**Controlling User Access**

In a multiple-user environment, you want to maintain security of the database access and use. With Oracle Server database security.

you can do the following:

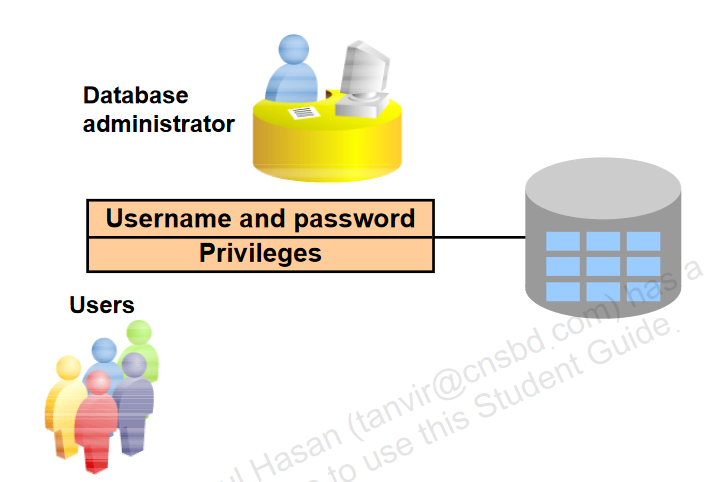
* Control database access.
* Give access to specific objects in the database.
* Confirm given and received privileges with the Oracle data dictionary.

Database security can be classified into two categories:

1. System security
2. Data security.

System security: System security covers access and use of the database at the system level, such as the username and password, the disk space allocated to users, and the system operations that users can perform.

Data security: Database security covers access and use of the database objects and the actions that those users can perform on the objects.



**Privileges**

A privilege is 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. Users require system privileges to gain access to the database and 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.

* Database security:
  + System security
  + Data security
* System privileges: Performing a particular action within the database
* Object privileges: Manipulating the content of the database objects
* Schemas: Collection of objects such as tables, views, and sequences

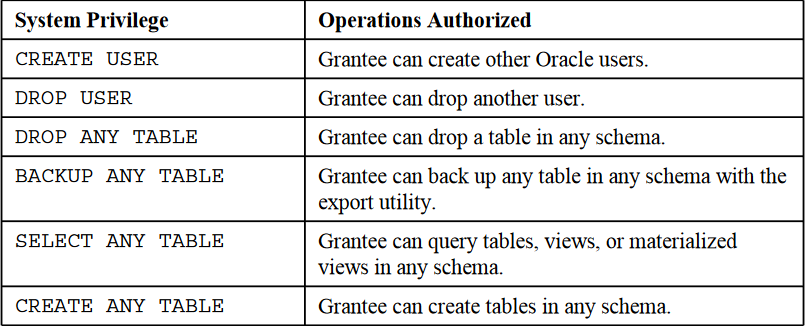
**Schemas**

A schemais 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.

A system privilege is the right to perform a particular action, or to perform an action on any schema objects of a particular type. An object privilege provides the user the ability to perform a particular action on a specific schema object.

**System Privileges**

* More than 100 privileges are available.
* The database administrator has high-level system privileges for tasks such as:
  + Creating new users
  + Removing users
  + Removing tables
  + Backing up tables



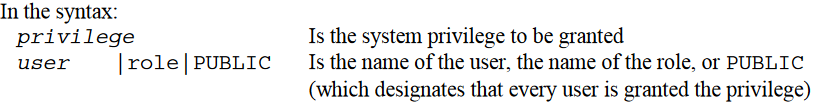
**Creating Users**

|  |
| --- |
| * The DBA creates users with the CREATE USER statement.       sqlplus sys/sys@orcl as sysdba    CREATE USER shafin  IDENTIFIED BY shafin;    conn shafin/shafin@orcl    Note: Starting with Oracle Database 11g, passwords are case-sensitive. |

