Summary:

This article “Metalink Hacking” reveals how one can retrieve sensitive oracle & customer related information from Metalink. This, incidentally is not illegal.

The name “Metalink Hacking” is an analogy to the term Google Hacking (see also Google Hacking of Oracle Technologies and Yahoo Hacking of Oracle Technologies).
Sensitive Oracle customer information can for example be “an Oracle configuration file” (tnsnames from a large 3-letter agency or other configuration details) which customer normally supplies to Oracle during the TAR creation process. A more sensitive and dangerous customer information would be “unpublished/unknown Oracle security bugs”.
In one search alone, 42 unknown security bugs were found which related to every product/ version and patchset.

What is Metalink?
Metalink is the support services premier web support services from Oracle and is free for all customers from Oracle with valid product support contract. Metalink users are able to search the global repository of technical knowledge and to query the bug database for known issues.

How many users have Metalink access?
Thousands of Oracle customers have limited, thousands of Oracle employees and Oracle subcontractors have full access to Metalink and can see every bug and every TAR (Technical Assistant Request)

How can I get Metalink access?
Only Oracle customers with valid support contracts are able to access Metalink. The cheapest way to become an Oracle customer with Metalink support is to buy a single user license of the Oracle Collaboration Suite (http://www.oracle.com/products/buy/index.html). A single user license costs approximately 60 EUR which includes 1 year support via Metalink.

Security Permission in Metalink
Metalink has several security permission levels. An Oracle employees is able to access the entire Metalink database (service requests (SR/TAR), bugs, forum entries and notes)
A normal customer is however limited to their own TAR’s, known as public bugs, public forum entries and public notes depending on the licensed Oracle software.

It is very astonishing for the kind of data that is available on this knowledge base even for a customer with a limited permission.

OK, let's start with our research.

After login to Metalink (http://metalink.oracle.com)

Let's enter "Hacker" and click submit

Some results:

DBMS_SYS_SQL.Parse_as_user Has a Security Concern
This note (272381.1) explains how to become DBA via the package dbms_sys_sql. Wow, this package contains the necessary exploit code and also demonstrating how to do this.

HOW TO SET ORACLE PRIVILEGES BASED ON TOOL USED
Show different possibilities how to do this and how a hacker could circumvent the chosen solution (e.g. via trace-files, renaming files …)

Security hole in http://your_webserver/rwows60_virtual_path/showenv
Get sensitive information from the reports server. This note is from 12-DEC-2000. 2 years later this bugs was reported on 12-nov-2002 by Integrigy.

Next string: "Security bug"

Some results:

Another ias8i (1.01) security bug!! From 15-DEC-2000
Describes the information disclosure vulnerability in iAS 1.0.1

Re: Executing scheduler job makes me SYS! (07-OCT-2004)
Contains a problem, that select username from dual returns SYS after running a job. It is reproducible from other users. However, this bug seems to have been fixed in Version 10.1.0.4. but not in earlier versions. We found out first the unknown security bug.
➔ This forum entry is now blocked by Oracle.

Now, we resort the results by date to see the latest issues.

Some results:

Perwspdc Attachment Form Shows All Attachments (27-JAN-2005)
If you open this document, you could not find the string "security bug" in the note 272234.1. This means that there must be a hidden string (comment from Oracle analyst?) in this note. The explanation is sufficient.

Attachments in Person on Special Info Types (SIT), Appearing for Everybody (29-DEC-2004)
This bug contains detailed exploit code and describes how to reproduce this issue.

Search String: "denial of Service"

Some results:

DO YOU NEED TO PASSWORD PROTECT THE LISTENER? 3-Jan-2005 650995.999
Answer from an Oracle employee: "I know no one likes to use the password protection in the listener. I used to be one of the first people to turn it off when working with customer."

Funny comment from an Oracle employee. I believe she is not aware how easy it is to become DBA or destroy a database via an unprotected listener. (See Become DBA via TNS Listener)

Search String: "password protect the listener"

Some results:

Password Protect the Listener in an OFS Environment 635173.999 19-JUL-2004
Some customers are reporting that it is not possible to set a listener password in an Oracle Failsafe environment. Happy hacking for hackers?

Search String: "hacking"

Some results:

MIME.TYPES MAKES SERVLET'S URL-PATTERN TO BE DEALT WITH CASE INSENSITIVE 3861451 21-APR-2005

Search string: "Kornbrust"

Some results:

1. Visualsdo.exe stores unencrypted Password

Then, I also checked for entries from the usual suspects “Pete Finnigan”, “David Litchfield”, “Stephen Kost”, “Cesar Cerrudo”, but, I didn’t find useful information.

Search string: “NSA”, “FBI” or “DOD”

Some results:

The results “Function based Index” and “Date of Death” are not security related. The “NSA” string returns a forum entry from an NSA employee.

Forum entries and Metalink notes normally contain more generic information. The bug database contains sensitive information like test cases. A test case is nothing else than proof-of-concept code for a bug. If a bug is security related then a test case becomes an exploit code.

First a few words on the Oracle bug database. The BugDB is Oracle's bug database which contains all the bugs found within or related to the Oracle products. Bugs can be public or classified. This status (type of bug) is set by a flag and like every flag (it is set by humans) and it can sometimes be set up wrongly.
Often security related bugs are classified incorrectly. This is due to the fact that a security bug starts off often as a normal bug and later changes to a security bug. Then, it is necessary for the analysts to change the flag from public to classified and sometimes, this important change get forgotten!

