Department of Software Engineering
Mehran University of Engineering and Technology, Jamshoro

Course: SW215 – Database System			
Instructor	Ms Shafiya Qadeer	**Practical/Lab No.**	10
Date	25-02-2021	**CLOs**	2
Signature		**Assessment Score**	2 Marks

Topic	**To Grant privileges to users and creating user accounts**
Objectives	- To become familiar with Granting & revoking Access Rights

Lab Discussion: Theoretical concepts and Procedural steps

Controlling User Access:

In a multi 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.
- Create synonyms for database objects.

Database security can be classified into two categories:

- 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: Covers access and use of the database objects and the actions that those users can have on the objects.

Privileges:

Privileges are the rights to execute particular SQL statements. The DBA is a high level user with the ability to grant users access to the database and its objects. The users require system privileges to gain access to the database and object privileges to manipulate the content of the objects in the database.

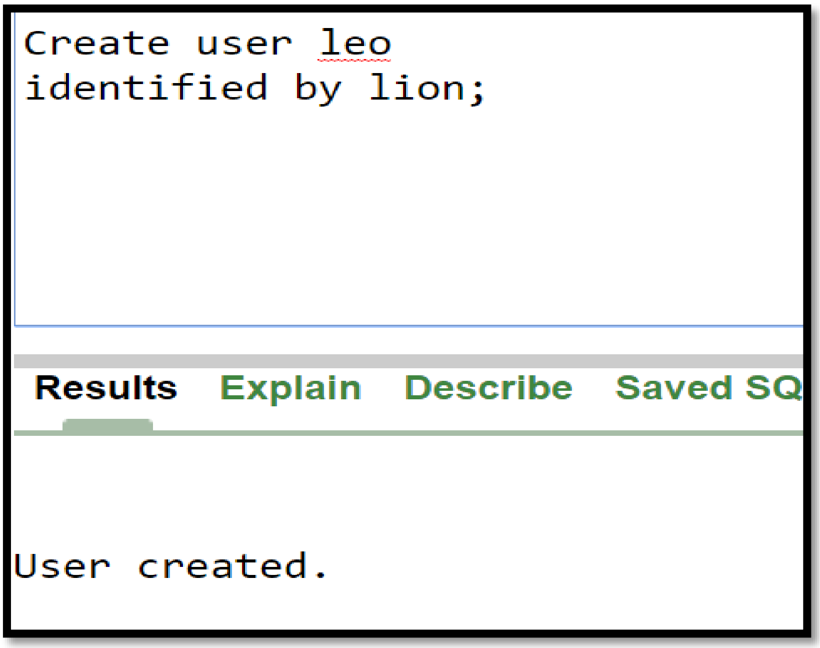
System Privilege	**Operations Authorized**
CREATE USER	Grantee can create Oracle users.
DROP USER	Grantee can drop another user.

DROP ANY TABLE	Grantee can drop a table in any schema.
BACKUP ANY TABLE	Grantee can backup any table in any schema with the export utility.
SELECT ANY TABLE	Grantee can query tables, views or snapshots in any schema.
CREATE ANY TABLE	Grantee can create tables in any schema.

CREATE USER:

Syntax:

```
  CREATE USER username
    IDENTIFIED BY password;
```



```
Create user leo
identified by lion;
```

```
User created.
```

Granting Privileges:

Once a user is created, the DBA can grant specific system privileges to a user.

