CS 3306-01 Databases 2

Instructor: Professor David Nagus

Name: Ryohei Hayashi

Learning Journal 4

**Introduction**

In this assignment, I will create a new table, "DriverAccidentCount," to record the number of accidents per driver based on a car insurance company's database. Additionally, access privileges will be granted to the "Manager" role only. We will also create views based on specific locations and explain how these contribute to improving database security. The goal is to deepen understanding of database management and security.

**Creation of DriverAccidentCount Table and Granting Manager Privileges**

a. Table Creation and Privilege Granting

I will create a new table, "DriverAccidentCount," and restrict access to this table so that only managers can view it. The following SQL statements will be used:

SQL Statements:

```sql

CREATE TABLE DriverAccidentCount AS

SELECT driverID, COUNT(accidentNo) AS accidentCount

FROM Owns

JOIN AccidentDetails USING (PossessID)

GROUP BY driverID;

GRANT SELECT ON DriverAccidentCount TO ROLE Manager;

```

Explanation:

1. `CREATE TABLE DriverAccidentCount AS SELECT`

This statement calculates the number of accidents each driver has been involved in and stores the result in the "DriverAccidentCount" table. It joins the `Owns` table with the `AccidentDetails` table and uses the `COUNT(accidentNo)` function to group by `driverID`, thus summarizing the accident count per driver.

1. `GRANT SELECT ON DriverAccidentCount TO ROLE Manager;

`This statement grants the `SELECT` privilege on the `DriverAccidentCount` table to users with the "Manager" role. This ensures that only users assigned the Manager role can view the table, protecting sensitive information.

b. How Role Restriction Enhances Database Security

Role-based access control (RBAC) is an effective way to enhance database security. By using the `GRANT` statement to restrict access to the "Manager" role, security is strengthened in the following ways:

1. Restricted Access and Management

With RBAC, only users with specific roles can access sensitive data, preventing unauthorized access. In this case, since the `DriverAccidentCount` table contains accident count information, limiting access to managers ensures that this information is secured.

1. Improved Auditing and Compliance

Clearly defined access restrictions make it easier to track who has access to specific data, which benefits auditing and compliance. This enables quicker response to any unauthorized use of data and ensures adherence to security regulations.

1. Implementation of the Principle of Least Privilege

By assigning users only the minimum necessary privileges for their tasks, RBAC helps enforce the Principle of Least Privilege. In this scenario, users other than managers are not granted access to view accident counts, ensuring data security by preventing unnecessary access.

**Creation of Views for Specific Locations**

a. View Creation

Next, I will create views based on specific locations. The following SQL statements will create views for accidents that occurred in "Southampton," "Leicester," and "Nottingham."

SQL Statements:

```sql

CREATE VIEW SouthhamptonView AS

SELECT \*

FROM Accident

WHERE location = 'Southampton';

CREATE VIEW LeicesterView AS

SELECT \*

FROM Accident

WHERE location = 'Leicester';

CREATE VIEW NottinghamView AS

SELECT \*

FROM Accident

WHERE location = 'Nottingham';

```

Explanation:

1. Creation of SouthhamptonView

This view displays accident information specifically for "Southampton." It filters the data from the `Accident` table where the location is "Southampton," ensuring that data from other locations is not accessed.

1. Creation of LeicesterView

Similarly, `LeicesterView` displays only accident data for "Leicester," allowing users to view location-specific data.

1. Creation of NottinghamView

The `NottinghamView` displays accident information for "Nottingham," ensuring data isolation for that specific location.

b. The Role of Views in Enhancing Security

Using views helps improve database security by limiting the data that users can access. Here’s how views enhance security:

1. Restricting Data Access

Views limit the data that users can access to only what is necessary for their tasks. For example, the `SouthhamptonView` only displays data related to "Southampton," preventing access to data from other locations, thus reducing the risk of unauthorized access.

1. Reducing the Risk of Data Leakage

By creating views for specific locations, the risk of data leakage is significantly reduced. Users only interact with the data relevant to their work, minimizing the chance of accessing other sensitive data.

1. Data Abstraction

Views provide data abstraction by hiding the underlying table structure. Users can retrieve the necessary data without needing to understand the complexity of the database. This abstraction further reduces the risk of misuse or accidental access to sensitive information.

**Conclusion**

In this assignment, I explored how RBAC and views can improve database security. By granting role-specific privileges and restricting access to specific data through views, I significantly enhance the confidentiality and security of the database. This highlights the importance of protecting company data effectively.

Word Count: 728

References

1. Chaffey, D. (2019). *Digital business and e-commerce management: Strategy, implementation and practice (7th ed.).* Pearson.