Oracle Database Security Assessment Tool

Learn how secure your databases are with DBSAT

November, 2023, Version 1.0.1

Public

In the age of data breaches and ever-evolving data protection and privacy regulations, it is more important than ever for organizations to be confident that their databases are secure. However, it can be difficult to know whether the databases are configured correctly, who has access to it, and where sensitive data is stored. 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. DBSAT will recommend changes and controls to help you mitigate those risks.

Evolving regulatory compliance

Security configuration scanning has become essential to many regulations, such as the EU General Data Protection Regulation (EU GDPR), Payment Card Industry Data Security Standard (PCI-DSS), state and local laws, and industry standards. In addition, various organizations such as the Center for Internet Security (CIS) and the U.S. Department of Defense, 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 most prominent challenges organizations face before implementing new controls is understanding of 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 their entitlements are, and what security controls are implemented.

Whether your database runs on-premises or in the cloud, the Oracle Database Security Assessment Tool (DBSAT) identifies potentially 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 security risks. DBSAT further recommends target-specific 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, versions, 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 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.

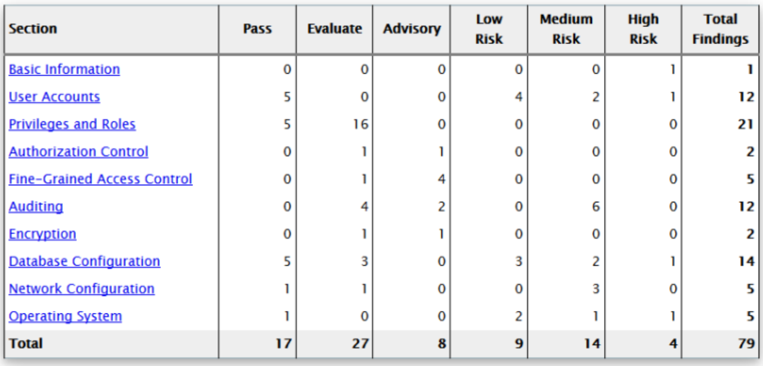
For example, if the data is encrypted, they probably need to get into the database as an authorized user. Are there users using default passwords? Once authenticated, can they escalate privileges? Is auditing on? Who has administrative privileges? What are the known vulnerabilities of this database version? Have those been patched? Which packaged applications are running? Are they running with powerful system privileges? What type of sensitive data do they process? These are only a few of the questions inside the hacker's mind, and the answers will help them devise a plan to break into the database and steal the data.

As the owners, controllers, or data processors, 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 a lack of database security expertise, shortage of time, lack of proper prioritization, or misunderstanding of the risks. Knowledge of securing a database might also be organizationally scattered between the database administrators (DBAs) and the IT Security team, which is mostly focused on protecting the network or the endpoints.

Oracle DBSAT accelerates the assessment process by collecting relevant configuration information from the database and evaluating the current security state to provide recommendations on mitigating the identified risks. DBSAT quickly provides insight into how securely the database is configured, who the users are and 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.

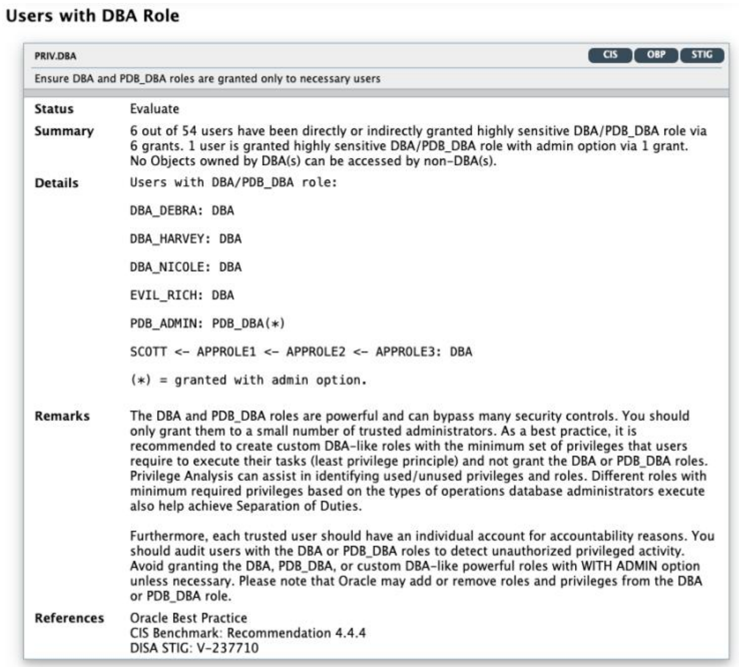
Figure 1. Current Security State Summary of an Oracle Database.



