



# secure auditor

## Audit Report

### Vulnerability comparison by machine with solutions

**Report Generated Time:** 10/13/2011 At 5:29:39PM

**Audit Name:** : Ora Audit With Test Profile(Oct 13

**Description:** : 2011\_10\_13\_5:28PM)  
Oracle Audit Report

**IP Count** : 2

**IPs:** : 192.168.100.51, 192.168.100.55



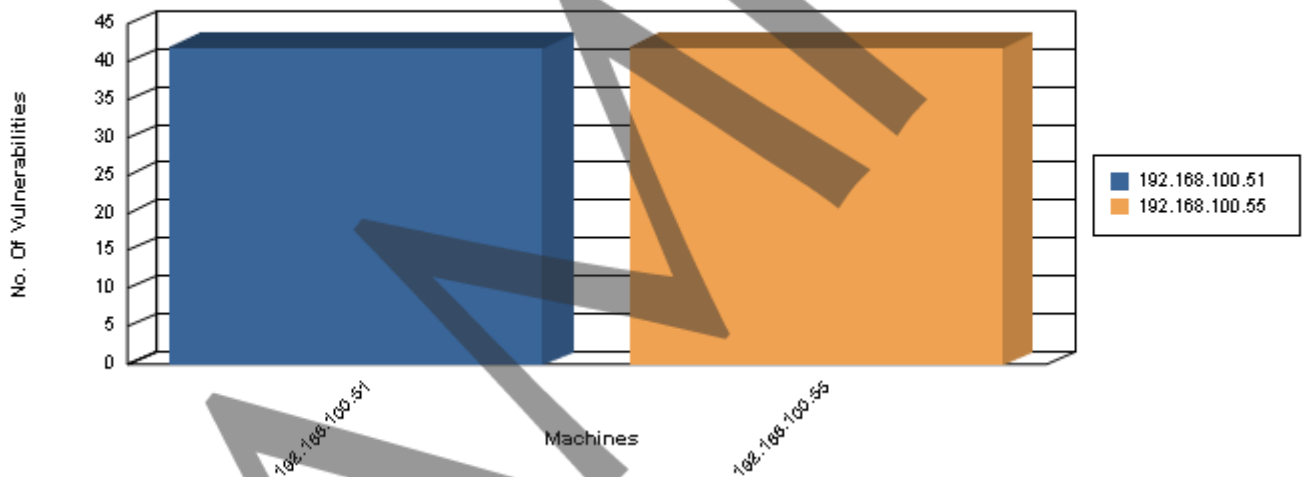


# Vulnerability Comparison by machine with solutions

Report generated on 13-Oct-2011 at 5:29:39PM

Oracle databases are precious ornaments for an organization as most of the information assets are denned there. A security scan was performed on your Oracle database or multiple oracle databases.This audit report will give you a complete picture of your database security pasture. This review was performed on your network for single or multiple IP's with their number of audits regarding to single or multiple databases. This Report shows audit detail for each machine and databasess name with port numbers. This report is designed to provide a wide-ranging description of vulnerability found on specific audits performed. You can also review the summarized overview of the vulnerabilities discovered. This report covers the maximum researched and checked information about vulnerability including the aspects, ways and areas sensitive or unsafe and usually takes up by attackers. It is recommended to take a thorough review of the vulnerabilities explored.

## Machine(s) and Vulnerabilities



## Summary Information

Machine IP	Database	Number of Vulnerabilities
Total Vulnerabilities on : 192.168.100.51	orcl	= 42
Total Vulnerabilities on : 192.168.100.55	orcl	= 42
<b>Total Vulnerabilities :</b>		<b>= 84</b>

## Vulnerability Comparison by machine with solutions

**Audit Performed:** Ora Audit With Test Profile(Oct 13 2011) **Selected Profile:** Testing

**Machine :** 192.168.100.51

**Database :** orcl

**Risk Level :** High

**Vulnerability Name** Profile settings - Failed Login Attempts

### Vulnerability Description :

Oracle Database provides a set of built-in password protections designed to protect your users' passwords. One of the way is by profile setting through which database resources and parameters in use for password management features can be limited.

Make a new profile and do the appropriate settings in it and then assign it to your newly created Users.

Filed\_login\_attempts is a feature that Sets the maximum times a user try to log in and to fail before locking the

account.Avoid setting this parameter to UNLIMITED value.It denotes that the account can only be unlocked by a user with the ALTER ANY USER system privilege.

Lets take an EXAMPLE:

Each user can create only two sessions.The session will be dropped by oracle after 30 minutes of idleness(doino nothing).

Long running processes are not idleafter three unsuccessful attempts, the account will be locked. After 1 day the account

will be unlocked automatically if it has been locked by failed\_attempts. The password will expire after 30 days, and there

will be 2 days grace period starting from the time the account is accessed beginning with the 30th day. The same password can

be reused again within 12 days.

```
create profile appl_profile limit
sessions_per_user      2 --
idle_time              30 -- minutes
failed_login_attempts  3 --
password_life_time     30 -- days
password_reuse_time    12 --
password_reuse_max     unlimited --
password_lock_time     1 -- days
password_grace_time    2 -- days
password_verify_function null;
```

If a session exceeds one of these limits, Oracle will terminate the session.

### Solution :



## Vulnerability Comparison by machine with solutions

To fix this problem, specify a limit in a number for failed login attempts feature in the FAILED\_LOGIN\_ATTEMPTS parameter.

It is possible by using two ways:

- 1) Creating the profile using the CREATE PROFILE statement.
- 2) Executing the ALTER PROFILE statement later.

Alter profile and set parameter value by using following command

a. ALTER PROFILE [profile name] LIMIT FAILED\_LOGIN\_ATTEMPTS xx

A profile must be assigned to user after it is configured using command:

b. ALTER USER [username] PROFILE [profile name]

c. A locked account can be unlocked by an account using the ALTER ANY USER

system privilege command:

ALTER USER [username] ACCOUNT UNLOCK

<b>Audit Performed:</b>	Ora Audit With Test Profile(Oct 13 2011)	<b>Selected Profile:</b>	Testing
-------------------------	--	--------------------------	---------

**Machine :** 192.168.100.51

**Database :** orcl

<b>Risk Level :</b>	Informational
---------------------	---------------

**Vulnerability Name** Database Banner

**Vulnerability Description :**

A DBA should have some informational data.

**Solution :**

This is an informative vulnerability therefore it does not require any solution.

**Vulnerability Name** Password Hashes

**Vulnerability Description :**

Getting information to check the hashes of passwords.A DBA should have some informational data.

**Solution :**

This is an informative vulnerability therefore it does not require any solution.

<b>Audit Performed:</b>	Ora Audit With Test Profile(Oct 13 2011)	<b>Selected Profile:</b>	Testing
-------------------------	--	--------------------------	---------

**Machine :** 192.168.100.55

**Database :** orcl

<b>Risk Level :</b>	High
---------------------	------

**Vulnerability Name** Profile settings - Failed Login Attempts

## Vulnerability Comparison by machine with solutions

### Vulnerability Description :

Oracle Database provides a set of built-in password protections designed to protect your users' passwords. One of the way is by profile setting through which database resources and parameters in use for password management features can be limited.

Make a new profile and do the appropriate settings in it and then assign it to your newly created Users.

Filed\_login\_attempts is a feature that Sets the maximum times a user try to log in and to fail before locking the

account.Avoid setting this parameter to UNLIMITED value.It denotes that the account can only be unlocked by a user with the ALTER ANY USER system privilege.

Lets take an EXAMPLE:

Each user can create only two sessions.The session will be dropped by oracle after 30 minutes of idleness(doining nothing).

Long running processes are not idleafter three unsuccessful attempts, the account will be locked. After 1 day the account

will be unlocked automatically if it has been locked by failed\_attempts. The password will expire after 30 days, and there

will be 2 days grace period starting from the time the account is accessed beginning with the 30th day. The same password can

be reused again within 12 days.

```
create profile appl_profile limit
sessions_per_user          2 --
idle_time                  30 -- minutes
failed_login_attempts      3 --
password_life_time        30 -- days
password_reuse_time        12 --
password_reuse_max        unlimited --
password_lock_time         1 -- days
password_grace_time        2 -- days
password_verify_function   null;
```

If a session exceeds one of these limits, Oracle will terminate the session.

### Solution :

## Vulnerability Comparison by machine with solutions

To fix this problem, specify a limit in a number for failed login attempts feature in the FAILED\_LOGIN\_ATTEMPTS parameter.

It is possible by using two ways:

- 1) Creating the profile using the CREATE PROFILE statement.
- 2) Executing the ALTER PROFILE statement later.

Alter profile and set parameter value by using following command

a. ALTER PROFILE [profile name] LIMIT FAILED\_LOGIN\_ATTEMPTS xx

A profile must be assigned to user after it is configured using command:

b. ALTER USER [username] PROFILE [profile name]

c. A locked account can be unlocked by an account using the ALTER ANY USER

system privilege command:

ALTER USER [username] ACCOUNT UNLOCK

<b>Audit Performed:</b>	Ora Audit With Test Profile(Oct 13 2011)	<b>Selected Profile:</b>	Testing
<b>Machine :</b>	192.168.100.55		
<b>Datebase :</b>	orcl		
<b>Risk Level :</b>	Informational		

**Vulnerability Name** Database Banner

**Vulnerability Description :**

A DBA should have some informational data.

**Solution :**

This is an informative vulnerability therefore it does not require any solution.

**Vulnerability Name** Password Hashes

**Vulnerability Description :**

Getting information to check the hashes of passwords.A DBA should have some informational data.

**Solution :**

This is an informative vulnerability therefore it does not require any solution.