Assignment 2: Database Security and Authorization

Date handed-out: May, 04, Monday, 2025
Date submission due: May, 16, Friday 2025 23:55

Objectives:

In this assignment, students will investigate the Discretionary Access Control for a company and use SQL to enforce it.

Notes:

1. Discretionary Access Control is based on the concept of access rights, or privileges, and mechanism for giving users such privileges.
2. A privilege allows a user to access some data object in a certain manner (e.g., to read or to modify).
3. A user who creates a database object such as a table or a view automatically gets all applicable privileges on that object.
4. The DBMS subsequently keeps track of how these privileges are granted to other users, and possibly revoked, and ensures that at all times only users with the necessary privileges can access an object.
5. SQL supports Discretionary Access Control through the GRANT and REVOKE commands.

Questions:

You are the DBA for the **Dream** Company, and you create a relation called Staff with fields staff_name, department, and salary. For authorization reasons, you also define views StaffNames (with staff_name as the only attribute) and DepartmentInfo with fields department and averagesalary. The latter lists the average salary for each department. For implementing the following questions you can use your choice of DBMS. You can use Oracle, MySQL or alternatives of MYSQL such as MariaDB or PostgreSQL.

1. Create an account called **DreamDBA** and create the Staff relation and the views specified above with this account. In your report, you need to include the relevant SQL queries, explain your response and you need to also include screenshots to demonstrate that you run the relevant queries.
2. Create another account called **passiveUser** such that he can only see the average department salaries.
3. Imagine that in your database you have information about two departments called Toy and CS. What privileges should be granted to **passiveUser** if he needs to know only average department salaries for the Toy and CS departments?
4. You want to authorize your assistant (**DreamAssistant**) to five people (you will probably tell him who to fire, but you want to be able to delegate this task), to check on who is an employee, and to check on average department salaries. What privileges should you grant?
5. Continuing with the preceding scenario, you want your assistant to be able to look at the salaries of individuals. Does your answer to the previous question ensure this? Be specific: Can your assistant possibly find out salaries of some individuals (depending on the actual set of tuples), or can your assistant always find out the salary of any individual that he wants to?

6. You want to give your assistant the authority to allow other people to read the StaffNames view. Show the appropriate commands.
7. Your assistant defines two new views using the StaffNames view. The first is called AtoRNames and simply selects names that begin with a letter in the range A to R. The second view is called HowManyNames and counts the number of names. You are so pleased with this achievement that you decide to give your assistant the right to insert tuples into the StaffNames view. Show the appropriate command, and describe what privileges your assistant has after this command is executed.
8. Your assistant allows **DreamTodd** to read the StaffNames relation and later quits. You then revoke the assistant's privileges. What happens to DreamTodd's privileges?
9. You decide to go on an extended vacation, and to make sure that emergencies can be handled, you want to authorize your boss **DreamBoss** to read and modify the Staff relation and the StaffName relation (and DreamBoss must be able to delegate authority, of course, since he is too far up the management hierarchy to actually do any work). Show the appropriate SQL statements. Can DreamBoss read DepartmentInfo view?
10. After returning from your (wonderful) vacation, you see a note from DreamBoss, indicating that he authorized his assistant **DreamBossAsist** to read the Staff relation. You want to revoke DreamBossAsisst's SELECT privilege on Staff, but you don't want to revoke the rights that you gave to DreamBoss, even temporarily. Can you do this in SQL?
11. Later you realize that DreamBoss has been quite busy. He has defined a view called AllNames using the view StaffNames, defined another relation called EmployeeNames that he has access to (but that you cannot access), and given his assistant DreamBossAssist the right to read from the AllNames view. DreamBossAssist has passed this right on to his friend Susan. You decide that even at the cost of annoying DreamBoss by revoking some of his privileges, you simply have to take away DreamBossAsisst and Susan's rights to see your data. What REVOKE statement would you execute? What rights does DreamBoss have on Staff after this statement is executed? What views are dropped as a consequence?

Deliverables:

1. You need to submit a report that includes all the answers for the questions above including your **SQL** statements and **screenshots** to demonstrate that you run the query. Please make sure that your SQL queries are clearly given and explained clearly what they do and their outputs.
2. You need to implement the given scenario in your choice of Database Management System and you will be also asked to give a **demo**. You can use Oracle, MySQL or alternatives of MYSQL such as MariaDB or PostgreSQL.

Rules:

1. If you took this course before, you need to use another DBMS and submit this assignment.
2. If you fail to give demo, you will receive zero automatically.