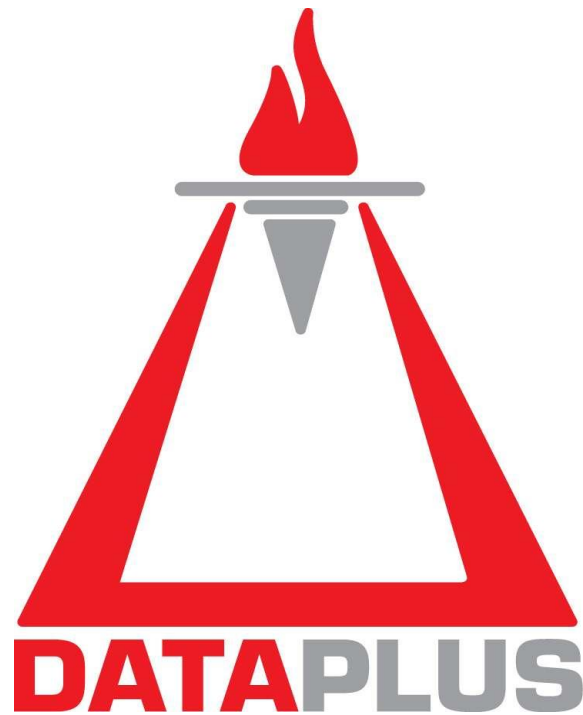


April, 2018

Omega DB Scanner TM

Standalone Free Edition
For Oracle Database, with Splunk support



OMEGA DB Scanner

Standalone Free Edition

For Oracle Database

User's Guide

2.1.0

www.dataplus-al.com

TABLE OF CONTENTS

1	Omega DB Scanner Standalone - Overview	3
1.1	Introducing Omega DB Scanner Standalone	3
1.2	Solution Architecture	3
1.3	How it works	4
1.4	Compatibility, Requirements and Limitations	6
1.5	What's new in 2.1	7
1.6	Software deploy and upgrade	8
1.6.1	Software Deploy	8
1.6.2	Software Upgrade	9
2	Omega DB Scanner Standalone Edition	10
2.1	Application's main form	10
2.2	Scan Target Database	11
2.3	Scan Data	12
2.3.1	Scan Name/Filename Format	13
2.3.2	Scan Dashboard	14
2.3.3	Scan Records	15
2.4	Vulnerabilities (Security Controls)	16
2.5	Vulnerability Scan	18
2.5.1	Parameters and List Values	18
2.5.2	"Classes" and Advanced Features	20
2.5.3	Vulnerability Item Scan	22
2.6	All Configurations (authorizations)	23
2.6.1	Parameter Multiple Operations	24
2.7	Scans Comparison	25
2.8	System Settings	28
3	Integration to SIEM	30
3.1	Splunk Interface	30
3.1.1	Solution Architecture	30
3.1.2	Splunk Upload	31
4	Appendixes	32
4.1	Appendix A1 - Oracle database scan account	32
4.2	Appendix A2 - Oracle connectivity and Character Set support	33
4.2.1	Oracle Client Connectivity	33
4.2.2	Character Set Support - NLS_LANG	33
4.3	Appendix A3 - Configurations imports (upgrade)	34
4.4	Appendix A4 - Use Case	35
4.5	Appendix B - Technical Support and Copyrights	39

1 Omega DB Scanner Standalone - Overview

1.1 Introducing Omega DB Scanner Standalone

Omega DB Scanner is a security auditing tool and vulnerability assessment scanner. It has been designed to give the user the **automated knowledge** in performing the complex task of assessment, evaluation and improvement of the security posture of his mission critical Oracle database.

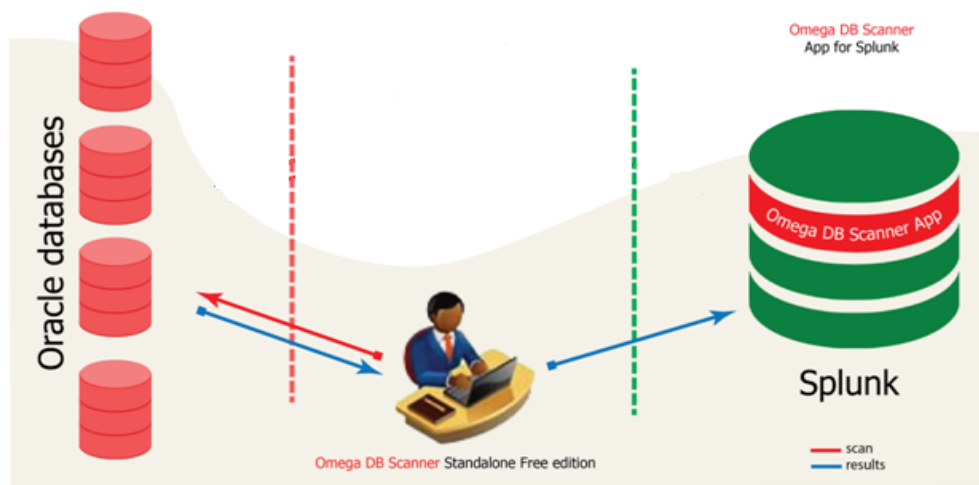
Omega DB Scanner is an out-of-box, software-only solution. As the name implies, this Standalone Free Edition is a simple client-side solution that is deployed on the user's PC within minutes. Omega DB Scanner is Agent-less and accesses the target database in read-only mode.



Omega DB Scanner is not just a scanner, but also an inventory of your Oracle database's security posture. It is Agent-less and accesses the target database in read-only mode.

1.2 Solution Architecture

Scan the Oracle database[s] from Omega DB Scanner Standalone. Send scan results to Splunk on the fly.



1.3 How it works

The Omega DB Scanner deploys a set of advanced, highly customizable and in-depth controls on important Oracle database security areas. Run a full scan on the target database, or individually scan any vulnerability; a control result Correct/Finding, a summary and detailed output is given on each scanned item.

Software implementation and use is summarized in the following phases below:

Phase I - Initialization

First Assessment of your DB security posture:

Download and Deploy Download the software from our site and set it up.

Run a full scan Connect to the target database and run your first full scan. View and save the scan data

Phase II - Establish and tune

Establishment and tuning of the DB security posture; analyze, authorize and remediate:

Analyze Findings Review each scan data result item, prioritize on Findings by severity.

Authorize Authorize exceptions (acceptances) to the security control. Authorization is the process of allowing acceptances to the vulnerability control's finding either at a whole or at entity level, depending on each vulnerability control. It is performed by using vulnerability control's List Values for "List" Format Parameters (refer to related topic).

Remediate Apply the remediation advises as given on each vulnerability control. Remediation is the process of fixing the vulnerability control's findings in the database environment, ex. revoking of a privilege, setting of an audit or changing of security parameter. Obviously remediation steps must first be tested successfully on test environments!

Important Note:

Both the Remediation and the Authorization processes are important; the Remediation because it strengthens in reality the security posture of your database in absolute value. The Authorization because it allows you to tailor the security posture according to your specific DB environment and accept needed security configurations.

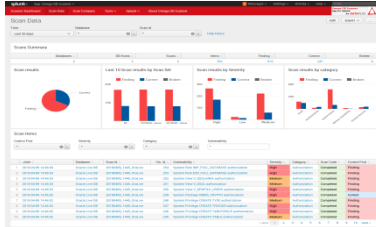
Phase III - Scan and Improve

Periodic maintenance and improvement of DB security posture:

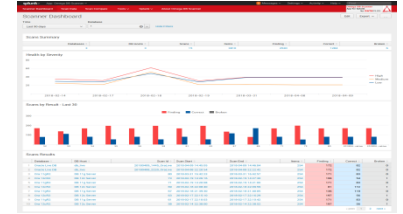
- Frequently scan your database.
- Detect and analyze changes in the security posture of your DB.
- Remediate and authorize your DB's security posture.

SIEM Integration - Interface to Splunk

Send your scan records straight to Splunk SIEM from Omega DB Scanner; thus enabling storage of your scans results in a central location, visualization and quick access of scan data history.



Monitor and assess the security posture of your Oracle database via the graphical interface of our next solution **Omega DB Scanner App for Splunk***, running on top of the Splunk system.



* Omega DB Scanner App for Splunk is a Splunk application made by DATAPLUS and is free to all Omega DB Scanner users!

1.4 Compatibility, Requirements and Limitations

Oracle Database support

Omega DB Scanner Standalone supports the following Oracle Database Versions and Releases:

- Oracle Database 10g Release 2
- Oracle Database 11g Release 1
- Oracle Database 11g Release 2
- Oracle Database 12c Release 2 (*)

* 12c Traditional Auditing mode only is supported for most Audit category vulnerabilities

Database support is independent of the operating system!

All commercial editions of the Oracle database, Standard Edition (One) to Enterprise, are supported!

Application requirements

The OS and software requirements of Omega DB Scanner Standalone application are:

- All x86/x64 Windows NT-based systems.
- NLS_LANG operating system environment variable (*)

* refer to "Appendix A2 - Oracle connectivity and Character Set support"

Limitations

Omega DB Scanner Standalone Edition has currently the following limitations:

1. Connectivity from Omega DB Scanner application is currently supported only on 32 Bit Oracle Clients; however this is the default and pre-deployed option - you don't have to change anything!
2. The Standalone Free Edition supports a single database only for authorization and configuration. This is a limitation of this edition. However there is no limit on the number of databases you can scan with no List Authorization.

Visit our website for news on current developments:

www.dataplus-al.com

1.5 What's new in 2.1

New Features/Enhancements in 2.1:

1. Real item scan date delivered to Splunk SIEM **highlighted**

When a database is scanned for vulnerability, the Scan DateTime Start and End in UTC string format are extracted from the scanned database, made part of the scan dataset and also saved to disk. These new fields are not visible in the Scan data form, but they are part of the record-set that is send to Splunk.

Furthermore, in the new Omega DB Scanner App for Splunk 1.5, the field `_TIME` is no more set with the Splunk record ingest time - but with the real time of the vulnerability scan of the Oracle database assessed.

Warning!

It will not be possible in form "Scan Data" to load from disk scans saved with the previous versions (2.0.1 and below) of this program that miss the two fields added. You will receive error "Scan load error: SCAN_DATA: Field 'UTC_Start' not found"!

But it is possible to open "old" scans for comparison in the "Scans Comparison" form!

2. Changes in Scan Code description

Before 2.1.0:

Completed	Scan completed successfully
System Error	Scan failed with program error
Oracle Error	Scan failed with Oracle error

2.1.0 And after:

Completed	Scan completed successfully
Error	Scan failed with program error
System Error	Scan failed with Oracle error

Bug fixes in 2.1:

The following bugs (present in 1.8.1 and 2.0.2) are fixed in 2.1:

Bug 1:

In the form "Scans Comparison", grid Baseline Scan, field Scan Code the Db Lookup Image Combo box has the wrong code for System Error, thus causing empty field value in the grid.

Bug 2:

In the form "Parameter Multiple Operations" fixes are applied in the Value Format Parameters and List Format Parameters grids for (multiple) check/uncheck operations to avoid un-saved records.

1.6 Software deploy and upgrade

1.6.1 Software Deploy

Omega DB Scanner software Install package is downloaded as a compressed file, named as:

OmegaDS_Std_[VS]_[MN]_[PT]_Install.zip

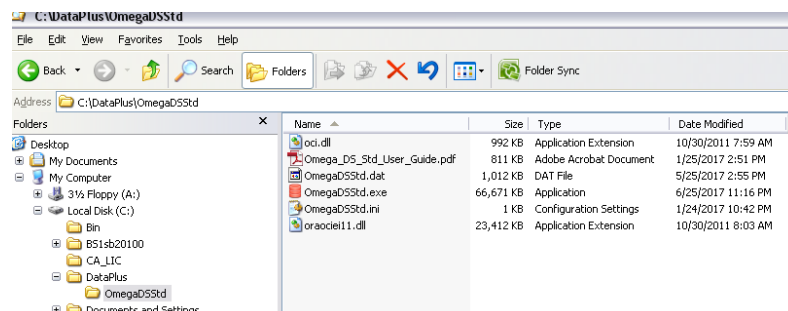
The acronyms are two digit numbers, 0 left padded and stand for:

VS - Version
MN - Maintenance Release
PT - Patch Number

There is no installation routine in the proper sense, no installer and no registry entries created, just the files you are extracting from the compressed package. Create a directory in your Windows Explorer, for example:

C:\DataPlus\OmegaDSStd

Put all the software package's files into this directory.



The application files deployed in this version are:

OmegaDSStd.exe	The application's executable binary file.
OmegaDSStd.dat	Deployed vulnerabilities binary file. It also stores end-user configurations and authorizations, bound to the vulnerability structure. Take special care to backup this file!
OmegaDSStd.ini	System parameters initialization file
Oracle DLLs	Oracle 11g R2 Instant Client binaries (oci.dll, oraociei11.dll)

Deployed is also this document - "Omega DB Scanner Standalone User Guide".

Create a shortcut to the **OmegaDSStd.exe** file and Paste it on your desktop.
Double-click on the shortcut to start the Omega DB Scanner Standalone application!

Before you start, carefully read topics "System Settings" and "Appendix A2 - Oracle connectivity and Character Set support".

Important Note:

Files deployed are opened and managed only by the executable! Compressing, modifying, or accessing them in any mode other than the indicated above may permanently damage your data (vulnerabilities deployed and your configurations/setups) and also lead to abnormal and erroneous software behavior and results!

1.6.2 Software Upgrade

1. Backup your current deployment.

Create a directory to store the current version before the upgrade, it is advised the directory names the old version, something like:

Old version C:\DataPlus\OmegaDSStd\Old\[VS]_[MN]_[PT]

Copy here all the files that are currently on C:\DataPlus\OmegaDSStd

2. Upgrade application files

Whenever you receive a new deployment of the Omega DB Scanner Standalone the first new "thing" in use will be the binary/executable file OmegaDSStd.exe, although this may not always be the case. What follows next is the compatibility of this executable with the other (existing) application files, as shown below.