What is a security bug in Oracle terms?
The question sounds straight forward but, it is the philosophical side that is however interesting! There can always be different explanations to a question and the following are some:

- Only security bugs announced and published by Oracle on OTN are security bugs.
- Every bug which could affect the stability or functionality of the database/application server/application in a negative way, is referred to as a security bug. Such negative events could be a database crash, 100% CPU usage, privilege escalation, …

I personally prefer the second approach as I believe it is a correct way. For example, if a normal database user (e.g. scott) could crash the database with a simple SQL-Statement or a PL/SQL-program or the CPU usage of 100% after submitting an SQL statement, then I believe this IS security related.

To search the bug database, try the advanced search mask option and check the bug database only. After entering the search string, hit the submit button.

We started the search with the string "ln 100% CPU" and found the following bug

SELECT POWER(:A + :B, :C) FROM DUAL" HANGS WITH A=1, B=0.03175655, C=1.825

The bug described that the following SQL statement made the CPU to hang on the 8i TRUE 64.

```
select power(1 + 0.03175655, 1.825) from dual;
```

If you are able to submit this statement (e.g. via SQL Injection) you could do a denial of service attack.

Now we search for "SQL Injection"

The first entry we get is

BACKPORT BUG 2853895 - 3.0.9.8.5: SQL INJECTION BUG FIX IN A SINGLE BUNDLE from 19-JAN-2005

Following the hyperlink of the bug 3068980, we ~~find~~ found the following text in the first line of the document:

Backport the bug 2853895: RELEASE FIX FOR SQL INJECTION BUGS IN A SINGLE

OK, now we know that multiple bugs are fixed by one single patch. The rest of this bug is not security relevant and we can skip the note.

But then, opening bug 2853895, the bug details contained the following 4 lines:

Bug 2846646 - BACKPORT: bug 2675316 - 9.0.2.3 : SQL INJECTION ATTACK THROUGH ORG_CHART.SHOW

Bug 2846654 - BACKPORT bug 2675332 - 9.0.2.3 : SQL INJECTION ATTACK THROUGH WWA_APP_MODULE

Bug 2846658 - BACKPORT bug 2675346 - 9.0.2.3 : SQL INJECTION ATTACK ON WWV_DYNXML_GENERATOR.SHOW

Bug 2846638 - SECURITY: BACKPORT bug 2597360 - 9.0.2.3 : WWV_FORM LOV ALLOWS ARBITRARY SELECT

A few lines later we found this:

Bug 2675300 - SQL INJECTION ATTACK IN WWV_UI_LOVF should also be included in the bundle.

We then, opened all the above mentioned security bugs and found almost all were classified with the exception of bug 2846638

Bug 2846638 contained the information that an unauthenticated user can select any data from any table.

```
st?p_fieldname=p_attributes&p_fieldname=p_attributenames&p_fie
ldname=p_attributedatatypes&p_fieldname=p_attributesiteid&p_lo
v=SEARCHATTRLOV&p_element_index=0&p_formname=SEARCH54_PAGESEAR
CH_899010056&p_where=for_search_criteria%20=%201%20order=1&p_f
ilter=%25
```

This causes the following SQL to be constructed and executed by the Portal...

```
select title,name,data_type,siteid from wwsbr_attribute$ a
Where for_search_criteria = 1 Order by 1
```

Again, we found exploit code on Metalink.

Hints for customers and Oracle employees:

- Customers should use, if possible, a freemail account in forum entries.
- Anonymous configuration files when posting on Metalink
- Remove passwords before posting content on Metalink
- If you are reporting a bug to Oracle think of the possibility that this bug could be security related and escalate it if necessary. Even, if this costs additional time and money it would make Oracle more secure in the long run.
- Oracle analysts should become more security aware and try to avoid providing insecure advices like removing listener passwords, submitting xhost+, …
- Oracle secalert should check Metalink on a regular basis because very often, customers post security details to public forums (see Switch SYS via dbms_scheduler)

Search hints:

- Always use the "Advanced " search option on the bug Database
- Increase the number of results to 200
- Use the sort by date option for search results

Useful search strings (not just for Metalink):

hacker, hacking, SQL Injection, Cross Site Scripting, CSS, XSS, Buffer Overflow, Denial of Service, D.o.S., ORA-00907, ORA-00933, ORA-01756, crash, memory leak, abort, corrupted, corrupt, CPU spin, CPU spins, 100% load, CPU hangs, …

History:

- 16-may-2005 - V1.00 Initial release
- 22-may-2005 - Oracle secalert informed
- 31-may-2005 - V1.01 Public release

Other Oracle security related documents from Red-Database-Security GmbH:

Whitepaper and Presentations:
http://www.red-database-security.com/whitepaper/oracle_security_whitepaper.html

Hardening Oracle Application Server 9i Rel.1, 9i Rel.2 and 10g:
http://www.red-database-security.com/wp/DOAG_2004_us.pdf

Hardening Oracle DBA and Developer Workstations:
http://www.red-database-security.com/wp/hardening_admin_pc_us.pdf

Database Rootkits and Oracle Rootkits:
http://www.red-database-security.com/wp/db_rootkits_us.pdf

Google Hacking of Oracle Technologies:
http://www.red-database-security.com/wp/google_oracle_hacking_us.pdf

Yahoo Hacking of Oracle Technologies:
http://www.red-database-security.com/wp/yahoo_oracle_hacking_us.pdf

About Red-Database Security GmbH:
Red-Database-Security GmbH is a specialist in Oracle Security. We are offerings Oracle security trainings, database and application server audits, penetration tests, oracle (security) architecture reviews and software security solutions against Oracle rootkits.

Contact:
If you have questions or comments you could contact us via

ak at red-database-security.com