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**

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 Best Practice, Oracle Database STIG Rule, Center for Internet Security (CIS) benchmark recommendation, or GDPR Articles/Recitals. The two findings below show which users have the powerful DBA role and how they have obtained that role (directly granted, granted via another role), plus which users have default passwords. Checks, details, and remarks are specific to the database target and whether it is deployed on-premises or in-cloud (Autonomous Databases Serverless and Dedicated, or Base Database).

Figure 2. Users granted the DBA role and its grant path.



Users with DBA Role

PRIV.DBA

Ensure DBA and PDB_DBA roles are granted only to necessary users

Status Evaluate

Summary 6 out of 54 users have been directly or indirectly granted highly sensitive DBA/PDB_DBA role via 6 grants. 1 user is granted highly sensitive DBA/PDB_DBA role with admin option via 1 grant. No Objects owned by DBA(s) can be accessed by non-DBA(s).

Details

```
Users with DBA/PDB_DBA role:

DBA_DEBRA: DBA

DBA_HARVEY: DBA

DBA_NICOLE: DBA

EVIL_RICH: DBA

PDB_ADMIN: PDB_DBA(*)

SCOTT <- APPROLE1 <- APPROLE2 <- APPROLE3: DBA

(*) = granted with admin option.
```

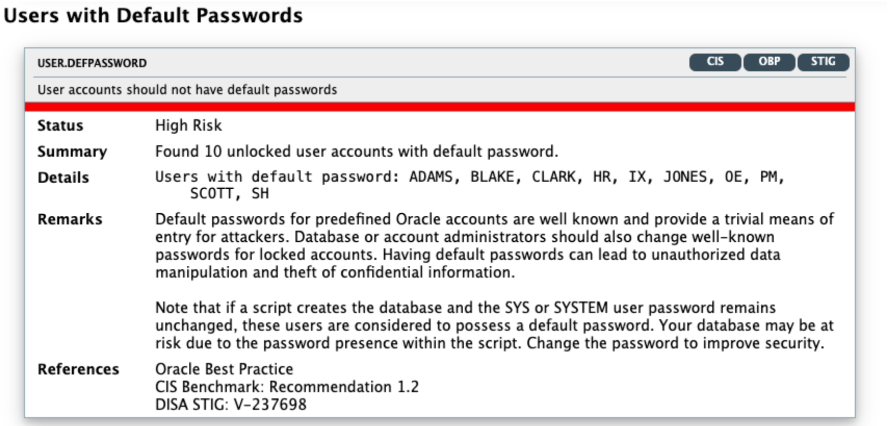
Remarks The DBA and PDB_DBA roles are powerful and can bypass many security controls. You should only grant them to a small number of trusted administrators. As a best practice, it is recommended to create custom DBA-like roles with the minimum set of privileges that users require to execute their tasks (least privilege principle) and not grant the DBA or PDB_DBA roles. Privilege Analysis can assist in identifying used/unused privileges and roles. Different roles with minimum required privileges based on the types of operations database administrators execute also help achieve Separation of Duties.

Furthermore, each trusted user should have an individual account for accountability reasons. You should audit users with the DBA or PDB_DBA roles to detect unauthorized privileged activity. Avoid granting the DBA, PDB_DBA, or custom DBA-like powerful roles with WITH ADMIN option unless necessary. Please note that Oracle may add or remove roles and privileges from the DBA or PDB_DBA role.

References Oracle Best Practice
CIS Benchmark: Recommendation 4.4.4
DISA STIG: V-237710

In an Oracle Database, the DBA role is powerful and can be used to bypass many security controls. In the example above, DBSAT reports that the user SCOTT was granted the DBA role indirectly via other roles grant (APPROLE3 to APPROLE2 to APPROLE1) while the DBA_DEBRA user was directly granted the DBA role.

Figure 3. Users with default passwords.



