Challenge 24

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

Username: user3

Password: password3

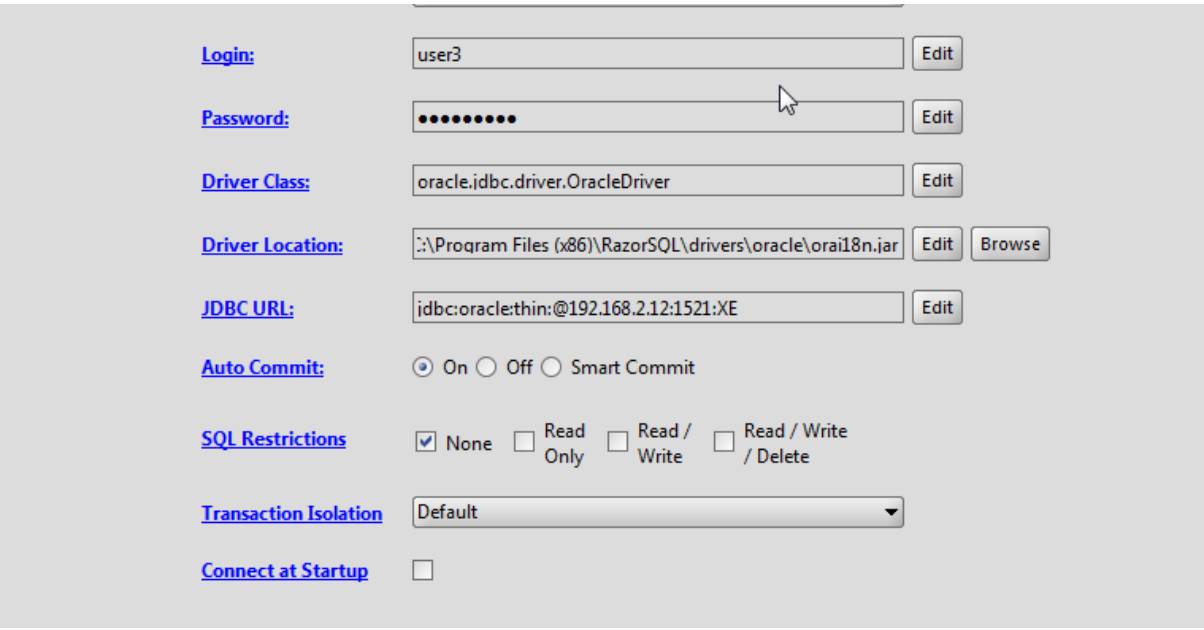
IP: 192.168.2.12

Port: 1521

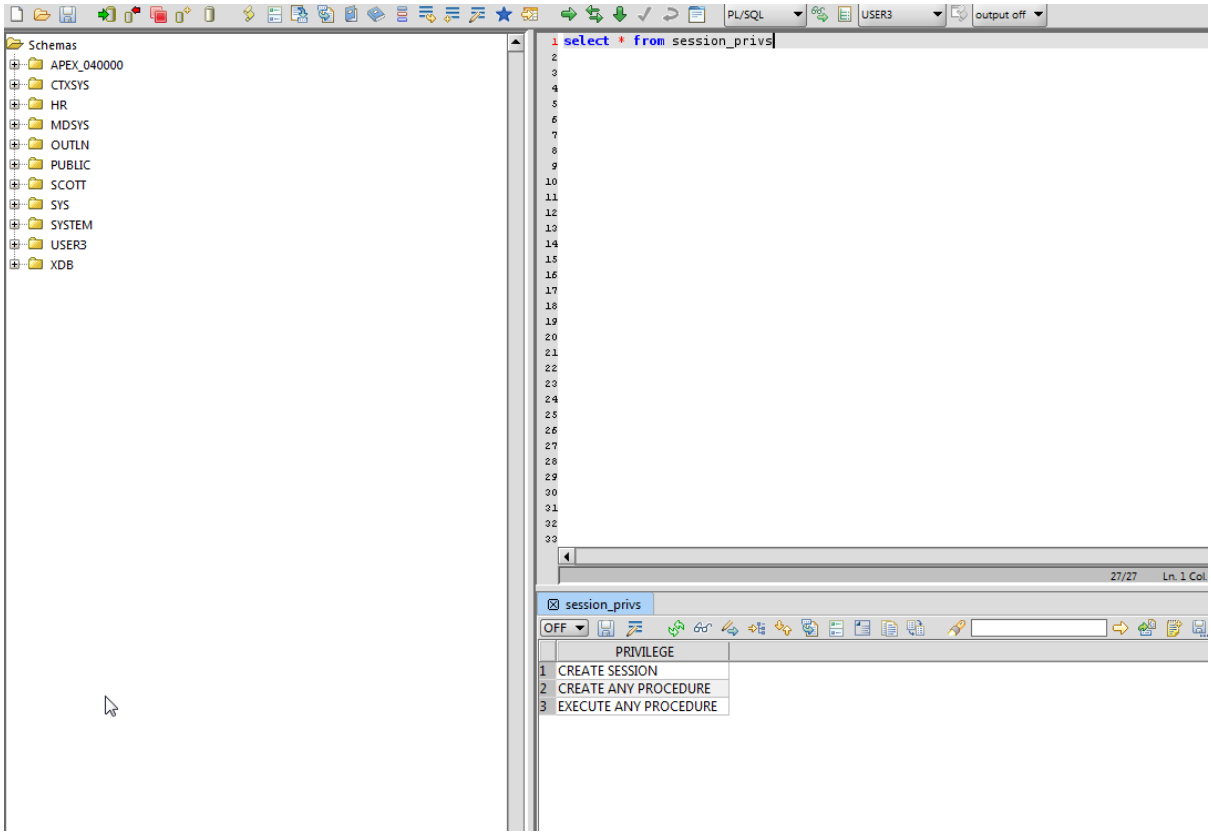
SID: XE

- List the permissions/privileges of current user.
- Escalate privileges and become DBA

Connect to the database:



List user's privileges:



Note that we have 2 high peivilges:

CREATE ANY PROCEDURE
EXECUTE ANY PROCEDURE

Note: There is difference in CREATE PROCEDURE and CREATE ANY PROCEDURE.

CREATE PROCEDURE lets you create procedure, but only in your user's schema. But, CREATE ANY PROCEDURE lets you create procedure in any user's schema (but not SYS). Thus, we can create a procedure