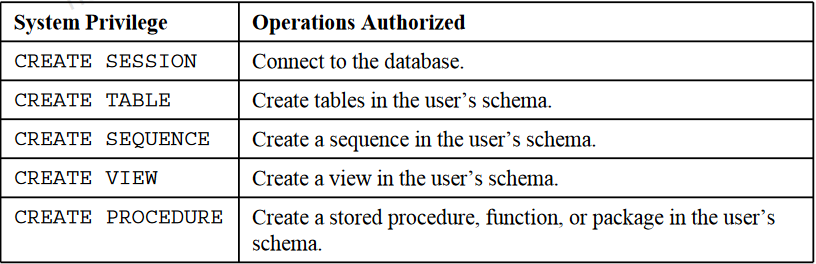
**User System Privileges**

* After a user is created, the DBA can grant specific system privileges to that user.





* An application developer, for example, may have the following system privileges:
  + CREATE SESSION
  + CREATE TABLE
  + CREATE SEQUENCE
  + CREATE VIEW
  + CREATE PROCEDURE



**Granting System Privileges**

The DBA uses the GRANT statement to allocate system privileges to the user. After the user has been granted the privileges, the user can immediately use those privileges.

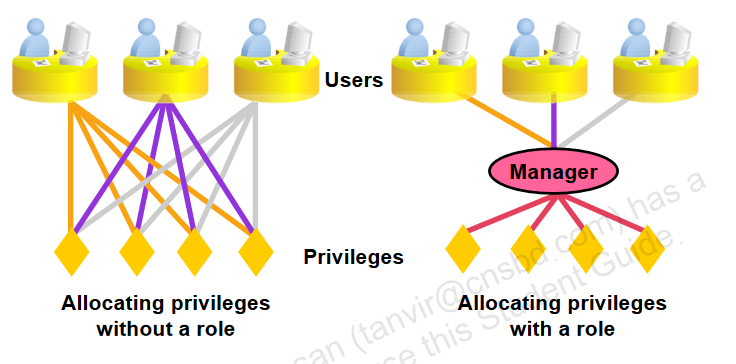
|  |
| --- |
| GRANT create session, create table,  create sequence, create view  TO shafin;    conn shafin/shafin@orcl |

**Creating a role**

What Is a Role?

A role is a named group of related privileges that can be granted to the user. This method makes it easier to revoke and maintain privileges.

A user can have access to several roles, and several users can be assigned the same role. Roles are typically created for a database application.



**Creating and Granting Privileges to a Role**

|  |
| --- |
| * Create a role:   CREATE ROLE manager;     * Grant privileges to a role:   GRANT create table, create view  TO manager;     * Grant a role to users:   GRANT manager TO Habib; |

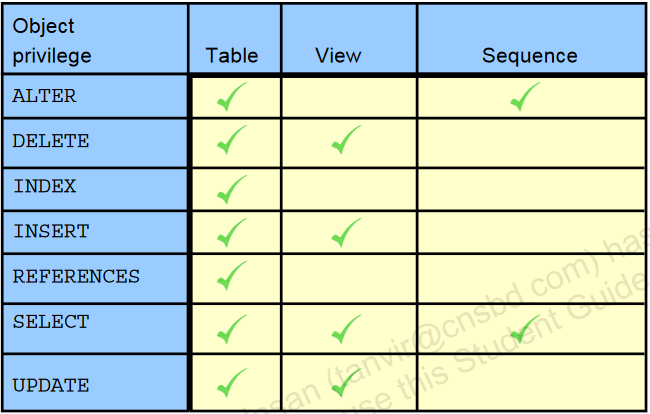
**Changing Your Password**

|  |
| --- |
| * The DBA creates your user account and initializes your password. * You can change your password by using the ALTER USER statement.   sqlplus sys/sys@orcl as sysdba    ALTER USER shafin  IDENTIFIED BY habib; |

