MT AG

APEX Security Grundlagen

Philipp Hartenfeller, Senior Consultant

DOAG K+A 2022

Nürnberg, 21.09.2022

Zahlen und Fakten.

Ihr Partner für den digitalen Wandel.
Individuelle IT-Lösungen aus einer Hand.

TOP 100 Top-Innovator 2022

CHIP TOP Arbeitgeber für IT-Jobs 2022

Hauptsitz
Ratingen
Niederlassungen
Frankfurt am Main,
Köln, München, Hamburg

> 125 Kunden

> 300 Beschäftigte

Zertifizierter Partner führender Technologiehersteller

ca. 44 Mio. €
Umsatz in 2021

Gründung 1994

Branchenübergreifend

Herstellerneutral

Ausbildungsbetrieb, Partner im dualen Studium

Inhabergeführt

MT AG

Über mich

Philipp Hartenfeller

- Aus Düsseldorf
- Master IT-Management
- Seit 2016 @ MT AG
- Senior Berater – Oracle APEX
- LCT-Entwickler (APEX Testing) (https://lct.software)

@phartenfeller

Blog: https://hartenfeller.dev/blog/

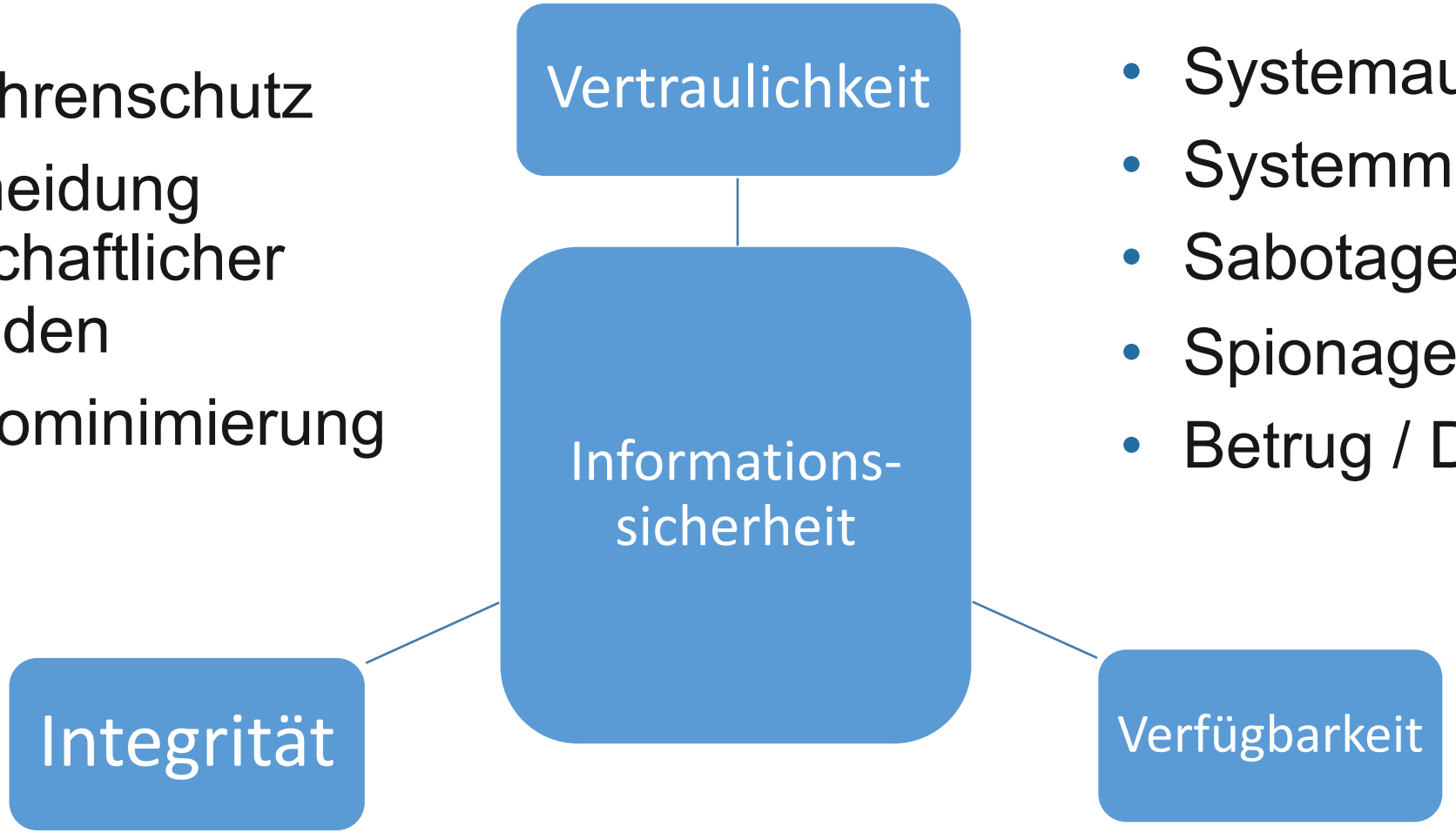
Agenda

1. Einleitung
2. Client vs. Server
3. Session State Protection / Checksummen
4. SQL Injection
5. Cross Site Scripting (XSS)
6. Weitere Tipps

1. Einleitung

Security?!

- Gefahrenschutz
- Vermeidung wirtschaftlicher Schäden
- Risikominimierung

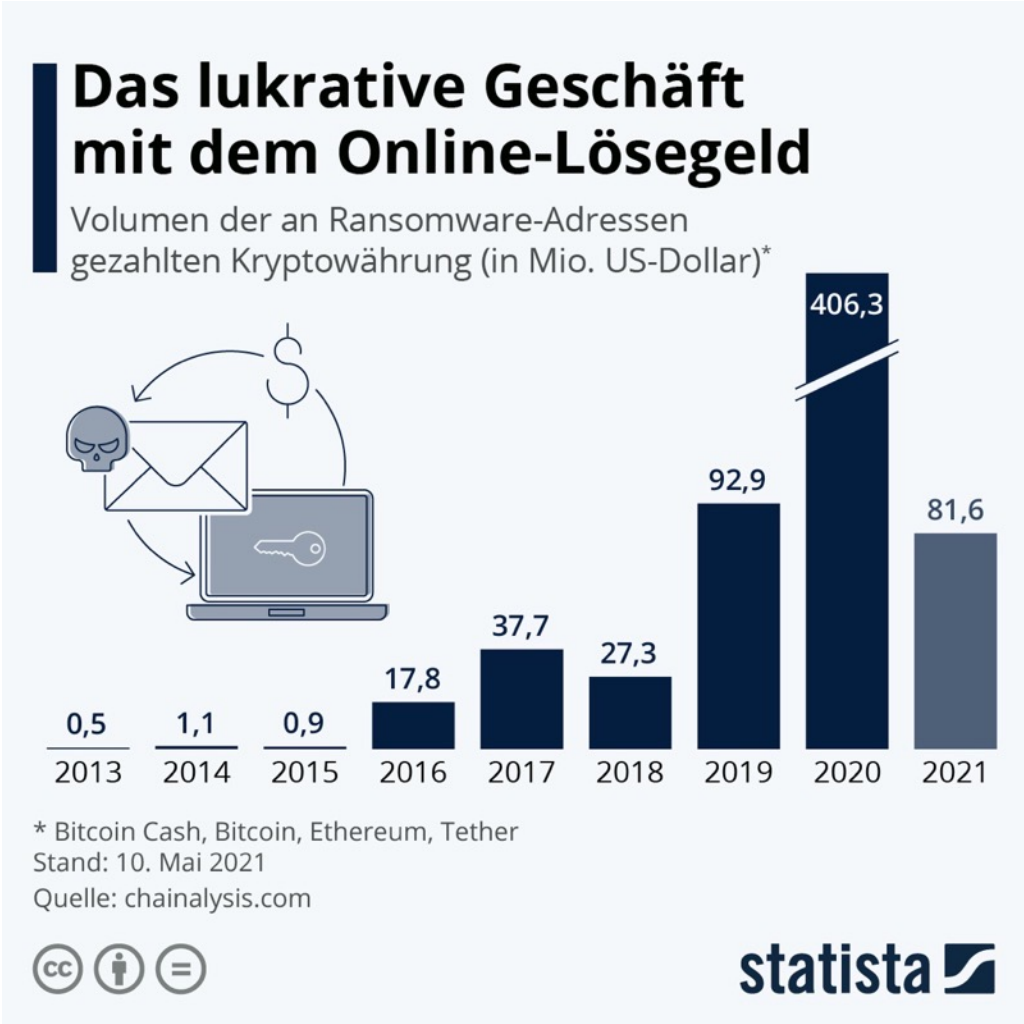


- Systemausfall
- Systemmissbrauch
- Sabotage
- Spionage
- Betrug / Diebstahl

Quelle

Folgen fehlender Security

- Ransomware legt Firmen, Universitäten und Krankenhäuser lahm
- Trojaner-Angriffe auf Smartphones vieler Politiker, Journalisten, Aktivisten etc.
- Einflussnahme auf Wahlen
  - Z. B. Frankreich, USA und Deutschland



