ORDIX® best practice

einfach. gut. beraten.

APEX-Security –
Ein Überblick für Einsteiger

DOAG
Konferenz + Ausstellung 2018
Nürnberg

Raphael Salguero

info@ordix.de www.ordix.de

Agenda

ORDIX AG

- Authentifizierung
- Autorisierung
- SQL-Injection
- Cross-Site-Scripting (XSS)
- Cross-Site-Request-Forgery (CSRF)
- Insecure Direct Object References

- Verschlüsselung

Demonstration

ORDIX AG

Authentifizierung und Autorisierung

Authentifizierung

ORDIX AG

- Anmeldung der Endbenutzer an die Anwendung

Open Door APEX-Benutzer Eigene Authentifizierung

Autorisierung

ORDIX AG

- Berechtigungskonzept für die Endbenutzer
- Zugriffseinschränkung feingranular
  - Applikation-Ebene
  - Page-Ebene
  - Item-Ebene
- Basierend auf:
  - SQL-Abfragen
  - APEX Benutzergruppen
  - Werte von Items

Demonstration

ORDIX AG

SQL-Injection

SQL-Injection

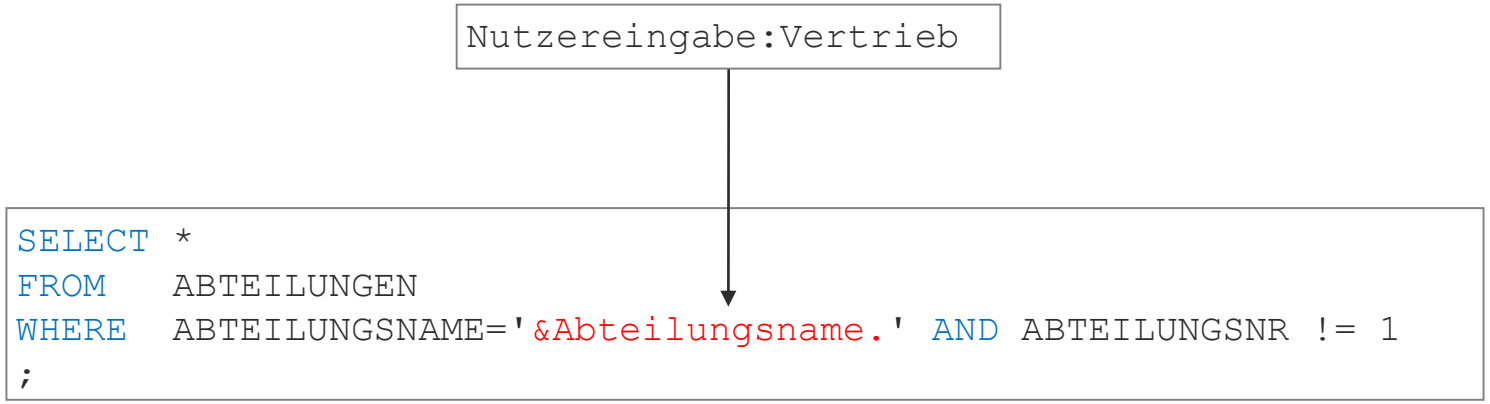
ORDIX AG

- Risiko bei Verarbeitung von Nutzereingaben
- Voraussetzung: Substitutions- anstatt Bind-Variablen
- Nutzer kann SQL-Statement manipulieren

```
SELECT *
FROM   ABTEILUNGEN
WHERE  ABTEILUNGSNAME='&Abteilungsname.' AND ABTEILUNGSNR != 1
;
```

SQL-Injection

ORDIX AG



SQL-Injection

ORDIX AG

```
Nutzereingabe:' or 1=1  --
```



```
SELECT *
FROM   ABTEILUNGEN
WHERE  ABTEILUNGSNAME='' or 1=1 -- ' AND ABTEILUNGSNR != 1
;
```

SQL-Injection absichern

ORDIX AG

- Bindvariablen schützen vor SQL-Injection
- Syntaxbeispiel: `:VARIABLENNAME`

```
SELECT *
FROM   ABTEILUNGEN
WHERE  ABTEILUNGSNAME = :Abteilungsnummer AND ABTEILUNGSNR != 1
;
```

Demonstration

ORDIX AG

Cross-Site-Scripting (XSS)

Cross-Site-Scripting (XSS)

ORDIX AG

- Einschleusen von Quellcode in Webseiten
  - Gästebuch
  - Kommentarfunktion
  - Datenerfassung
  - ...
- Interpretation des Quellcodes durch den Browser

Cross-Site-Scripting (XSS)

ORDIX AG

- Automatisches Herunterladen von Schadsoftware mittels „Drive by Download“
- Aufrufen von gefälschten Formularen zum Abgreifen von Nutzerdaten
- Weiterleiten auf kompromittierte Webseiten
- ...

Welche Komponenten in APEX sind anfällig?