Users with Default Passwords

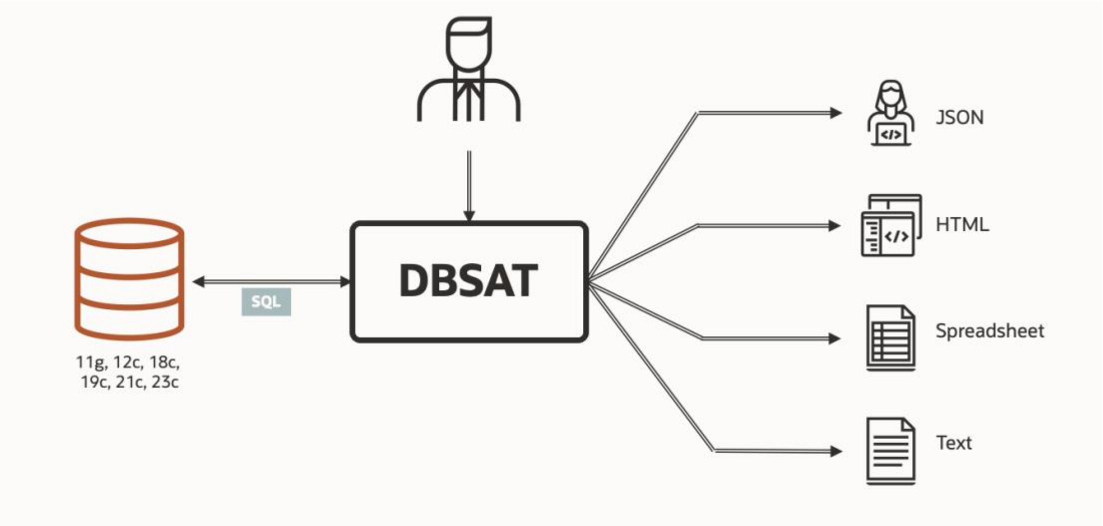
USER.DEFPASSWORD CIS OBP STIG

User accounts should not have default passwords

Status	High Risk
Summary	Found 10 unlocked user accounts with default password.
Details	Users with default password: ADAMS, BLAKE, CLARK, HR, IX, JONES, OE, PM, SCOTT, SH
Remarks	Default passwords for predefined Oracle accounts are well known and provide a trivial means of entry for attackers. Database or account administrators should also change well-known passwords for locked accounts. Having default passwords can lead to unauthorized data manipulation and theft of confidential information. Note that if a script creates the database and the SYS or SYSTEM user password remains unchanged, these users are considered to possess a default password. Your database may be at risk due to the password presence within the script. Change the password to improve security.
References	Oracle Best Practice CIS Benchmark: Recommendation 1.2 DISA STIG: V-237698

DBSAT Findings are provided in multiple formats, including HTML, Microsoft Excel, JSON, and text files, allowing organizations to integrate this data into their configuration and risk management tools.

Figure 4. DBSAT supported target versions and report output formats.

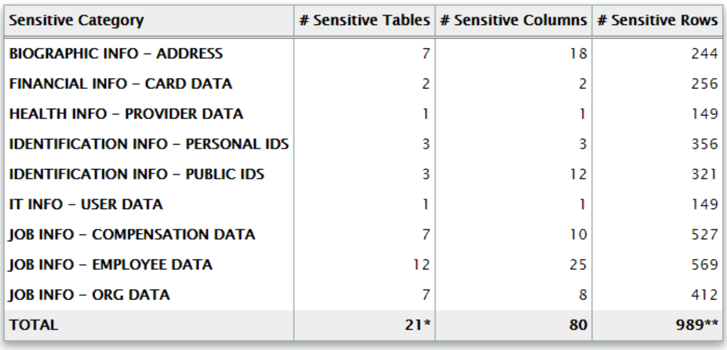


Discover sensitive data

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. In addition to being able 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, Greek, Portuguese, and Spanish. This gives organizations a deeper insight into how much sensitive data they have and where it resides, enabling them to 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.

Figure 5. Sensitive Data Landscape Summary.



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****

Assessment using Oracle Data Safe

You can also use Oracle Data Safe cloud service to assess the security of their databases running on the Cloud and on-premises. Oracle Data Safe is a database security cloud service that provides a comprehensive suite of security capabilities, including user and security assessments. Oracle Data Safe's tightly integrated assessment capabilities allow you to simultaneously run assessments on multiple databases, schedule assessments, establish a security baseline, and get a comparison report highlighting the drift between that baseline and the current database security assessment. Oracle Data Safe provides APIs that can be used to automate and integrate database security assessments into your CI/CD pipelines.

To learn more about Oracle Data Safe, please visit https://www.oracle.com/security/database-security/data-safe/.

Assessment using Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall (AVDF) 20.9 introduced Database Security Posture Management. AVDF now provides a centralized security assessment solution for enterprises by integrating the popular Database Security Assessment Tool for Oracle Databases. The full-featured assessment with compliance mappings and recommendations will help organizations understand their security posture for all their Oracle Databases in one central place.

To learn more about Oracle Audit Vault and Database Firewall, please visit https://www.oracle.com/security/database-security/audit-vault-database-firewall/.

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 make a 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.

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

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 major European languages.
- Recommends and prioritizes relevant security controls and findings.

Related products

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

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