OmegaDSStd.dat Application file to .dat file Compatibility Matrix:

OmegaDSStd.exe	OmegaDSStd.dat	Compatible
2.1.0	1.7.0	YES
2.1.0	1.8.1	YES
2.1.0	2.0.2	YES
2.1.0	2.1.0	YES

YES use the current .dat file, or optionally use the new one and perform Step 3 to import your settings
 NO change is needed, you must use the new .dat file and Step 3 is necessary!

Important Note:

Every OmegaDSStd.dat file contains a version number, visible in application and equal to the version of the OmegaDSStd.exe with which is together released. This does not mean that there is per force a change into the rest of content deployed with the OmegaDSStd.dat file.

As per an example from the matrix above - there is no need to update the OmegaDSStd.dat 1.7.0 or 1.8.1 file for version 2.1.0 - unless you want to visually see in the software full match of .exe and .dat version numbers.

OmegaDSStd.ini Application file to .ini file Compatibility Matrix:

OmegaDSStd.exe	OmegaDSStd.dat	Compatible
2.1.0	1.7.0	NO
2.1.0	1.8.1	NO
2.1.0	2.0.2	YES
2.1.0	2.1.0	YES

YES use the current .ini file
 NO change is needed, you must use the new .ini file and manually copy your settings from the old one!

3. Import Configurations (Authorizations):

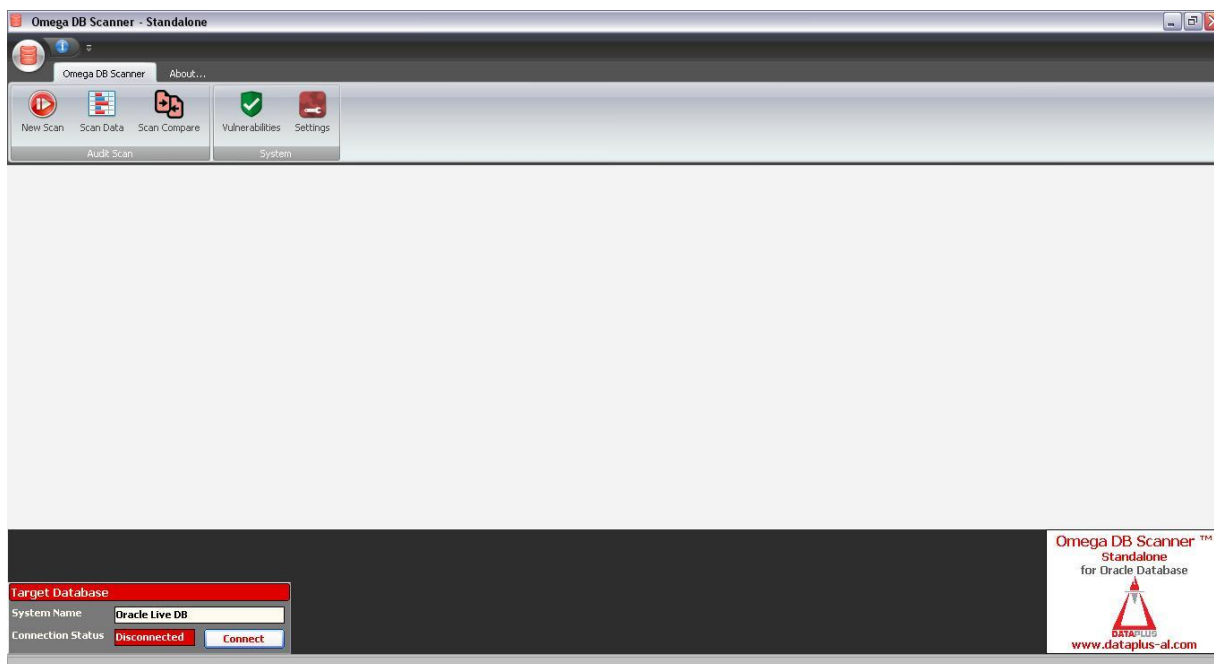
When you must use the new deployed OmegaDSStd.dat file, you must import into the new vulnerability structure (new OmegaDSStd.dat) your end-user configurations and authorizations stored into the old OmegaDSStd.dat file (backed-up before)!

Refer to the "Appendix A3 - Configurations imports (upgrade)".

2 Omega DB Scanner Standalone Edition

2.1 Application's main form

The main application's form is displayed below:



In the form's top menu, Omega DB Scanner tab, groups:

Audit Scan:

New Scan	Press button to open form Scan Target Database and run a new scan
Scan Data	Press button to open form Scan Data and view scan data dashboard and raw records
Scan Compare	Press button to open form Scans Comparison to compare two scans at each item level

System:

Vulnerabilities	Press button to open form Vulnerabilities and view all vulnerabilities deployed
Settings	Press button to open Opens form System Settings

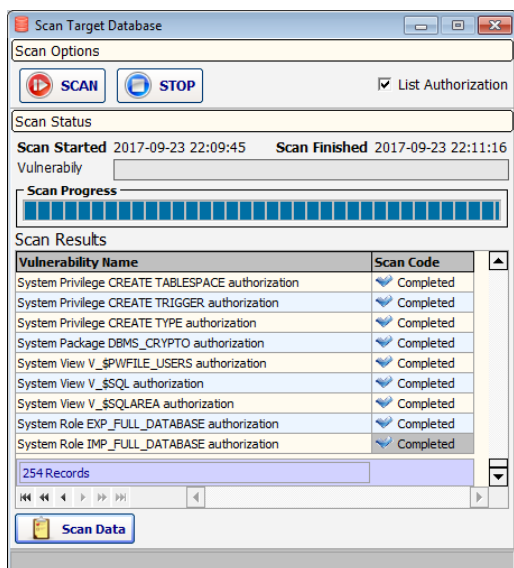
At the form's bottom-left, connection to target the Database is initiated.

Target Database:

System Name	Common system name of the target database, initialization parameter
Connection Status	Connection status of the target database: Connected/Disconnected
Connect [Disconnect]	Press button (caption changes by target database connection status):
Connect	opens the target database System Authentication logon prompt form
Disconnect	disconnects from the target database

2.2 Scan Target Database

In this form a full scan is performed on the target database. All vulnerabilities with status Active are scanned.



Connecting to Target Database

To perform a full or single item scan you must first be connected to the target database. In the application's main form, group Target Database left-below, click the button Connect.

The System Authentication logon prompt form will show:



Enter the password and press button Logon. Database connection parameters are managed in the System Settings form.

Scan Options group:

- SCAN** Press button to start a full new scan against the target database. All Active vulnerability controls will be scanned. You will receive a notification when the scan has completed.
- STOP** Press button to stop a running scan and wait for the scan stop confirm.
- List Authorization** Runs the scan applying authorizations as defined in parameter list values (default checked); when unchecked the scan will be performed without considering them.

Important Note:

List un-Authorization will allow scanning of multiple databases other than the single one in which configurations and authorizations are configured. The single DB limit of this edition stands for authorization and not scanning!

Close the Scan Data form if opened and not to interact with the application while the scan is running! Stopping the scan is the only exception to this!

Scan Status Group:

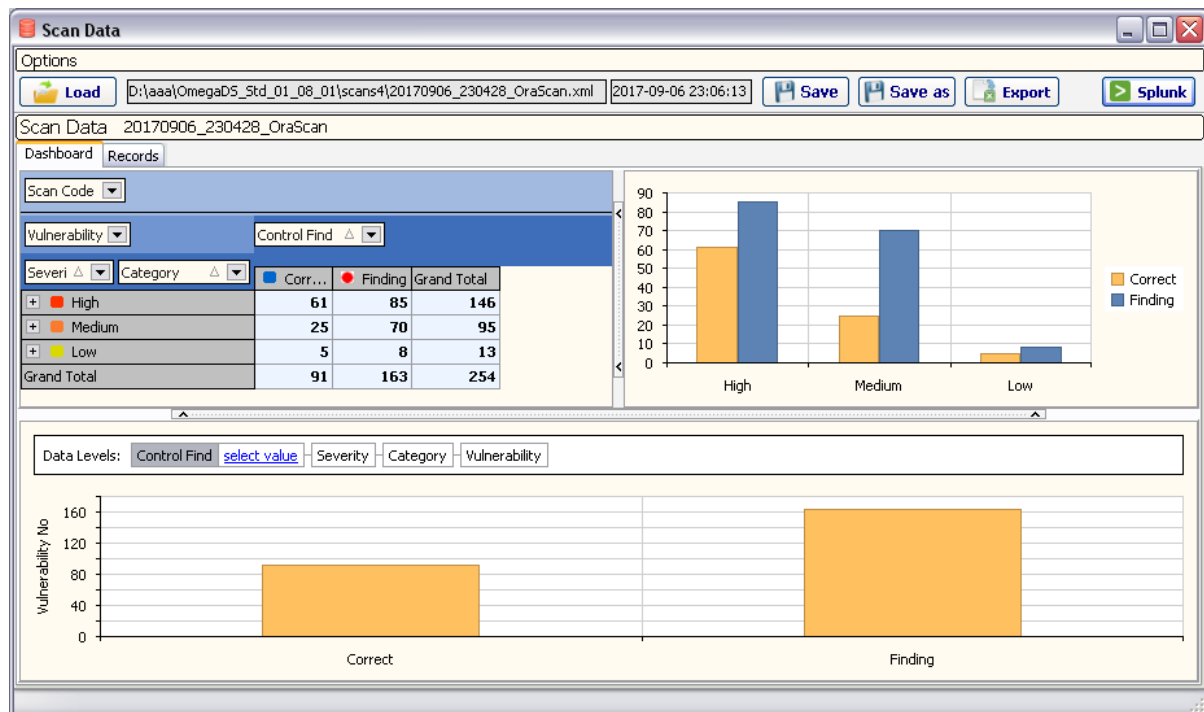
- Scan Started** Date and time the scan started. Will serve as a basis for Scan Name
- Scan Finished** Date and time the scan finished
- Vulnerability** Current vulnerability control being scanned
- Scan Progress** Progress bar showing scan run, advances on every item.
- Scan Results** Scan results grid in summary, with two columns:
- | Vulnerability Name | Scan Code |
|-----------------------------------|--------------------|
| Name of the vulnerability scanned | Status of the scan |
- Scan Data** Press this button immediately after the scan is finished to show in full and save the scan data!

2.3 Scan Data

This form shows the scan data, either generated from a new scan performed in the "Scan Target Database" form, or loaded from a file of a previously scan saved in disk. The scan is presented in two tabs:

- **Dashboard** displays pivot and chart drill-down analyses of scan data
- **Records** displays the full scan dataset in a grid

The Scan Data dataset is basically comprised of vulnerability record fields and scan specific fields.

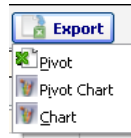


Options group:

This group is common to both Dashboard and Records tabs:

- Load *** Press this button to invoke a File Open dialog and load a scan from disk. This will update the File Path and File Dt. Mod. Edits (see below) and also the "Scan Name" label.
- File Path** Read-only edit box (next to Load button) shows the full path and name of the loaded scan file or it is empty for a new scan.
- File Dt. Mod.** Read-only edit box (next to "File Path") shows the date last modified of the loaded scan file, or it is empty for a new scan.
- Save *** Press button to save scan to disk. This will save a currently loaded scan, or invoke a File Save dialog to save a new scan. In the later the "File Path" will be updated, while the "File Dt. Mod." in both.
- Save As *** Press button to invoke a File Save dialog and save the scan to disk with a different name from a currently loaded one, or from a new scan. "File Path" and "File Dt. Mod." will be updated.
- Export** Press button to export form's multiple scan views in common file formats to disk.

When the Dashboard tab is active:
a popup menu will prompt user to:



- Save the pivot table as Excel
- Save the pivot-chart related as Bmp
- Save the drill-down chart as Bmp

When the Records tab is active:
this button will prompt directly save to Excel of all visible the records into the scan records grid.

Splunk Press button to open form "Splunk Upload" and send scan records to Splunk. Refer to the respective chapter below on Splunk Interface.

* refer to the "Scan Name/Filename Format" topic below when saving and loading scan sets.

2.3.1 Scan Name/Filename Format

The scan's filename without the extension represents the name of the scan! It is displayed in the label right to the "Scan Data" label.

The first time a new scan is run, its name is automatically generated according to the initialization parameters "Scan Save Time Format" and "Scan Save DB Code"!

For example, for a "Scan Save Time Format" set to "Date ss", a "Scan Save DB Code" set to "OraLive", running a new scan on 01 September 2017, time 19:33:00, will create a scan with a name as:

20170901_193300_OraLive

This is the prompted filename you will see in the save dialog when you first save the scan to disk after being run! When you load a scan from disk, the filename will set the name of the scan!

The scan name label will change in Red color and Bold when a scan is unsaved to disk after just being run, or when any of its vulnerabilities is saved after a re-run of it!

The naming schema above will compile the default scan name each time you first run a new one. It ensures:

- unique identification of the scan
- time and DB based codification
- visual ordering of the scan name

The choice of using a file-save dialog when saving the scan, instead of a simple folder-select one, is to let the user see other previously saved scan files present in the directory.