in SYSTEM schema called SYSTEM.GETDBA(), and then use our EXECUTE ANY PROCEDURE privilege to execute this procedure.

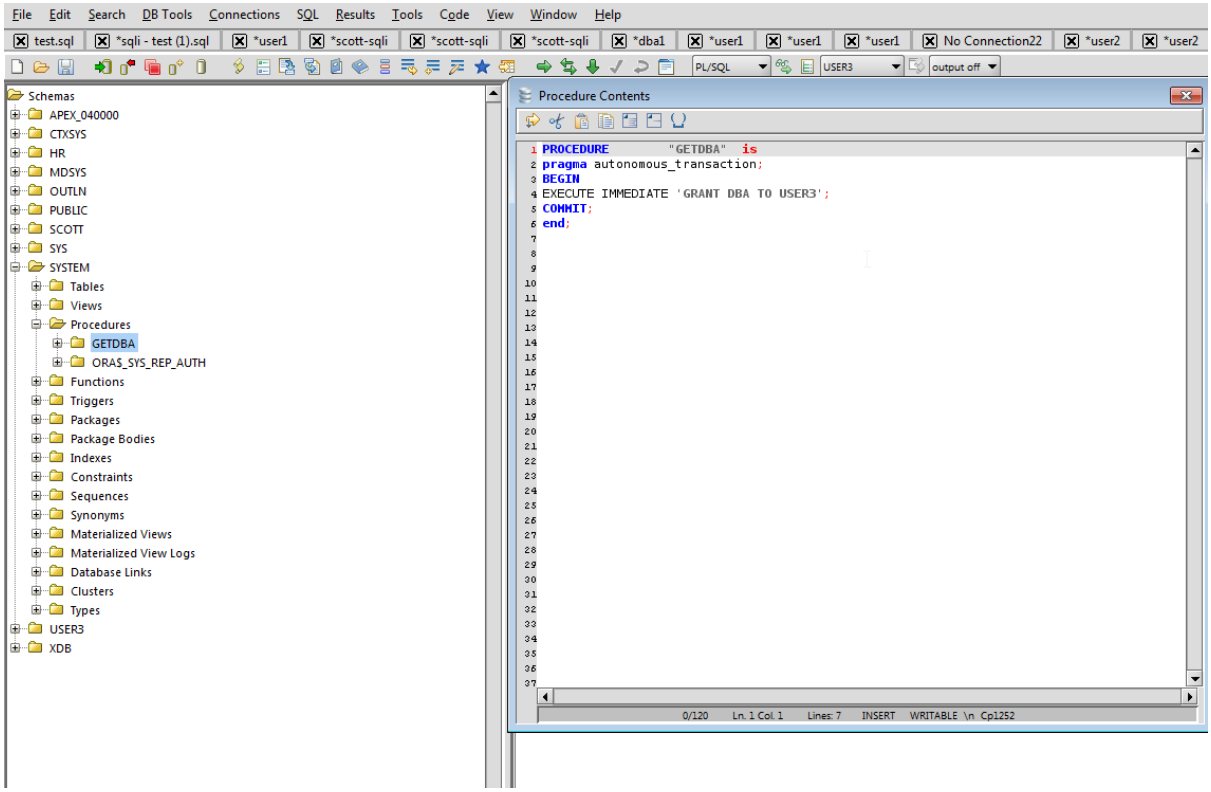
While you may argue that the procedure SYSTEM.GETDBA() was created by user3 and thus he is technically the DEFINER of this procedure and thus by default, the procedure should only execute with the privileges of DEFINER (user3). As far, as Oracle is concerned, the definer of an object is the schema in which it belongs and thus the definer of the procedure system.getdba is system and if this procedure does not have the keyword AUTHID CURRENT_USER defined, then irrespective of who executes this procedure, it will always run with privileges of definer (SYSTEM).