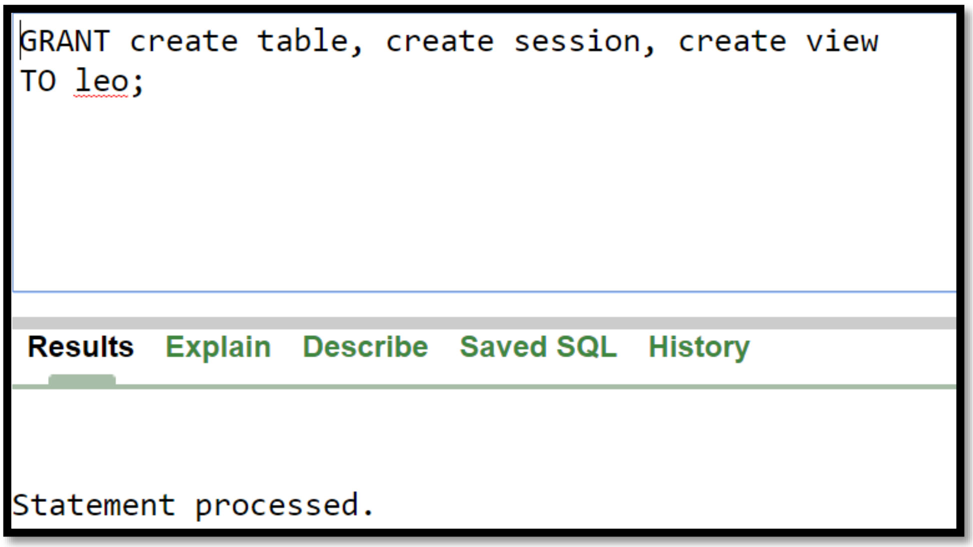
GRANT privilege [,privilege....]

TO user [,user/role, PUBLIC];

Typical User Privileges:

System Privilege	Operations Authorized
CREATE SESSION	Connect to the database.

CREATE TABLE	Create table in the user's schema.
CREATE SEQUENCE	Create a sequence in the user's schema.
CREATE VIEW	Create a view in the user's schema.
CREATE PROCEDURE	Create a stored procedure, function or package in the user's schema.



```
GRANT create table, create session, create view
TO leo;
```

```
Statement processed.
```

Role:

A **role** is a set or group of privileges that can be granted to users or another role. This is a great way for database administrators to save time and effort.

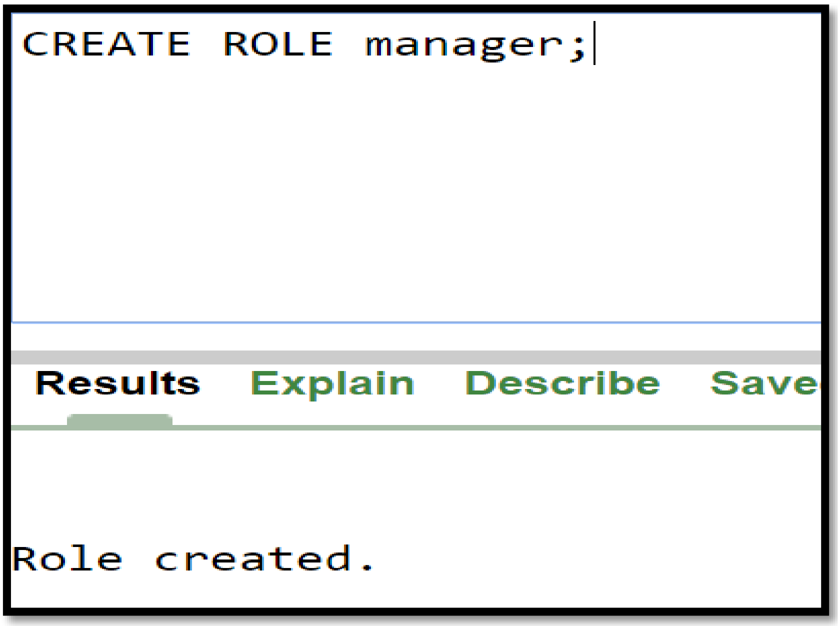
CREATE ROLE:

You may wish to create a role so that you can logically group the users' permissions. Please note that to create a role, you must have CREATE ROLE system privileges.