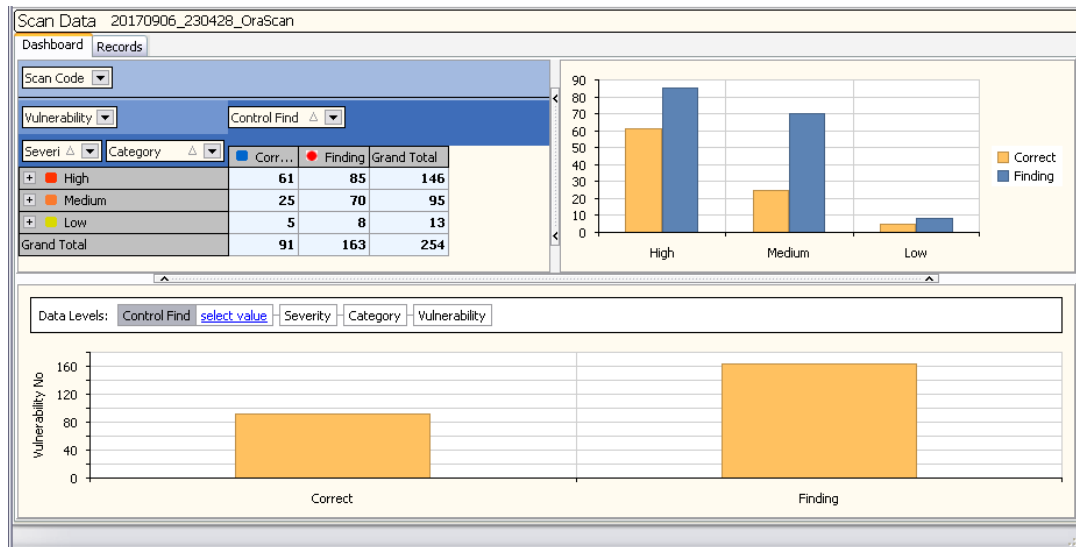
Important Note:

All scan naming features are important in Omega DB Scanner and especially in the "SIEM Integration" parts of this software, as they are also of most importance to the Omega DB Scanner App for Splunk!

IT IS STRONGLY ADVISED THAT YOU DO NOT CHANGE THE GENERATED SCAN NAME WHEN YOU SAVE THE FILE TO DISK!

2.3.2 Scan Dashboard

The first tab Dashboard shows summary graphical information of the full scan performed or loaded in graphical data-aware components which are all based on the same Scan Data dataset.



Scan Pivot table

On the top-left a pivot table enables end-user to re-arrange scan data fields in rows and columns with drag-and-drop functionality and having row, column and grand totals calculated on the fly. Can interchange columns and rows on the fly, filter and sort items in different ways, and also collapse and expand data at different levels.

Areas of the pivot:

Filter Header Area	filter operations only fields, will not show in pivot table, default field "Scan Code"
Data Header Area	measure field "Vulnerability" in Count, this area is the only fixed and cannot be changed
Row Header Area	dimension row fields, default "Severity" and "Category"
Column Header Area	dimension column fields, default "Control Find"

Scan Pivot Chart

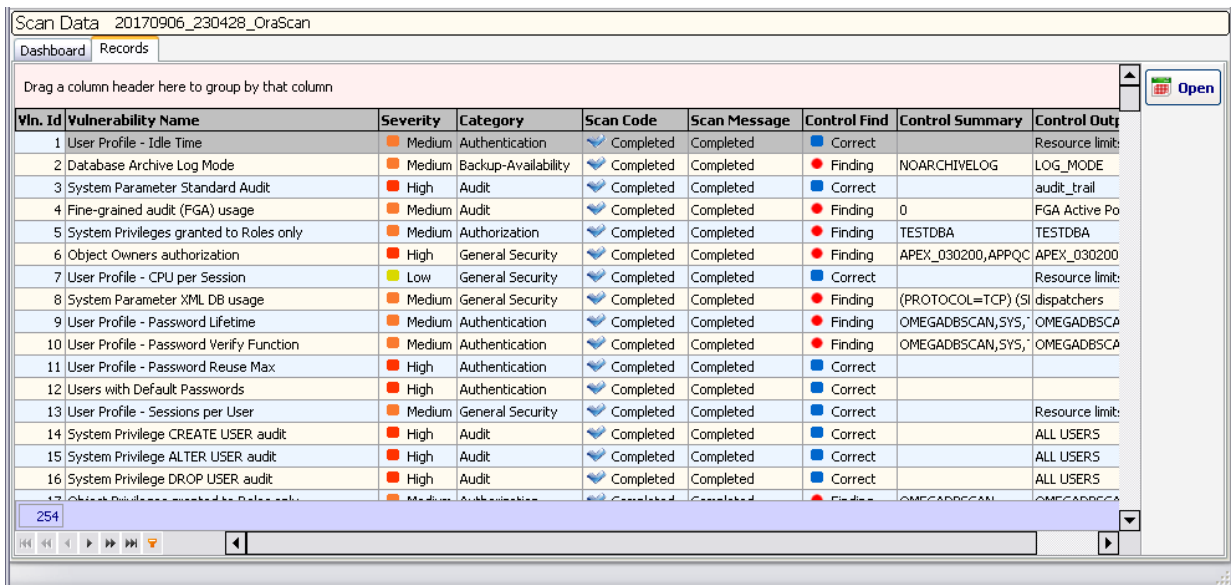
On the top-right a scan data chart component responds dynamically to the related pivot. Chart's vertical axis is the pivot Data Area measure (Count) field Vulnerability; in the horizontal axis are the pivot's rows, while the diagram's vertical bars represent the pivot's columns. In both later expand and collapse is reflected.

Scan Drill-down Chart

On the bottom alternative scan data chart with bar drill down functionality and Data Levels hierarchy reorder. Reorder the fields by drag-and-drop, click on the bars, or select drop-down values for hierarchy drill-down.

2.3.3 Scan Records

The second tab Records shows raw records in table view of the scan performed or loaded:



Vln. Id	Vulnerability Name	Severity	Category	Scan Code	Scan Message	Control Find	Control Summary	Control Output
1	User Profile - Idle Time	Medium	Authentication	Completed	Completed	Correct		Resource limit
2	Database Archive Log Mode	Medium	Backup-Availability	Completed	Completed	Finding	NOARCHIVELOG	LOG_MODE
3	System Parameter Standard Audit	High	Audit	Completed	Completed	Correct		audit_trail
4	Fine-grained audit (FGA) usage	Medium	Audit	Completed	Completed	Finding	0	FGA Active Po
5	System Privileges granted to Roles only	Medium	Authorization	Completed	Completed	Finding	TESTDBA	TESTDBA
6	Object Owners authorization	High	General Security	Completed	Completed	Finding	APEX_030200, APPQC	APEX_030200
7	User Profile - CPU per Session	Low	General Security	Completed	Completed	Correct		Resource limit
8	System Parameter XML DB usage	Medium	General Security	Completed	Completed	Finding	(PROTOCOL=TCP) (SI	dispatchers
9	User Profile - Password Lifetime	Medium	Authentication	Completed	Completed	Finding	OMEGADBSCAN, SYS,	OMEGADBSCA
10	User Profile - Password Verify Function	Medium	Authentication	Completed	Completed	Finding	OMEGADBSCAN, SYS,	OMEGADBSCA
11	User Profile - Password Reuse Max	High	Authentication	Completed	Completed	Correct		
12	Users with Default Passwords	High	Authentication	Completed	Completed	Correct		
13	User Profile - Sessions per User	Medium	General Security	Completed	Completed	Correct		Resource limit
14	System Privilege CREATE USER audit	High	Audit	Completed	Completed	Correct		ALL USERS
15	System Privilege ALTER USER audit	High	Audit	Completed	Completed	Correct		ALL USERS
16	System Privilege DROP USER audit	High	Audit	Completed	Completed	Correct		ALL USERS
17	Object Privileges granted to Roles only	Medium	Authorization	Completed	Completed	Finding	OMEGADBSCAN,	OMEGADBSCA

Beside common vulnerability fields, Scan-related fields are:

Scan Code

Return Code of the Scan, available values are:



Completed
Error
System Error

Scan completed successfully, normally the only returned
Scan failed with program error
Scan failed with Oracle error

Scan Message

Return Message of the Scan, related to the Scan Code, available values are:

Completed
<Error>
<Oracle Error>

Scan completed successfully
Returned program error message
Returned Oracle error code ORA-XXXXX and message

Control Find

This is the field that indicates the result of the control.
Available values are:



Correct
Finding
Broken

Vulnerability control is correct
Vulnerability control is a Finding
Vulnerability control has not run because of errors.

Control Summary

Vulnerability control's summary result; comma-separated when multiple values, in the later it contains values (ex. user accounts granted the assessed system privilege) that can be used for Authorization of the security control via "List" Format Parameters!

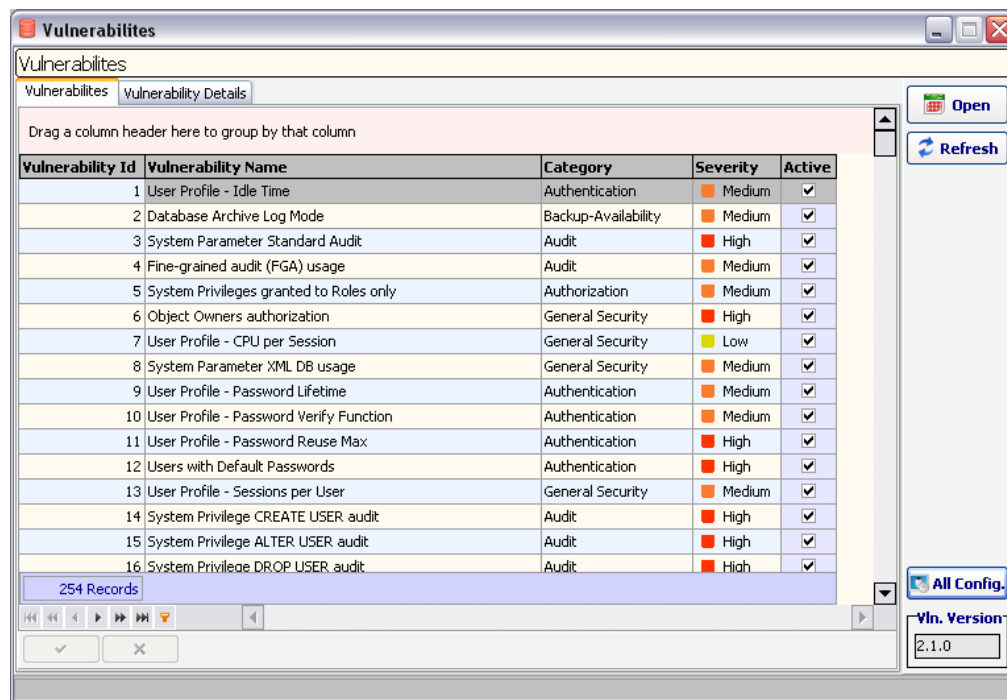
Control Output

Vulnerability control's full result; mostly grouped by item assessed within the control, gives detailed information on the control's security posture, valid for remediation and authorization.

Press the button Open to show the Vulnerability Scan form with the current's item data loaded.

2.4 Vulnerabilities (Security Controls)

In this form all the deployed vulnerabilities (security controls) are displayed:



Vulnerability Id	Vulnerability Name	Category	Severity	Active
1	User Profile - Idle Time	Authentication	Medium	<input checked="" type="checkbox"/>
2	Database Archive Log Mode	Backup-Availability	Medium	<input checked="" type="checkbox"/>
3	System Parameter Standard Audit	Audit	High	<input checked="" type="checkbox"/>
4	Fine-grained audit (FGA) usage	Audit	Medium	<input checked="" type="checkbox"/>
5	System Privileges granted to Roles only	Authorization	Medium	<input checked="" type="checkbox"/>
6	Object Owners authorization	General Security	High	<input checked="" type="checkbox"/>
7	User Profile - CPU per Session	General Security	Low	<input checked="" type="checkbox"/>
8	System Parameter XML DB usage	General Security	Medium	<input checked="" type="checkbox"/>
9	User Profile - Password Lifetime	Authentication	Medium	<input checked="" type="checkbox"/>
10	User Profile - Password Verify Function	Authentication	Medium	<input checked="" type="checkbox"/>
11	User Profile - Password Reuse Max	Authentication	High	<input checked="" type="checkbox"/>
12	Users with Default Passwords	Authentication	High	<input checked="" type="checkbox"/>
13	User Profile - Sessions per User	General Security	Medium	<input checked="" type="checkbox"/>
14	System Privilege CREATE USER audit	Audit	High	<input checked="" type="checkbox"/>
15	System Privilege ALTER USER audit	Audit	High	<input checked="" type="checkbox"/>
16	System Privilege DROP USER audit	Audit	High	<input checked="" type="checkbox"/>

In the first tab Vulnerabilities, the following fields and components are displayed:

Vulnerability Id Unique identification number of the deployed vulnerability control

Vulnerability Name Unique name of the deployed vulnerability control

Category Functional categorization of the security area/control:

- Audit
- Authentication
- Authorization
- Backup-Availability
- General Security

Severity Severity of the vulnerability:

- High
- Medium
- Low

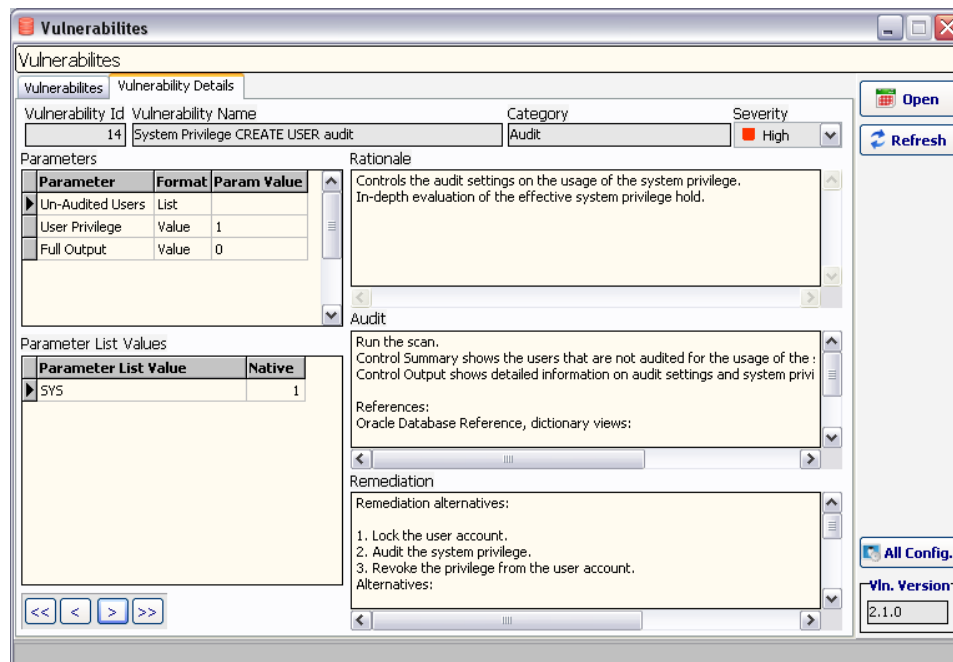
Active This is the status of the vulnerability, inactive controls are excluded from the full scan

Note

The field Active is the only editable in the Vulnerabilities dataset. Setting to Inactive (unchecked) will exclude item from full table scans. Use the bottom-left navigator buttons Post and Cancel as needed.