Abgrenzung des Vortrags

Security findet fast überall statt

Nicht technisch:

- Zugangsschutz
- Social Engineering
- Standortwahl
- Enterprise-Architekturen / Personalrollen

Technisch:

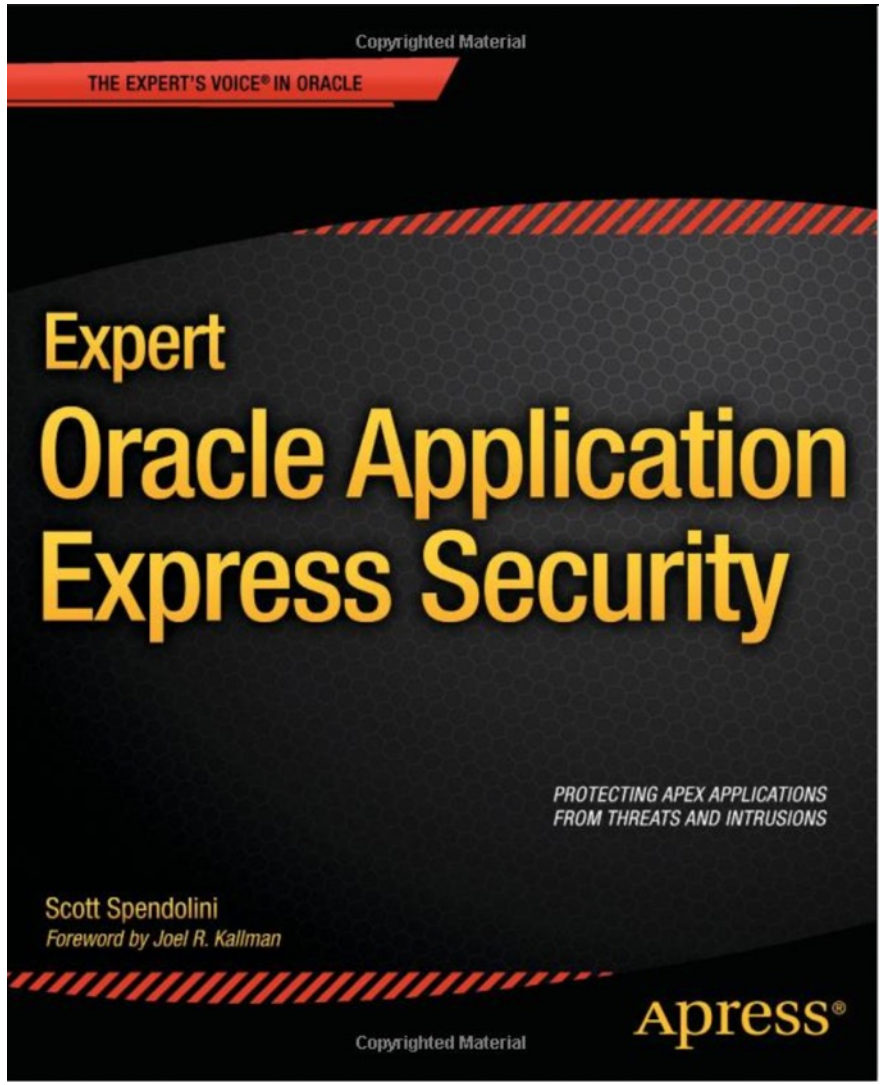
- Netzwerke
- Betriebssystem
- Verschlüsselung
- Backups
- Datenbankeinstellungen
- Webservereinstellungen

In diesem Vortrag: Was können APEX Devs tun?

