



DATABASE PROGRAMMING

Instructions

- Complete all tasks below.
- **TOPIC:** SECURITY AND USER MANAGEMENT

QUESTION

1. Creating Users

- Write a SQL statement to create a new user named `app_user` with a password `securePassword123`.

2. Granting Privileges

- Write a SQL statement to grant `SELECT` and `INSERT` privileges on the `employees` table to the user `app_user`.

3. Revoking Privileges

- Write a SQL statement to revoke the `INSERT` privilege from `app_user` on the `employees` table.

4. Creating Roles

- Write a SQL statement to create a role named `HR` and assign the ability to perform `SELECT`, `INSERT`, and `UPDATE` on the `employees` table.

5. Assigning Roles to Users

- Write a SQL statement to assign the `HR` role to the user `app_user`.

6. Viewing User Privileges

- Write a query to list all privileges granted to `app_user`.

7. Modifying User Permissions

- Write a SQL statement to change the password for `app_user` to `newSecurePassword456`.

8. Dropping Users

- Write a SQL statement to drop the user `app_user` from the database.

9. Security Best Practices

- Discuss three best practices for securing SQL databases and provide examples of how to implement them.

10. Database Encryption

- Explain the importance of data encryption at rest and in transit, and provide an example of how to enable encryption for sensitive data.

11. Auditing User Activity

- Write a SQL statement that enables auditing on the `employees` table to track changes made by users.

12. Role-Based Access Control

- Describe how role-based access control (RBAC) improves security and give an example of its implementation in SQL.

13. User Authentication Methods

- Discuss different methods of user authentication in SQL and provide a SQL command for each method.

14. Session Management

- Write a SQL query to view active user sessions in the database and explain what information can be obtained from this view.

15. Blocking Unauthorized Access

- Write a SQL statement that sets up a rule to block login attempts from users who exceed a specified number of failed login attempts. ***END***