Oracle Database Security Assessment Tool 2.1
Know Your Security Posture Before Hackers Do

Pedro Lopes
Product Manager
Oracle Database Security
March 1, 2019
Data – Your Most **Valuable** Asset

Driver’s License Number, Passport Number, Tax Payer ID, Health Insurance Numbers, ...

Credit/Debit Card Number, Security Code, SSN, Age, Names, DOB, ...
Evolving Regulatory Landscape

- EU General Data Protection Regulation (EU GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley (SOX)
- HIPAA/HITECH
- Numerous breach notification laws
Who Wants Your Data?

- Insiders
- Former Employees
- Curiosity Seekers
- Customers
- Competitors
- Hacktivists
- Criminals
- Nation States
- Personal Data
- Financial Data
- Trade Secrets
- Regulated Data
- Former Employees
- Curiosity Seekers
- Customers
- Competitors
- Hacktivists
- Criminals
- Nation States
- Personal Data
- Financial Data
- Trade Secrets
- Regulated Data
Evolving **Attack Tools** and Techniques

- Stolen Credentials
- Phishing
- SQL Injection
- Privilege Escalation
- Buffer Overflow
- App Exploits
- XSS Attacks
- Unpatched Systems
Think Alike
Attacker vs Owner of the Data

Insider / Outsider

- Open Ports
- Database SIDs
- Known Users
- Common Passwords
- Encrypted Data
- Auditing On
- Privileged Users
- Database Version
- Known Vulnerabilities
- Known Packaged Apps
Where To Start & What to look for

Where does sensitive data reside?
Who are the users and their entitlements?
What controls do I have in place?
Is my Database securely configured?

Do we have a Database Security Team? Knowledge?
Analysis time?
Introducing
Oracle Database Security Assessment Tool
Oracle Database Security Assessment Tool (DBSAT)

Know Your Security Posture Before Hackers Do

• Understand how (in)secure your database is
  – Report on overall security status
  – Find the users, entitlements, and risks
  – Discover sensitive data in English, German, Dutch, French, Italian, Spanish & Portuguese *

• Actionable Assessment Reports
  – Summary and detailed information
  – Prioritized recommendations
  – Mapping to EU GDPR, CIS Benchmark and STIG *

• Stand-alone light weight tool: Quick, Easy

• FREE to current Oracle customers

* New in 2.1
What does DBSAT Check?

1. **Security Configuration**
   - Data Encryption
   - Auditing Policies
   - Fine-grained Access Control
   - Database and Listener Configuration
   - OS File permissions
   - Security Patches

2. **Users and Entitlements**
   - User Accounts, Privileges and Roles

3. **Sensitive Data**
   - Which type, where, how many

For Oracle Databases 10g and later
2.0.1 DBSAT New Features

• References to CIS Benchmark recommendations
• References to GDPR Articles/Recitals
• JSON output for integration with other tools
• Introduced Sensitive Data Discovery
  – English pattern file included out of the box
  – Customizable
2.0.2 DBSAT New Features

Introduced in July

- Support for Discoverer to Connect to Database servers over SSL channel
- Discover Sensitive Data in Exadata Express CS and ADW
- Discovered Sensitive Data columns can be imported into AVDF to power new Data Privacy Reports
2.1.0 DBSAT New Features

• **STIG** rules highlighting
• **New findings** on password file, global names, instance name RMAN backups and more
• Simplify identification of directly granted System Privileges.
  – Now marked with (D)
• Certified for Oracle Database 18c, 19c and **Autonomous Databases**

• Now includes sensitive pattern files for **German, Dutch, French, Spanish, Italian and Portuguese**
• New Sensitive Types, Categories and Subcategories
• Sensitive Data Categories now grouped by Risk Level
• Report include remarks and recommended controls for different Risk Levels
How does it work?

Oracle Database Security Assessment Tool
Easy as Download and count to 3!

