

Inhaltsverzeichnis

Inhaltsverzeichnis für Security_I (c) 1998 - 2024 by Muniqsoft Training GmbH

1. Security I

© 2002-2022 by Muniqsoft Training GmbH

Kapitel 1 Einleitung

2. Werbung: Oracle Unbreakable
3. Übersicht der Oracle Exploits (Stand 11/24)
4. Einleitung
8. Rechtliche Hinweise
9. Generelle Tipps
12. Oracle überwacht ...
13. Die größten Hackerangriffe
14. Was lernt man aus den Hackerangriffen
15. Gute Webseiten

Kapitel 2 Netzwerksicherheit

2. Einleitung
3. Listener Kompatibilität
4. Listener absichern - Logging
5. Neue Ordnerstruktur für Log / Trace
6. Allgemeines zur Log-Datei
7. Listener absichern – Änderungen verhindern
8. Listener absichern – Tracing
9. Dynamische Listener-Registrierung
10. Externe Prozeduren (Security Alert #29)
12. Tipps & Tricks
13. Überprüfen der Netzwerkdateien
14. Hashen der Netzwerkdateien
15. Überprüfen der Listener.log
16. Listener.log als External Table
17. Überprüfen der Listener.log
18. Clients von Anmeldung ausschließen

Inhaltsverzeichnis

19. Erweitertes Valid Node Checking (VNC)
20. Erweitertes Valid Node Checking
21. Netzwerkverschlüsselung
23. SQLNET.ORA Parameter
24. Integritätsprüfung (Stand 04/2021)
25. Einstellung in der SQLNET.ORA
26. Client/Server Einstellkombinationen
27. Funktionstest der Verschlüsselung
28. Prüfung ob Verschlüsselung in sqlnet.ora
29. Prüfung durch Tracing des Netzverkehrs
30. Zusammenfassung wichtiger Parameter

Kapitel 3 Betriebssystem-Sicherheit

2. Tipps für Linux / Unix
3. Passwörter knacken
4. Eigene Mount Points
5. Fail2Ban
6. VPN Server
7. Firewall
8. UNIX Remote Anmeldung als root verhindern
9. Benutzer in Gruppen via SSH anmelden
10. SSH-Schlüssel statt Passwörter
11. Anmeldung mit Passwort verbieten
12. Rechtevergabe
13. Mitgliedschaft in Gruppen prüfen
14. Chronik der Shell löschen
15. Historyeinträge verhindern
16. Start von Skripten
17. Dateirechte
18. Stichpunkte für Sicherheitschecks
19. Tipps für Windows
20. Doskey
21. Windows Netzwerkfreigaben
22. Windows Autostart-Programme
23. Berechtigungen innerhalb der Registry
24. Anzeige der Windows Benutzer/Gruppen
25. Überwachung fehlerhafter Anmeldungen
26. Firewalls

Inhaltsverzeichnis

- 27. Windows Firefall konfigurieren
- 29. Firewall Probleme
- 30. Ausführen - Verlauf löschen
- 31. Bildschirmschoner
- 32. Fail2Ban unter Windows
- 33. Windows Updates
- 34. Passwörter knacken
- 35. Autologon / Pagefile

Kapitel 4 Init.ora Parameter

- 2. INIT.ORA Parameter (Nicht dokumentiert)
- 3. INIT.ORA Parameter
- 11. INIT.ORA Parameter Änderungen
- 13. INIT.ORA Parameter
- 24. Prüfung mittels SELECT

Kapitel 5 Audit

- 2. Audit
- 3. Init.ora Parameter AUDIT_TRAIL
- 4. Allgemeines

Inhaltsverzeichnis

6. Audit-Arten
7. Audit-Einstellungen
8. Objekt Auditing
9. Privileg Auditing
10. Syntax für Privileg Auditing
11. Beispiele
13. Syntax für Objekt-Auditing
14. Mögliche Objekt-Audits
15. Beispiel für Objekt-Auditing
17. Objekt-Auditing
18. Auswertung des Objekt-Audits
19. Welche Systemrechte überwachen?
20. Was soll überwacht werden – Beispiel
21. Privileg-Auditing ausschalten
22. Beispiele
23. Objekt-Auditing ausschalten
24. Beispiele
25. Auswertung des Audits
26. Verschieben der Audit-Tabelle
27. Automatisches Audit (ab 11g)
28. Tablespaceänderung von AUD\$ (ab 11g)
29. Verzeichnisänderung für Audit-Logs
30. Aufräumen in den Audit-Logs
31. Einträge vom Audit ausschliessen
32. Automatisches Aufräumen in Audit-Logs
33. Auswertung des SYS Audits unter Windows
34. Auswertung des SYS Audits unter Unix
35. Fine Grain Auditing
37. Erklärung der Parameter
38. Mögliche Operationen mit FGA
40. FGA auf mehrere Spalten
41. Tabellen für FGA
42. Wichtige Data Dictionary-Views

