Sichere Datenbankanfragen

OpenText WebSiteManagement (Delivery Server)

Axel Reinhardt

Agenda

- ✓ Was ist SQL-Injection?
- ✓ Beispiel eines Bestellprozesses
- ✓ Vorgehen eines Angreifers
- ✓ Härten der Web-Seite – Schritt für Schritt
- ✓ Was kann/sollte man beim Design der Datenbank beachten?

Was ist SQL-Injection?

SQL-Injecetion ➔ SQL-Einschleusung

SQL-Injection bezeichnet das Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken, die durch mangelnde Maskierung oder Überprüfung von Metazeichen in Benutzereingaben entsteht. Der Angreifer versucht dabei, über die Anwendung, die den Zugriff auf die Datenbank bereitstellt, eigene Datenbankbefehle einzuschleusen.

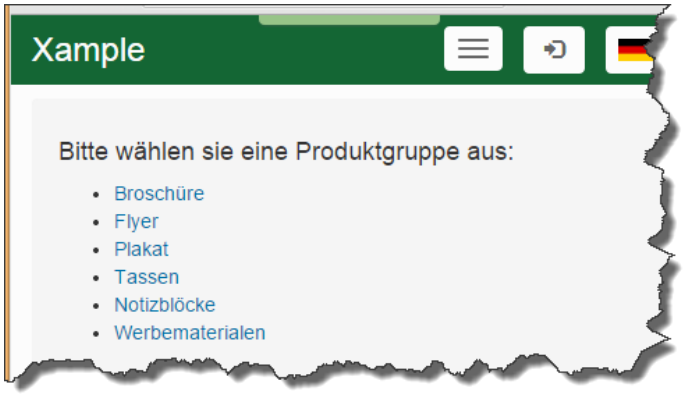
Das Ziel ist es:

- Daten auszuspähen
- in seinem Sinne zu verändern
- die Kontrolle über den Server zu erhalten
- einfach größtmöglichen Schaden anzurichten

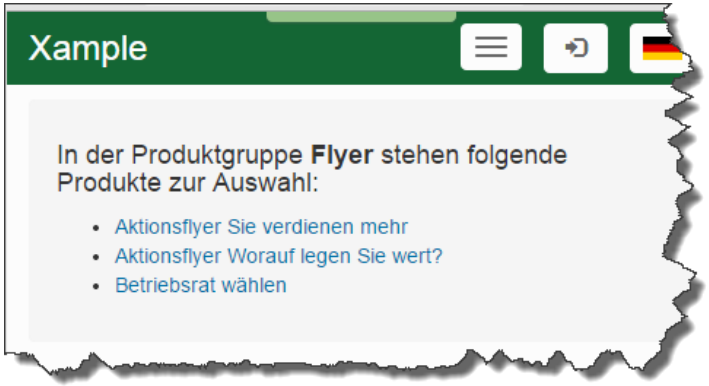
(aus Wikipedia)

Beispiel
Ein einfacher Bestellprozess (1)

- Auswahl einer Produktgruppe:
  http://www.xxx.de/cps/rde/xchg/xample/rdesrdef.xsl/-/AR/ar02.htm/-



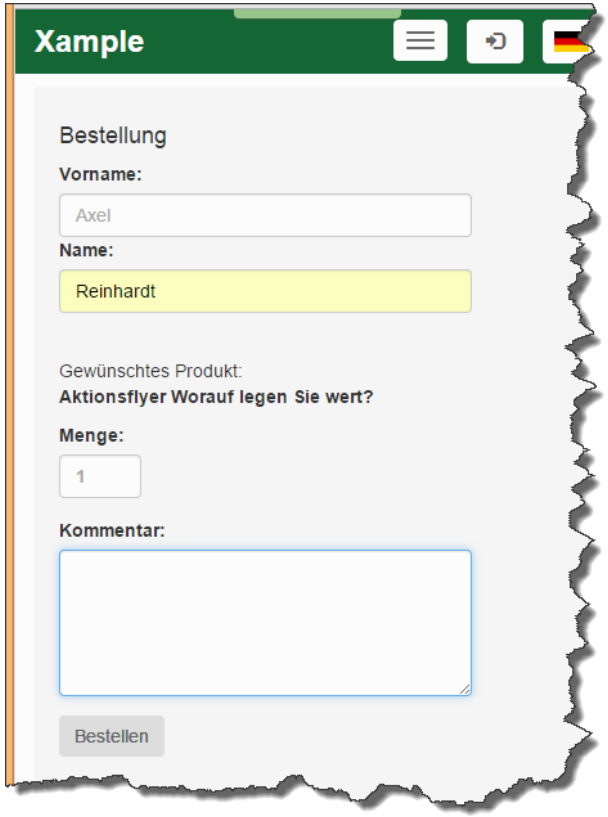
- Produkt wählen:
  http://www.xxx.de/cps/rde/xchg/xample/rdesrdef.xsl/-/AR/ar03.htm/-?**gr_id=3**



