ORACLE

Oracle Database Security Assessment Tool

Learn how secure your databases are with DBSAT

May, 2020 | Version 1.01

Public

With data breaches growing every day along with the evolving set of data protection and privacy regulations, protecting business sensitive and regulated data is mission critical. However, knowing whether the database is securely configured, who can access it, and where sensitive personal data resides is a challenge for most organizations. As part of Oracle's defense-in-depth capabilities, the Oracle Database Security Assessment Tool (DBSAT) helps identify areas where your database configuration, operation, or implementation introduces risks and recommends changes and controls to mitigate those risks.

EVOLVING REGULATORY COMPLIANCE

Security configuration scanning has become an important part of many regulations such as the EU General Data Protection Regulation (EU GDPR), Payment Card Industry Data Security Standard (PCI-DSS), and numerous breach notification laws. Various organizations such as the Center for Internet Security (CIS) and U.S. Department of Defense also have recommendations for security configuration best practices. The importance of security controls cannot be understated as new regulations are being released and existing regulations are evolving aiming to protect the most valuable asset of many organizations – the data.

One of the biggest challenges organizations face before they put new controls in place is understanding their database security posture. They need to quickly identify how securely their databases are configured, where sensitive data is, how much sensitive data they have, which users have access to that data, what are their entitlements, and what security controls are implemented.

Whether your database is running on-premises or in the Cloud, the Oracle Database Security Assessment Tool (DBSAT) identifies potential sensitive data and areas where your database configuration, operation, or implementation introduces risk. DBSAT collects and analyzes different types of data from the database to identify the security risks. DBSAT further recommends changes and controls to mitigate those risks.

THINK LIKE A HACKER

Attackers typically spend considerable time understanding their target. They may use several tools that automate the discovery of databases, open ports, known vulnerabilities, and privileged user accounts. They may then launch various attacks including password theft, brute force password cracking, privilege escalations, and SQL injection attacks. Once they finish probing, they identify the weakest links and then determine their next steps. In essence, the attackers first evaluate the current security status to find the easiest way to get to the sensitive data without being caught.

For example, if the data is encrypted, they probably need to get into the database as an authorized user. Are there users using default passwords? Can I escalate privileges? Is auditing on? Who has DBA-like privileges? What are the known vulnerabilities of this database version? Have those been patched? Which packaged applications are running? Are they running with powerful system privileges? What type of sensitive data do they process? All these and many more questions are inside

Key Business Benefits

Quickly assess the current security status and identify sensitive data within the Oracle database

Reduce risk exposure using proven Oracle Database Security best practices, STIG, and CIS benchmark recommendations

Leverage security findings to accelerate compliance with EU GDPR and other regulations

Installs and provides valuable reports in minutes

Provided at no additional cost to Oracle customers

Key Features

Identify configuration settings that may increase your risk exposure

Identify sensitive user accounts, their entitlements, and security policies

Discover sensitive data in English based data dictionaries and in major European languages

Recommend and prioritize relevant security controls

the hacker's mind, and these answers help them come up with a plan to break into the database and steal your data.

As the owners, controllers, or processors of data, organizations need to think similarly, but to improve the security posture before the hackers target their databases.

Despite knowledge of what is needed to evaluate the current security posture and avoid being caught off guard, many organizations struggle to assess the security of their databases due to lack of database security expertise, shortage of time, lack of proper prioritization, or misunderstanding of the risks. Knowledge of how to secure a database might also be organizationally scattered between the DBAs and the IT Security team that is mostly focused on protecting the network or the endpoints.

Oracle DBSAT accelerates the assessment process by collecting relevant types of configuration information from the database and evaluating the current security state to provide recommendations on how to mitigate the identified risks. DBSAT quickly provides a view on how securely the database is configured, who are the users and what are their entitlements, what security policies are in place, what security controls are implemented, and where sensitive data resides. The figure below summarizes the security status of a sample database and categorizes its findings by risk levels.

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	**1**
User Accounts	5	0	0	4	2	1	**12**
Privileges and Roles	5	16	0	0	0	0	**21**
Authorization Control	0	1	1	0	0	0	**2**
Fine-Grained Access Control	0	1	4	0	0	0	**5**
Auditing	0	4	2	0	6	0	**12**
Encryption	0	1	1	0	0	0	**2**
Database Configuration	5	3	0	3	2	1	**14**
Network Configuration	1	1	0	0	3	0	**5**
Operating System	1	0	0	2	1	1	**5**
Total	**17**	**27**	**8**	**9**	**14**	**4**	**79**

Figure 1. Current Security State Summary of an Oracle Database.

DBSAT reports the results of its analysis in the form of a series of Findings. Each Finding provides high-level status, risk levels, summary, details, and references as appropriate. It points out if the finding relates to an Oracle Database STIG Rule, Center for Internet Security (CIS) benchmark recommendation, or to GDPR Articles/Recitals. The two findings below show which users have the powerful DBA role, how that role was obtained (directly granted, granted via another role), and users with default passwords.

