APEX Security - Wie sicher sind Ihre Anwendungen?

Denes Kubicek
BI-Cubes
Bensheim

Schlüsselworte:

APEX, Security, APEX 5.0, Sichere Anwendungen

Einleitung

APEX hat mit den Versionen 4.1 und 4.2 gleich mehrere große Schritte in Punkto Sicherheit gemacht.

In früheren Versionen war es möglich z.B. Hidden und Protected Items zu manipulieren – Firebug / HTML Code / Checksum / Fehlermeldung. Mit der Version 4.2 ist APEX vergleichbar sicher wie die Oracle Datenbank selbst Sicherheitsmechanismen sind keine Higlights – dadurch erreicht man keine sichtbaren Verbesserungen in der Anwendung.
Dadurch erreicht man vor allem Anwendungen, die gegen Manipulationen geschützt sind
Eine Anwendung ist nie sicher genug bzw. nicht jede Anwendung benötigt das gleiche Sicherheitslevel.

APEX Security

APEX 4.2 – Session State Protection Settings für Page Items, Application Items und Seiten

APEX kann folgende Elemente in Session-State schützen:

- Seiten
- Seitenelemente (Eingabe und Display)
- Anwendungselemente

APEX verfügt über vier bzw. fünf Levels der Protection für die Elemente (Seitenelemente und Anwendungselemente):

- Unrestricted
- Checksum Required

- Application,
- Session und
- User Level

May not be set from Browser für Anwendungselemente und Display Elemente

Session State Protection – per Funktion erstellen – URL‘s im SQL

Manchmal können URL‘s nicht an der vordefinierten Stelle erstellt werden. Dynamische URL‘s werden dann im SQL zusammengestellt:

apex_util.prepare_url

API wird zum Einsatz kommen, falls eine Prüfsumme erstellt werden muss. Diese Fuktion kennt drei Modi bzw. sechs Werte für den Typ der Prüfsumme:

SESSION oder 3,

PRIVATE_BOOKMARK oder 2,

PUBLIC_BOOKMARK oder 1

Hidden Items / Display Only Items / Read Only Items

Ein vernünftiger Schutz der Hidden-Items kam mit der Version 4.0. Davor war eine Manipulation der Items mit Hilfe von Firebug möglich. Mit den Versionen 4.1 und 4.2 wurde ein Zusatzschutz eingeführt für die Items vom Typ:

Display Only

Conditional Read Only Items Ein vernünftiger Schutz der Hidden-Items kam mit der Version 4.0. Bei dem Item Typ „Display Only“ kann die Option „Save Session State“ zusätzlich aktiviert werden. „Read Only“ Bedingung dagegen schützt ein Item von jeglicher Manipulation wenn die Kondition wahr ist.

No URL Access für Seiten – wie schütze ich eine Seite von URL Manipulation?

In manchen Anwendungen können Seiten existieren, die nicht per URL erreicht werden sollen. Für diese Zwecke setzt man die Seite auf „No URL access“ unter Security – Page Access Protection. Dadurch ist es nicht mehr möglich durch die Manipulation der URL auf die Seite zu gelangen.

HTTPS Access in einer Anwendung aktivieren

Wenn die Anwendung im HTTPS Modus betrieben werden muss, kann HTTPS im Internal Workspace unter Manage Instance > Security aktiviert werden.

Beispiel einer zentralen Anwendung als Loginanwendung mit Deep Linking und HTTPS – Session Cookie

Anwendungen können im Workspace installiert werden und miteinander über den sog. Session Cookie verbunden werden. Eine Zentrale Anwendung hat die Aufgabe die Logins zu steuern. Die restlichen Anwendungen im Verbund leiten alle Logout- bzw. Invalid Session Anfragen auf die Zentrale Anwendung.

Application Item Scope – Global

Application Item – Anwendungselement – mit der Einstellung Global, kann von mehreren Anwendungen benutzt werden. Achtung! Muss in jeder Anwendung erstellt werden, damit es benutzt werden kann. Da die Anwendungselemente keine Anzeigewerte sondern nur Session State haben, sind diese gegen eine Manipulation viel besser geschützt

Wenn der Schutz richtig eingestellt ist, kann ein Anwendungselement unmöglich durch einen Anwendungsbenutzer verändert werden.

Der Vorteil von dem Anwendungselemente mit Scope Global ist, dass die Informationen zwischen der Anwendungen ausgetauscht werden können, ohne, dass eine erneute Abfrage aus der Datenbank notwendig ist.

Authorization

Eine der wichtigsten Funktionen, die oft falsch eingesetzt wird. Wir erklären, wie man Authorization effizient einsetzten kann und dabei keine Performance-Nachteile tragen.

Authentication

Wir erklären auch verschiedene Möglichkeiten die Authentifizierung an die bestehenden Systeme anzukoppeln.

APEX 5.0 und Security

Wir zeigen die wichtigsten neuen Features bezüglich Security in APEX 5.0

Fazit

Security wird groß geschrieben und meistens am Ende vernachlässigt. Wir werden versuchen zu erklären, wie man ein vernünftiges Level mit vergleichbar wenig Aufwand erreichen kann. Zudem machen wir auf die häufigsten Lücken in der praktischen Umsetzung aufmerksam.

Kontaktadresse:

Denes Kubicek

Berliner Ring 105,
64625 Bensheim
Deutschland

Email: deneskubicek@yahoo.de
Mobil: 0049 151 2300 1297
Fax: 0049 6251 984 220

BLOG: http://www.deneskubicek.blogspot.com/
WEB: http://www.opal-consulting.de/training
Demo Application: http://apex.oracle.com/pls/otn/f?p=31517:1
Oracle Forum: http://forums.oracle.com/forums/forum.jspa?forumID=137