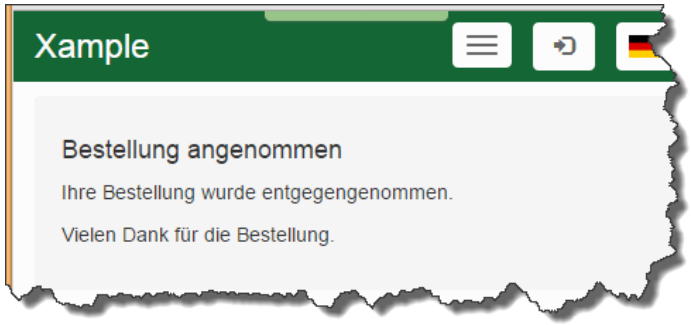
Beispiel
Ein einfacher Bestellprozess (2)

- Bestelldaten erfassen:

http://www.xxx.de/cps/rde/xchg/xample/rdesrdef.xsl/-/AR/ar04.htm/-?**id=2**



http://www.xxx.de/cps/rde/xchg/xample/rdesrdef.xsl/-/AR/ar05.htm/-?vorname=Axel&nachname=Reinhardt&prod_id=2&menge=1&kommentar=

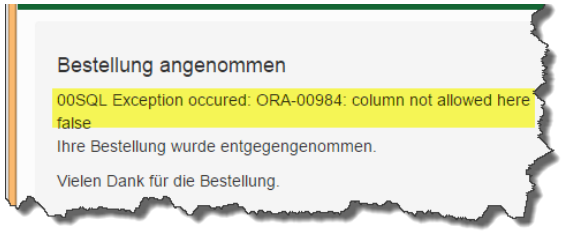


Vorgehen eines Angreifers
Schwachstellen?

Suchen von Schwachstellen

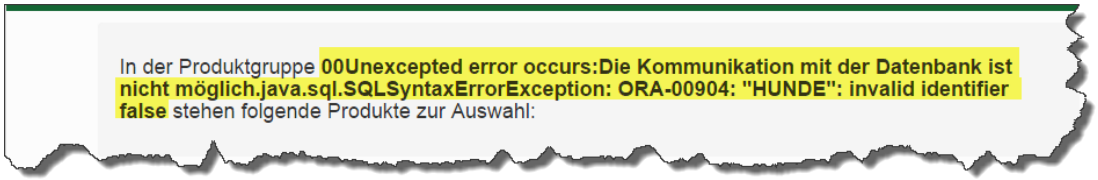
- Formulare
  - Sehr lange Texte
  - Sonderzeichen wie z.B. '
  - Datumseingabe
  - Texteingabe bei numerischen Feldern z.B. bei Mengen

http://www.xxx.de/cps/rde/xchg/xample/rdesrdef.xsl/-/AR/ar05.htm/-?vorname=Axel&nachname=Reinhardt&prod_id=2&menge=**hund**&kommentar=



- URLs mit Parametern (besonders IDs)

http://www.xxx.de/cps/rde/xchg/xample/rdesrdef.xsl/-/AR/ar03.htm/-?gr_id=hunde



Vorgehen eines Angreifers
Analyse der Schwachstellen (1)