In the second tab Vulnerability Details, more fields and components are displayed:

Parameters	vulnerability parameters
Parameters List Values	list values for parameters with format List
Rationale	description of the vulnerability (security control)
Audit	audit description of the security control
Remediation	general advise on the remediation of the security control



Vulnerabilities

Vulnerabilities | Vulnerability Details

Vulnerability Id: 14 | Vulnerability Name: System Privilege CREATE USER audit | Category: Audit | Severity: High

Parameters

Parameter	Format	Param Value
Un-Audited Users	List	
User Privilege	Value	1
Full Output	Value	0

Rationale

Controls the audit settings on the usage of the system privilege. In-depth evaluation of the effective system privilege hold.

Audit

Run the scan. Control Summary shows the users that are not audited for the usage of the : Control Output shows detailed information on audit settings and system privi

References:
Oracle Database Reference, dictionary views:

Remediation

Remediation alternatives:

1. Lock the user account.
2. Audit the system privilege.
3. Revoke the privilege from the user account.

Alternatives:

Parameter List Values

Parameter List Value	Native
SYS	1

Buttons: Open, Refresh, All Config., Vln. Version: 2.1.0

In the panel right-sided, find the following:

Open	press button open form "Vulnerability Scan", where a scan is performed on the target database for the selected vulnerability and also parameter values and parameter list values are managed.
Refresh	press button to refresh all vulnerabilities, parameters and parameters list values.
All Config.	press button to open form "All Configurations", described in respective topic.
Vln. Version	this group box contains the version number of the deployed vulnerabilities set.

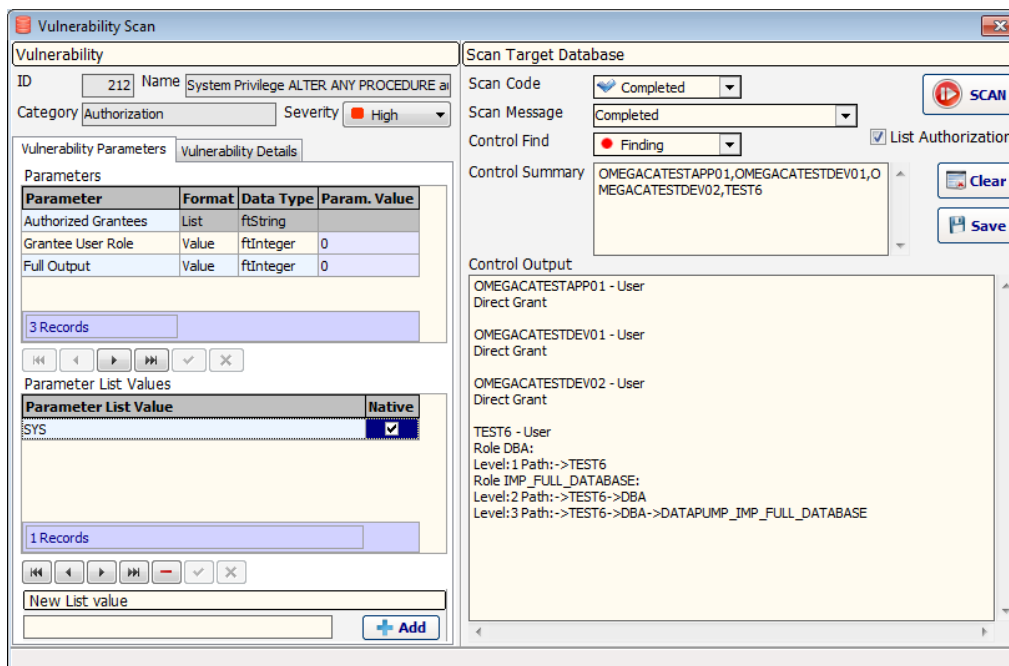
2.5 Vulnerability Scan

This form serves two main functionalities, however closely related to each-other:

Manages Vulnerability Parameters customize, authorize and use advanced features of the security control through Parameters and Parameter List Values.

Scan the Vulnerability scans the target database for this vulnerability control.

This form is invoked from the Scan Data, Scan Comparison and Vulnerabilities forms.



The selected vulnerability control is viewed in the Vulnerability group on the left. Here the Parameters of the control and optionally Parameter List Values are displayed and managed.

In the Scan Target Database group on the right, as the name implies, a scan of the selected control is displayed and performed into the target database.

2.5.1 Parameters and List Values

Parameters

Most vulnerability contains input parameters that allow for customization, authorization and use of advanced features of the security control. Parameters of common types are used to different vulnerabilities.

Parameters are displayed in the Parameters grid and cannot be changed, except for their input Parameter Value which is managed according to the two available Parameter Formats:

Value Parameter's value is set directly in the Parameters grid in the field "Param. Value"
List Parameter value is built as a list of values from the Parameter List Values (empty "Param. Value")

"Value" Format Parameters:

Parameters with a Format of type Value are used for customization and advanced features of the security control.

Common parameters and respective Value settings are listed below:

Full Output	<p>This parameter controls the full output of the vulnerability scan. Used in all Categories; almost all vulnerability controls. Allowed values are:</p> <p>0 - Only Findings information is returned; this is the default option. 1 - Both Findings and Correct information is returned.</p>
Grantee User Role	<p>This parameter defines whether the control is done at User only, or at both User and Role level. Used in Category Authorization for vulnerabilities of kind:</p> <ul style="list-style-type: none"> • System Privileges authorization • Role Privileges authorization • Object Privileges authorization <p>Allowed values are:</p> <p>0 - At User level only (since using role hierarchy control). This is the default and advised option. 1 - At User and Role level.</p>
User Privilege	<p>This parameter defines whether the evaluation performed is related to the fact of privilege being granted. Used in Category Audit for vulnerabilities of System Privilege audit. Allowed values are:</p> <p>0 - Evaluation performed independently of the Privilege granted or not. 1 - Evaluation performed only when privilege is granted. This is the default and advised option.</p>
Profile Limit	<p>This parameter defines user profile limits. Used in Category Authentication, for vulnerabilities of kind User Profile Resource [non Password].</p>
Others	<p>other vulnerability specific parameters:</p> <p>"Max. Enabled roles" "Max. Failed Login"</p>

Change the value directly on the Parameters grid, field "Param. Value".
Use the navigator buttons Post and Cancel as needed.

"List" Format Parameters:

Parameters with a Format of type List are used for authorizations on the security control.

For Vulnerability parameters of type "List", the list values are displayed in the Parameter List Values grid; you can edit the field Parameter List Value on the grid. You can add a new parameter list value in the bottom group New List Value; and also delete one using the right-aligned navigator Delete button. Use the navigator buttons Post and Cancel as needed.

Native parameter list values are only those that came with the software deployment.

Populate the Parameter List Values grid with values for common parameters as listed below:

Authorized Grantees	<p>This list defines authorized grantees allowed to the assessed privilege[s]. Used in Category Authorization for vulnerabilities of:</p> <ul style="list-style-type: none"> • System Privileges authorization • Role Privileges authorization • Object Privileges authorization • Others - privilege authorization related
Authorized Users	<p>This list defines authorized users allowed to the assessed privilege[s]. Used in Categories Authentication, Authorization and General Security for vulnerabilities of kind:</p> <ul style="list-style-type: none"> • User Profiles - Password and Resource • Others - privilege authorization related
Un-Audited Users	<p>This list defines authorized un-audited users allowed to the assessed privilege. Used in Category Audit for all vulnerabilities of System Privilege audit</p>
Authorized Owners	<p>This list defines object owners authorized to the assessed control. Used in Categories Authorization, Backup-Availability and General Security</p>
Authorized Link Owners	<p>This list defines DB Link owners authorized to the assessed control.</p>

2.5.2 "Classes" and Advanced Features

1. Vulnerability "Classes":

Vulnerabilities can further be classified (other than for Category and Severity) into certain "classes" according to the Oracle area of security interest which is assessed by the scan; this is logically related with the approach of the scan and obviously impacts the content of the scan result.

Important Note:

This concept is not directly presented in the vulnerability's dataset, like the Category and Severity (fields) are. However visualization of this concept is presented in the naming of the vulnerabilities (mostly conforming to a schema) and also in the result of the scan, the content fields Control Summary and Control Output of the scan dataset.

Different vulnerability "Classes" are described below:

System Privilege <SYSTEM PRIVILEGE> authorization	<p>Control the grants on system privileges. Evaluation of the effective privilege (role hierarchy) in hold.</p> <p>Control Summary shows the grantees that effectively hold the system privilege. Control Output shows detailed information on grant of system privilege grouped by each grantee.</p>
System Privilege <SYSTEM PRIVILEGE> audit	<p>Control the audit settings on the usage of the system privilege. Evaluation of the effective privilege (role hierarchy) in hold. Enables (default) assessments of accounts that have the privilege only.</p> <p>Control Summary shows the users that are not audited for the usage of the system privilege. Control Output shows detailed information on audit settings and system privilege grants grouped by each user account.</p>
System Role <ROLE> authorization	<p>Control the grants on the system roles. Evaluation of the effective</p>

	<p>privilege (role hierarchy) in hold.</p> <p>Control Summary shows the grantees that effectively hold the role.</p> <p>Control Output shows detailed information on grant of role grouped by each grantee.</p>
System Package <OBJECT> authorization System Table <OBJECT> authorization System View <OBJECT> authorization	<p>Control the grants on the system dictionary objects (package, table and view) privileges.</p> <p>Control Summary shows the grantees that effectively hold the object privilege. Control Output shows detailed information on grant of privilege grouped by each grantee</p>
System Parameter <Parameter>	<p>Control the value of the initialization parameters, most normal but also a few hidden ones.</p> <p>Control Summary shows the parameter value when Finding. Control Output shows the parameter name and value.</p>
User Profile - Password [Resource Name] User Profile - [Resource Name]	<p>Control the usage of User Profile of type Password Vs Kernel (others).</p> <p>Control Summary shows the user accounts that do not satisfy the profile limit. Control Output shows detailed information on profile limit grouped by each user account.</p>
User account <Account>	<p>Control status of important user schema accounts.</p> <p>Control Summary shows the user account status when Finding.</p> <p>Control Output shows the user account name and status.</p>
OTHERS	<p>Mixed Controls on different aspects of oracle database security settings.</p> <p>Control Summary and Output generally follow same principles as in other "Classes", however advanced features are not available here (as per few exceptions).</p>

2. Advanced Features:

Below some of the advanced features are explained:

Account Status evaluation:

Whenever an Oracle user account is involved in a vulnerability scan, the status of the account will determine if it will be considered correct (and eventually continuing), or it will cause the result to be a Finding.

Correct: LOCKED, EXPIRED & LOCKED, EXPIRED(GRACE) & LOCKED

Finding: OPEN, EXPIRED, EXPIRED(GRACE), LOCKED(TIMED), EXPIRED & LOCKED(TIMED), EXPIRED(GRACE) & LOCKED(TIMED)

Effective privilege (role hierarchy) evaluation:

A system, object or role privilege is granted to a grantee (user account or role) with respective Oracle commands. This is easily verifiable in respective Oracle dictionary views, which is the simplest approach; however a grantee might have in-force the same privilege not granted (and verified) directly, but hidden after a "chain" of roles granted to each other and having the privilege granted to the role at the end of the "chain".

The feature above ensures the evaluation considers not only a direct grant, but also an "inherited" one. It is built-in in most controls, whenever privilege-related controls are available, and is quite visible in the Control Output scan field, where the path and level of role grant hierarchy is displayed for each grantee.

Account based evaluation:

Scanning effective privilege grant instead of only direct ones enables assessing at Oracle user account level only and not roles, as roles are just containers of privileges and do not represent operating entities per se, like humans or credentialed interfaces - as user accounts do. This feature is controlled by Parameter "Grantee User Role".

Intelligent Scan:

When scanning system privilege audits, if audit is not set for a user account, the account effectively holding (or not) the privilege assessed impacts the decision on Correct/Finding. This feature is controlled by Parameter "User Privilege".

Others:

Public Grants Control Output highlight
Audit user-wide Control Output highlight
Full audit syntax support

2.5.3 Vulnerability Item Scan

On the right side of the Vulnerability Scan form, the Scan Target Database group enables scanning of the target database for the selected vulnerability.

All the scan data elements: Scan Code/Message and Control Find/Summary/Output are logically columns of the Scan Data dataset and are described in the respective topic.