1. Download

2. To get a Database **Security Assessment** report
   • Execute DBSAT Collector
   • Execute DBSAT Reporter

3. To get a Database **Sensitive Data Assessment** report
   • Execute DBSAT Discoverer
E.g. Assessment Flow Steps for Data Privacy initiative
From Discovery to Recommendations

Discover Sensitive Data
- Database Sensitive Data Assessment report

Assess Overall Security Configuration
- Database Security Assessment report

Examine Report Findings

Implement Security Controls / Tune Config
Discover Sensitive Data
Find What You Have, Where, How Much

- Review / Edit Configuration Parameters
  - Database connection
  - Sensitive Categories
  - Risk Levels
  - Include/Exclude Lists

- Review / Edit Patterns for Sensitive Types
  - Out-of-the-box Types
  - Add your own to search column name/comments

- Run DBSAT Discoverer

- Examine Report

[DATE OF BIRTH]
COL_NAME_PATTERN = DOB$|BIRTH.?((DT|DATE) | (DT|DATE)).*BIRTH
COL_COMMENT_PATTERN = \bDOB\b|BIRTH.?DATE|DATE.*BIRTH
SENSITIVE_CATEGORY = Biographic Info - Extended PII
Report: What Sensitive Data Do We Have? How Much?

Sensitive Data Landscape

<table>
<thead>
<tr>
<th>Sensitive Category</th>
<th># Sensitive Tables</th>
<th># Sensitive Columns</th>
<th># Sensitive Rows</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIOGRAPHIC INFO - ADDRESS</td>
<td>7</td>
<td>16</td>
<td>244</td>
</tr>
<tr>
<td>FINANCIAL INFO - CARD DATA</td>
<td>2</td>
<td>2</td>
<td>256</td>
</tr>
<tr>
<td>HEALTH INFO - PROVIDER DATA</td>
<td>1</td>
<td>1</td>
<td>149</td>
</tr>
<tr>
<td>IDENTIFICATION INFO - PERSONAL IDS</td>
<td>3</td>
<td>3</td>
<td>356</td>
</tr>
<tr>
<td>IDENTIFICATION INFO - PUBLIC IDS</td>
<td>3</td>
<td>12</td>
<td>321</td>
</tr>
<tr>
<td>IT INFO - USER DATA</td>
<td>1</td>
<td>1</td>
<td>149</td>
</tr>
<tr>
<td>JOB INFO - COMPENSATION DATA</td>
<td>7</td>
<td>10</td>
<td>527</td>
</tr>
<tr>
<td>JOB INFO - EMPLOYEE DATA</td>
<td>12</td>
<td>25</td>
<td>569</td>
</tr>
<tr>
<td>JOB INFO - ORG DATA</td>
<td>7</td>
<td>8</td>
<td>412</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>21</strong></td>
<td><strong>80</strong></td>
<td><strong>989</strong></td>
</tr>
</tbody>
</table>

* Number of unique Tables with Sensitive Data.  
** Number of unique Rows with Sensitive Data.
Report: Recommended controls

Security for Environments with High Value Data: Detective plus Strong Preventive Controls

Highly sensitive and regulated data should be protected from privileged users, and from users without a business need for the data. Activity of privileged accounts should be controlled to protect against insider threats, stolen credentials, and human error. Who can access the database and what can be executed should be controlled by establishing a trusted path and applying command rules. Sensitive data should be redacted on application read only screens. A Database Firewall ensures that only approved SQL statements or access by trusted users reaches the database – blocking unknown SQL injection attacks and the use of stolen login credentials.

Recommended controls include:

- Audit all sensitive operations including privileged user activities
- Audit access to application data that bypasses the application
- Encrypt data to prevent out of band access
- Mask sensitive data for test and development environments
- Restrict database administrators from accessing highly sensitive data
- Block the use of application login credentials from outside of the application
- Monitor database activity for anomalies
- Detect and prevent SQL injection attacks
- Evaluate: Oracle Audit Vault and Database Firewall, Oracle Advanced Security, Oracle Data Masking and Subsetting, Oracle Database Vault

Tables Detected within Sensitive Category: FINANCIAL INFO – CARD DATA

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Summary</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Risk</td>
<td>Found FINANCIAL INFO – CARD DATA within 2 Column(s) in 2 Table(s)</td>
<td>HCMI.HRM_EXTENDED, HCMI.SUPPLEMENTAL_DATA</td>
</tr>
</tbody>
</table>

E.g. Audit sensitive operations
Encrypt data
Mask data on Test & Dev
# Report: Which Tables Have Sensitive Data? How Much?