- Über die Fehlermeldung kann man erkennen, um welches DB-System es sich handelt!
- Durch Analyse des Quellcodes, kann auf das Websitemanagment-System geschlossen werden!

```
    <div cla s="ro.. ">
     <div class="col-md-9">
      <div class="well" id="maincontent"><!--ARARAR-->
<h4>In der Produktgruppe <b><!-- DynaMent-Report:
<report code="-9001" dynament="XmlRdbDynaMent" general-code="-1"><rde-rd:message code="-9001" dynament="XmlRdbDynaMent"
general-code="-1">Allgemeiner Fehler im RDB-DynaMent.</rde-rd:message><rde-rd:dynament alias="AR_DEMO" chunk="1"
chunksize="1000" destination="." maxrows="0" mode="query" name="XmlRdbDynaMent" report-tag="report" result-
attribute="rdbStatus" row="row" sql="select NAME from PRODUKT_GRUPPE where ID =hunde;" tag="result" timeout="-1" /><rde-
rd:details dynament="XmlRdbDynaMent"><rde-rd:detail code="-9001" general-code="-1" seq="1"><rde-rd:level>Warn</rde-
rd:level><rde-rd:message>Allgemeiner Fehler: Unexcepted error occurs:Die Kommunikation mit der Datenbank ist nicht
möglich.java.sql.SQLSyntaxErrorException: ORA-00904: "HUNDE": invalid identifier
</rde-rd:message></rde-rd:detail></rde-rd:details></report>
 -->

00Unexcepted error occurs:Die Kommunikation mit der Datenbank ist nicht möglich.java.sql.SQLSyntaxErrorException: ORA-
00904: "HUNDE": invalid identifier
false</B> stehen folgende Produkte zur Auswahl</h4>
<ul>
</ul>

    </div>
```

Vorgehen eines Angreifers
Analyse der Schwachstellen (2)

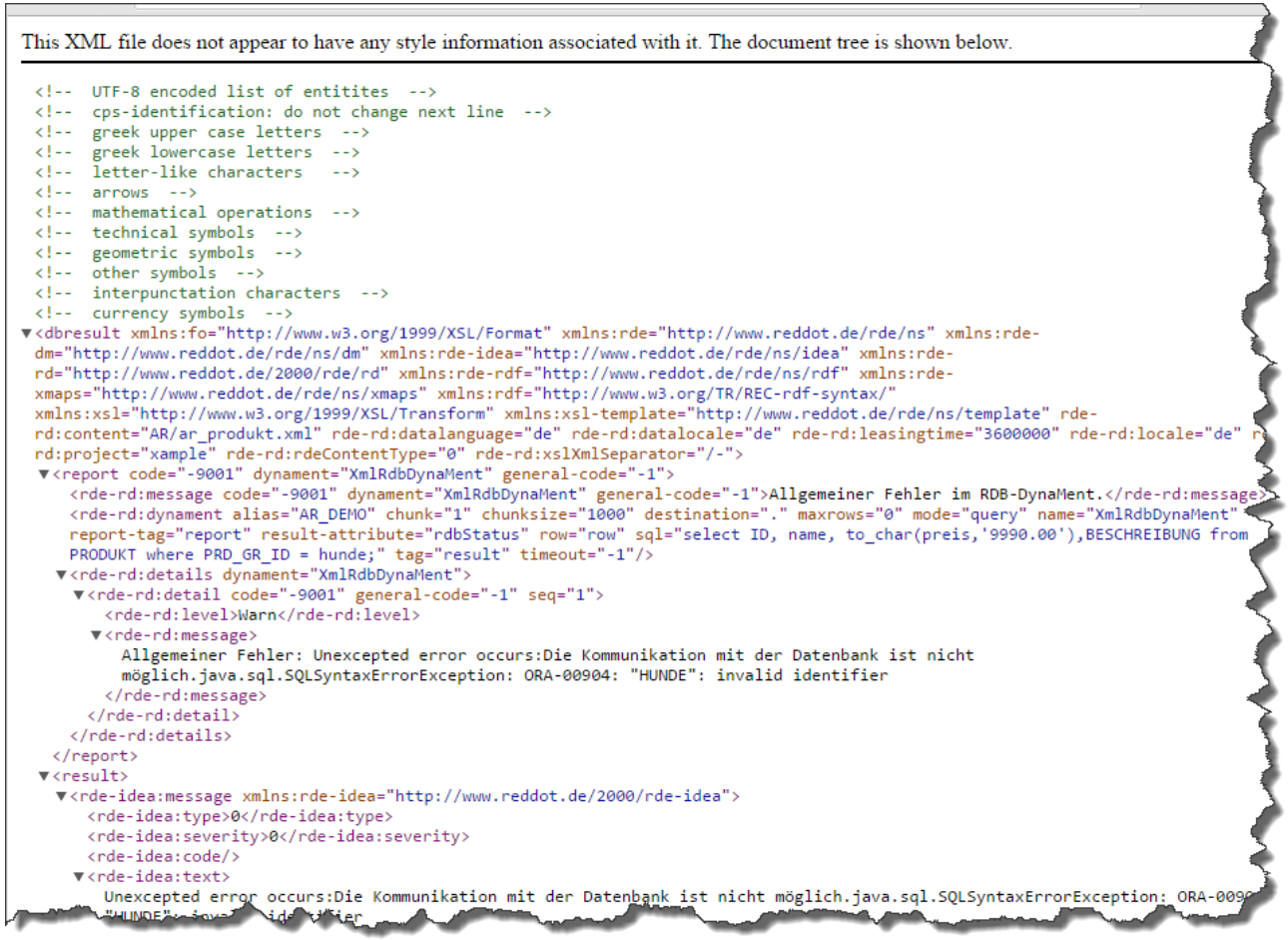
Es ist ein OpenText WebSiteManagement (DS) → mal ohne Style

