**INT207 Lab 4**

## Basic Database Administration: User Management

***Creating Users***

The DBA creates the user by executing the CREATE USER statement. The user does not have any privileges at this point. The DBA can then grant privileges to that user. These privileges determine what the user can do at the database level.

## CREATE USER Syntax:

**CREATE USER *username***

**IDENTIFIED BY *password***

**[QUOTA n[M|G] ON tablespace\_name];**

**ALTER USER *username***

***IDENTIFIED BY password;***

**[QUOTA n[M|G] ON tablespace\_name];**

**Note**: Authorization rules must be checked for each access request.

***Naming Rules***

For username and password:

* + Username is a unique name
  + Must begin with a letter
  + Must be 1–30 characters long
  + Must contain only A–Z, a–z, 0–9, \_, $, and #
  + Must not be an Oracle server reserved word (SQL keywords)

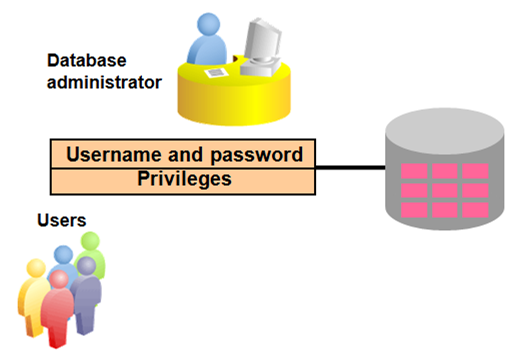
***Schemas***

# A schema is a collection of objects such as tables, views, and sequences. The schema is owned by a database user and has the same name as that user.

**SELECT \* | col1 [,col2,col3, …]**

**FROM [*schema*.]table\_name;**

***Controlling User Access***



***Privileges***

# Privileges are the right to execute particular SQL statements. The database administrator (DBA) is a high-level user with the ability to *create users* and grant users access to the database and its objects. There are two types of privileges:

# System Privileges: to gain access to the database. System privileges typically are provided by the database administrator.

|  |  |
| --- | --- |
| **System Privilege** | **Operations Authorized** |
| CREATE SESSION | Connect to the database |
| CREATE TABLE | Create tables in the user’s schema |
| CREATE VIEW | Create a view in the user’s schema |
| CREATE USER | Create a database user |
| CREATE PROCEDURE | Create a stored procedure, function, or package in the user’s schema |
| CREATE SYNONYM | Create synonyms in the user’s schema |
| UNLIMITED TABLESPACE | To permit a user to use an unlimited amount of any tablespace in the database |

# GRANT/REVOKE System Privileges Syntax:

**GRANT *system\_priv1* [,*system\_priv2,…*]**

**TO *user1 [,user2,…]***

***[WITH ADMIN OPTION]*;**

**REVOKE *system\_priv1* [,*system\_priv2,…*]**

**FROM *user1 [,user2,…]*;**

A privilege that is granted with the ***WITH ADMIN OPTION*** clause can be passed on to other users and roles by the grantee.

**Example:** SQL> GRANT create session, create view, create table TO scott;

# Confirming Granted Privileges:

You can access the data dictionary to view the database information. The data dictionary is created and maintained by the Oracle server and contains information about the database called *metadata*. The data dictionary is structured in tables and views, just like other database data. Not only is the data dictionary central to every Oracle database, but it is an important tool for all users, from end users to application designers and database administrators.

You can access the data dictionary view named ***USER\_SYS\_PRIVS*** to view the system privileges that you have.

SQL> SELECT \* FROM user\_sys\_privs ;

# Object Privileges: to manipulate the content of the objects in the database. Users can also be given the privilege to grant additional privileges to other users or to roles, which are named groups of related privileges.

|  |  |  |  |
| --- | --- | --- | --- |
| **Object Privilege** | **Table** | **View** | **Procedure** |
| **ALTER** | 🗸 |  |  |
| **DELETE** | 🗸 | 🗸 |  |
| **EXECUTE** |  |  | 🗸 |
| **INDEX** | 🗸 |  |  |
| **INSERT** | 🗸 | 🗸 |  |
| **REFERENCES** | 🗸 | 🗸 |  |
| **UPDATE** | 🗸 | 🗸 |  |
| **SELECT** | 🗸 | 🗸 |  |

# GRANT/REVOKE Object Privileges Syntax:

**GRANT *object\_priv1* [,object*\_priv2,…*]**

**ON *[schema.]object\_name***

**TO *user [,user2,…]***

***[WITH GRANT OPTION]*;**

**REVOKE *object\_priv1* [,object*\_priv2,…*]**

**ON *[schema.]object\_name***

**FROM *user [,user2,…]*;**

A privilege that is granted with the ***WITH GRANT OPTION*** clause can be passed on to other users and roles by the grantee. Object privileges granted with the WITH GRANT OPTION clause are revoked when the grantor’s privilege is revoked

**Example:** SQL> GRANT select, update ON scott.student TO bob;

You can access the data dictionary view named ***USER\_TAB\_PRIVS*** to view the object granted to the current user, the object privileges granted by the current user, and the list of object privileges granted for objects owned by the current user.