Kapitel 6 Unified Auditing

2. Audit bis Version 11.2
3. Rückwärtskompatibilität
4. Empfehlungen
5. Unified Auditing
6. Unified Auditing alleinig aktivieren
8. Unified Auditing Speichermethoden
10. Wo wird das Audit gespeichert?
11. Unified Auditing – Rechte
12. Lebenszyklus der Audit Policy
13. CREATE AUDIT POLICY Syntax
14. AUDIT POLICY Syntax
15. Unified Auditing – WHEN-Klausel
16. Beispiele zur WHEN Klausel
17. Audit aktivieren
18. Audit deaktivieren
19. Unified Auditing – Beispiel: DML Befehle
20. Unified Auditing – Beispiel: Rollen
21. Unified Auditing – Beispiel: Privilegien
22. Interessante Privilegien zum Audit
23. Unified Auditing – Beispiel: Packages
24. Interessante Packages zum Audit
25. Unified Auditing – Beispiel: Packages
26. Audit auf Objekte
27. Unified Auditing – Weitere Beispiele
28. Unified Auditing – SQL*Loader
29. Vordefinierte Policies
30. Policy Änderung
31. Policy Änderung – Beispiel
32. Audit Auswertung
33. Unified Audit Tabellenspalten (Auswahl)
34. Audit löschen
35. Audit Einträge zeitgesteuert löschen
36. Zeitstempel setzen
37. Audit Einträge manuell löschen
38. Audit Einträge löschen in Read Only DB
39. Mandatory Auditing
40. Auditierung des Sys Benutzers

41. Audit Views

Inhaltsverzeichnis

Kapitel 7 Diverses

2. Diverses
3. GLOGIN.SQL
4. LOGIN.SQL
5. Schutz der Backups/Klone
6. Schutz der Redologdateien
7. SQL*Plus Schutzmechanismen

Kapitel 8 Rechte

2. Einleitung
4. Rechte bei Rollen
5. Rechte mit ANY
6. Top 10 der wichtigsten Rechte für Entwickler
7. Top 15 der wichtigsten Rechte für DBA
8. Top 20 der gefährlichsten Rechte
10. Neue Rechte in 12.1.0.2
11. Neuerung bei Rechten in 12.1.0.2
12. Gefährliche Rechte
15. Rechte Scoring
16. Privilegien-Eskalation
20. WITH ADMIN / GRANT OPTION
21. Was macht ein Hacker?
24. Öffentliche Rechte
26. Gefährliche Java Rechte
27. Inherit Privileges (ab 12c)

Inhaltsverzeichnis

28. Inherit Privileges
29. Beispiel zu Inherit Privileges
31. Packageaufruf
32. Doppelte Packages
33. Gefährliche Packages
37. Volle Schema-Qualifizierung
38. Gefährliche Packages an Public
39. Gefährliche Packages
40. Oracle Maintained Rollen/Benutzer
41. Application Roles (EE)
42. Ports sperren bzw. freigeben
43. DBMS_NETWORK_ACL_ADMIN (12c)
44. Fine Grain Access für andere Rechner (12c)
45. DBMS_NETWORK_ACL_ADMIN (ab 12c)
46. Beispiel zu APPEND_HOST_ACE
47. Parameter zu APPEND_HOST_ACE
49. Beispiel zu REMOVE_HOST_ACE
50. ACL Views
51. ACL – Was sollte vermieden werden?
52. Externe Authentifizierung der Rollen
53. Data Dictionary Zugriff
55. Rechte auf Views
56. SELECT/UPDATE Rechte Bug
57. DBMS_PRIVILEGE_CAPTURE (ab 12c)
58. Ablauf der Rechteerfassung
59. CREATE_CAPTURE-Prozedur
60. CREATE_CAPTURE – Beispiele
62. Start bzw. Ende der Erfassung
63. Übersicht der Ausgabe
64. Beispielausgabe
65. Kostenfreie Alternative
66. Neu ab 23ai: Schema Rechte
67. Rechte an Objekten in einem Schema
68. Beispiele