Syntax

The syntax for creating a role in Oracle is:

```
CREATE ROLE role_name
```



```
CREATE ROLE manager;
```

```
Role created.
```

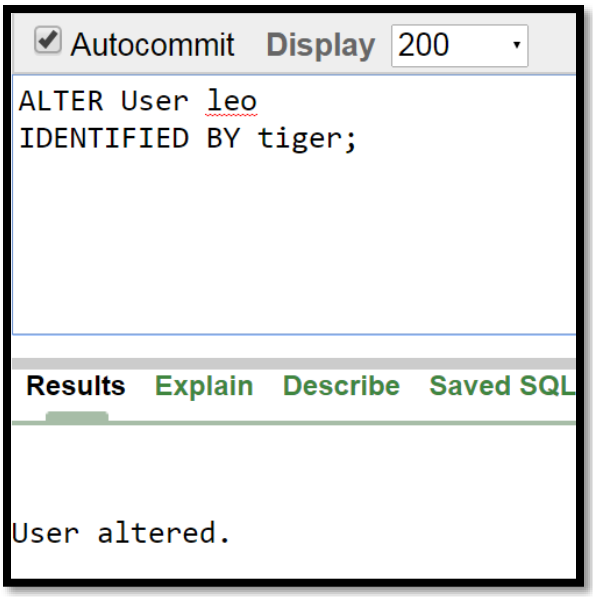
CHANGE A USER'S PASSWORD IN ORACLE:

To change a user's password in Oracle, you need to execute the *alter user* command.

SYNTAX

The syntax for changing a password in Oracle is:

ALTER USER *user_name* IDENTIFIED BY *new_password*;



☑ Autocommit Display 200

```
ALTER User leo
IDENTIFIED BY tiger;
```

```
User altered.
```

Object Privileges:

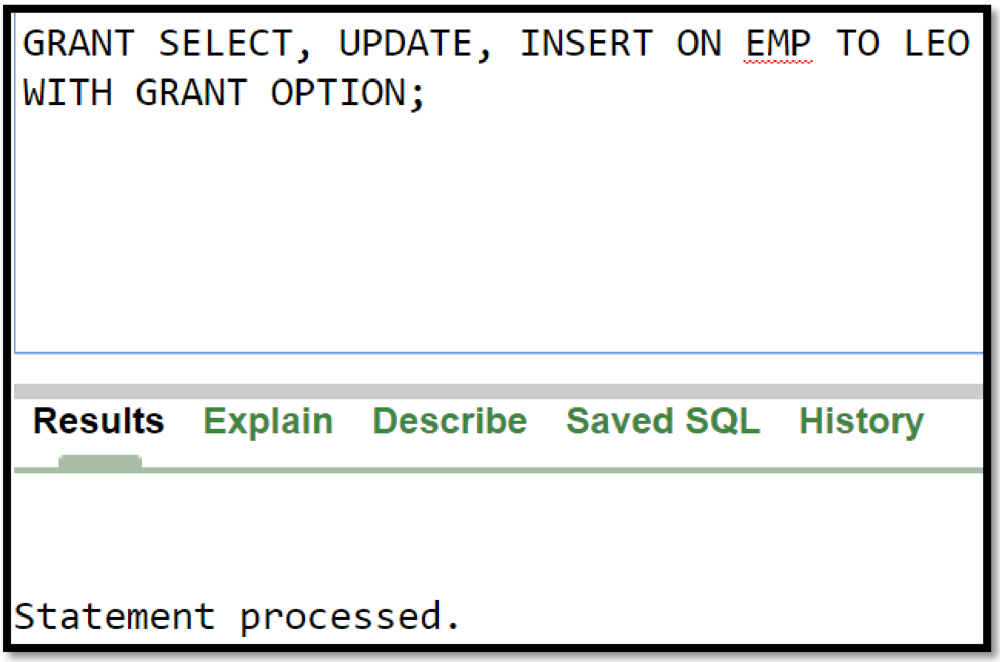
An object privilege is the right to perform a particular action on an object or to access another user's object. Objects include tables, views, materialized views, indexes, synonyms, sequences, cache groups, replication schemes and PL/SQL functions, procedures and packages. An object's owner has all object privileges for that object, and those privileges cannot be revoked. The object's owner can grant object privileges for that object to other database users. A user with ADMIN privilege can grant and revoke object privileges from users who do not own the objects on which the privileges are granted.