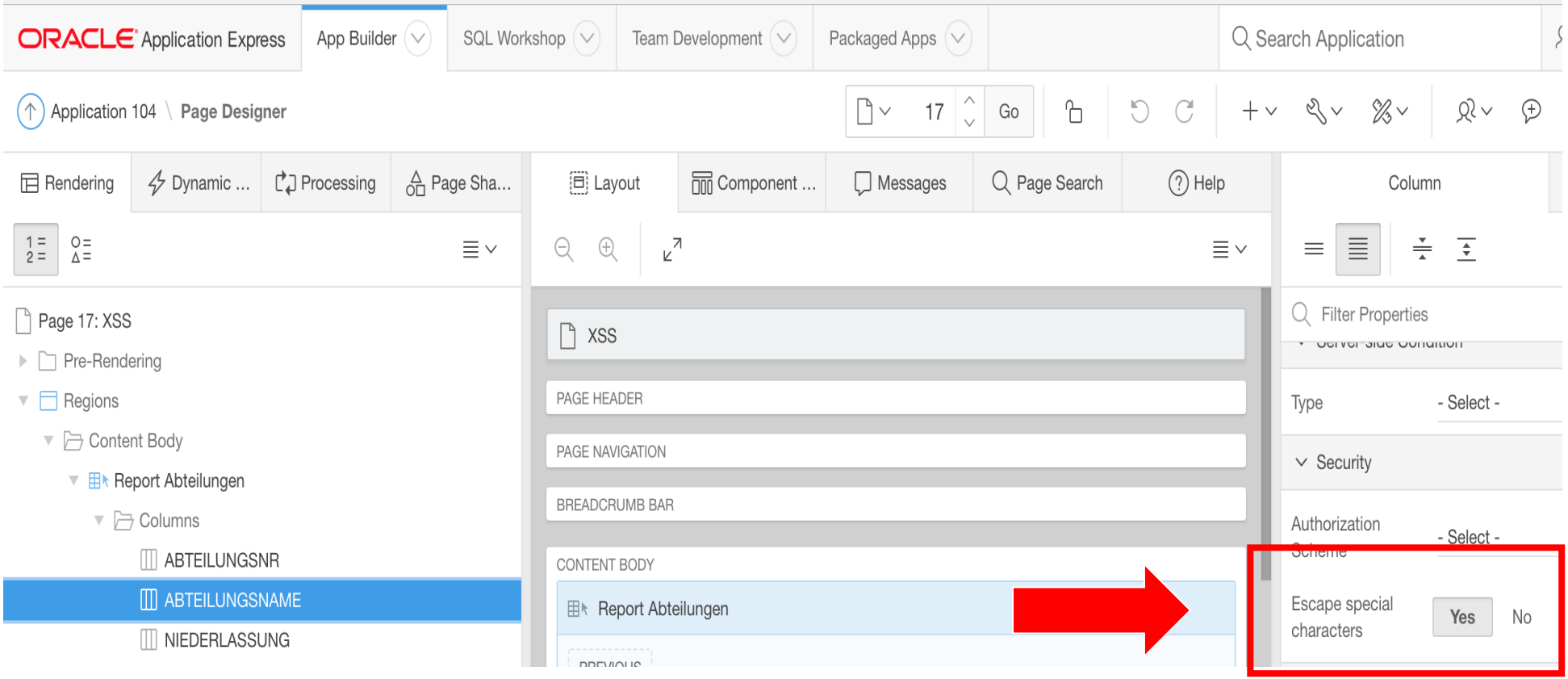
ORDIX AG

- „Display-Only“-Felder
- Checkboxen
- Radio Groups
- Textfelder mit „Autocomplete“-Funktion
- alle Report Spalten
- Kalender Regionen“
- Tree Regionen
- Diagramm Regionen

Cross-Site-Skripting absichern

ORDIX AG

- Einschalten der Security-Option „Escape special characters“



Demonstration

ORDIX AG

Cross-Site-Request-Forgery (CSRF)