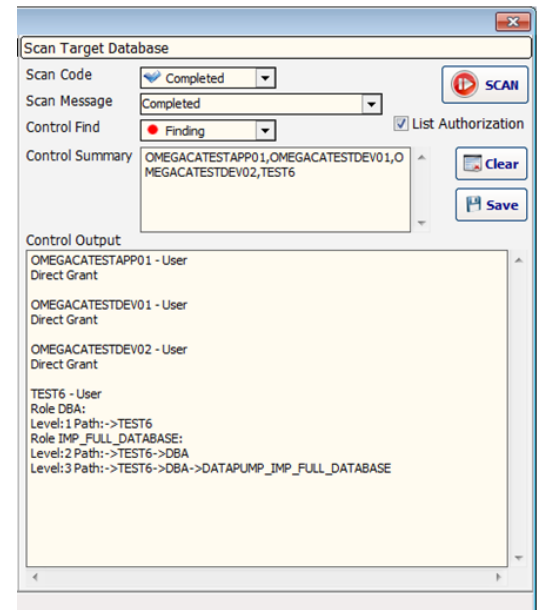
The data elements will be loaded with the scan data of the form invoking - Scan Data or Scan Comparison (Scan Run data); will be empty when invoked from the Vulnerabilities form.

Buttons and options on the right are:

- **SCAN** - Performs a scan for this item on the target database. You must be connected first. A successful scan will update all groups scan data elements.
- **List Authorization** - Runs the scan applying authorizations as defined in parameter list values (default checked); when unchecked the scan will be performed without considering them!
- **Clear** - Clears values of the scan data elements
- **Save** - Save scan item to the Scan Data dataset, enabled only when invoked from the Scan Data and Scans Comparison (Scan Run) forms.

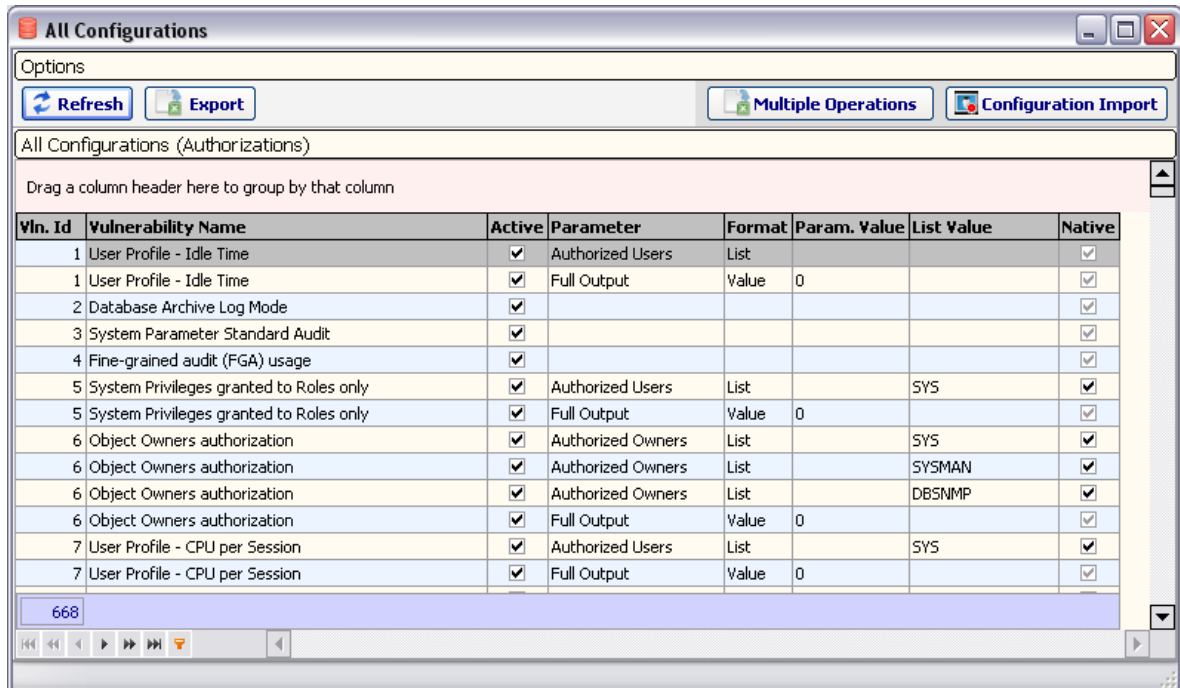
Note:

Saving the Scan Data and Scan (comparison) Run records in this form leaves the respective datasets in a different state from the files in disk from which they are loaded. This is highlighted in respective Scan Name labels that change to Red and Bold. Use the forms respective Save (Save as) buttons to permanently save these datasets to disk.



2.6 All Configurations (authorizations)

This form is opened from the form Vulnerabilities by pressing button "All Config.". Here all vulnerabilities, their parameter values and list values are presented in a single dataset that represents all configurations and authorizations done by the end-user, thus representing the whole set of your authorization/configuration on the security posture of the database!



The screenshot shows a window titled "All Configurations" with a toolbar containing "Refresh", "Export", "Multiple Operations", and "Configuration Import". Below the toolbar is a table with the following data:

Vln. Id	Vulnerability Name	Active	Parameter	Format	Param. Value	List Value	Native
1	User Profile - Idle Time	<input checked="" type="checkbox"/>	Authorized Users	List			<input checked="" type="checkbox"/>
1	User Profile - Idle Time	<input checked="" type="checkbox"/>	Full Output	Value	0		<input checked="" type="checkbox"/>
2	Database Archive Log Mode	<input checked="" type="checkbox"/>					<input checked="" type="checkbox"/>
3	System Parameter Standard Audit	<input checked="" type="checkbox"/>					<input checked="" type="checkbox"/>
4	Fine-grained audit (FGA) usage	<input checked="" type="checkbox"/>					<input checked="" type="checkbox"/>
5	System Privileges granted to Roles only	<input checked="" type="checkbox"/>	Authorized Users	List		SYS	<input checked="" type="checkbox"/>
5	System Privileges granted to Roles only	<input checked="" type="checkbox"/>	Full Output	Value	0		<input checked="" type="checkbox"/>
6	Object Owners authorization	<input checked="" type="checkbox"/>	Authorized Owners	List		SYS	<input checked="" type="checkbox"/>
6	Object Owners authorization	<input checked="" type="checkbox"/>	Authorized Owners	List		SYSMAN	<input checked="" type="checkbox"/>
6	Object Owners authorization	<input checked="" type="checkbox"/>	Authorized Owners	List		DBSNMP	<input checked="" type="checkbox"/>
6	Object Owners authorization	<input checked="" type="checkbox"/>	Full Output	Value	0		<input checked="" type="checkbox"/>
7	User Profile - CPU per Session	<input checked="" type="checkbox"/>	Authorized Users	List		SYS	<input checked="" type="checkbox"/>
7	User Profile - CPU per Session	<input checked="" type="checkbox"/>	Full Output	Value	0		<input checked="" type="checkbox"/>

At the bottom of the window, there is a status bar showing the number 668 and navigation controls.

The triple master-slave structure of Vulnerability, Parameters and List Values is been presented here in a single view to allow browsing and viewing of all information, without being fragmented in multiple forms navigation.

Refresh refreshes data in the grid.

Export exports grid as an Excel file. This is de-facto a report of all your configuration settings and authorizations maintained in parameter values and their list values.

Multiple Operations opens form "Parameter Multiple Operations", for working with parameters in multiple vulnerability controls - explained in details in respective topic.

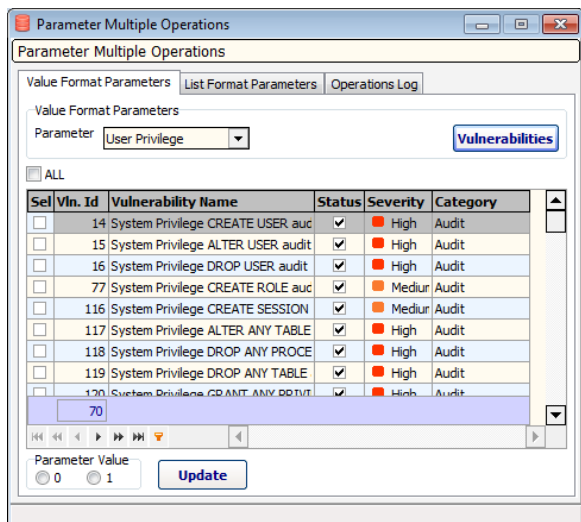
Configuration Import opens the form "Configurations Import"; used only for upgrade after the deployment of a new version of vulnerabilities (OmegaDSSStd.dat), refer to the "Appendix A3 - Configurations imports (upgrade)".

Note

The grid is intended for reporting and not to manage, as such it is read-only; parameter values and list values are managed in forms "Vulnerability Scan" and "Parameter Multiple Operations" - both explained in details in respective topics below.

2.6.1 Parameter Multiple Operations

This form enables multiple operations to be performed on most common parameter values and list values for all vulnerabilities in which the parameter is used.



Sel	Vln. Id	Vulnerability Name	Status	Severity	Category
<input type="checkbox"/>	14	System Privilege CREATE USER auc	<input checked="" type="checkbox"/>	High	Audit
<input type="checkbox"/>	15	System Privilege ALTER USER audit	<input checked="" type="checkbox"/>	High	Audit
<input type="checkbox"/>	16	System Privilege DROP USER audit	<input checked="" type="checkbox"/>	High	Audit
<input type="checkbox"/>	77	System Privilege CREATE ROLE auc	<input checked="" type="checkbox"/>	Medium	Audit
<input type="checkbox"/>	116	System Privilege CREATE SESSION	<input checked="" type="checkbox"/>	Medium	Audit
<input type="checkbox"/>	117	System Privilege ALTER ANY TABLE	<input checked="" type="checkbox"/>	High	Audit
<input type="checkbox"/>	118	System Privilege DROP ANY PROCEDURE	<input checked="" type="checkbox"/>	High	Audit
<input type="checkbox"/>	119	System Privilege DROP ANY TABLE	<input checked="" type="checkbox"/>	High	Audit
<input type="checkbox"/>	120	System Privilege GRANT ANY PRIVILEGE	<input checked="" type="checkbox"/>	High	Audit

In the first tab Value Format Parameters, the 0/1 value for the common parameters "Full Output", "Grantee User Roles" and "User Privilege" is set.

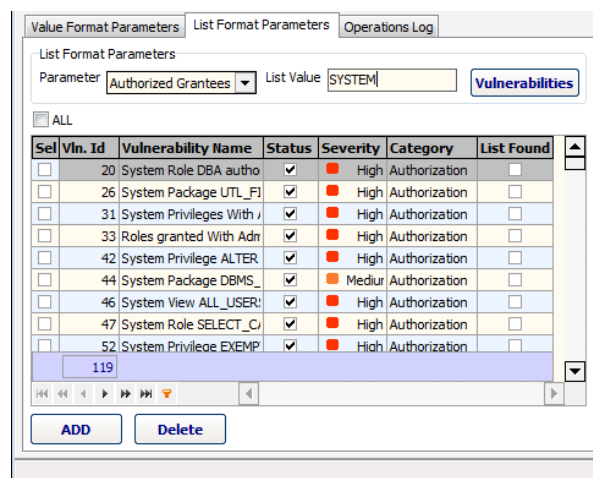
Chose the parameter and press the Vulnerabilities button. In the grid will be displayed all vulnerabilities in which the chosen parameter is used. Use the checkboxes in each record to determine appliance of the action.

Chose a parameter value 0/1 in the Radio group below and press button Update.

In the second tab List Format Parameters, a list value can be inserted to or deleted from the common parameters "Authorized Grantees", "Authorized Users", "Authorized Owners" and "Un-audited Users".

Chose the parameter, complete the List Value and press the Vulnerabilities button. In the grid will be displayed all vulnerabilities in which the chosen parameter is used. Furthermore the special field "List Found" will indicate if the List Value entered is present in each parameter's list or not. Use the checkboxes in each record to determine appliance of the action.

Press buttons Add or Delete to respectively insert or delete the list value in the parameter's list.



Sel	Vln. Id	Vulnerability Name	Status	Severity	Category	List Found
<input type="checkbox"/>	20	System Role DBA author	<input checked="" type="checkbox"/>	High	Authorization	<input type="checkbox"/>
<input type="checkbox"/>	26	System Package UTL_FILE	<input checked="" type="checkbox"/>	High	Authorization	<input type="checkbox"/>
<input type="checkbox"/>	31	System Privileges With	<input checked="" type="checkbox"/>	High	Authorization	<input type="checkbox"/>
<input type="checkbox"/>	33	Roles granted With Adm	<input checked="" type="checkbox"/>	High	Authorization	<input type="checkbox"/>
<input type="checkbox"/>	42	System Privilege ALTER	<input checked="" type="checkbox"/>	High	Authorization	<input type="checkbox"/>
<input type="checkbox"/>	44	System Package DBMS_	<input checked="" type="checkbox"/>	Medium	Authorization	<input type="checkbox"/>
<input type="checkbox"/>	46	System View ALL_USERS	<input checked="" type="checkbox"/>	High	Authorization	<input type="checkbox"/>
<input type="checkbox"/>	47	System Role SELECT_C	<input checked="" type="checkbox"/>	High	Authorization	<input type="checkbox"/>
<input type="checkbox"/>	52	System Privilege EXEMP	<input checked="" type="checkbox"/>	High	Authorization	<input type="checkbox"/>

Important Notes:

1. In operations performed in both tables, grid local filtering:
 - Is not considered in the Update, Add and Delete functionalities (called by respective buttons)
 - Is considered when marking Vulnerabilities Active/Inactive
2. Check selected status for the generated vulnerabilities is decided by status of respective ALL checkboxes

Thus it is advised that you use filtering just to decide what to check/uncheck; and then you un-filter and verify all before processing!