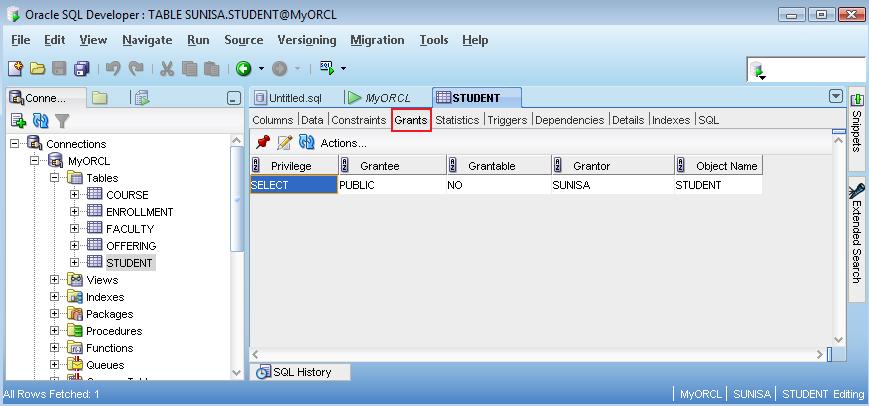
SQL> SELECT \* FROM user\_tab\_privs ;

Data dictionary for object privileges: ***USER\_TAB\_PRIVS\_RECD*** and ***USER\_TAB\_PRIVS\_MADE***

## 

## Using SQL Developer:

To view object privileges on the table:



***Practice:* *Controlling User Access***

**As Username <DBxxx>:**

**\*\*\* Please change your password from <dba> to your new password \*\*\***

## Create a table named PhoneList with two columns: Friend\_Name and Phone\_Number. Set the Friend\_Name column as a Primary Key. Add two new rows into the PhoneList table with the following command:

## INSERT INTO PhoneList (Friend\_Name,Phone\_Number) VALUES (‘Bill Gates’,’088-000-1144’) ;

## INSERT INTO PhoneList (Friend\_Name,Phone\_Number) VALUES (‘Steve Jobs’,’089-123-5555’) ;

## INSERT INTO PhoneList (Friend\_Name,Phone\_Number) VALUES (‘Your Name’,’099-888-5555’) ;

COMMIT;

## Create a new database user named <APPxxx> with password <int207>. After created, test the new user. Connect the database as user <APPxxx>.

## What happens? If an error is returned, Please resolve it.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## You (as DBxxx) want the user <APPxxx> can create view in his schema. Please grant the appropriate privilege to the user.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Grant only SELECT privilege on PhoneList table to the user <APPxxxx> with pass along privilege to other users on your table.

Is this a system or an object privilege? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

View the granted privilege on the PhoneList table from SQL Developer. See GRANTS tab, the value of GRANTEE column should be <**APPxxxx**>.

## Switch to connect the database as username <APPxxxx>:

* 1. Write a command to view all system privileges are granted to the <**APPxxxx**> user.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Write a command to change password from <**int207**> to new password <***dbms****>*.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Write and execute a command to retrieve the rows with Phone\_Number *ending with 5* from the PhoneList table of <**DBxxxx**> schema.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Can the user <APPxxxx> select data from the table? [Y | N]

Why? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Write a command to insert a new record with ***Mark Zuckerberg*** as friend’s name and ***087-080-9898*** as phone number into the PhoneList table of <**DBxxxx**> schema.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Can you insert the new record into the **PhoneList** table of <**DBxxxx**> schema?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Write a command to delete the row with the friend name of ***Bill Gates*** from the **PhoneList** table of <**DBxxxx**> schema.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Can the user <**APPxxxx**> delete data from the table of **DBxxxx**? [Y | N]

Why? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. In order to complete the tasks in 5.4 and 5.5. What would you do? Write your commands:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Write a command to grant the SELECT privilege on the <**DBxxxx**>.**PhoneList** table to another friend.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Can the user <**APPxxxx**> grant the privilege to another user? [Y | N]

Why? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Switch to connect the database as an original username <DBxxxx>.

## Write a command to revoke the SELECT privilege on the PhoneList table from the <APPxxxx> user.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## After that, the SELECT privilege is revoked from <APPxxx> user. How about another friend that was granted by <APPxxx> (in question 5.7).

## Can another friend still select data from <DBxxxx>. PhoneList table? [Y | N]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Create a new table named Users with five columns: ID, Fname, Lname, Username and PWD. Please set the constraint(s) that appropriate to the Users table. Add one row into the Users table (data created by your own) and then issue the COMMIT command.

What do you think about the security on the *Users* table?