Primär Page Designer + Datenbankcode

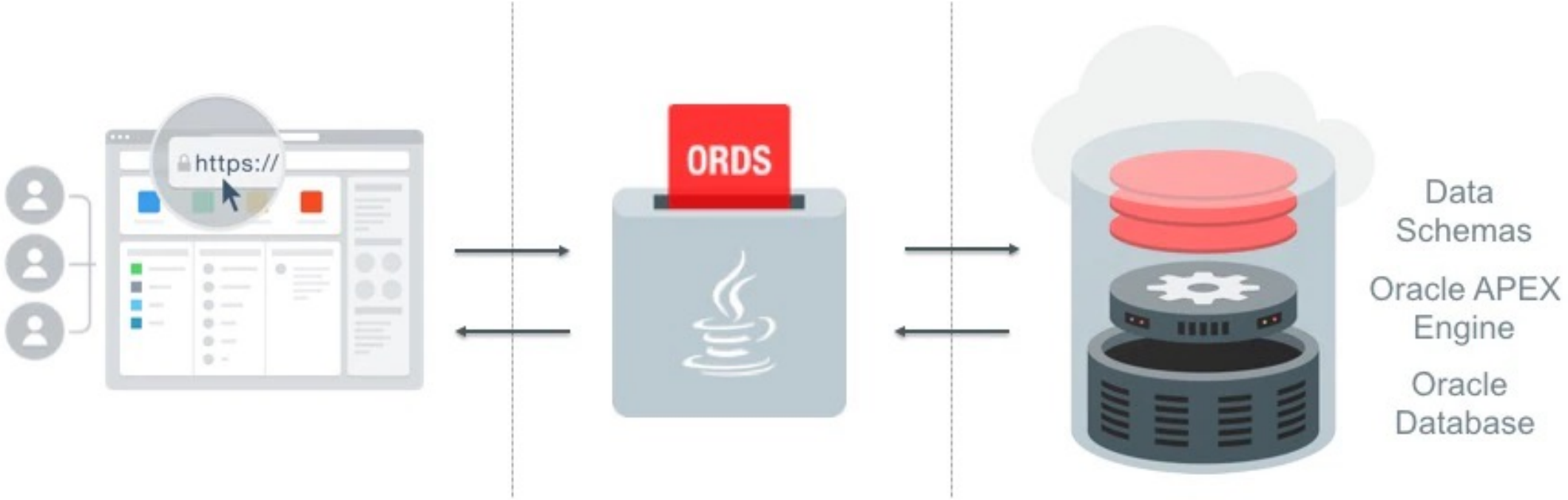
>>lediglich Grundlagen<<

Zum Weiterlesen



- Expert Oracle Application Express Security
- Autor: Scott Spendolini
- 22. April **2013**
- ISBN: 978-1430247319

APEX Architektur



2. Client vs. Server

Was ist Client was ist Server?

Server	Client
Sprachen: SQL und PL/SQL Ausblenden: • Server-side-conditions und Authorization-Schemes → Auf Items, Spalten etc.	Sprache: JavaScript (jQuery) Ausblenden: • Fast alle Dynamic Actions (z. B. hide) • Items vom Typ „hidden“

Wir haben keinen Einfluss auf den Client

- Sensible Daten müssen serverseitig gefiltert werden, sodass sie niemals den Client erreichen
  - Browser Entwicklertools
  - JS muss nicht ausgeführt werden und kann auf dem Client manipuliert werden

- Auch auf dem Server prüfen, ob ein Nutzer eine Aktion durchführen darf
  - Buttons sind lediglich Interaktionselemente
  - Ein ausgeblendeter Button verhindert nicht die Aktion

Demo: Client vs. Server

Die Nutzung der Browser Dev-Tools ist strafbar?!

@GovParsonMO/Twitter

Governor wants to prosecute journalist for right-clicking on a government website, thinks it's hacking

Apparently viewing a page source makes you a hacker, according to the Missouri governor.

Andrew Wyrich Tech Posted on Oct 14, 2021 Updated on Oct 15, 2021, 9:13 am CDT

- https://www.dailydot.com/debug/missouri-governor-reporter-hacker-mocked/

3. Session State Protection / Checksummen

Session State Protection / Checksummen

Was ist das?

- Ziel: verhindern, dass Nutzer Parameter im Browser verändern **(wenn sie es nicht sollen)**
- Beispiel Link: apex....p12_id=3...&cs=1lhBP1wVra-7EvlWFg...
- Funktionsweise wie bei Hashfunktionen → kryptischer Prüfwert den nur Server erzeugen kann
  - Wird mit eigentlichen Daten an den Client geliefert
  - Ist deterministisch für den Server erzeugbar
- Beim verarbeiten eines Submits:
  - Server prüft Input über dasselbe Verfahren auf Manipulationen
-

