Reidy Database Consulting, LLC Database Security and Risk Assessmen

Oracle Database Security and Audit

Beyond Checklists

Convight © 2014 Reidy Database Consulting 110

Reidy Database Consulting, LLC Database Security and Risk Assessmen

Audit key data

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

Copyright © 2014, Reidy Database Consulting, LLC

Reidy Database Consulting, LLC
Database Security and Risk Assessment

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.ht

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

USER_HISTORY\$ also contains password hashes.

Redy Dumbase Considing LLC
Dumbase Security and Risk Assessment

Base tables:
LINK\$

who_can_access: Release 1.0.3.0.0 - Production on Sat Mar 22 19:19:52 2014
Copyright (c) 2004 PeteFinnipan.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.

Ready Database Consuling LLC
Discharts Security and Ruik Assessment

Consular dischart to \$15.00 SER

Ready Database Consuling LLC
Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

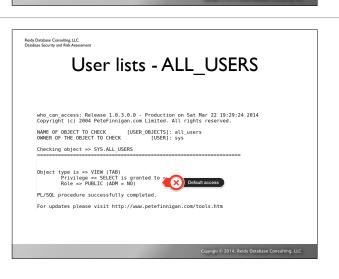
Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.00 SER

Ready Database Consuling LLC

Discharts Security on \$1.



```
Relationables Considering LIC Disables Considering LIC Disables Security and Risk Assessment

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_logs

OWHER OF THE OBJECT TO CHECK [USER_OBJECTS]: fsa_logs

Checking object > SYS, FGA_LOGS

Checking object > SYS, FGA_LOGS

Object type is => TABLE (TAB)

Privilege => DELETE is granted to =>

Role => DELETE (ATALOS, GOLE (ADM = NO) which is granted to =>

User => SYS (ADM = YES)

User => SYS (ADM = YES)

User => SYSTEM (ADM = YES)

User => SYSTEM (ADM = NO)

User => SYSTEM (ADM = NO)

User => SYSTEM (ADM = NO)

PL/SQL procedure successfully completed.

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

Base table for all fine grained audit.

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

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.

Reidy Database Consulting, LLC
Database Security and Risk Assessment

Core configuration

- DBA SOURCE
- ALL SOURCE
- Base table SOURCE\$
- DBA TRIGGERS
- ALL TRIGGERS
 - Base table TRIGGER\$

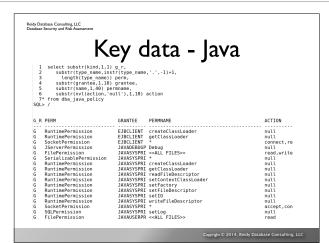
Convicts © 2014 Reidy Database Consulting 110

Reidy Database Consulting, LLC Database Security and Risk Assessmen

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

Conversely © 2014 Reidy Database Consulting 11



Use the query java.sql.

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

Reidy Database Consulting, LLC
Database Security and Risk Assessmen

Key data - Java (2)

- Review all the built in Java roles with respect to grants to non system users
- Review executé 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

_			
	Reidy Database Consulting, LLC Database Security and Risk Assessment		
		O 0 A	
		Q&A	