**Object Privileges**

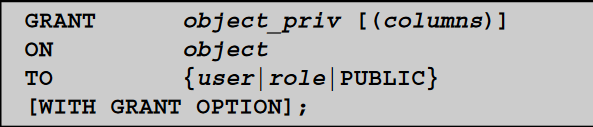
* An object privilege is a privilege or right to perform a particular action on a specific table, view, sequence, or procedure.
* Each object has a particular set of grantable privileges.
* The table in the slide lists the privileges for various objects. Note that the only privileges that apply to a sequence are SELECT and ALTER. UPDATE, REFERENCES, and INSERT can be restricted by specifying a subset of updatable columns.
* A SELECT privilege can be restricted by creating a view with a subset of columns and granting the SELECT privilege only on the view.
* A privilege granted on a synonym is converted to a privilege on the base table referenced by the synonym.

Note: With the REFERENCES privilege, you can ensure that other users can create FOREIGNKEY constraints that reference your table.



**Object Privileges**

* Object privileges vary from object to object.
* An owner has all the privileges on the object.
* An owner can give specific privileges on that owner’s object.



**Granting Object Privileges**

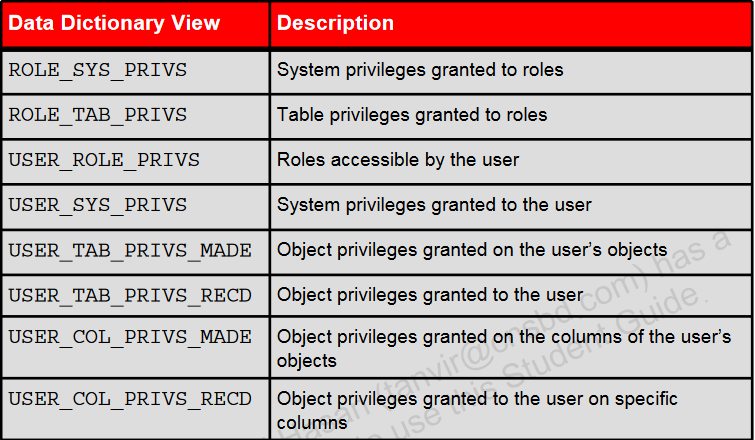
* To grant privileges on an object, the object must be in your own schema, or you must have been granted the object privileges WITH GRANT OPTION.
* An object owner can grant any object privilege on the object to any other user or role of the database.
* The owner of an object automatically acquires all object privileges on that object.

|  |
| --- |
| * Grant query privileges on the EMPLOYEES table:   1st I connect hr/hr@orcl  conn hr/hr@orcl    GRANT select  ON employees  TO shafin;    conn shafin/habib@orcl    select \* from hr.employees;     * Grant privileges to update specific columns to users and roles:   conn hr/hr@orcl    GRANT update (department\_name, location\_id)  ON departments  TO shafin, manager; |

**Passing On Your Privileges**

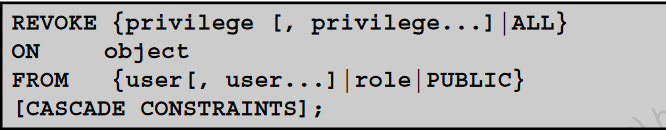
|  |
| --- |
| * Give a user authority to pass along privileges:   GRANT select, insert  ON departments  TO demo  WITH GRANT OPTION;   * Allow all users on the system to query data from Alice’s DEPARTMENTS table:   GRANT select  ON alice.departments  TO PUBLIC;  **WITH GRANT OPTION Keyword**  A privilege 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  **PUBLIC Keyword**  An owner of a table can grant access to all users by using the PUBLIC keyword.  The second example allows all users on the system to query data from Alice’s  DEPARTMENTS table. |

**Confirming Granted Privileges**



**Revoking object privileges**

* You use the REVOKE statement to revoke privileges granted to other users.
* Privileges granted to others through the WITH GRANT OPTION clause are also revoked.



**Revoking Object Privileges**

|  |
| --- |
| * Revoke the SELECT and INSERT privileges given to the shafin user on the DEPARTMENTS table   REVOKE select, insert  ON departments  FROM shafin; |