

Inhaltsverzeichnis

Inhaltsverzeichnis für APEX_SEC (c) 1998 - 2023 by Muniqsoft Training GmbH

Kapitel 1 Einleitung

- 2. Oracle ist Unbreakable
- 3. Übersicht der Oracle Exploits
- 4. OWASP

- 6. Einleitung
- 10. Rechtliche Hinweise
- 11. Übersicht zum Thema Sicherheit
- 12. Generelle Tipps
- 15. Oracle überwacht ...
- 16. Interessante Links

Kapitel 2 Sicherheitsprüfungen

- 2. Übersicht des Security Bereichs
- 3. Was lässt sich in APEX schützen ?
- 4. Einrichtung der Prüfung
- 6. Vorlagen der Prüfung
- 7. Ideen für Prüfungen
- 9. Beispiele für Prüfroutinen
- 10. Liste der nutzbaren Seite in Tabelle
- 11. Sicherheitsprüfung einer Seite
- 12. Sicherheitsprüfung bei Reports
- 13. Sicherheitsprüfung bei Items/Buttons/Spalten
- 14. Manipulationsmöglichkeiten
- 15. Session State Protection
- 16. Session State Protection: Einstellungen
- 17. Prüfsummen
- 18. Itemwerte selbst verschlüsseln
- 19. Beispiel: Hidden-Elemente verschlüsseln
- 20. Beispiel: Hidden-Elemente entschlüsseln

Inhaltsverzeichnis

- 21. Report=>Formular ID Verschlüsselung
- 23. Gefälschte Formularwerte
- 24. Gefälschte Formularwerte: Lösung
- 26. Länge der Eingabefelder
- 27. Automatische Prüfung der Feldlänge
- 28. Application Items

Kapitel 3 Verschlüsselung

- 2. Einleitung
- 3. Übersicht der Verschlüsselung
- 4. Der Translate Befehl
- 5. Datenkonvertierung in RAW
- 6. XOR Verschlüsselung
- 7. DBMS_CRYPTO
- 8. DBMS_CRYPTO Verschlüsselung
- 9. dbms_crypto Beispiel
- 10. Gängige Verschlüsselung-Typen
- 11. Empfehlungen
- 12. Verschlüsselung von Spalten (EE)
- 13. Wallet konfigurieren
- 14. Wallet
- 15. Spalten verschlüsseln
- 18. Kostenlose Spaltenverschlüsselung
- 19. Verschlüsselung von Oracle Passwörtern
- 20. Redaction (Oracle 12c EE+ASO)
- 21. Redaction Einschränkungen
- 22. Weitere Packageaufrufe vom DBMS_REDACT
- 23. Tipps & Tricks zu den Parametern
- 26. Beispiele zum Expression Parameter
- 27. Vordefinierte Shortcuts
- 28. Beispiele für die Parameter
- 29. Redaction VerwaltungsvIEWS
- 30. DBMS_REDACT Beispiel

Inhaltsverzeichnis

- 32. Probleme mit DBMS_REDACT
- 33. Wrapping
- 34. PL/SQL Code-Wrapping
- 35. Online Wrapping

Kapitel 4 SQL Injection

- 2. SQL Injection Einleitung
- 3. Was ist möglich mit SQL Injection
- 5. SQL Injection
- 8. SQL Injection Beispiel:
- 9. SQL Injection Tipps & Tricks
- 10. Gefährliche Module für SQL Injection
- 11. Ausführungsplan gegen SQL Injection
- 12. Items gegenüber Sonderzeichen schützen
- 14. Modales Fenster für aktuelle Items
- 15. SQL Injection: Lösungen
- 19. SQL Injection und reguläre Ausdrücke
- 20. Eingabe des Benutzers maskieren
- 21. Validation mit Zeichenfilter

Kapitel 5 APEX Repository

- 2. Einführung
- 3. APEX Repository (Reports)
- 4. APEX Repository (Applikations Prozesse)
- 5. APEX Repository (Seiten Prozesse)
- 6. APEX Repository (Computations)
- 7. APEX Repository (Page Charts)
- 8. APEX Repository (Validierungen)
- 9. APEX Repository (Authentifizierungen)

Inhaltsverzeichnis

Kapitel 6 APEX & VPD

- 2. APEX und VPD (nur in Enterprise Ed.)
- 3. APEX VPD Beispiel
- 8. Policy refreshen / löschen
- 9. Policy deaktivieren / aktivieren
- 10. Trigger liest Apex Variablen
- 11. Trigger liest APEX Variablen aus
- 15. Tabelle und Trigger in DB anlegen
- 16. APEX Schritte

Kapitel 7 Authorisierung

- 2. Benutzergruppen
- 4. Benutzerauthentifizierung
- 5. Benutzerauthentifizierung durch LDAP
- 6. Hinweis für Benutzer in LDAP
- 7. Benutzerauthentifizierung durch LDAP
- 8. AD Prüfung auf DOS Ebene
- 9. Prüfung der AD Authentisierung
- 10. Eigene Authentifizierung der Benutzer

Kapitel 8 SSL

- 2. Allgemeine Sicherheitsbetrachtungen
- 3. Einrichtung von SSL Verbindungen
- 4. Wallet
- 6. Internes Gateway mit SSL
- 7. Einrichtung im TomCat

Inhaltsverzeichnis

9. Let's encrypt auf Ubuntu
10. Let's encrypt auf Centos
11. Automatische Aktualisierung des Zertifikats

Kapitel 9 ACLs

2. Oracle 11g und ACL
3. ACLS Beispiel in 11g
4. Fine Grain Access für andere Rechner
5. Package dbms_network_acl_admin
6. APPEND_HOST_ACE Beispiel für >=V 12
7. APPEND_HOST_ACE Parameter
9. Freigabe aufheben
10. ACL für User einrichten
11. ACL Views ab 12c
12. SQL Developer ACL bei Remote Debugging