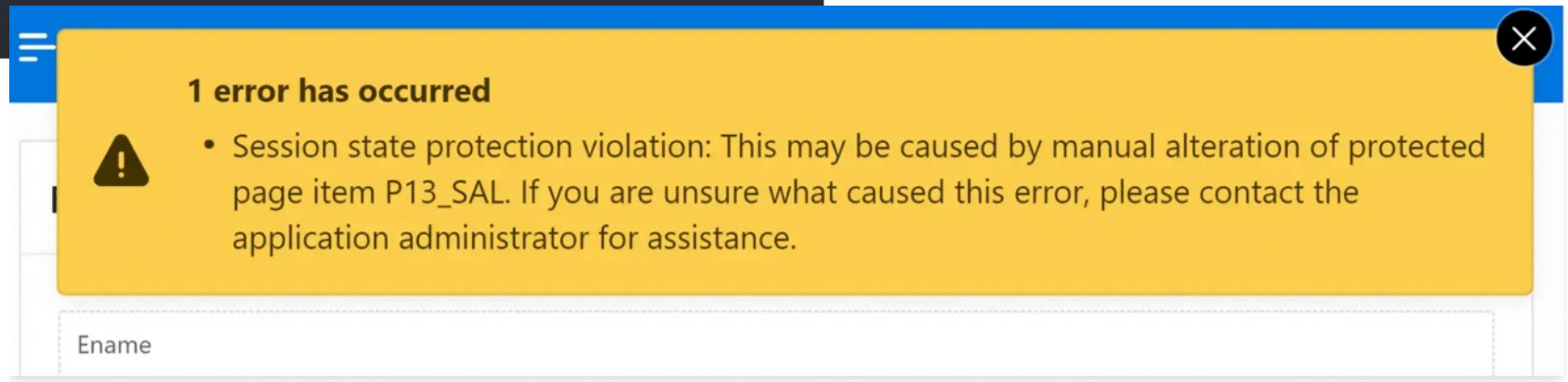
Demo: Checksummen in Links

Session State Protection / Checksummen

Read Only Items

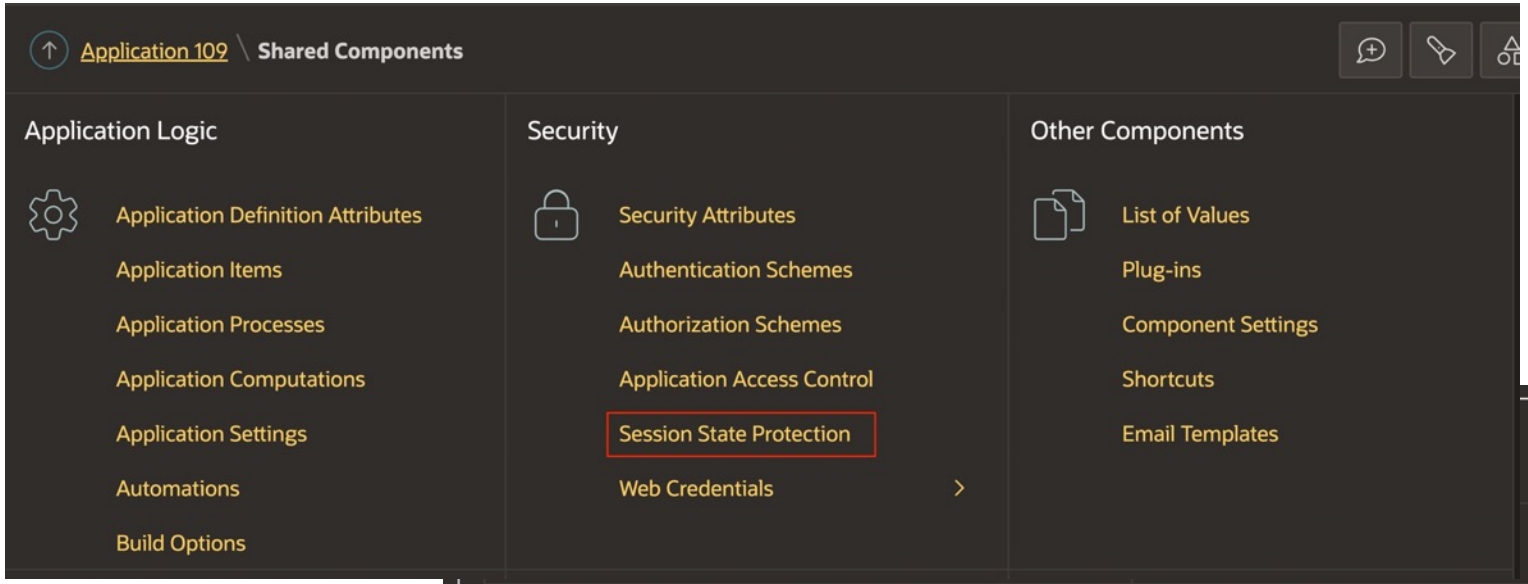
- Können je nach Autorisierung editierbar sein
- Falls read-only -> Checksumme wird mitgeliefert