## Sensitive Table Summary

<table>
<thead>
<tr>
<th>Schema</th>
<th>Table Name</th>
<th>Columns</th>
<th>Sensitive Columns</th>
<th>Rows</th>
<th>Sensitive Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>FINACME</td>
<td>COMPANY_DATA</td>
<td>9</td>
<td>4</td>
<td>100</td>
<td>BIOGRAPHIC INFO – ADDRESS, IDENTIFICATION INFO – PERSONAL IDS</td>
</tr>
<tr>
<td>HCM1</td>
<td>COUNTRIES</td>
<td>3</td>
<td>1</td>
<td>25</td>
<td>BIOGRAPHIC INFO – ADDRESS</td>
</tr>
<tr>
<td>HCM1</td>
<td>DEPARTMENTS</td>
<td>4</td>
<td>1</td>
<td>27</td>
<td>JOB INFO – ORG DATA</td>
</tr>
<tr>
<td>HCM1</td>
<td>EMPLOYEES</td>
<td>11</td>
<td>8</td>
<td>107</td>
<td>IDENTIFICATION INFO – PUBLIC IDS, JOB INFO – COMPENSATION DATA, JOB INFO – EMPLOYEE DATA, JOB INFO – ORG DATA</td>
</tr>
<tr>
<td>HCM1</td>
<td>EMP_EXTENDED</td>
<td>3</td>
<td>3</td>
<td>107</td>
<td>FINANCIAL INFO – CARD DATA, IDENTIFICATION INFO – PERSONAL IDS, JOB INFO – EMPLOYEE DATA</td>
</tr>
</tbody>
</table>

Candidate tables for Encryption / Privileged user access/processor restriction?
### Report: Which Columns Have Sensitive Data? How Much?

#### Sensitive Column Details

<table>
<thead>
<tr>
<th>Schema Name</th>
<th>Table Name</th>
<th>Column Name</th>
<th>Column Comment</th>
<th>Sensitive Category</th>
<th>Sensitive Type</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>FINACME</td>
<td>COMPANY_DATA</td>
<td>CITY</td>
<td>--</td>
<td>BIOGRAPHIC INFO - ADDRESS</td>
<td>CITY</td>
<td>High Risk</td>
</tr>
<tr>
<td>FINACME</td>
<td>COMPANY_DATA</td>
<td>STATE</td>
<td>--</td>
<td>BIOGRAPHIC INFO - ADDRESS</td>
<td>STATE</td>
<td>High Risk</td>
</tr>
<tr>
<td>FINACME</td>
<td>COMPANY_DATA</td>
<td>TAX_PAYER_ID</td>
<td>--</td>
<td>IDENTIFICATION INFO - PERSONAL IDS</td>
<td>TAX ID NUMBER (TIN)</td>
<td>High Risk</td>
</tr>
<tr>
<td>FINACME</td>
<td>COMPANY_DATA</td>
<td>ZIP</td>
<td>--</td>
<td>BIOGRAPHIC INFO - ADDRESS</td>
<td>POSTAL CODE</td>
<td>High Risk</td>
</tr>
<tr>
<td>HCMI</td>
<td>COUNTRIES</td>
<td>COUNTRY_NAME</td>
<td>--</td>
<td>BIOGRAPHIC INFO - ADDRESS</td>
<td>COUNTRY</td>
<td>High Risk</td>
</tr>
<tr>
<td>HCMI</td>
<td>DEPARTMENTS</td>
<td>DEPARTMENT_NAME</td>
<td>--</td>
<td>JOB INFO - ORG DATA</td>
<td>DEPARTMENT NAME</td>
<td>Low Risk</td>
</tr>
<tr>
<td>HCMI</td>
<td>EMPLOYEES</td>
<td>EMAIL</td>
<td>This is the email address</td>
<td>IDENTIFICATION INFO - PUBLIC IDS</td>
<td>EMAIL ADDRESS</td>
<td>High Risk</td>
</tr>
<tr>
<td>HCMI</td>
<td>EMPLOYEES</td>
<td>EMPLOYEE_ID</td>
<td>This is the unique employee identifier</td>
<td>JOB INFO - EMPLOYEE DATA</td>
<td>EMPLOYEE ID NUMBER</td>
<td>High Risk</td>
</tr>
<tr>
<td>HCMI</td>
<td>EMPLOYEES</td>
<td>FIRST_NAME</td>
<td>--</td>
<td>IDENTIFICATION INFO - PERSONAL IDS</td>
<td>FIRST NAME</td>
<td>High Risk</td>
</tr>
</tbody>
</table>