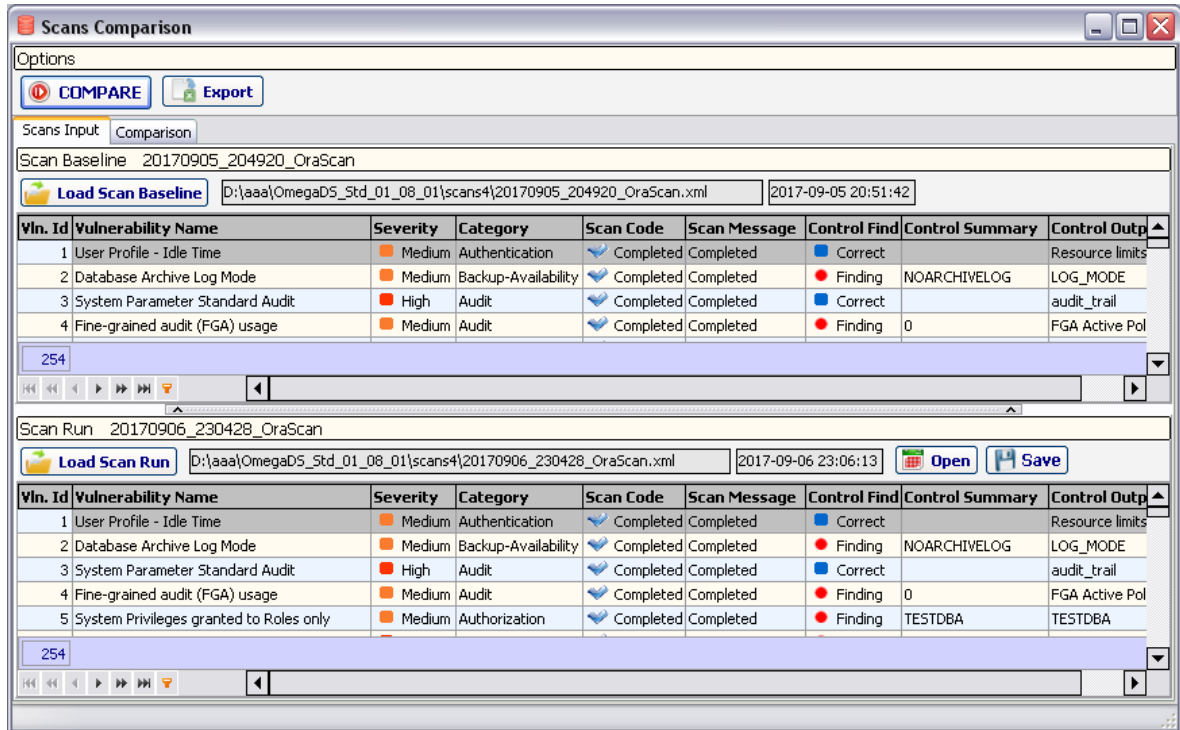
In the third tab "Operations Log", a trail of the multiple operations displays output for each command with an indication of success or error.

2.7 Scans Comparison

In this form a comparison is performed between two scans: The Scan (usually the last) Run versus the Baseline Scan. This is a top feature and important tool that spots changes into the security posture of the Oracle database, and also helps and guides the process of improvement: authorization and remediation.

This form has two main tabs:

- Scans Input - (Last) Run and Baseline Scans are loaded here.
- Comparison - displays the Scan comparison report in graphical analyses and raw records views.



Scans Comparison

Options

COMPARE **Export**

Scans Input Comparison

Scan Baseline 20170905_204920_OraScan

Load Scan Baseline D:\aaa\OmegaDBS_std_01_08_01\scans4\20170905_204920_OraScan.xml 2017-09-05 20:51:42

Vln. Id	Vulnerability Name	Severity	Category	Scan Code	Scan Message	Control Find	Control Summary	Control Output
1	User Profile - Idle Time	Medium	Authentication	Completed	Completed	Correct	Resource limits	
2	Database Archive Log Mode	Medium	Backup-Availability	Completed	Completed	Finding	NOARCHIVELOG	LOG_MODE
3	System Parameter Standard Audit	High	Audit	Completed	Completed	Correct	audit_trail	
4	Fine-grained audit (FGA) usage	Medium	Audit	Completed	Completed	Finding	0	FGA Active Pol

254

Scan Run 20170906_230428_OraScan

Load Scan Run D:\aaa\OmegaDBS_std_01_08_01\scans4\20170906_230428_OraScan.xml 2017-09-06 23:06:13 **Open** **Save**

Vln. Id	Vulnerability Name	Severity	Category	Scan Code	Scan Message	Control Find	Control Summary	Control Output
1	User Profile - Idle Time	Medium	Authentication	Completed	Completed	Correct	Resource limits	
2	Database Archive Log Mode	Medium	Backup-Availability	Completed	Completed	Finding	NOARCHIVELOG	LOG_MODE
3	System Parameter Standard Audit	High	Audit	Completed	Completed	Correct	audit_trail	
4	Fine-grained audit (FGA) usage	Medium	Audit	Completed	Completed	Finding	0	FGA Active Pol
5	System Privileges granted to Roles only	Medium	Authorization	Completed	Completed	Finding	TESTDBA	TESTDBA

254

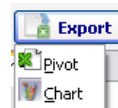
Options group:

This group is common to both Scans Input and Comparison tabs:

COMPARE Press button to generate a comparison report of Scan Run versus the Baseline Scan. This will take you to the second tab Comparison.

Export Press button to export form's multiple scan comparison views in common file formats to disk.

When the Comparison/Dashboard sub-tab is active:
a popup menu will prompt user to:

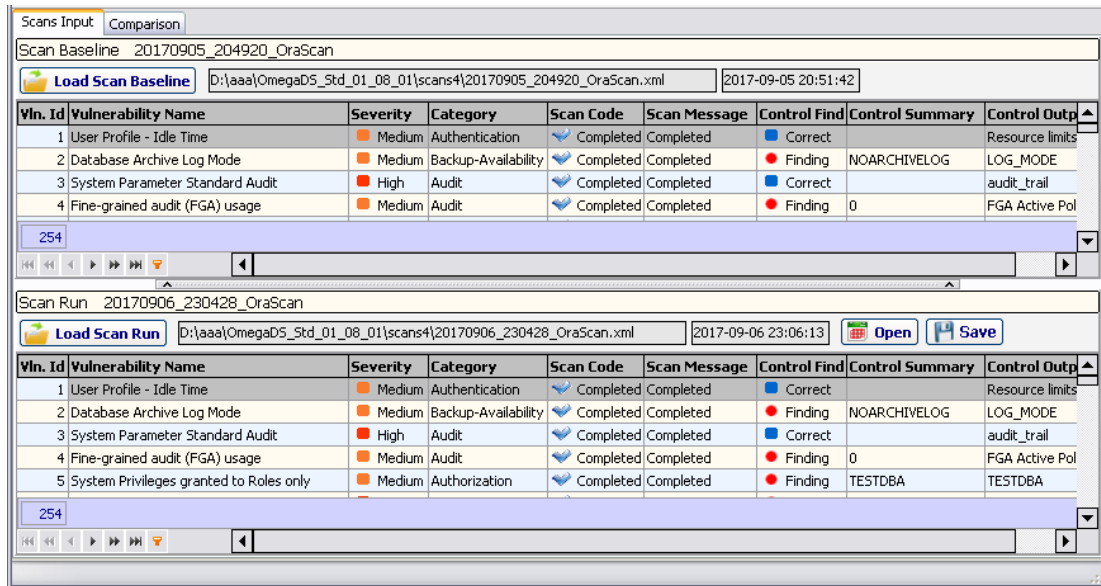


- Save the pivot table as Excel
- Save the drill-down chart as Bmp

When the Comparison/Report sub-tab is active:
this button will directly prompt to save as Excel all visible records in the scan comparison grid.

Scans Input tab

Load Baseline Scan and Run Scan to compare with the baseline.



Vln. Id	Vulnerability Name	Severity	Category	Scan Code	Scan Message	Control Find	Control Summary	Control Output
1	User Profile - Idle Time	Medium	Authentication	Completed	Completed	Correct	Resource limits	
2	Database Archive Log Mode	Medium	Backup-Availability	Completed	Completed	Finding	NOARCHIVELOG	LOG_MODE
3	System Parameter Standard Audit	High	Audit	Completed	Completed	Correct	audit_trail	
4	Fine-grained audit (FGA) usage	Medium	Audit	Completed	Completed	Finding	0	FGA Active Pol

Vln. Id	Vulnerability Name	Severity	Category	Scan Code	Scan Message	Control Find	Control Summary	Control Output
1	User Profile - Idle Time	Medium	Authentication	Completed	Completed	Correct	Resource limits	
2	Database Archive Log Mode	Medium	Backup-Availability	Completed	Completed	Finding	NOARCHIVELOG	LOG_MODE
3	System Parameter Standard Audit	High	Audit	Completed	Completed	Correct	audit_trail	
4	Fine-grained audit (FGA) usage	Medium	Audit	Completed	Completed	Finding	0	FGA Active Pol
5	System Privileges granted to Roles only	Medium	Authorization	Completed	Completed	Finding	TESTDBA	TESTDBA

Scans Baseline Group:

In this panel the Baseline Scan is loaded from disk. The name of the scan is displayed in the "Baseline Scan Name" label next to the "Scan Baseline" label.

Load Scan Baseline Press button to invoke a File Open dialog and load a scan from disk that will serve as a Baseline for comparison. This will update the File Path and File Dt. Mod. Edits (see below) and also the name of the "Baseline Scan Name" label.

File Path Read-only edit (next to Load) shows the full path and name of the loaded Baseline scan file.

File Dt. Mod. Read-only edit (next to "File Path") shows the date last modified of the loaded Baseline scan file.

Scans Run Group:

In this panel the Run Scan is loaded from disk to be compared with the previously loaded Baseline Scan. The name of the scan is displayed in the "Run Scan Name" label next to the "Scan Run" label.

Load Scan Run Press button to invoke a File Open dialog and load a scan from disk that will be compared to the Baseline scan. This will update the File Path and File Dt. Mod. Edits (see below) and also the name of the "Run Scan Name" label.

File Path Read-only edit box (next to Load button) shows the full path and name of the loaded Run scan file.

File Dt. Mod. Read-only edit box (next to "File Path") shows the date last modified of the loaded Run scan file.

Open Press the button to show the Vulnerability Scan form with the current's item data loaded.

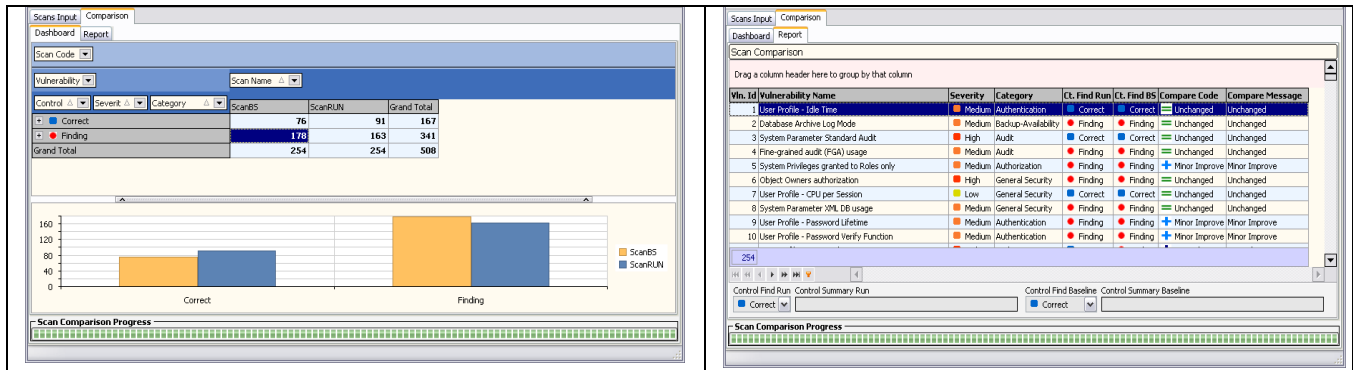
Save Press button to save the Run Scan as to disk. This will update the "File Dt. Mod.".

The "Run Scan Name" label will change in Red color and Bold when a scan is unsaved to disk!

Comparison tab

In this tab the generated scan comparison is displayed in graphical analyses form and also as a full dataset. In this tabs there are two sub-tabs:

- **Dashboard** displays pivotal and chart drill-down analyses of scan data
- **Report** displays the full scan dataset in a grid



Dashboard sub-tab:








In this sub-tab Pivot table and related chart of the generated scan comparison data are displayed. Notice the new dimension Scan Name default presented as the single Column in the pivot. The two available values are:

ScanBS Baseline Scan - serves as such
ScanRUN Run Scan - to be compared with the baseline one

Report sub-tab:

A full dataset in table view of the scan comparison report is displayed into this sub-tab. Each item of the Run Scan is compared with the respective item in the Baseline Scan and a result (Compare Code) is produced. Beside common vulnerability fields, can comparison-related fields are:

Compare Code Code of Scan Item to Item comparison, available values are:

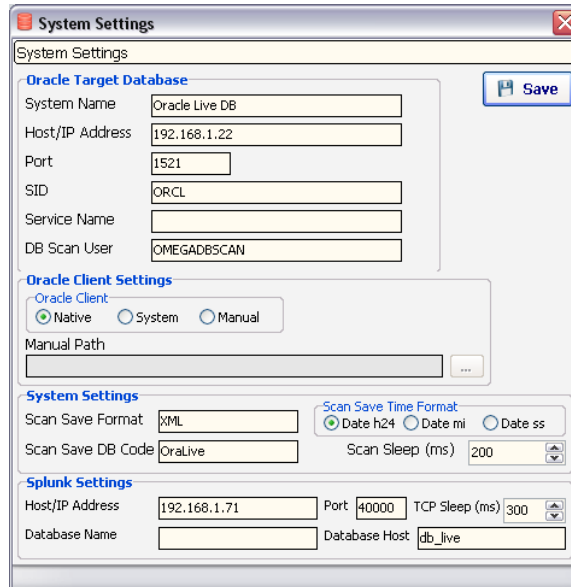
-  **Error** Run Item comparison failure.
-  **Control Improve** Item's Control Find is a Finding in Baseline and Correct in Run
-  **Control Decline** Items' Control Find is Correct in Baseline and a Finding in Run
-  **Minor Improve** Item's Control Find is a Finding in both Baseline and Run, but fewer items are found in the Scan Run item's Control Summary.
-  **Minor Decline** Item's Control Find is a Finding in both Baseline and Run, but more items are found into the Scan Run item's Control Summary.
-  **Changed** Item's Control Find is a Finding in both Baseline and Run, but there is change in the Control Summary field between Scan Run and Baseline.
-  **Unchanged** Item's Control Find is the same in both Baseline and Run items

Compare Message Return Message of item's Scan comparison, related to the Compare Code.

