**22920212204392 黄勖**

**1.什么是数据库的安全性?**

答：数据库的安全性是指对数据库中存储的数据进行保护和防护，以确保数据不会被未经授权的人员或系统访问、修改、删除或泄露。

**2.举例说明对数据库安全性产生威胁的因素。**

答：数据库安全性可能受到以下因素的威胁：

1. 未授权访问：未经授权的用户或黑客可能会尝试访问数据库，以获取敏感信息或进行破坏。
2. 数据泄露：数据库可能被黑客攻击或内部泄露，导致敏感信息泄露。
3. 注入攻击：黑客可以通过恶意注入代码来执行未经授权的操作，例如删除数据或获取敏感信息。
4. 无效授权：如果数据库管理员或应用程序开发人员在配置访问控制时疏忽大意，则可能会导致错误的授权，从而允许用户访问他们不应该访问的数据。
5. 数据库漏洞：数据库软件中的漏洞可能会被黑客攻击，以获取敏感信息或执行未经授权的操作。
6. 社交工程攻击：黑客可能会使用社交工程技巧来欺骗用户或管理员，以获取访问数据库所需的凭据。
7. 身份验证问题：弱密码或没有适当的身份验证措施可能使黑客能够轻松地登录数据库系统，以获取敏感信息或执行未经授权的操作。

**4.试述实现数据库安全性控制的常用方法和技术。**

答： 以下是实现数据库安全性控制的常用方法和技术：

1. 访问控制：通过为用户或组分配权限和角色来限制访问数据库的能力。这包括控制对表、视图和存储过程的访问权限，以及限制对敏感数据的访问权限。
2. 数据加密：使用加密技术来保护数据库中的数据。这可以通过使用对称密钥加密、公钥加密或哈希算法等技术来实现。
3. 审计跟踪：记录数据库中的所有活动，包括对数据的访问、修改和删除。这可以帮助识别潜在的安全问题，以及跟踪可能的数据泄露。
4. 安全配置：通过配置安全设置，如启用强密码策略、关闭不必要的服务和端口等来减少数据库的攻击面。
5. 数据备份和恢复：定期备份数据库可以保护数据免受丢失和损坏的影响。此外，备份还可以用于恢复数据，以应对数据泄露和其他安全事件。
6. 更新和修补：定期更新数据库软件和操作系统可以减少潜在的漏洞和安全问题。此外，及时修补已知的漏洞和安全问题也可以保护数据库免受攻击。
7. 网络安全：保护数据库服务器免受网络攻击，包括防火墙和入侵检测系统等。

**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?**

答：数据库中的自主访问控制方法和强制访问控制方法是两种不同的访问控制方法：

1. 自主访问控制方法（Discretionary Access Control，简称 DAC）：是一种基于主体的访问控制方法，即访问数据库中的对象（如表、视图、存储过程等）由主体（如用户、角色或组）自行决定。在这种方法中，主体被赋予一定的权限来访问对象，这些权限可以是读、写、修改或删除等。这种访问控制方法的优点是灵活性高，可以满足不同用户的不同需求。但是，缺点是可能导致管理员失去对数据库的控制。
2. 强制访问控制方法（Mandatory Access Control，简称 MAC）：是一种基于标签的访问控制方法，即访问数据库中的对象由系统根据预定义的安全策略来决定。在这种方法中，每个对象都被分配了一个安全级别或标签，访问对象的主体也被分配了一个安全级别或标签，系统会根据这些安全级别或标签来控制对对象的访问。这种方法的优点是可以强制执行安全策略，防止信息泄露和未经授权的访问。但是，缺点是缺乏灵活性，不太适用于需要灵活管理访问控制的情况。

**6.** **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）**

**使用GRANT完成下列授权功能：**

（1） 授予用户U1拥有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 TO R1;

（5） 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 GRANT OPTION;

**7．今有两个关系模式：**

**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和REVOKE语句（加上视图机制）完成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 WHEN 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所有权限（读，插，改，删数据），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，他不能查看每个人的工资。

CREATE VIEW 部门工资 AS

SELECT 部门.名称 MAX(职工.工资),MIN(职工.工资),AVG(职工.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;

GRANT SELECT ON 部门工资 TO 杨兰;

**8.针对习题7中(1) ~ (7)的每一种情况，撤销各用户所授予的权限。**

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

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

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

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

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

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

(7) REVOKE SELECT ON TABLE 部门工资 FROM 杨兰；

DROP VIEW 部门工资；

**9.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（Subject）：指可以访问系统资源的实体，如用户、进程、程序等。在MAC机制中，主体被分配了一个安全级别或标记，该标记表示主体的安全级别，控制主体对系统资源的访问。

客体（Object）：指系统资源，如文档、目录、数据库等。在MAC机制中，每个客体也被分配了一个安全级别或标记，该标记表示客体的安全级别，控制主体对客体的访问。

敏感度标记（Security Label）：指用于标识客体或主体的安全级别或标记，也称为安全属性或安全标记。在MAC机制中，敏感度标记被用于控制主体对客体的访问，如主体只能访问安全级别等于或低于其自身安全级别的客体。

**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。**

答：强制访问控制（Mandatory Access Control，MAC）机制是一种基于标记的访问控制方法，它通过为主体和客体分配安全级别或标记来控制主体对客体的访问。下面是一个例子，说明MAC机制如何确定主体能否访问客体：

假设有两个文档A和B，它们分别被分配了不同的安全级别，文档A的安全级别为“秘密”，文档B的安全级别为“机密”。现在有两个用户Alice和Bob，他们的安全级别分别为“秘密”和“机密”。根据MAC机制的规则，只有Alice可以访问文档A，只有Bob可以访问文档B。因为Alice和Bob的安全级别分别等于或高于他们要访问的文档的安全级别，所以他们可以访问文档。而如果有一个用户Charlie，他的安全级别为“公开”，那么他既不能访问文档A也不能访问文档B，因为他的安全级别低于这些文档的安全级别。

**11．什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指记录和跟踪数据库操作的功能，可以记录数据库中的访问、修改、删除等操作，并保存这些操作的详细信息以供审计。数据库的审计功能是一个非常重要的安全措施，它可以帮助管理员追踪和识别可能存在的安全漏洞、违规操作和未经授权的访问。

为什么要提供审计功能？首先，审计功能可以帮助数据库管理员监测和检测数据库中的安全事件和异常行为，如非法登录、数据泄漏、数据篡改等。其次，审计功能可以提供完整性证据和法律依据，用于支持法律诉讼和监管合规性要求。此外，许多行业标准和法规要求数据库必须具备审计功能，如金融行业的PCI-DSS（Payment Card Industry Data Security Standard）标准、医疗行业的HIPAA（Health Insurance Portability and Accountability Act）法规等。