Candidate columns for Masking, Pseudonymization, Audit Policies
Database Security Assessment Report
Security Configuration Status, Users and their Entitlements

- Run DBSAT Collector
- Run DBSAT Reporter
- Examine Findings Report

Output Formats:
- HTML
- Excel
- Text
- JSON
## Anatomy of a Finding

**Category of the Finding**

**Details of the Finding**

**Rationale and Recommendations**

**Mapping to Regulations**

**Can be Evaluate, Advisory, Pass, Low Risk, Medium Risk, High Risk**

**Applicability to Regulations**

---

### Example Finding

**Status:** High Risk

**Summary:** Examined 3 audit trails. Found no audit records. No errors found in audit initialization parameters.

**Details:**

- Traditional Audit Trail: No records found
- FGA Audit Trail: No records found
- Unified Audit Trail: No records found

### Remarks

Auditing is an essential component for securing any system. The audit trail allows for monitoring the activities of highly privileged users. For any attack that exploits gaps in other security policies, auditing cannot prevent the attack but it forms the critical last line of defense by detecting the malicious activity. Oracle Database 12c introduced Unified Auditing and this is the recommended auditing mode moving forward (pure Unified Audit mode). It adds several benefits as centralized audit logs in a single audit trail, improved performance, simplified management and security. The AUDIT_FILE_DEST controls the OS directory to which the audit trail is written if using AUDIT_TRAIL=os, xml, or xmlextended. This directory should be prevented from any unauthorized access. Sending audit data to a remote system is recommended in order to prevent any possible tampering with the audit records. The AUDIT_SYSLOG_LEVEL parameter can be set to send an abbreviated version of some audit records to a remote syslog collector. A better solution is to use Oracle Audit Vault and Database Firewall to centrally collect full audit records from multiple databases.

### References

- **CIS Oracle Database 12c Benchmark v2.0.0:** Recommendation 2.2.2
- **EU GDPR 2016/679:** Article 30, 33, 34
- **Oracle Database 12c STIG v1 r10:** Rule SV-75899r1, SV-76111r1, SV-76117r1, SV-76123r1, SV-76125r1, SV-76127r1, SV-76129r1, SV-76455r3
# Use Case: Is the Database Securely Configured?

## Summary Output with Prioritized Findings

<table>
<thead>
<tr>
<th>Section</th>
<th>Pass</th>
<th>Evaluate</th>
<th>Advisory</th>
<th>Low Risk</th>
<th>Medium Risk</th>
<th>High Risk</th>
<th>Total Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Information</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>User Accounts</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>Privileges and Roles</td>
<td>5</td>
<td>16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>21</td>
</tr>
<tr>
<td>Authorization Control</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Fine-Grained Access Control</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Auditing</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>Encryption</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Database Configuration</td>
<td>5</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Operating System</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>17</strong></td>
<td><strong>27</strong></td>
<td><strong>8</strong></td>
<td><strong>9</strong></td>
<td><strong>14</strong></td>
<td><strong>4</strong></td>
<td><strong>79</strong></td>
</tr>
</tbody>
</table>
Use Case: Users and Their Entitlements?

Directly Granted System Privileges

1342 grants of system privileges (17 with admin option). 122 Privileges are granted directly.