So, let's create a procedure in SYSTEM schema:

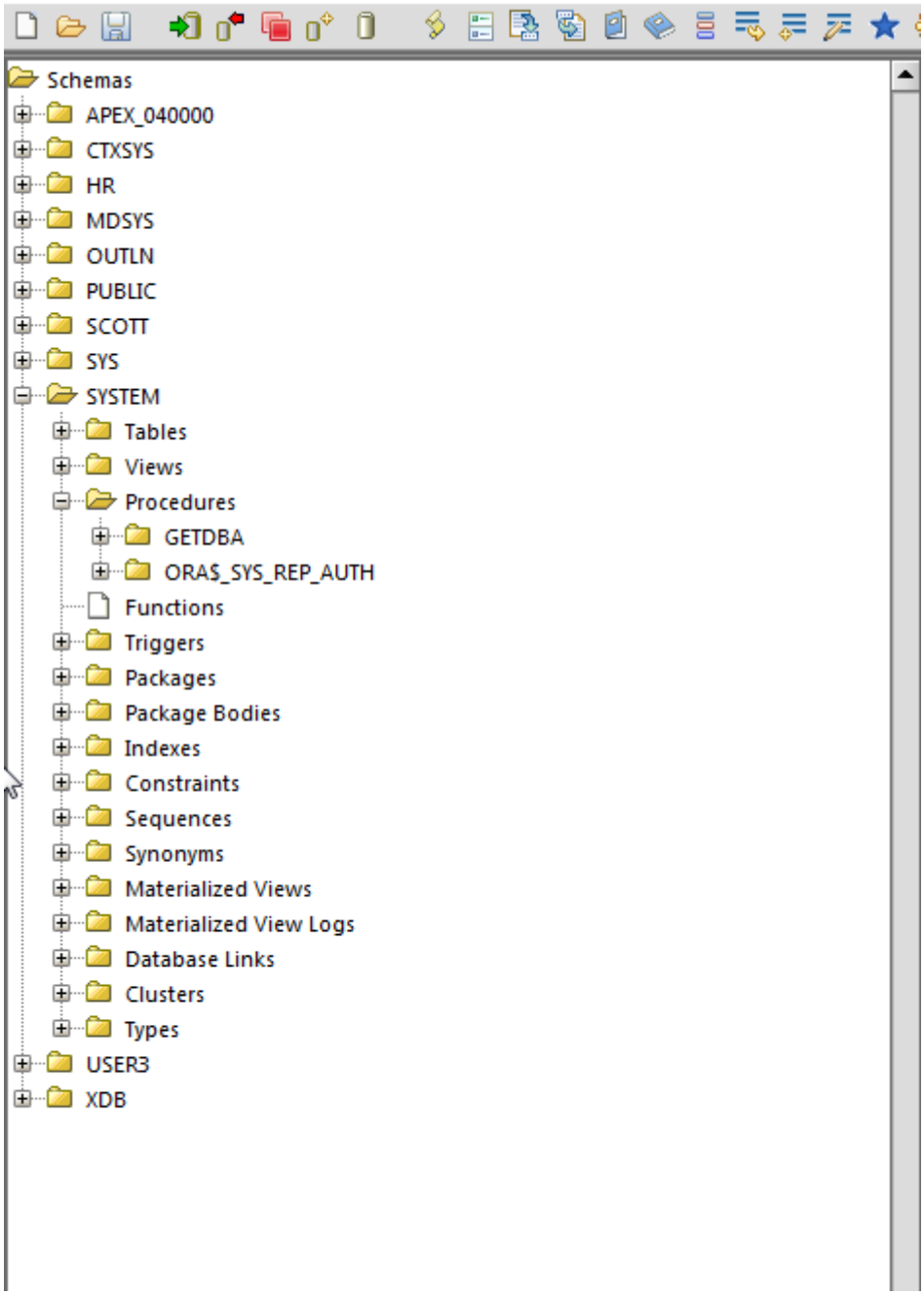
```
CREATE OR REPLACE PROCEDURE SYSTEM."GETDBA" is

pragma autonomous_transaction;

BEGIN
```

```
EXECUTE IMMEDIATE 'GRANT DBA TO USER3';

COMMIT;

end;
```

