sentrigo™

MRI

Reseler for Adriatic region

Introduction to Database Security

Uroš Majcen uros.majcen@mri.si

Aci Polajnar acip@mri.si

Real Database Security

Agenda:

- The term from Hecker's Handbook with an Example
  SQL Injection
- Database Audit and Security, state of the art
- Major security problems of databases Password and resource management
- Finding security problems within my database using Repscan

The Term from Hacker's Handbook with an Example

SQL Injecton:

- Triggering normal DML procedure or package using non-normal set of input parameters
- SQL Injection is the most dangerous security vulnerability in (web) application.
- Many developers and "developers" still think that this is often just cosmetic problem…
- But, let us see an example

The Term from Hacker's Handbook with an Example

Example: Normal Usage

- SELECT UTL_INADDR.get_host_name ('127.0.0.1') FROM DUAL;
  Results: share1 (My computer name)

- SELECT UTL_INADDR.get_host_name (‘share1') FROM DUAL;
  Results: 127.0.0.1 (My computer IP)

The Term from Hacker's Handbook with Examples

Example: SQL Injection(1)

- SELECT UTL_INADDR.get_host_name (‘
  'Accounts=‘ || (SELECT COUNT (DISTINCT (username)) || ';' AS string
  FROM all_users)) FROM DUAL;

Results: ORA-29257: host Accounts=32; unknown
ORA-06512: at "SYS.UTL_INADDR", line 4
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at line 1

Database Audit and Security, state of the art

- Users / Schemas
- Roles
- System privileges
- Password and resource management
- Audit features via:
  - Core audit
  - Fine Grained Audit (FGA)
  - Triggers
- Identification and authentication
- Virtual Private Database (VPD) => Also Oracle Label Security (OLS)
- Built-in encryption – for database and file system (Transparent Data Encryption) (TDE)
- Network encryption solutions

Major security problems of databases

Problem	Cause	Solution
Databases with old versions and without support	Many customers still have installed old and vulnerable data base versions	To upgrade to a version with support
Definition of easy passwords to guess or permanence of the default passwords	Most of the databases still use the default passwords or the most common passwords are easy to guess	Reviewing the databases regularly and avoid defining simple passwords
Insecure configuration, too many privileges	Ignorance of the database administrators, not controlled access to the database by applications developed by third parties	To train DBAs
Insecure access through applications	Lack or no access training to database developers	To train the developers
Without audit	Fear on the work time impact and productivity, fear of the services suspension	Use products for auditing that will have no impact on the production environments

Finding security problems within my database using Repscan

- The world's most advanced Oracle vulnerability assessment and security scanning tool
- Developed based on the knowledge of Alexander Kornbrust, one of the world's best known authorities in Oracle security and CEO of Red-Database-Security
- Tested and deployed by leading enterprises in Europe and the U.S.

red database security

sentrigo

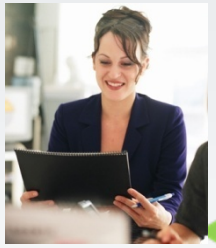
Repscan's philosophy and uniqueness

- Build on deep practial security knowledge (vs. DBMS vendor's "security guidelines")
- Test and report on real issues (vs. lengthy unreadable reports)
- Provide practical remedy advice / solutions
- Allow easy automation and integration with other products
- Create different outputs for dissimilar stakeholders (DBAs, developers, IT Security)
- Centralized reporting for up to thousands of db instances

Repscan's key features

- Over 3000 security verifications (Oracle databases and applications)
- Extremely fast weak password detection
- Central check for patch levels
- Detailed remedy reporting
- Changed database object detection:
  - Rootkits and other suspicious changes
  - View into changes caused by vendor updates
- Custom code testing for vulnerable coding
- Easy to use UI
- CLI option for automation and scripting

Repscan architecture



red database security

sentrigo

Feature details
Weak password detection

- Weak password are still the #1 security problem in applications
- Repscan provides the fastest password checking available
- Checks Oracle hashed passwords (SHA-1, MD5, DES)
- OID and APEX password checks
- Checks based on rainbow table technology and SAP password checks to be added soon
- Innovative plug-in technology, extensible with custom plugins

Password report sample

Check Passwords - Repscan 2.50 - Database Assessment Report

Repscan Report Created: Wed Apr 22 14:49:24 2009 GMT

Scanned databases

Database Name	Checksum(s)	Scan-Result
XE	dbchecksums\XE_sig.csv	failed

In XE the following weak passwords in database were found:

User name	Password	Status	Type	PW Type
SCOTT	TIGER	Open	Oracle DES	from dictionary
SYS	ORACLE	Open	Oracle DES	from dictionary
SYSTEM	ORACLE	Open	Oracle DES	from dictionary
SYSTEM	oracle	Open	APEX 2.1	from dictionary (lowercase)
DBSNMP	DBSNMP	Expired and Locked	Oracle DES	password=username
DIP	DIP	Expired and Locked	Oracle DES	password=username
HR	HR	Expired and Locked	Oracle DES	password=username
MDSYS	MDSYS	Expired and Locked	Oracle DES	password=username

Feature details - reports

- Reports in xml format
- Easy to integrate into other systems
- Easily configurable by customer
- Reports according to stakeholders:
  - **DBAs:** password reports, vulnerability report, sql fix report
  - **Developers:** PL/SQL security report
  - **IT security:** patch level, backdoor, Hedgehog rule report
  - **Auditors:** PCI-DSS report

Thank You!

Reseler for Adriatic Region

Uroš Majcen
Uros.majcen@mri.si
Aci Polajnar
acip@mri.si
Marjana Kovačič
Marjana.kovacic@mri.si