Inhaltsverzeichnis

Kapitel 9 Rollen

2. Rechte bei Rollen
3. Verschiedene Rollen in den Versionen
4. Standard Rollen

7. Data Dictionary Rollen
8. Standard Rollen und deren Rechte
9. Neue Rollen in 12-23c
12. Rollen ab 12c (Database Vault)
13. Rollen ab 12c (DV)
14. Rollenkonzept in PL/SQL
16. Das Rollenkonzept in PL/SQL
17. Secure Application Roles (EE)
20. Rollen an PL/SQL-Code vergeben (ab 12c)
21. Rollen an PL/SQL-Code vergeben – Beispiel
22. Rollen an PL/SQL-Code vergeben - Beispiel

Kapitel 10 Benutzer

2. Einleitung
3. Schema Only Accounts (ab 18c)
4. Benutzeridentifizierung
6. Benutzer
7. SYSDBA Ersatz
8. Anmeldung als SYSBACKUP
9. Administrationsbenutzer
10. Übersicht der Rechte pro Benutzer
11. Wie kann man Accounts schützen?
12. Proxy User
14. Proxy User – Anmeldung
15. Proxy User – Verwaltung

Inhaltsverzeichnis

- 16. Einige Demo-Schemata
- 17. Extra Monitoring Benutzer
- 18. Technische Benutzer

Kapitel 11 Passwörter

- 2. Benutzerpasswörter
- 3. Optimierung von Passwörtern
- 4. Benutzerpasswörter
- 5. Die häufigsten Passwörter (Rockyou Webseite)
- 6. Zeit zum Knacken des Passworts
- 7. Passwort ändern auf dem Client
- 8. Passwort-Hackmethoden
- 11. Benutzerpasswörter (APEX)
- 12. Benutzerpasswörter
- 19. Passwörter in Skripten
- 20. Passwörter für Skripten die DB speichern
- 21. Schutz durch Profile
- 25. Schutz durch Passwort-Funktion
- 28. Die Passwort-Funktion als Spion ?
- 29. Neue Passwort-Prüffunktion in 12c
- 30. Hinweis zur Passwort-Funktion
- 31. Neuer Profil Parameter (ab 21c)
- 32. Lockdown Profil (ab 12.2)
- 33. Lockdown Profil
- 34. Lockdown Profil – Beispiele

Inhaltsverzeichnis

- 36. Anmeldung mit verschlüsseltem Passwort
- 39. Netzwerkdateien anpassen
- 41. Anmeldung mit verschlüsseltem Passwort
- 42. Wartung der Wallet Einträge
- 43. Übersicht der Kommandos von mkstore
- 45. Neuer / alter Password Hash
- 47. Abschalten des alten PWD Algorithmus
- 49. Neue Passwortverschlüsselung in 12.1.0.2

Kapitel 12 Trigger

- 2. Überwachung mittels Trigger
- 3. Trigger – Beispiel
- 4. Systemrechte für Trigger
- 5. Problemstellung zu DDL Triggern
- 6. Logon Trigger – Beispiel
- 7. System Trigger
- 8. System Trigger – Beispiel
- 9. System Trigger
- 10. DDL Trigger
- 15. DDL Trigger – Beispiel

Kapitel 13 Row Level Security

- 2. Row Level Security (VPD) Einleitung
- 4. Query Ergänzung
- 5. Notwendige Rechte

Inhaltsverzeichnis

- 6. Konzeptbeispiel
- 7. Besonderheiten
- 9. Beispiel
- 10. Logon Trigger
- 11. LOGON TRIGGER Syntax
- 12. SYS_CONTEXT
- 13. Application Context
- 14. sys_context Parameter (Auswahl)
- 19. SYS_CONTEXT Beispiele
- 21. Eigene Context Funktionen
- 23. Beispiel: Eigener Context
- 26. DBMS_RLS Konfiguration
- 28. Hinweis zur RLS Funktion
- 29. DBMS_RLS Konfiguration
- 30. DBMS_RLS Komplettparameter
- 31. DBMS_RLS Konfiguration
- 33. Hinweise zu den RLS Policy Parametern
- 37. Performance durch POLICY_TYPE
- 40. Empfehlungen für die Einstellungen
- 43. Policy Type Matrix
- 44. Hinweise
- 46. Filter-Beispiele
- 47. Filter Beispiele