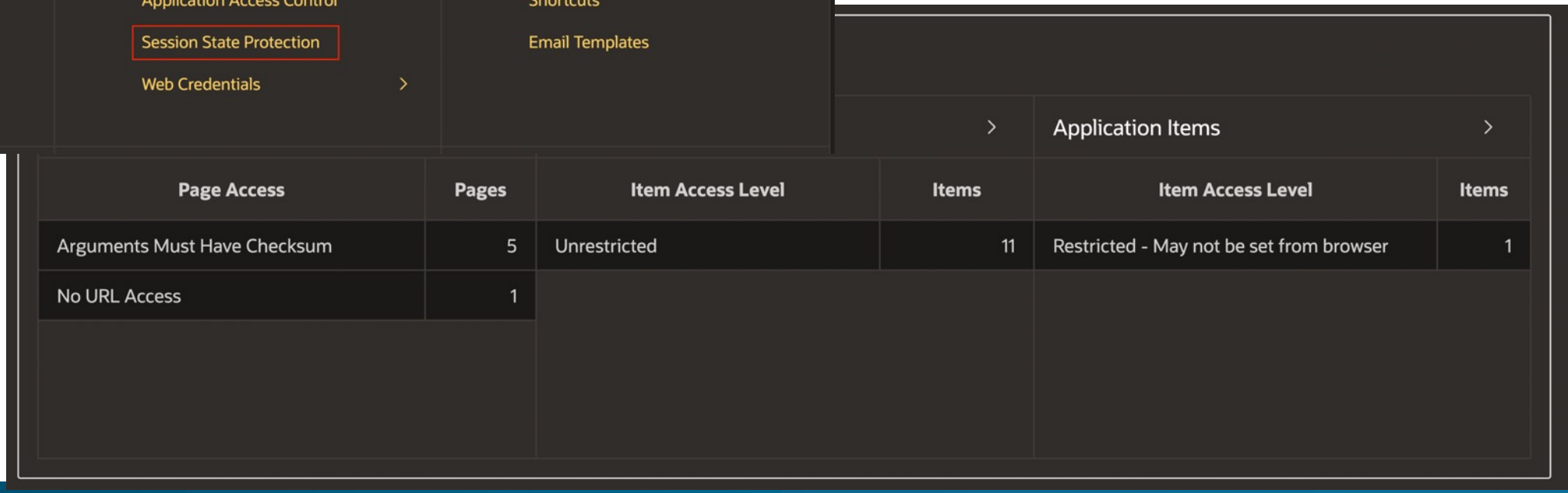
```
1 $s('P13_SAL', 123);
2 apex.submit({ request: 'SAVE' });
3
```