Kapitel 10 Diverses

2. Verfügbarkeit der Applikation
3. Session Timeout
4. Cross Site Scripting
5. HTTP Packages gegen Cross Site Scripting
6. HTF Escaping Beispiel
7. White List / Black List
8. Download von Reports (Classic)
9. Download von Reports (interactive Reports)
10. Formularschutz
11. Site Access Control
12. Seite Access Control
13. Benutzer und Passwörter
14. Neuer Admin für Internal Workspace
15. Überwachung von Logins
16. Hidden & Protected
17. Anmeldung über mehrere Apps hinweg
18. Diverse APEX Security Tipps
20. APEX Runtime Installation
21. Parameter von apex_instance_admin

Inhaltsverzeichnis

- 22. Weitere Parameter von apex_instance_admin
- 24. Tracing / Logging ausschalten
- 25. Internal Workspace / Security
- 28. APEX Security Check Tools

Kapitel 11 Webserver Security

- 2. Allgemeines
- 3. Tomcat Installation (Unix)
- 4. TomCat start/stop
- 5. TomCat Konfig-Datei
- 6. TomCat mit SSL
- 7. SSL als verpflichtende Verbindung
- 8. Verzeichnisse des TomCat
- 9. Root Seite vom TomCat
- 10. Diverses
- 11. TomCat als Non Root User (Unix)
- 12. TomCat als normale Benutzer (Win)
- 13. Diverses
- 14. Schutz vor Brute Force Attack
- 15. Server Banner unterdrücken
- 16. Stehlen oder manipulieren von Sessions

Kapitel 12 Apache Security

- 2. Einleitung
- 3. Prüfungen
- 4. Apache Version aktualisieren
- 5. Apache Konfiguration
- 6. Weitere Interessante Informationen
- 7. Test String
- 8. CGI Parameter
- 12. Apache Rewrite Regeln
- 13. Virtuelle Verzeichnisse

Inhaltsverzeichnis

14. Virtuelle Verzeichnisse: AllowOverride
15. Virtuelle Verzeichnisse: Options
17. Virtuelle Verzeichnisse: Order, Allow, Deny
19. Beispiele zu allow,deny
20. Beispiele zu Zugriffen: Require
21. Virtuelle Verzeichnisse Beispiele
22. Apache als Reverse Proxy
24. Apache Security Tipps
25. Berechtigungen
26. Apache Security Tipps
27. Log File Format
28. Log File Format Parameter
29. Log File Format
30. Apache HTTP-Header Einstellungen
34. Apache HTTPS einrichten
35. robots.txt
36. Was ist HSTS?
37. Wie kann man HSTS aktivieren?
38. Weitere praktische Unix-Packages
39. Whois installieren
40. at installieren
41. at Kommando unter Linux
42. Hackerangriffe via Firewall blocken
43. Apache Logfiles per SQL auswerten
44. External Table auf Logfile
45. Beispiel für die Auswertung
46. Geo Blocking Installation
47. Geo Blocking Konfig
48. Blacklisting
49. Whitelisting
50. Geo Blocking

Inhaltsverzeichnis

Kapitel 13 mod_security

2. Einleitung
3. Was kann mod_security erkennen ?
4. Wie funktioniert mod_security?
5. Vorab-Prüfungen
6. mod_security auf CentOS 7 (RHEL 7) installieren
7. mod_security Modul in Apache aktivieren
8. Prüfen ob alles richtig geladen hat
9. Wichtige Parameter
10. Audit reduzieren
11. Regeln ausschalten
12. Regeln mit Bedingung ausschalten
13. Regeln für bestimmte Pfade setzen

Kapitel 14 Nginx Security

2. Einleitung
3. Installation des NGINX
4. Tests
5. Let's encrypt mit NGINX
6. Defaults.conf Datei
9. Geo Blocking
10. Geo Update
11. Log Format

Kapitel 15 LDAP-Authentifizierung

2. LDAP Authentifizierung
4. beispielhafte Vorgehensweise
5. Access Control List freischalten
7. LDAP Authentifizierung
8. Authentication: Applikations-Ebene

Inhaltsverzeichnis

- 12. Authentication: Workspace-Ebene
- 14. LDAP-Benutzer in APEX anlegen
- 15. Anmeldung testen
- 16. LDAP Group Authorization
- 19. Plugin LDAP Group Authorization
- 20. Post Authentication Function

- 2. Übungen 1**
- 3. Übungen 2**
- 4. Übungen 3**
- 5. Übungen 4**
- 6. Übungen 5**
- 7. Übungen 6**
- 8. Übungen 10**

- 2. Lösungen zu Kapitel 1**
- 3. Lösungen zu Kapitel 1**
- 4. Lösungen zu Kapitel 1**
- 5. Lösungen zu Kapitel 1**
- 6. Lösungen zu Kapitel 2**
- 7. Lösungen zu Kapitel 3**

Inhaltsverzeichnis

- 8. Lösungen zu Kapitel 3
 - 9. Lösungen zu Kapitel 3
 - 10. Lösungen zu Kapitel 3
 - 11. Lösungen zu Kapitel 3
 - 12. Lösungen zu Kapitel 3
 - 13. Lösungen zu Kapitel 3
 - 14. Lösungen zu Kapitel 4
 - 15. Lösungen zu Kapitel 5
 - 16. Lösungen zu Kapitel 10
 - 17. Lösungen zu Kapitel 10
 - 18. Notizen
-
- 2. Impressum