Inhaltsverzeichnis

48. Refresh Policy
49. Policy nachträglich ändern
50. Generelle Beispiele
51. Spalten ausblenden
52. Ausblenden von Spalten
53. DBMS_RLS – Weiteres Beispiel
54. Weitere Beispiel: Spalten verstecken
56. sec_relevant_cols_opt=DBMS_RLS.ALL_ROWS
57. sec_relevant_cols_opt=NULL
58. Praxisbeispiele
59. Praxisbeispiel 1
60. Praxisbeispiel 1 – User anlegen
61. Praxisbeispiel 1 – Rechte vergeben
63. Beispiel 1 – Context und Package anlegen
64. Praxisbeispiel 1– Package Body erstellen
65. Praxisbeispiel 1 – On Logon Trigger
66. Praxisbeispiel 1 – Policy Funktion erstellen
67. Praxisbeispiel 1 – Alles testen
68. Beispiel 2: Einleitung
69. Beispiel 2: Rollen anlegen
70. Beispiel 2: Funktion anlegen
71. Beispiel 3: Policy anlegen
72. Ungünstige Szenarien
73. Beispiel 2: Test
74. Debugging der Filter
78. Debugging der Filter mittels Tracing
79. Grenzen der Filter
80. Debugging der Filter mittels Tracing
81. Views zu den Policies
83. Gruppen Policies
84. Einleitung Gruppen Policies
85. DBMS_RLS POLICY GROUPS
86. Gruppe erstellen
87. Gruppe mit Policy erstellen
88. Grouped Policy erstellen
89. Funktion zum Spaltenausblenden

Inhaltsverzeichnis

- 90. Context erzeugen
- 91. Context zur Poliy hinzufügen
- 92. Jeweilige Gruppe aktivieren
- 93. Gruppe löschen
- 94. Gruppe ausschalten
- 95. Gruppe wieder einschalten
- 96. Gruppe refreshen
- 97. APEX und VPD
- 99. APEX VPD Beispiel
- 103. Trigger liest APEX Variablen aus
- 107. Tabelle und Trigger in DB anlegen
- 108. APEX Schritte

Kapitel 14 Verschlüsselung

- 2. Einleitung
- 3. Übersicht über Verschlüsselungskonzepte
- 4. Die TRANSLATE-Funktion
- 5. Verbesserung der Low-Level Verschlüsselung
- 6. Datenkonvertierung in RAW
- 7. XOR Verschlüsselung
- 8. Vor und Nachteile von XOR
- 9. DBMS_OBFUSCATION Toolkit
- 10. DBMS_OBFUSCATION
- 12. DBMS_CRYPTO
- 14. DBMS_CRYPTO – Verschlüsselung
- 15. DBMS_CRYPTO – Beispiel
- 16. Übersicht der Konstanten
- 20. Gängige Verschlüsselung-Typen

Inhaltsverzeichnis

- 21. Empfehlungen
- 22. Verschlüsselung durch das BS
- 24. Data Pump Verschlüsselung (EE)
- 25. RMAN Backup Verschlüsselung
- 26. Wrapping
- 27. PL/SQL Code-Wrapping
- 28. Online Wrapping

Kapitel 15 Wallet und TDE

- 2. Einleitung
- 3. Rechte
- 4. Anmeldung als SYSKM
- 5. Wallet konfigurieren
- 7. Wallet Parameter (ab 19c)
- 10. Wallet erzeugen (Non-CDB)
- 11. Wallet erzeugen (Autologin, Non-CDB)
- 12. Autologin Wallet
- 14. Wallet nachträglich zum Autologin machen
- 15. Wallet erzeugen (CDB)
- 16. Wallet öffnen
- 17. Wallet (Keystore) sichern
- 18. Wallet (Keystore) sichern mit Tag
- 19. Wallet Passwort ändern
- 20. Wallet Rekeying
- 21. Übersicht der letzten Keys
- 22. Wallet schließen
- 23. Oracle Wallet Manager (OWM)
- 24. Oracle Wallet Manager – Menü Wallet
- 25. Oracle Wallet Manager – Menü Vorgänge
- 26. Spalten verschlüsseln
- 30. Restriktionen der Spaltenverschlüsselung
- 31. Tablespaces verschlüsseln

Inhaltsverzeichnis

- 32. Tablespace Verschlüsselung
- 33. Nachträgliche Tablespace Verschlüsselung
- 34. Vergleich verschlüsselt/ unverschlüsselt
- 35. Live Conversion (ab 12.2)
- 36. Prüfung der Verschlüsselung
- 37. Default Verschlüsselung für neue TBS
- 38. Beschränkungen der TBS Verschlüsselung
- 40. Fehler ORA-28374
- 41. Fehler ORA-46635
- 42. Fehler ORA-28365
- 43. Performance Auswirkungen
- 44. Verschlüsselung in der Pluggable Database
- 45. TDE in der Pluggable Database
- 47. TDE Master Key erstellen
- 48. TDE in der Pluggable Database
- 49. Klonen einer Pluggable Database
- 50. Klonen einer PDB
- 51. Erstellen einer PDB
- 52. Unplug / Plug einer PDB