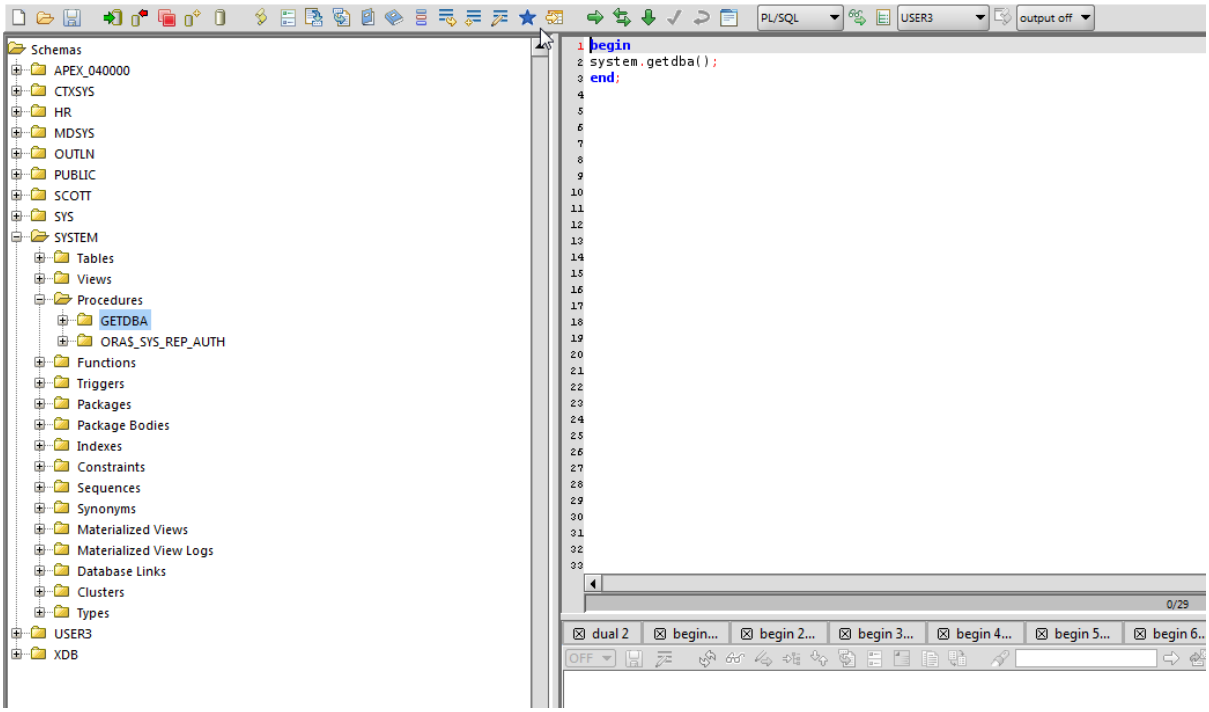
Note: in the above procedure we have explicitly left out the statement AUTHID CURRENT_USER



