APEX geht schnell…

…, aber ist es auch sicher?

Überblick

Zugriff kontrollieren

- Anwendung
- Daten

Bedrohungen mildern

- URL Manipulation
- Session State Protection
- SQL Injection
- Cross Site Scripting

Ist APEX sicher?

APEX ist sicher

- umfangreicher Testprozess bei Oracle
- Entwickler können immer noch unsichere Anwendungen verursachen

APEX bietet diverse Sicherheitsfeatures

- Authentifizierungs- und Autorisierungsschemata
- Session State Protection
- diverse andere Sicherheitseinstellungen

Zugangskontrolle

Anwendungsebene

- Wer kann auf die Anwendung, Funktion oder Komponente zugreifen?
- Authentifizierung, Autorisierung

Datenebene

- Welche Datensätze kann eine User sehen?
- WHERE Klausel nutzen

Authentifizierungsschemata

Anwender identifizieren

- überlicherweise per Username und Passwort

Häufig genutzte Schemata

- LDAP, HTTP Header, Custom

Open Door für Test als Anwender

Autorisierungsschemata

Wer kann und sieht was?

- überlicherweise per Gruppenzugehörigkeit
- greift erst nach Authentifizierung
- Schemakonfiguration kann angepasst werden
  - typischerweise basierend auf Rollen
  - kann auch auf Funktionen basieren

Alle notwendigen Komponenten sichern

- Seite, Regionen, Items, Button, Prozesse, etc.

Conditions vs. Authorisation

Condition für Allgemeines

- Beispiel: "Anlegen" Button verbergen, wenn Datensatz bearbeitet wird

Autorisierung, wenn relevant für Sicherheit

- Beispiel: "Anlegen" Button verbergen, wenn User kein Admin ist
- nicht vergessen: zugehörigen "Anlegen"-Prozess ebenfalls sichern

DEMO

Anforderung

- Nur Admins und Basisuser sollen Zugriff auf die Anwendung erhalten.

DEMO

Anforderung

- Nur Admins dürfen Reports sehen
- Nur Admins dürfen Orders löschen

Erst das Ziel, dann der Weg…

Tabs, Buttons, etc. sind der Weg zum Ziel

- diese müssen gesichert werden
- wichtiger ist aber das Ziel zu sichern

Seiten, Prozesse, etc. sind das Ziel

- Ziel sichern, testen und anschließend die Wege absichern, die zum Ziel führen

DEMO

Anforderung

- Nur Admins dürfen Reports sehen
- Nur Admins dürfen Orders löschen

DEMO

Anforderung

- Nur Admins dürfen Orders bearbeiten, die sie nicht selbst erstellt haben.
- Nur Admins dürfen die Spalten Sales Rep sehen

WHERE-Klausel im Report ist nicht genug

Runtime WHERE-Klausel

- Nervig, aber sicher

Virtual Private Database

- Noch besser
- Erfordert aber Enterprise Edition

DEMO

- Runtime WHERE Klausel

Session State Protection

Session State Protection in APEX

- Verhindert Manipulation der Itemvalues in URL

Sonstiges

- Validierung auf Serverseite
- Hidden-Items schützen
- Read-Only-Items schützen

DEMO

Session State Protection

SQL Injection

grundlegende Probleme

- Verwendung von Substitution Strings
- Dynamische SQL Statements

Lösung

- Verwendung von Bind-Variablen und der V-Funktion
- NIEMALS User-Input vertrauen
- Nutzereingaben mit DBMS_ASSERT „säubern“

DEMO

SQL Injection

Cross Site Scripting (XSS)

Wir erwarten, das User bestimmte Daten eingeben…

- … ABER, das tun sie nicht immer.
- … und Browser führen Code aus, wenn er nicht escaped wird.

APEX bietet deklarative Optionen für Escaping

- HTTP.p(apex_escape.html(:SOME_ITEM));
- Sichere Item Display Types
- Eingabe in Items beschränken

DEMO

Cross Site Scripting

Kontakt

Anja Hildebrandt

buw Management Holding GmbH & Co. KG

E-Mail: anja.hildebrandt@buw.de

LinkedIn: https://de.linkedin.com/pub/anja-hildebrandt/b7/33a/680

XING: http://www.xing.com/profile/Anja_Hildebrandt

Twitter: @anjeli2001