Session State Protection / Checksummen

Übersicht ob Items abgesichert sind





Application Items

Page Access	Pages
Arguments Must Have Checksum	5
No URL Access	1

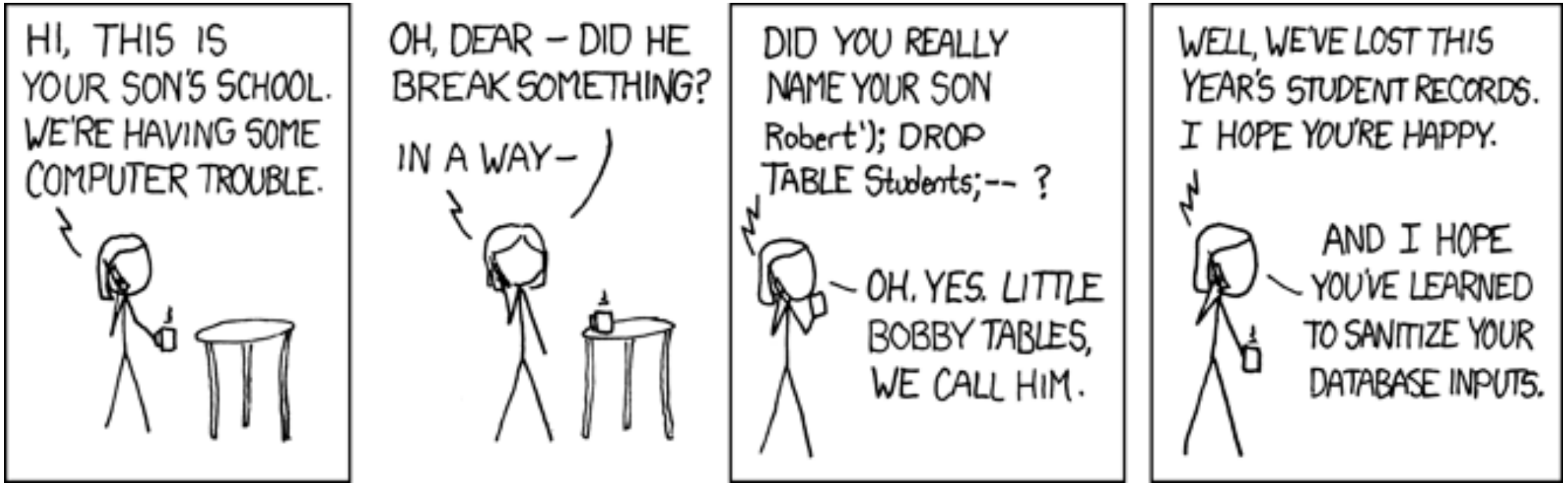
Item Access Level	Items
Unrestricted	11

Item Access Level	Items
Restricted - May not be set from browser	1

4. SQL Injection

SQL Injection?!

Nutzer können von außen Datenbankbefehle „einschleusen“, die auch verarbeitet werden



Quelle

Gefahrenzonen

- Kein Problem bei APEX SQL-Feldern
  - --> Sicher gebindet mit :P100_ITEM

- Dynamisches SQL
  - --> Inputs überprüfen
  - --> Werte mit :var binden
  - --> dbms.assert verwenden
  - --> dbms.sql verwendent

Demo: SQL Injection

5. Cross Site Scripting (XSS)

XSS?!

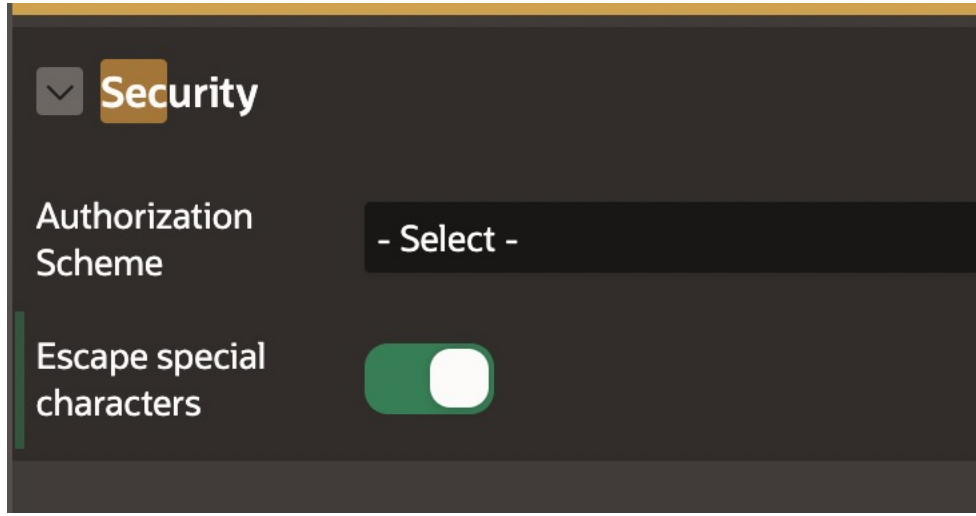
- Nutzer können von außen JavaScript-Befehle „einschleusen“, die auch verarbeitet werden
- Quasi SQL-Injection für JS

```
First Name
<script>alert('XSS!')</script>
```

- Mögliche Folgen:
  - geheime Daten abgreifen
  - für andere Personen etwas ausführen
  - etc.