Kapitel 16 PL/SQL Security

- 2. Einleitung
- 3. EXECUTE IMMEDIATE
- 4. EXECUTE IMMEDIATE – Syntax
- 5. EXECUTE IMMEDIATE – Beispiel
- 6. EXECUTE IMMEDIATE – Fallen
- 8. Dynamische Cursor – REF CURSOR
- 9. REF CURSOR – Beispiel
- 10. REF CURSOR
- 11. Sichere und unsichere Ref Cursor
- 12. Starke und schwache REF CURSOR
- 13. REF CURSOR als Return-Typ einer Funktion
- 14. DBMS_SQL
- 15. Wann braucht man DBMS_SQL

Inhaltsverzeichnis

19. Generischer Code für DDL-Befehle
20. gefährliche Module für SQL Injection
21. DBMS_ASSERT
29. Reguläre Ausdrücke
30. Prüfung durch Konvertierung
31. VALIDATE_CONVERSION (ab 12.2)
32. Konvertierungsfehler abfangen (ab 12.2)
33. CAST-Funktion bei Fehlerbehandlung (12.2)

Kapitel 17 Verschleierung

2. Einleitung
3. Redaction (Oracle 12c EE+ASO)
4. Redaction Einschränkungen
5. Neue System Rechte für Redaction
6. Weitere Packageaufrufe vom DBMS_REDACT
7. Tipps & Tricks zu den Parametern
10. Beispiele zum Expression Parameter
11. Vordefinierte Shortcuts
12. Beispiele für die Parameter
13. Beispiel für Partial auf String Spalten
14. Function String
15. Redaction VerwaltungsvIEWS
16. DBMS_REDACT – komplettes Beispiel
17. DBMS_REDACT – Beispiel
18. Änderung der Verschleierungswerte
19. Probleme mit DBMS_REDACT
20. Transparent Sensitive Data Protection
21. Views

Inhaltsverzeichnis

22. Rechte
23. Einrichtung der TSDP
24. Import der Daten durch Cloud Control
25. Einrichtung der TSDP für Number Spalte
26. Einrichtung der TSDP für Char Spalte
27. Einrichtung der TSDP
28. Policy für weitere Spalten aktivieren
29. Policy löschen
30. Nachträgliches Ändern der Policy
31. Auswahl der Spalten im EM
32. Notizen

Anhang A Checkliste

2. Einleitung
3. Passwörter ändern/Benutzer sperren
4. Rechteüberprüfung/Netzwerk
5. INIT.ORA Parameter Prüfung
6. Prüfung auf neusten Patch
7. Prüfung auf neuen PWD Algorithmus
8. Welche Policies sind im Einsatz
9. Welche Directories sind angelegt
10. Welche DB Links existieren ?
11. Welche Objekte sind verschlüsselt?
12. Wird die Passwort Prüf Funktion verwendet ?
13. Prüffunktionen
14. Welche Objekte wurden kürzlich neu erzeugt?

Anhang B Central Managed User

2. Voraussetzungen
3. Anlegen eines Oracle Service Account
4. Anlegen des Oracle Users im AD
5. Rechtevergabe an den Benutzer im AD
8. Tool opwdintg.exe
9. Root Certificat vom AD Server holen
10. Neue AD Gruppen
11. SQLNet Konfiguration

Inhaltsverzeichnis

12. Datei dsi.ora
13. Wallet einrichten
15. MS ActiveDirectory Server Root Zertifikat
16. DB Parameter ändern
17. DB Benutzer einrichten
18. Globale Rollen
19. Anmeldung an der DB
20. Prüfung der Verbindung
21. Allgemeines zum AD Konto

Übungen

12. Notizen

Lösungen

- 2. Lösungen zu Kapitel 2: Netzwerksicherheit**
- 3. Lösungen zu Kapitel 3: Betriebssysteme**
- 4. Lösungen zu Kapitel 4: init.ora**
- 5. Lösungen zu Kapitel 5: Audit**
- 6. Lösungen zu Kapitel 5: Audit**

Inhaltsverzeichnis

7. Lösungen zu Kapitel 6: Unified Auditing
8. Lösungen zu Kapitel 7: Verschlüsselung
9. Lösungen zu Kapitel 8/9 Benutzer/Rechte
10. Lösungen zu Kapitel 11: Passwörter
11. Lösungen zu Kapitel 12: Trigger
12. Lösungen zu Kapitel 12: Trigger
13. Lösungen zu Kapitel Checkliste
14. Notizen