Users directly or indirectly granted each system privilege:

- ADMINISTER ANY SQL TUNING SET: DEBRA, OUTSRC_DBA, SCOTT, SSADMIN, SYSTEM(*), U1(D), U2(D)(*), U3(*)
- ADMINISTER DATABASE TRIGGER: DEBRA, OUTSRC_DBA, SCOTT, SSADMIN, SYSTEM
- ADMINISTER RESOURCE MANAGER: DEBRA, OUTSRC_DBA, SCOTT, SSADMIN, SYSTEM
- ADMINISTER SQL MANAGEMENT OBJECT: DEBRA, OUTSRC_DBA, SCOTT, SSADMIN, SYSTEM

(D) - Directly granted
(*) - With Admin option
Use Case: Users and Their Entitlements?

Users with DBA Role Granted Directly and Indirectly

User DEBRA got the DBA role indirectly via the role APP_ROLE.
Report in Multiple Formats

**HTML**

```
<table>
<thead>
<tr>
<th>USER.DEFPWD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td><strong>Summary</strong></td>
</tr>
<tr>
<td><strong>Details</strong></td>
</tr>
<tr>
<td><strong>Remarks</strong></td>
</tr>
<tr>
<td><strong>References</strong></td>
</tr>
</tbody>
</table>
```

**JSON**

```
{
  "severity": "5",
  "title": "Users with Default Passwords",
  "remarks": "Default account passwords for predefined Oracle accounts are well known. Open accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.",
  "details": "Users with default password: HR, SCOTT",
  "refs": [
    {
      "CIS": "Recommendation 1.2"
    }
  ],
  "type": "finding",
  "id": "USER.DEFPWD",
  "summary": "Found 2 unlocked user accounts with default password."
}
```

**Spreadsheet**

```
<table>
<thead>
<tr>
<th>Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Client Authentication Version</td>
</tr>
<tr>
<td>Minimum client version is not configured correctly.</td>
</tr>
</tbody>
</table>

Status: High Risk
Summary: Found 2 unlocked user accounts with default password.
Details: Users with default password: HR, SCOTT
Remarks: Default account passwords for predefined Oracle accounts are well known. Open accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.
References: CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.2
```

**Text**

```
* Users with Default Passwords *
Summary: High Risk
Summary: Found 2 unlocked user accounts with default password.
Details: Users with default password: HR, SCOTT
Remarks: Default account passwords for predefined Oracle accounts are well known. Open accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.
References: CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.2
```
Start Today!
Your attackers have already started!
Easy to Install and Run

• Download DBSAT 2.1 today from http://www.oracle.com/technetwork/database/security/dbsat.html
• Available to all Oracle database customers with active support contract
• Collect security config data by running ‘dbsat collect’ on the target
• Run ‘dbsat report’ on the target or elsewhere
• Run ‘dbsat discover’ on the target to generate sensitive data report
• Restrict access to the generated reports as they have sensitive data
Where To Start & What to look for

- Where does sensitive data reside?
- Who are the users and their entitlements?
- What controls do I have in place?
- Is my Database securely configured?

Do we have a Database Security Team? Knowledge? Analysis time?
Summary

• Quickly assess the current security status of database before hackers do
• Identify sensitive data to determine risk and appropriate security controls
  – In English and major European languages
• Reduce risk exposure using proven best practices as CIS and STIG
• Accelerate compliance with EU GDPR and other regulations
• Support Oracle Database 10g, 11g, 12c, 18c, 19c and Autonomous DBs
• Provided at no additional cost
• Quick to deploy and use
Download it Today

- OTN page
- Use #DBSAT on Social Networks

- Database Security and GDPR Whitepaper
  https://go.oracle.com/LP=54366

- Know more about GDPR
  www.oracle.com/goto/gdpr

- Know more about Database Security
  http://oracle.com/database/security
Q & A
Connect With Us

/oracleDatabase #DBSAT
/oracleSecurity
/blogs.oracle.com/SecurityInsideOut
/oracleDatabaseInsider
/oracle/database
/oracleLearning

oracle.com/database/security
oracle.com/technetwork/database/security
Integrated Cloud
Applications & Platform Services