

# Oracle Database Security and Audit

Beyond Checklists

Copyright © 2014, Reidy Database Consulting, LLC

## Audit key data

- Base tables
- User lists
- FGA
- Audit trail
- Core configuration
- Java
- Backup

Copyright © 2014, Reidy Database Consulting, LLC

### Base tables:

### USER\$, USER\_HISTORY\$

who can access: Release 1.0.3.0.0 - Production on Sat Mar 22 19:17:22 2014  
Copyright (c) 2004 Petefinnigan.com Limited. All rights reserved.

NAME OF OBJECT TO CHECK [USER\_OBJECTS]: user\$  
OWNER OF THE OBJECT TO CHECK [USER]: sys

Checking object => SYS.USER\$

=====

Object type is => TABLE (TAB)  
Privilege => SELECT is granted to =>  
User => APEX\_040000 (ADM = NO)  
User => CTXSYS (ADM = NO)  
User => XDB (ADM = NO)

PL/SQL procedure successfully completed.

For updates please visit <http://www.petefinnigan.com/tools.htm>

Copyright © 2014, Reidy Database Consulting, LLC

USER\$ contains password hashes. We saw earlier that access to these can lead to cracked passwords.

USER\_HISTORY\$ also contains password hashes.

Base tables:  
LINK\$

who\_can\_access: Release 1.0.3.0.0 - Production on Sat Mar 22 19:19:52 2014  
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

```
NAME OF OBJECT TO CHECK      [USER_OBJECTS]: link$
OWNER OF THE OBJECT TO CHECK [USER]: sys
```

```
Checking object => SYS.LINK$
```

PL/SQL procedure successfully completed.

For updates please visit <http://www.petefinnigan.com/tools.htm>

Prior to 10gR2, passwords for database links were plain text!

# Password hashes can be taken and cracked.

Checking object => SYS.DBA\_USERS

[illegible]

## User lists - DBA\_USERS

## User lists - ALL\_USERS

who\_can\_access: Release 1.0.3.0.0 - Production on Sat Mar 22 19:29:24 2014  
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

```
NAME OF OBJECT TO CHECK      [USER_OBJECTS]: all_users
OWNER OF THE OBJECT TO CHECK [USER]: sys
```

Checking object => SYS.ALL\_USERS

```
Object type is => VIEW (TAB)
Privilege => SELECT is granted to *
Role => PUBLIC (ADM = NO)
```

PL/SQL procedure successfully completed.

For updates please visit <http://www.petefinnigan.com/tools.htm>

## Key data - FGA\_LOG\$

who can access: Release 1.0.3.0.0 - Production on Sat Mar 22 19:32:51 2014  
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF OBJECT TO CHECK [USER\_OBJECTS]: fga\_log\$  
OWNER OF THE OBJECT TO CHECK [USER]: sys

Checking object => SYS.FGA\_LOG\$

Object type is => TABLE (TAB)  
Privilege => DELETE is granted to =>  
Role => DELETE\_CATALOG\_ROLE (ADM = NO) which is granted to =>  
User => SYS (ADM = YES)  
Role => DBA (ADM = YES) which is granted to =>  
User => SYS (ADM = YES)  
User => PHPDEMO (ADM = NO)  
User => SYSTEM (ADM = YES)  
User => U296006 (ADM = NO)

PL/SQL procedure successfully completed.

For updates please visit <http://www.petefinnigan.com/tools.htm>

Copyright © 2014, Reidy Database Consulting, LLC

Base table for all fine grained audit.

Test all FGA views and base tables. No components should be PUBLIC.

## Audit trail - AUD\$

who can access: Release 1.0.3.0.0 - Production on Sat Mar 22 19:35:44 2014  
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF OBJECT TO CHECK [USER\_OBJECTS]: aud\$  
OWNER OF THE OBJECT TO CHECK [USER]: sys

Checking object => SYS.AUD\$

Object type is => TABLE (TAB)  
Privilege => DELETE is granted to =>  
Role => DELETE\_CATALOG\_ROLE (ADM = NO) which is granted to =>  
User => SYS (ADM = YES)  
Role => DBA (ADM = YES) which is granted to =>  
User => SYS (ADM = YES)  
User => PHPDEMO (ADM = NO)  
User => SYSTEM (ADM = YES)  
User => U296006 (ADM = NO)

PL/SQL procedure successfully completed.

Copyright © 2014, Reidy Database Consulting, LLC

Also test all audit views – DBA\_AUDIT\_TRAIL, DBA\_AUDIT\_SESSION, DBA\_AUDIT\_STATEMENT, and all option views. The audit trail should never be seen by schema accounts or user accounts of any kind.

## Core configuration

- DBA\_SOURCE
- ALL\_SOURCE
  - Base table - SOURCE\$
- DBA\_TRIGGERS
- ALL\_TRIGGERS
  - Base table - TRIGGER\$

Copyright © 2014, Reidy Database Consulting, LLC

## Core data

- Source code in the database is just as good as documentation
  - Intellectual property
  - System access
- Used by hackers and researchers to locate SQL Injection vulnerabilities

Copyright © 2014, Reidy Database Consulting, LLC

## Key data - Java

```
1 select substr(kind,1,1) g,r,
2   substr(type_name,instr(type_name,'.',-1)+1,
3   length(type_name)) perm,
4   substr(grantee,1,10) grantee,
5   substr(name,1,40) permname,
6   substr(nvl(action,'null'),1,10) action
7* from dba_java_policy
SQL> /
```

G_R	PERM	GRANTEE	PERMNAME	ACTION
G	RuntimePermission	EJBCLIENT	createClassLoader	null
G	RuntimePermission	EJBCLIENT	getClassLoader	null
G	SocketPermission	EJBCLIENT	*	connect,re
G	JServerPermission	JAVADEBUG	Debug	null
G	FilePermission	JAVASVPRI	<<ALL FILES>>	read,write
G	SerializablePermission	JAVASVPRI	*	null
G	RuntimePermission	JAVASVPRI	createClassLoader	null
G	RuntimePermission	JAVASVPRI	getClassLoader	null
G	RuntimePermission	JAVASVPRI	readFileDescriptor	null
G	RuntimePermission	JAVASVPRI	setContextClassLoader	null
G	RuntimePermission	JAVASVPRI	setFactory	null
G	RuntimePermission	JAVASVPRI	setFileDescriptor	null
G	RuntimePermission	JAVASVPRI	setIO	null
G	RuntimePermission	JAVASVPRI	writeFileDescriptor	null
G	SocketPermission	JAVASVPRI	*	accept,con
G	SQLPermission	JAVASVPRI	setLog	null
G	FilePermission	JAVASERPR	<<ALL FILES>>	read

Copyright © 2014, Reidy Database Consulting, LLC

Use the query java.sql.

Test who has the system privileges listed in the “GRANTEE” column do not forget database roles!).

## Key data - Java (2)

- Review all the built in Java roles with respect to grants to non system users
- Review execute privileges on the DBMS\_JAVA% packages
- Review access to the external java programs loadjava
- Review the Java security model
  - The java model is very large and complex. Ensure that non system users do not have access to the Java environment and if java is used in the application review database and Java privileges assigned
- Review access to the Java views for structure and functionality and privileges

Copyright © 2014, Reidy Database Consulting, LLC

# Q&A