Scan Summary Run and BS are default hidden, to show them right-click on field headers and click Field Chooser.

2.8 System Settings

In this form the Omega DB Scanner settings are viewed and managed. Press the button Save to permanently save your settings!



Oracle Target Database:

System Name	Oracle database conventional (IT/business) system name, max 20 characters. This name shows in the logon prompt System Authentication form and also the application's main form.
Host/IP Address	Hostname or IP Address of the Oracle database server.
Port	Oracle Listener Port, default 1521.
SID	Oracle target Database Instance name, used by default.
Service Name	Oracle target Database Service name, used for RAC compliance. Null when no RAC used. Effective only when SID is left NULL - for RAC usage.
DB Scan User	Oracle user account used for performing the scan. When completed shows in target database System Authentication form into a read-only Username field. When empty the Username field will be empty and editable.

Oracle Client Settings:

Oracle Client	Oracle client connectivity settings, available options are: <ul style="list-style-type: none"> Native built-in application connectivity, OCI deployed files System operating system installed and default Oracle client Manual manual Oracle client oci.dll path specification, usually for Oracle Instant Client, but others (non-Instant) can be referenced too.
---------------	---

Note:

Changing the Oracle Client requires an application restart to take effect!
Refer to the "Appendix A2 - Oracle connectivity and Character Set support"!

System Settings:

Scan Save Format Format of scan file saved to disk: XML (default), XML_UTF8 or BINARY. The first two XML options will set a file extension of .xml, the third (BINARY) will set a .dat extension. Do not mismatch the later with the OmegaDSStd.dat file deployed!

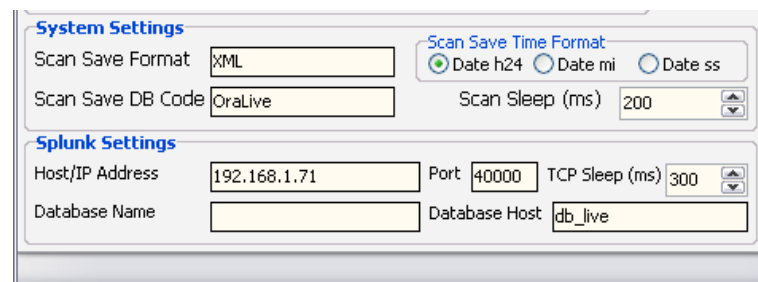
Scan Save Time Format will set the first part of the filename of the saved scan according to options:

- Date h24 yyyyymmdd_hh24
- Date mi yyyyymmdd_hh24mi
- Date ss yyyyymmdd_hh24miss

where yyyy mm dd hh24 mi ss stands for year to second; month to second will have a 0 added before if it is single digit.

Scan Save DB Code short 8 character unique code for the Database; will set the second part of the filename of the saved scan!

Scan Sleep (ms) Time in milliseconds the full scan process "sleeps" on every item while scanning the database. This is necessary just in case not to create any burden, minimal however, or trigger any third-party protection system. If you are in hurry, set this to 0!



Important Note:

Carefully read the "Scan Name/Filename Format" topic when working with the initialization parameters "Scan Save Time Format" and "Scan Save DB Code"!

Splunk Settings:

Host/IP Address Hostname or IP Address of the Splunk server.

Port Splunk TCP Data Input Port.

TCP Sleep (ms) Time in milliseconds the "Upload to Splunk" process "sleeps" on every scan record sent. Differently from the Sleep of the Oracle Scan this parameter must not be set to 0! It must have a greater value (keep the default 300, or even more) - refer to the **Splunk TCP Data Input Hint** note on the Splunk Interface topic below.

Database Name name of the database to appear in Splunk. When empty (default), the "System Name" is used instead.

Database Host name of the database host to appear in Splunk.

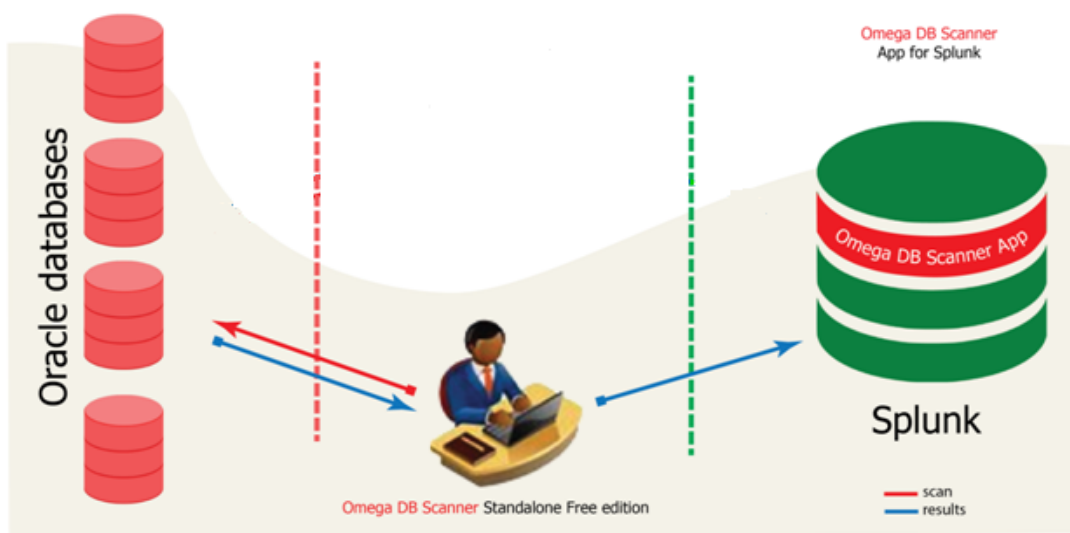
3 Integration to SIEM

3.1 Splunk Interface

Omega DB Scanner Standalone edition supports delivery of scan records to Splunk SIEM

3.1.1 Solution Architecture

Oracle databases are scanned and the results sent to Splunk by the Omega DB Scanner Standalone edition. In the Splunk repository scans are managed and visualized via the Omega DB Scanner App for Splunk.



Delivery of records is performed "on-the-fly" and Agent-less via Splunk TCP Data Input! Nothing to install!

Splunk Requirements:

- Minimal for loading a Splunk Index, a Source Type and an active TCP Data Input port *
- Minimal for reporting Splunk Search and Reporting App - built-in Splunk distribution
- Advanced Omega DB Scanner App for Splunk *

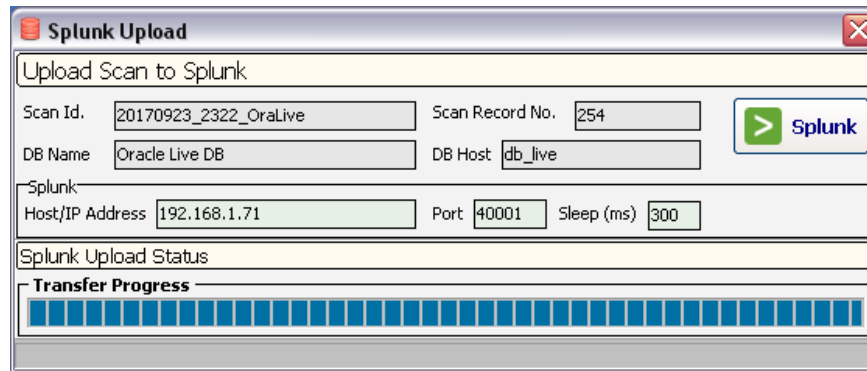
* refer to the Omega DB Scanner App for Splunk User Guide

Splunk Warnings:

- Upload scan only once in Splunk!
- Upload only scans that do comply with the scan naming schema, as described in the topic "Scan Name/Filename Format", thus ensuring scan naming uniqueness!
- Create the Splunk index and the source type to ensure correct delivery of data

3.1.2 Splunk Upload

The Splunk Upload form, as the name implies, performs the delivery of scan records to Splunk. The records are those currently loaded in form "Scan Data", from which the former is invoked by pressing the button Splunk on top-left!



The data elements of this form are all read-only, mostly as a last review before you upload

Scan Id. Unique scan name used as the "Scan Id" in the Omega DB Scanner App for Splunk. This field is set according to the scan name set in the Scan Data form next to the Scan Data label.*

Scan Record No. Number of the scan records the scan set contains. **

DB Name Name of the database to appear in Splunk, as defined in the initialization parameters either "System Name" in section "Oracle Target database" or "Database Name" in section "Splunk Settings".

DB Host Name of the database host to appear in Splunk as defined in the initialization parameter "Database Host" in section "Splunk Settings"

* refer to the "Scan Name/File name Format" topic for detailed information on this important condition!

** refer to the Splunk TCP Data Input Hint below

In the Splunk group box Host/Ip Address, Port and Sleep (ms) are displayed as set in respective initialization parameters file, section "Splunk Settings".

To upload the scan records to Splunk, press the Splunk button and confirm the operation!
Do not interact with the application until the upload completes!

Splunk TCP Data Input Hint:

Omega DB Scanner Standalone edition uses Splunk TCP Data Input for pushing its scan records to Splunk! Just in case to avoid any overloading on both sides, thus eventual loss of records, it is recommended that you do keep a delay (sleep) time between each scan record transfer, setting defined in the "Sleep (ms)" above.

4 Appendixes

4.1 Appendix A1 - Oracle database scan account

Omega DB Scanner is Agent-less and accesses the target database in a read-only mode. Of course an Oracle user account is necessary to access the target database and perform the scan. This account is created with the CREATE SESSION only system privilege and SELECT only privileges in certain Oracle dictionary views, necessary to extract the security information.

Use the SQL commands below in 3 Steps to create the scan user account and assign privileges:

-- STEP 1. Create the user account

-- Username OMEGADBSCAN is optional, however recommended. Replace <Password> with your choice.

```
SQL>create user OMEGADBSCAN identified by <Password>;
```

-- STEP 2. Grant connect privilege

```
SQL>grant create session to OMEGADBSCAN;
```

-- STEP 3. Grant object privileges

```
SQL>grant select on DBA_ALL_TABLES to OMEGADBSCAN;
SQL>grant select on DBA_AUDIT_POLICIES to OMEGADBSCAN;
SQL>grant select on DBA_COL_PRIVS to OMEGADBSCAN;
SQL>grant select on DBA_DB_LINKS to OMEGADBSCAN;
SQL>grant select on DBA_INDEXES to OMEGADBSCAN;
SQL>grant select on DBA_LOBS to OMEGADBSCAN;
SQL>grant select on DBA_OBJECTS to OMEGADBSCAN;
SQL>grant select on DBA_PROFILES to OMEGADBSCAN;
SQL>grant select on DBA_ROLES to OMEGADBSCAN;
SQL>grant select on DBA_ROLE_PRIVS to OMEGADBSCAN;
SQL>grant select on DBA_SEGMENTS to OMEGADBSCAN;
SQL>grant select on DBA_STMT_AUDIT_OPTS to OMEGADBSCAN;
SQL>grant select on DBA_SYS_PRIVS to OMEGADBSCAN;
SQL>grant select on DBA_TABLESPACES to OMEGADBSCAN;
SQL>grant select on DBA_TAB_PRIVS to OMEGADBSCAN;
SQL>grant select on DBA_TRIGGERS to OMEGADBSCAN;
SQL>grant select on DBA_USERS to OMEGADBSCAN;
SQL>grant select on DBA_USERS_WITH_DEFPWD to OMEGADBSCAN;
SQL>grant select on PROXY_USERS to OMEGADBSCAN;
SQL>grant select on V_$CONTROLFILE to OMEGADBSCAN;
SQL>grant select on V_$DATABASE to OMEGADBSCAN;
SQL>grant select on V_$LOG to OMEGADBSCAN;
SQL>grant select on V_$LOGFILE to OMEGADBSCAN;
SQL>grant select on V_$PARAMETER to OMEGADBSCAN;
SQL>grant select on V_$PWFILE_USERS to OMEGADBSCAN;
```

Note:

Granting to DBA_USERS_WITH_DEFPWD will fail up to Oracle 10g R2; this view is introduced in Oracle 11g R1!

Alternatively (but not recommended) all the last step's (STEP 3) commands can be replaced by:

```
SQL>grant SELECT ANY DICTIONARY to OMEGADBSCAN;
```

To drop the scan user account, run the following SQL command:

```
SQL>drop user OMEGADBSCAN;
```


4.2 Appendix A2 - Oracle connectivity and Character Set support

4.2.1 Oracle Client Connectivity

Omega DB Scanner application's connectivity is supported only on 32bit version of Oracle Clients! However this is also a built-in and pre-deployed functionality of the application.

Thus you don't have to setup or install anything, at least as long as Oracle Client setting is set (default) to Native into the System Settings form; just make sure the deployed OCI files are in the same folder with the application's .exe.

You can connect also with any 32 Bit Oracle Client (11g R2 recommended), installed or instant. In case you have an OS default existing Oracle Client 64 bit, or even a Multiple Oracle Homes (Clients) environment, you can still use the built-in application's Native connectivity (default), or use another Oracle Instant Client 32 bit.

4.2.2 Character Set Support - NLS_LANG

Omega DB Scanner uses the NLS_LANG system environment variable to specify locale settings for the Oracle client software used by the application. This variable sets the language and territory and also indicates the client's character set, which corresponds to the character set for data to be entered or displayed by a client program.