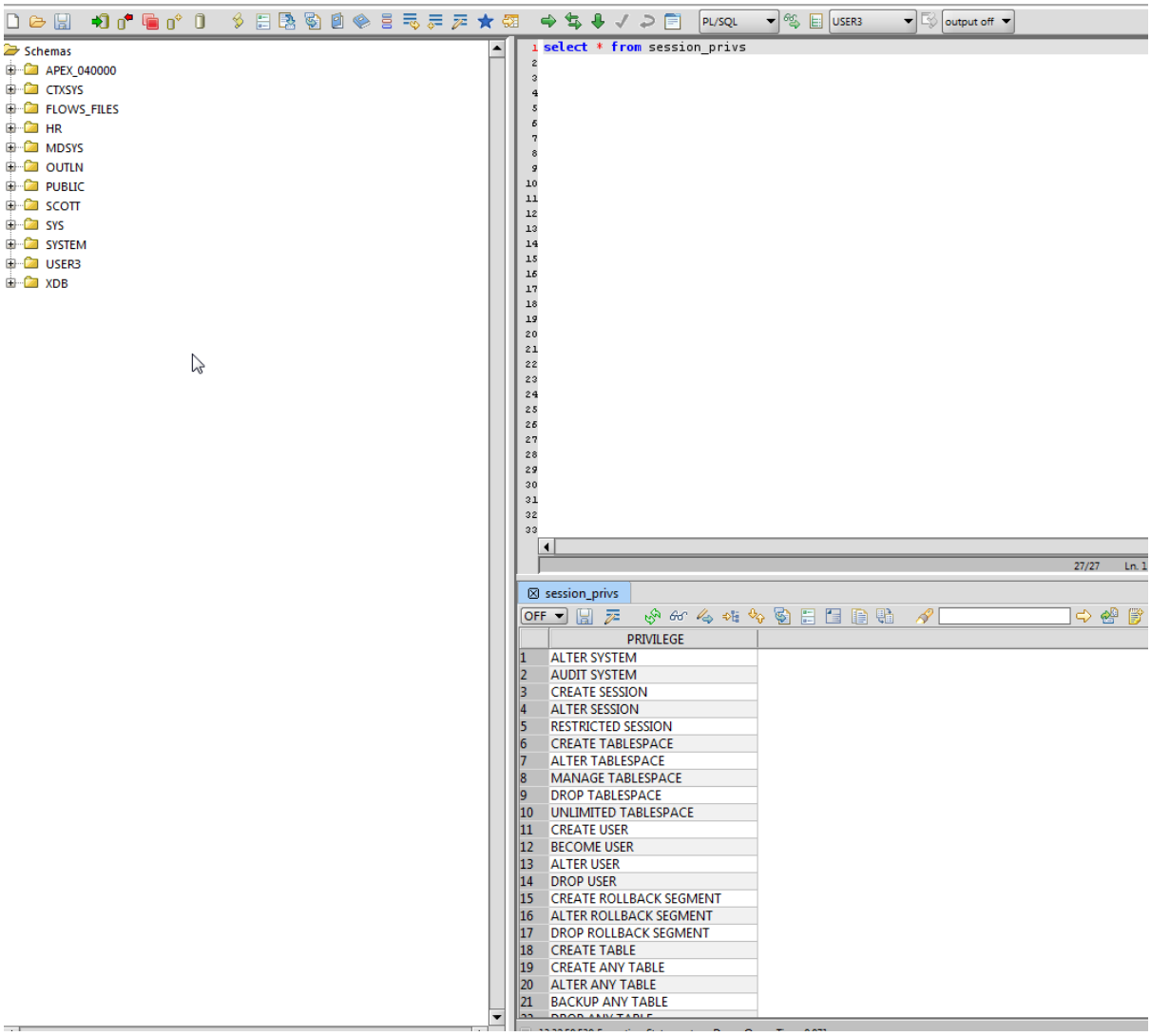
You can expand the SYSTEM schema and check the procedure is created.



Now we can just execute this procedure and this should give us DBA role:



Now, if we login again as user3, the user should have DBA role:



Remember to run:

```
drop procedure system.getdba
```

and then:

```
Revoke dba from user3
```