Cross-Site-Request-Forgery

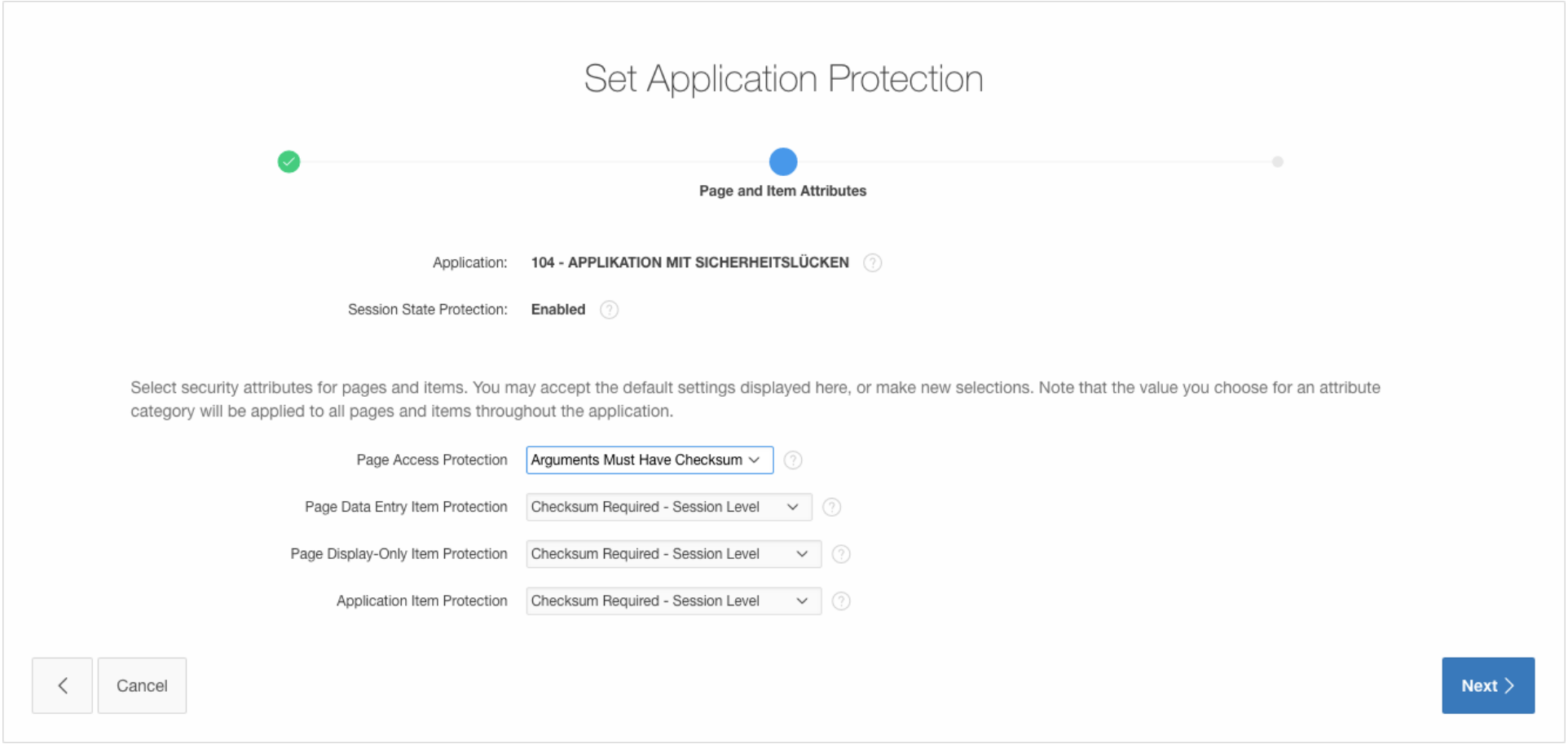
ORDIX AG

- Nutzer ist mit einem Browser in Facebook eingeloggt
- Nutzer ruft eine manipulierte Webseite auf
- Manipulierte Webseite postet automatisch etwas auf Facebook

Cross-Site-Request-Forgery absichern

ORDIX AG

- Die Session State Protection aktivieren



Demonstration

ORDIX AG

Insecure Direct Object References

Insecure Direct Object References

ORDIX AG

- Direkte Objektreferenzen beispielsweise bei Master-Detail-Reports
- Übergabe von Primary Keys über die URL

.../f?p=101:2:117585177892266::NO:3:P3_EMPNO:1

Insecure Direct Object References absichern

ORDIX AG

- Mapping von Primary Key
- Mögliche Zugriffsberechtigung durch Autorisierungsschemata einschränken
- Session State Protection aktivieren

Demonstration

ORDIX AG

Verschlüsselung

Verschlüsselung

ORDIX AG

- Der EPG unterstützt standardmäßig kein SSL!
  - ➢ Advanced Security Option notwendig

- SSL durch Kombination aus ORDS und Webserver (z.B. Apache Tomcat)
- SSL durch die Verwendung des Oracle HTTP Servers

Zusammenfassung

ORDIX AG

- Authentifizierungsmöglichkeiten ausnutzen und wenn möglich SSL verwenden
- Autorisierungsschemata feingranular verwenden
- Bindvariablen anstatt Substitutionsvariablen verwenden
- „Escape special characters“ aktivieren
- Session State Protection verwenden
- SSL in der Produktion verwenden

Vielen Dank für Ihre Aufmerksamkeit!

ORDIX AG

Zentrale Paderborn
Karl-Schurz-Straße 19a
33100 Paderborn
Tel.: 05251 1063-0
Fax: 0180 1 67349 0

Seminarzentrum Wiesbaden
Kreuzberger Ring 13
65205 Wiesbaden
Tel.: 0611 77840-00

Weitere Geschäftsstellen
in Essen, Gersthofen,
Köln und Münster

info@ordix.de
www.ordix.de