Oracle Default Users, Passwords and Hashes

By <u>Pentest Limited</u>

This paper contains links to a repository of Oracle default users and passwords. Password hashes are included so that an SQL script can be easily generated against the list of users to compare the hash with the one stored for the user in the database. The purpose of this repository is to provide a single source for all default users, to make it easier for the *dba* or security consultant to ensure all default users have either been removed if possible or at least had the passwords changed.

Updates to the list

Pentest intend to keep this list updated as we become aware of additional default users and passwords. We invite anyone to contribute to this list. If you have new users and passwords then please email <u>default@pentest.co.uk</u>.

Would you like to be notified of changes

If you would like to be made aware when this list changes by email then please send a blank email to <u>default-sub@pentest.co.uk</u>. If you would like to un-subscribe then please send a blank email to <u>default-unsubscribe@pentest.co.uk</u>.

SQL scripts to check your own database for default passwords

An SQL script has been generated from the table below that will check the users in your database to see if any default users have been installed and still have password set to the default value. Click here <u>check_users.sql</u> to download the script. This script needs to be run as a *dba* so that the view dba_users can be accessed.

The script now has a "connect internal" in it and an "exit" at the end. If you wish to run the script as another *dba* or not exit then please be aware that you will need to remove these two lines.

A second script has been generated that checks for default roles with default passwords. The table of default roles with default is available further down this page. Click here <u>check_roles.sql</u> to obtain this script. This script also needs to be run as *SYS* or *INTERNAL* so that the table SYS.USER$ can be accessed. Again there is a "connect internal" and "exit" in the script. Please comment out or delete if you wish to not exit or use *INTERNAL*.

Default Users, Passwords and hash's

The linked <u>repository</u> has been compiled as work in progress by Pentest Limited and lists the known default users, passwords and hashes. Where a password is not known but the hash is a password of "UNKNOWN" has been used.

A <u>CSV file</u> is also provided for use within scripts that check for default users and passwords.

Roles with default passwords

This section provides a table of default roles where there is a default password that is known. The entries are also available in the repository.

ROLE NAME	PASSWORD	HASH
ORD_SERVER	ODS	C6E799A949471F57
WKADMIN	WKADMIN	888203D36F64C5F6
WKUSER	WKUSER	8B104568E259B370

Non Database usernames and passwords

This section describes users and passwords where the username and password are not stored in the SYS.USER$ table in the database. This section will be increased as more become known.

USERNAME	PASSWORD	APPLICATION
INTERNAL	ORACLE	Password File Authentication
Administrator	Administrator	WebCache
User ID cn=orcladmin	welcome	Internet Directory Service

Oracle Based Applications

This section will be added to include default users and passwords for Oracle based applications where an Oracle database or applications are used and default users and passwords are installed.

Notes

There have been some big changes to the list and the list is now the biggest list of default users and passwords we know about on the Internet for Oracle. Some of the users in the repository benefit from additional comments.

USERNAME	COMMENTS
PERFSTAT	The spelling of this user is correct in the list. We have also seen this username spelled as PERSTAT in another list on the Internet. We could not find this spelling in any Oracle distribution we have but if anyone can confirm PERSTAT does exist then we will promote it to the list and scripts.
!DEMO_USER	We have seen the user !DEMO_USER quoted on some lists on the Internet. We have checked out the install scripts included with Oracle and this is used as a substitution variable and is not a default user. If anyone can confirm that this is indeed a genuine user then we will promote it to the list and scripts
ORACACHE	This user has a password of "ORACACHE" in some sources. This user in later versions of Oracle has a random password and therefore cannto be checked for. We have left this user

	in the list above with this default password for completeness.
OSE$HTTP$ADMIN	This user has a password of "INVALID" in some sources. This user in later versions of Oracle has a random password and therefore cannto be checked for. We have left this user in the list above with this default password for completeness.
AURORAJISUTILITY$	This user has a password of "INVALID" in some sources. This user in later versions of Oracle has a random password and therefore cannto be checked for. We have left this user in the list above with this default password for completeness.
REP_OWNER	This user has been found by myself and another source with two differing passwords, REP_OWNER and DEMO. Therefore it is in the list twice and in the scripts twice.
USER	This user is listed on one list we found with a password of USER. We cannot find this in any of the installations we have. The name is obviously an Oracle keyword and as such the only way to create this user is to quote the word USER both for the password and for the username. Because Oracle is not case sensitive the username whether it's upper case or lower case will create the same hash. The script above assumes that the username is uppercase. If you wish to check for lower case as well, please alter the script. If anyone can confirm this is a genuine default user, then please let us know.

It is worth remembering that it's the data in the actual database that should be protected. It's not necessary to get SYS, SYSTEM or even to have DBA privileges to get at user data in an Oracle database. A user such as DBSNMP or OUTLN can access a list of users in the database. The actual user information is stored in a database table called USER$ owned by the user SYS. Unless you are very lucky and someone has inadvertently granted access to this table you will not be able to see it unless you are logged on as SYS. There is also a view DBA_USERS that accesses this SYS table. Access is granted to select from this view to users who are DBA, or who have been granted permission to SELECT ANY VIEW. All is not lost however as any user who has the minimum permissions such as DBSNMP can access another view called ALL_USERS. This view doesn't let you see the password hash, but does let you get a list of all of the database users. If you can get a users password and quite often they are set to USER_NAME/USER_NAME then you can probably access the production schema and certainly do SQL Injection on the application. Using one of the innocent users such as DBSNMP or OUTLN you can glean a lot of information about a database, and who uses it.

Also for both Linux and Windows NT installations the internal users default password is set to oracle. This user name is used to connect effectively as SYS without having the SYS password. It should be noted that the use of connect internal has been deprecated in Oracle 9i.

Credits

Pentest would like to credit the following people for either directly supplying us with default users and passwords or because we found some default users and / or passwords that we did not know about on their sites or in papers produced by them.

Aaron C Newman	www.appsecinc.com
David Litchfield	www.nexgensys.com
Tom Morgan	www.thales-tracs.com
Mark Edge	.
cirt	www.cirt.net

About Pentest

Established in 2001, Pentest Limited is a leading international provider of IT security, specialising in Web Application Security and Penetration Testing services. Pentest provides independent, practical advice to a wide range of clients across the UK, Europe, USA and Asia. For more information, or for further details about Pentest's services, please visit www.pentest.co.uk or call +44 (0) 161 233 0100.