Related Products

Oracle Database Defense-In-Depth Security Products:

- Oracle Advanced Security
- Oracle Key Vault
- Oracle Database Vault
- Oracle Data Masking and Subsetting
- Oracle Label Security
- Oracle Audit Vault and Database Firewall

DBA Role

PRIV.DBA	CIS
Status	Evaluate
Summary	6 grants of DBA role.
Details	Grants of DBA role: DBSAT <- APPROLE1 <- APPROLE2 <- APPROLE3: DBA DBSAT <- APPROLE2 <- APPROLE3: DBA DBSAT <- APPROLE3: DBA MYDBA: DBA SCOTT: DBA SCOTT <- APPROLE1 <- APPROLE2 <- APPROLE3: DBA
Remarks	The DBA is a powerful role and can be used to bypass many security controls. It should be granted to a small number of trusted administrators. As a best practice, it is recommended to create custom DBA-like roles with minimum set of privileges that users require to execute their tasks (least privilege principle) and do not grant the DBA role. Privilege Analysis can assist in the task of identifying used/unused privileges and roles. Having different roles with minimum required privileges based on types of operations DBAs execute also helps to achieve Separation of Duties. Furthermore, each trusted user should have an individual account for accountability reasons. Avoid granting the DBA or custom DBA-like powerful roles WITH ADMIN option unless absolutely necessary. Please note that Oracle may add or remove roles and privileges from the DBA role.
References	CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 4.4.4

Figure 2. Current Security State Summary of an Oracle Database.

In the example above, DBSAT reports that the user SCOTT got the DBA role indirectly via other roles grant (APPROLE3 to APPROLE2 to APPROLE1) while the MYDBA user was directly granted the DBA role.

Users with Default Passwords

USER.DEFPWD	CIS STIG
Status	High Risk
Summary	Found 2 unlocked user accounts with default password.
Details	Users with default password: HR, SCOTT
Remarks	Default passwords for predefined Oracle accounts are well known and provide a trivial means of entry for attackers. Well-known passwords for locked accounts should be changed as well.
References	CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.2 Oracle Database 12c STIG v1 r10: Rule SV-76031r1, SV-76339r1

Figure 3. Users with Default Passwords.

Findings are provided in multiple formats including HTML, Microsoft Excel, JSON, and text file so that organizations can incorporate this data as part of their configuration and risk management tools.

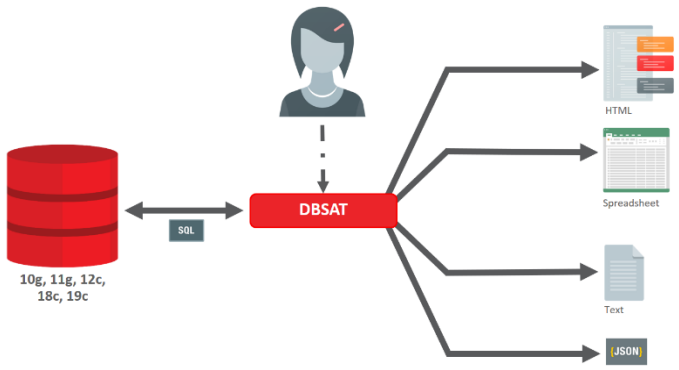

Figure 4. DBSAT Reports.

DISCOVER SENSITIVE DATA

Regulations such as the EU GDPR require organizations to protect Personally Identifiable Information (PII) data; however, they first need to know what personal data they have and where.

DBSAT scans the database metadata for sensitive data using customizable regular expression patterns, and reports on the amount and type of sensitive data found. Besides providing the ability to search for sensitive data on English based data dictionaries (column names and comments) it also includes support for additional major European languages such as Dutch, French, Italian, German, Portuguese, and Spanish. This provides organizations with a deeper insight into how much sensitive data they have and where it resides, enabling them to then protect their databases through appropriate access controls, auditing, masking, and encryption. The figure below shows a summary report from a scan of the database metadata.

Sensitive Category	# Sensitive Tables	# Sensitive Columns	# Sensitive Rows
BIOGRAPHIC INFO – ADDRESS	7	18	244
FINANCIAL INFO – CARD DATA	2	2	256
HEALTH INFO – PROVIDER DATA	1	1	149
IDENTIFICATION INFO – PERSONAL IDS	3	3	356
IDENTIFICATION INFO – PUBLIC IDS	3	12	321
IT INFO – USER DATA	1	1	149
JOB INFO – COMPENSATION DATA	7	10	527
JOB INFO – EMPLOYEE DATA	12	25	569
JOB INFO – ORG DATA	7	8	412
TOTAL	21*	80	989**

Figure 5. Sensitive Data Landscape Summary.

SUMMARY

Knowing where sensitive data is, and how the database is configured is the foundation for implementing a defense-in-depth strategy. No system is 100% secure but overlooking the basics will only make break-in easier for attackers.

Oracle Database Security Assessment Tool (DBSAT) quickly identifies sensitive data and areas where your database configuration, operation, or implementation introduces risk.

DBSAT is provided at no additional cost to Oracle customers with an active support contract. For more information, or to download DBSAT, visit www.oracle.com/database/technologies/security/dbsat.html.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle