secure auditor

Audit Report

Vulnerability categorization by machine

Report Generated Time: 10/13/2011 At 5:31:24PM

Audit Name: : Ora Audit With Test Profile(Oct 13 2011 5:28PM)
Description: : Oracle Audit Report
IP Count : 2
IPs: : 192.168.100.51, 192.168.100.55

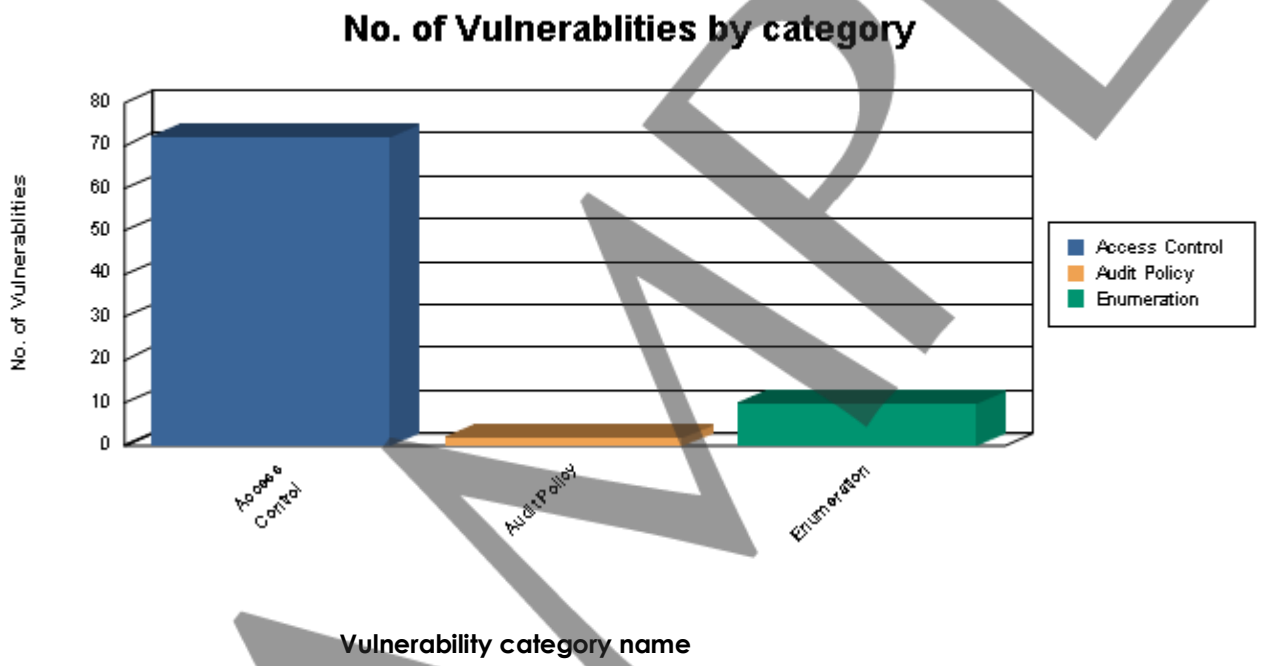
Licensed To : Support
Company Name : Secure Bytes

SECURE BYTES

Vulnerability categorization by machine

Report generated on 13-Oct-2011 at 5:31:24PM

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 databases 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.



Vulnerability categorization by machine

Category	**Access Control**
Audit Performed :	**Ora Audit With Test Profile(Oct 13 2011 5:28PM)** **Selected Profile:** **Testing**

Machine IP **192.168.100.51** **Machine Port :** **1,521**

Database **orcl**

Risk Level : Informational

Name Password Hashes

Description

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

192 Vulnerability/ies of type Access Control

Category	**Audit Policy**
Audit Performed :	**Ora Audit With Test Profile(Oct 13 2011 5:28PM)** **Selected Profile:** **Testing**

Machine IP **192.168.100.51** **Machine Port :** **1,521**

Database **orcl**

Risk Level : High

Name Profile settings - Failed Login Attempts

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(doing 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.

Vulnerability categorization by machine

```
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.

3 Vulnerability/ies of type Audit Policy

Category Enumeration

Audit Performed : Ora Audit With Test Profile(Oct 13 2011 5:28PM) **Selected Profile:** Testing

Machine IP 192.168.100.51 **Machine Port :** 1,521

Database orcl

Risk Level : Informational

Name Database Banner

Description

A DBA should have some informational data.

190 Vulnerability/ies of type Enumeration

Category Access Control

Audit Performed : Ora Audit With Test Profile(Oct 13 2011 5:28PM) **Selected Profile:** Testing

Machine IP 192.168.100.55 **Machine Port :** 1,521

Database orcl

Risk Level : Informational

Name Password Hashes

Description

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

192 Vulnerability/ies of type Access Control

Category Audit Policy

Audit Performed : Ora Audit With Test Profile(Oct 13 2011 5:28PM) **Selected Profile:** Testing

Machine IP 192.168.100.55 **Machine Port :** 1,521

Database orcl

Risk Level : High

Vulnerability categorization by machine

Name	Profile settings - Failed Login Attempts

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(doing 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.

3 Vulnerability/ies of type Audit Policy			
Category	**Enumeration**		
Audit Performed :	**Ora Audit With Test Profile(Oct 13 2011 5:28PM)**	**Selected Profile:**	**Testing**

Machine IP 192.168.100.55 **Machine Port :** 1,521

Database orcl

Risk Level :	Informational
Name	Database Banner

Vulnerability categorization by machine

Description

A DBA should have some informational data.

190	**Vulnerability/ies of type**	**Enumeration**
Total Vulnerabilities:	**84**	