The NLS_LANG is an operating system environment variable that relates exclusively to Oracle client software. In case of a clean Windows install will not be present! You can create and manage it as any other Windows environment variable. For example on a Windows 7 machine at Control Panel -> System -> Advanced System Settings - and in the System Properties form that opens, selected tab Advanced, press the "Environment Variables..." button. This will open the Environment Variables form, look for System Variables below!

If your Oracle database uses pure Latin/ASCII Western European languages character sets, you don't need to create and set the NLS_LANG at all!

You must create and set this system variable if you need to support:

- Western European Languages in full - with special characters like ë, Ë, ç, Ç, ö, Ö!
- Other single-bytes character sets
- Unicode character sets - for all languages!

The NLS_LANG environment variable has the following format:

`NLS_LANG = LANGUAGE_TERRITORY.CHARSET`

Example 1

Western European Languages full character support:

`NLS_LANG= AMERICAN_AMERICA.WE8MSWIN1252`

Example 2

Unicode character support:

`NLS_LANG= AMERICAN_AMERICA.AL32UTF8`

In general, settings of NLS_LANG are required and set according to Oracle Client Vs Oracle Database technology character sets configurations; the Omega DB Scanner uses and relies on the Oracle Client for connectivity like many other Oracle-related software do.

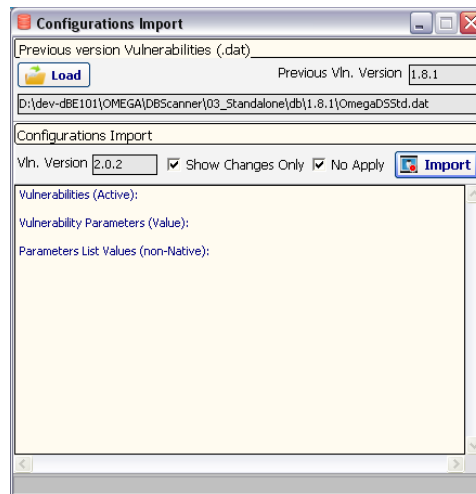
For more, see the Oracle Documentation on "Choosing a Locale with the NLS_LANG Environment Variable"!

https://docs.oracle.com/cd/E18283_01/server.112/e10729/ch3globenv.htm#insertedID2

4.3 Appendix A3 - Configurations imports (upgrade)

When you must use the new version of the OmegaDSSt.dat file after an upgrade, you must import your current configurations and authorizations which are stored into the previous' version of the OmegaDSSt.dat. These configurations and authorizations consist in Vulnerability Active status, Parameter Values and Parameter List Values.

This is done in the form "Configurations Import", which is opened by pressing the button "Configuration Import" in the form All Configurations.



Previous version Vulnerabilities (.dat) group

Load press button to load previous' version OmegaDSSt.dat

Previous Vln. Version number of the previous' version OmegaDSSt.dat

Also displayed is the full file path of the previous OmegaDSSt.dat

Configurations Import group

Vln. Version number of the current version OmegaDSSt.dat

Show Changes Only when (default) checked will display import log only for changes (imports to be performed). When unchecked will display full log output

No Apply when (default) checked will produce log report only and make no import!
When unchecked (highlighted in red color) will run the import!

Import press this button to start the procedure of importing end-user configurations and authorizations from the old OmegaDSSt.dat to the current environment

In the memo below the log of Import operation is displayed.

CHANGE	indicates an import to be performed
FIXED	no import performed
WARN	vulnerability or parameter not found in old version, ex. due to new developments in the new one

4.4 Appendix A4 - Use Case

The following provides a simplified use case and demonstration of the solution's features and operations.

Prerequisites:

1. Setup Omega DB Scanner Standalone on a new clean environment.
2. Install a new test Oracle Database 11g R2, OS independent and with the most default settings, whenever presented by the setup routine. This will be used as the target database to be scanned.
3. Omega DB Scanner is set up for the target Oracle database and ready to scan.

* Oracle 11g and above is recommended because of user accounts and objects involved in this test

Use Case Rationale:

This use case demonstrate the capabilities and approach of Omega DB Scanner Standalone when dealing with a most common security concern, wide-spread in most IT systems and not only in Oracle database: system's default accounts. We will follow some common measures in such case, consisting of:

- Reducing the attack surface by disabling unneeded components
- Revoking privileges where they are granted in excess (ex. PUBLIC)
- Replace default active privileges accounts with your own making username unknown to attacker

After the installation of the test target Oracle database, you are supposed to see (between many others) the following Oracle accounts created by default:

DBSNMP	used by the Management Agent component of Oracle Enterprise Manager
MGMT_VIEW	used by Oracle Enterprise Manager Database Control
SYSMAN	used to perform Oracle Enterprise Manager database administration tasks
SYSTEM	default generic database administrator account for Oracle databases

Refer to the following Oracle documentation on the predefined administrative accounts created:
https://docs.oracle.com/cd/E11882_01/server.112/e10575/tdpsg_user_accounts.htm#TDPSTG20301

In this use case we will:

- **remediate** the security posture of the DB by (1) locking unneeded Oracle components accounts, (2) locking the Oracle default DBA user SYSTEM and (3) revoking PUBLIC privileges from some DBMS_% packages.
- create a new DBA user account in place of the locked account SYSTEM.
- **authorize** this new DBA account in the security posture of the database by inserting the new DBA username as a parameter list value in all vulnerabilities that apply.

Watch each scan set in the form Scan Data. Use the Scan Compare form to compare each scan with the previous!

Important Note

The Revoke and Lock SQL commands given in this use case are intended for Oracle database test and demo systems only! The remediation process in reality is more complex and not always possible on every item; and this would be the case for authorization. Obviously we should authorize and not just lock the user accounts of the Oracle Agent and Enterprise, should those components be in use!

Use case Scans:

1. First scan set:

Rationale:

The first scan will assess and collect the existing database's security posture and serve as a starting point. Do perform on the test target Oracle database in its state immediately after install.

Action:

Run the 1-st scan and save it to disk!

Diagnostics:

Notice that the Oracle user accounts mentioned above count for many Findings reported - note the same accounts in the "Control Summary" field of the scan.

2. Second scan set

Rationale:

Supposedly we make no use of Management Agent, Oracle Enterprise Manager Database Control and Oracle Enterprise Manager, thus we respectively lock the unneeded DBSNMP, MGMT_VIEW and SYSMAN Oracle accounts (and we stop the components too, but this is not in the scope of this use case).

Action:

In Oracle database lock user accounts DBSNMP, MGMT_VIEW and SYSMAN with the following SQL commands:

```
SQL>alter user DBSNMP account lock;
SQL>alter user MGMT_VIEW account lock;
SQL>alter user SYSMAN account lock;
```

Run the 2-nd scan and save it to disk!

Diagnostics:

Compare Scan Run No 2 vs. Scan Baseline No 1! Notice the **improved** changes in security controls.

Control Summary contains	Control Find BS	Control Find Run	Compare Code
DBSNMP and/or MGMT_VIEW and/or SYSTEM	Finding	Correct	Control Improve
DBSNMP and/or MGMT_VIEW and/or SYSTEM + another account	Finding	Finding	Minor Improve

3. Third scan set

Rationale:

Lock the well-known Oracle DBA user account SYSTEM. It will be later replaced with a new DBA user.

Action:

In Oracle database lock user SYSTEM with the following SQL command:

```
SQL>alter user SYSTEM account lock;
```

Run the 3-d scan and save it to disk!

Diagnostics:

Compare Scan Run No 3 vs. Scan Baseline No 2! Notice the **improved** changes in security controls.

Control Summary contains	Control Find BS	Control Find Run	Compare Code
SYSTEM	Finding	Correct	Control Improve
SYSTEM + another account	Finding	Finding	Minor Improve

4. Fourth scan set

Rationale:

Revoke certain system packages Execute privilege from PUBLIC (remember we are on a test DB. In a "live" one this is easier said than done!).

Action:

In Oracle database revoke certain object privileges from the PUBLIC with the following SQL commands:

```
SQL>revoke EXECUTE on UTL_TCP from PUBLIC;
SQL>revoke EXECUTE on UTL_HTTP from PUBLIC;
SQL>revoke EXECUTE on UTL_SMTP from PUBLIC;
SQL>revoke EXECUTE on UTL_FILE from PUBLIC;
SQL>revoke EXECUTE on DBMS_RANDOM from PUBLIC;
SQL>revoke EXECUTE on DBMS_LOB from PUBLIC;
SQL>revoke EXECUTE on DBMS_SQL from PUBLIC;
SQL>revoke EXECUTE on DBMS_JOB from PUBLIC;
SQL>revoke EXECUTE on DBMS_SCHEDULER from PUBLIC;
SQL>revoke EXECUTE on OWA_UTIL from PUBLIC;
```

Run the 4-th scan and save it to disk!

Diagnostics:

Compare Scan Run No 4 vs. Scan Baseline No 3! Notice the **improved** changes in security controls.

Control Summary contains	Control Find BS	Control Find Run	Compare Code
PUBLIC	Finding	Correct	Control Improve

5. Fifth scan set

Rationale:

Create a new TESTDBA user to replace locked SYSTEM DBA account.

Action:

In Oracle database create the new user TESTDBA and grant it the DBA role with the following SQL commands:

```
SQL>create user TESTDBA identified by <password>;
SQL>grant DBA to TESTDBA;
```

Run the 5-th scan and save it to disk!

Diagnostics:

Compare Scan Run No 5 vs. Scan Baseline No 4! Notice the **declined** changes in security controls.

Control Summary contains	Control Find BS	Control Find Run	Compare Code
TESTDBA	Finding	Correct	Control Decline
TESTDBA + another account	Finding	Finding	Minor Decline

6. Sixth scan set

Rationale:

Other measures left apart (unneeded component accounts and PUBLIC privileges), in DBA terms we are exactly at the starting point, just we now have a TESTDBA (and DBA) user, instead of the default SYSTEM one.

So far we have used **remediation** (account locking, privilege revoking...) to handle the findings and improve the security posture. However in the real life it comes out that privileges are made to be used, that sometimes so are even some PUBLIC ones (your applications might need it; or your scripts need them). And that some security settings require being relaxed too for the same reasons as above; or that not every kind of audit can be set on any account, for example if the later is working application schema owner, this can overload the audit trail. And many more... .

And of course every Oracle database has at least one DBA. This is why in this round we don't revoke anything, let alone lock the account, but we use **authorization** of this new DBA account in Omega DB Scanner by inserting it's name as a parameter list value in all vulnerabilities. Thus it will not count for a Finding!

Action:

In Omega DB Scanner Standalone application, form "Parameter Multiple Operations", second tab "List Format Parameters", complete the "List Value" edit box as TESTDBA and find all vulnerability controls that contain the parameters:

- Authorized Grantees
- Authorized Users
- Authorized Owners
- Un-audited Users

Press the Add button below after every search for each the parameters above to insert the TESTDBA account name as a parameter list value in all vulnerabilities.

Run the 6-th scan and save it to disk!

Diagnostics:

Compare Scan Run No 6 vs. Scan Baseline No 5! Notice the **improved** changes in security controls.

Control Summary contains	Control Find BS	Control Find Run	Compare Code
TESTDBA	Finding	Correct	Control Improve
TESTDBA + another account	Finding	Finding	Minor Improve

Conclusions:

The use case presented so far was a simplified simulation to demonstrate the skills and features Omega DB Scanner Standalone edition. Simplification is done for the sake of the easiness of the tester; however the later is encouraged to go further in testing, as of course the use case above is just a start on the subject.

Even with the above said, care is taken that many of the features of the software are explored, and those advanced too, as for example the "Effective privilege (role hierarchy) evaluation" - demonstrated above in the impact of assigning the DBA role.

4.5 Appendix B - Technical Support and Copyrights

Support:

The Omega DB Scanner Standalone Edition is free to use in live, production, commercial and test systems! DATAPLUS is committed to its further development and improvement, as this work is a courtesy of DATAPLUS to all Oracle database security related professionals!

For product documentation, forum and knowledge base, please visit our site:

www.dataplus-al.com

For technical issues, comments, ideas and impressions, please e-mail us at:

support@dataplus-al.com

Support Levels:

- | | |
|-------------|--|
| 1. Basic | new versions, upgrades, fixes and new vulnerability controls, documentations. |
| 2. Medium | general software usage issues, for both the scanner and the Splunk interface. |
| 3. Advanced | Oracle database security support on scan output content, remediation and authorization |

The first level Basic is **free** and no strings attached! The Medium and Advanced are **commercial** options. Details on all the three options are found at our website, Omega DB Scanner part.

SLA:

Response Time SLA:	2 Business Days
Support Call/Online:	09:00 GMT to 21:00 GMT, Monday to Friday
Emergencies:	we are here to help
Resolution Time:	case-related

DATAPLUS

Tirana, Albania

Street Address: Bul. Zog I, P. "Edicom", 8F.

E-Mail: info@dataplus-al.com

Cel: +355 68 2061664

Tel: +355 42419275

Follow us on the following social media sites:

YouTube DATAPLUS channel: <https://www.youtube.com/channel/UCa59qQuGg5tvd2vIe1MsMOw>

LinkedIn DATAPLUS page: <https://www.linkedin.com/company/dataplus-al>

Peerlyst DATAPLUS page: <https://www.peerlyst.com/companies/dataplus/dashboard>

Copyright:

Copyright © 2007-2018 DATAPLUS. All rights reserved. Omega DB Scanner is registered at US Copyrights Office and is protected by US and international copyright laws. No part of this work may be reproduced, stored in a retrieval system, adopted or transmitted in any form or by any means, electronic or otherwise, translated in any language or computer language, without the prior written permission of DATAPLUS. Omega DB Scanner and the DATAPLUS logo are trademarks of DATAPLUS. All other trademarks are the property of their respective owners.