Privilege	**Object type**	**Description**
DELETE	Table	Enables a user to delete from a table.
INDEX	Table or materialized view	Enables a user to create an index on a table or materialized view.
INSERT	Table or synonym	Enables a user to insert into a table or into the table through a synonym.
SELECT	Table, sequence, view, materialized view, or synonym	Enables a user to select from a table, sequence, view, materialized view, or synonym. The SELECT privilege enables a user to perform all operations on a sequence. A user can be granted the SELECT privilege on a synonym or a view without being explicitly granted the SELECT privilege on the originating table.
UPDATE	Table	Enables a user to update a table.
ALL		All privileges on table.

Syntax

The syntax for granting privileges on a table in Oracle is:

```
GRANT privileges ON object TO user;
```



```
GRANT SELECT, UPDATE, INSERT ON EMP TO LEO
WITH GRANT OPTION;
```

```
Statement processed.
```

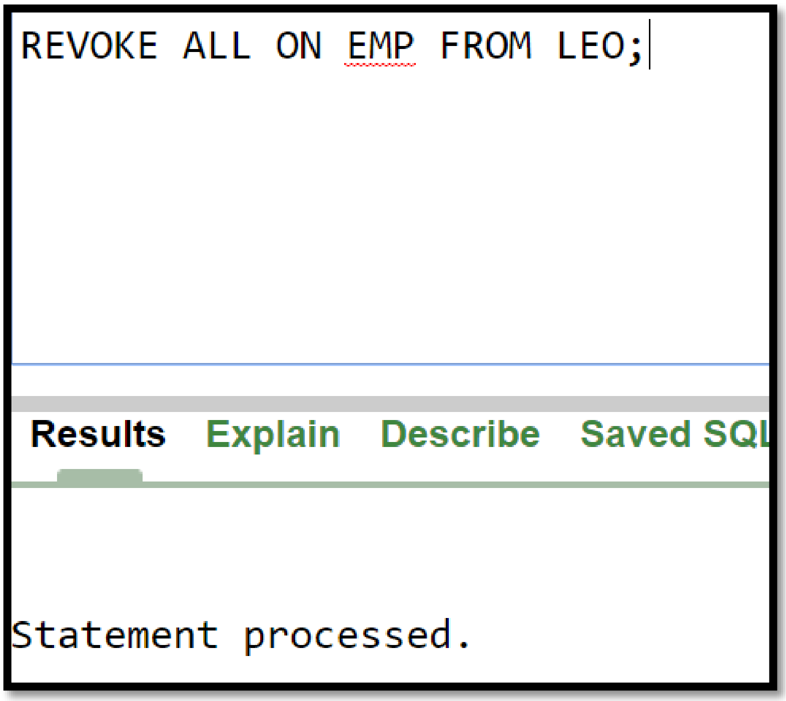
REVOKE PRIVILEGES ON TABLE:

Once you have granted privileges, you may need to revoke some or all of these privileges. To do this, you can run a revoke command. You can revoke any combination of SELECT, INSERT, UPDATE, DELETE, REFERENCES, ALTER, INDEX, or ALL.

Syntax

The syntax for revoking privileges on a table in Oracle is:

```
REVOKE privileges ON object FROM user;
```



```
REVOKE ALL ON EMP FROM LEO;
```

```
Statement processed.
```

Lab Tasks

1. Create 3 different users.
2. Assign different system privileges to any one of the three users.
3. Assign different object privileges to any one of the three users.
4. Create a role named manager, assign different privileges to that role and then finally assign that role to one of the three users.
5. Revoke all the privileges from all of the three users.