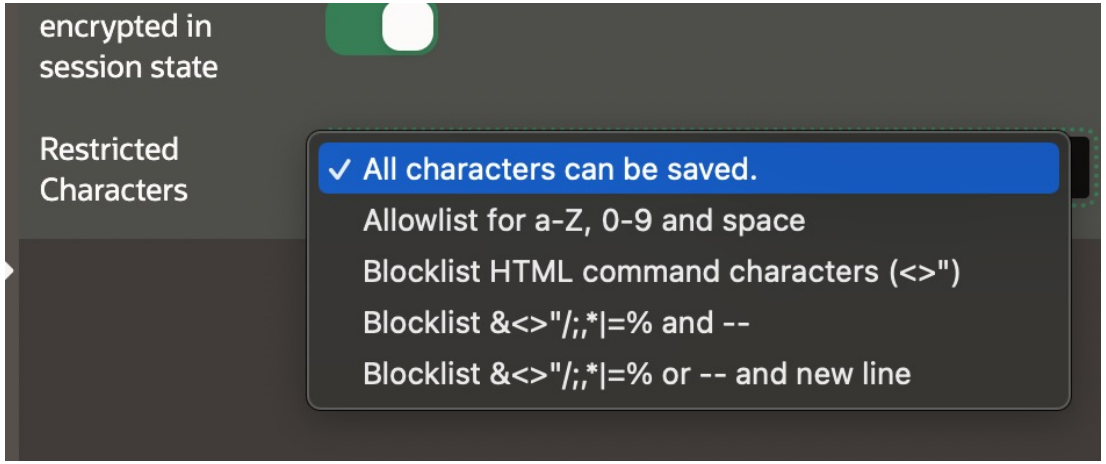
Gefahrenzonen

- htp.p
  - → APEX_ESCAPE Paket
- Report Spalten / Rich Text Editor...
  - → Escape special characters



Auch möglich:

- Input Items
- **Besser: Sicherheitslücke schließen**



Demo: XSS

6. Weitere Tipps

Weitere Tipps

Datenbankfeatures nutzen:

- Mehrere Schemen nutzen + nur nötige Rechte vergeben
- Virtual Private Databases (Enterprise)
- Oracle Auditing („Fine-grained Auditing” Enterprise)

Scanner:

- APEX Advisor (integriert)
- ApexSec (kommerziell)
- APEX-SERT (OpenSource)

Weitere Tipps

Single Sign-On

- Zentrale Authentifizierung
- Weniger Passwörter

Flexible und granulare Autorisierungskonzepte

- Definition Rechte (z. B. Nutzer lesen, bearbeiten, löschen…)
- Definition Rollen (z. B. PO, Analyst, Admin, Gast…)
- Zuordnung Rollen <-> Rechte
- Regelmäßig testen!!!

Weitere Tipps

Logging

- Jegliche Operationen protokollieren
- Nachvollziehbarkeit + Debugging
- Missbrauch überhaupt feststellen
- Z. B. OraOpenSource/Logger

Infrastruktur

- Patches zeitlich einspielen
- TLS verwenden + Security Header einstellen

Weitere Tipps

Keine Kopien von Anwendungen oder Seiten produktiv halten

- Können gescannt → gefunden werden
- Doppelter „Schatten“-Code

KISS - Keep it simple, stupid

- Mehr Komplexität → mehr Fehlerpotenzial

Weitere Tipps

APEX sind normale Webanwendungen

- → Generell über Securirty für das Web informieren
- Z. B. OWASP Top 10

- Selbstkritisch und aufmerksam programmieren
- Codereviews

„Testers don't break the code, they break your illusions about the code.“

Vielen Dank für Ihre Aufmerksamkeit!

Philipp Hartenfeller
Senior Berater

philipp.hartenfeller@mt-ag.com
@phartenfeller
https://hartenfeller.dev/blog

MT AG
Balcke-Dürr-Allee 9
40882 Ratingen

www.mt-ag.com

MT AG

Vorträge Mittwoch, 21.09.2022

Titel	Uhrzeit	Raum	Referent:in
You‘ve got Mail!	15.00–15.45 Uhr	Istanbul	 Timo Herwix
Mobile frei definierbare & skalierbare DevOp’s Umgebung (Docker, Oracle, APEX)	15.00–15.45 Uhr	Kopenhagen	 Guido Sokolis
Web-Server und Apache Tomcat verstehen	16.00–16.45 Uhr	Kopenhagen	 Robin Schulz
Der „Hype“ Podcast: Von der Idee zur Umsetzung #DevsOnTape	16.00–16.45 Uhr	Budapest	 Kai Donato und Carolin Hagemann
Ein Einstieg in Oracle REST Data Services für autonome Datenbanken	17.00–17.45 Uhr	Kopenhagen	 Timo Herwix