http://www.xxx.de/cps/rde/xchg/xample/**rdesrdef.xsl/**-/AR/ar03.htm/-?gr_id=hunde →
http://www.xxx.de/cps/rde/xchg/xample/-/AR/ar03.htm/-?gr_id=hunde

Vorgehen eines Angreifers
Analyse der Schwachstellen (3)

XML direkt aufrufen

http://www.xxx.de/cps/rde/xchg/xample/-/AR/ar_produkt.xml/-?gr_id=hunde



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<!-- UTF-8 encoded list of entitites -->
<!-- cps-identification: do not change next line -->
<!-- greek upper case letters -->
<!-- greek lowercase letters -->
<!-- letter-like characters -->
<!-- arrows -->
<!-- mathematical operations -->
<!-- technical symbols -->
<!-- geometric symbols -->
<!-- other symbols -->
<!-- interpunctation characters -->
<!-- currency symbols -->
▼<dbresult xmlns:fo="http://www.w3.org/1999/XSL/Format" xmlns:rde="http://www.reddot.de/rde/ns" xmlns:rde-
dm="http://www.reddot.de/rde/ns/dm" xmlns:rde-idea="http://www.reddot.de/rde/ns/idea" xmlns:rde-
rd="http://www.reddot.de/2000/rde/rd" xmlns:rde-rdf="http://www.reddot.de/rde/ns/rdf" xmlns:rde-
xmaps="http://www.reddot.de/rde/ns/xmaps" xmlns:rdf="http://www.w3.org/TR/REC-rdf-syntax/"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:xsl-template="http://www.reddot.de/rde/ns/template" rde-
rd:content="AR/ar_produkt.xml" rde-rd:datalanguage="de" rde-rd:datalocale="de" rde-rd:leasingtime="3600000" rde-rd:locale="de" r
rd:project="xample" rde-rd:rdeContentType="0" rde-rd:xslXmlSeparator="/-">
 ▼<report code="-9001" dynament="XmlRdbDynaMent" general-code="-1">
    <rde-rd:message code="-9001" dynament="XmlRdbDynaMent" general-code="-1">Allgemeiner Fehler im RDB-DynaMent.</rde-rd:message>
    <rde-rd:dynament alias="AR_DEMO" chunk="1" chunksize="1000" destination="." maxrows="0" mode="query" name="XmlRdbDynaMent"
    report-tag="report" result-attribute="rdbStatus" row="row" sql="select ID, name, to_char(preis,'9990.00'),BESCHREIBUNG from
    PRODUKT where PRD_GR_ID = hunde;" tag="result" timeout="-1"/>
  ▼<rde-rd:details dynament="XmlRdbDynaMent">
    ▼<rde-rd:detail code="-9001" general-code="-1" seq="1">
       <rde-rd:level>Warn</rde-rd:level>
      ▼<rde-rd:message>
         Allgemeiner Fehler: Unexcepted error occurs:Die Kommunikation mit der Datenbank ist nicht
         möglich.java.sql.SQLSyntaxErrorException: ORA-00904: "HUNDE": invalid identifier
       </rde-rd:message>
     </rde-rd:detail>
   </rde-rd:details>
 </report>
 ▼<result>
  ▼<rde-idea:message xmlns:rde-idea="http://www.reddot.de/2000/rde-idea">
     <rde-idea:type>0</rde-idea:type>
     <rde-idea:severity>0</rde-idea:severity>
     <rde-idea:code/>
    ▼<rde-idea:text>
       Unexcepted error occurs:Die Kommunikation mit der Datenbank ist nicht möglich.java.sql.SQLSyntaxErrorException: ORA-0090
       "HUNDE": invalid identifier
```

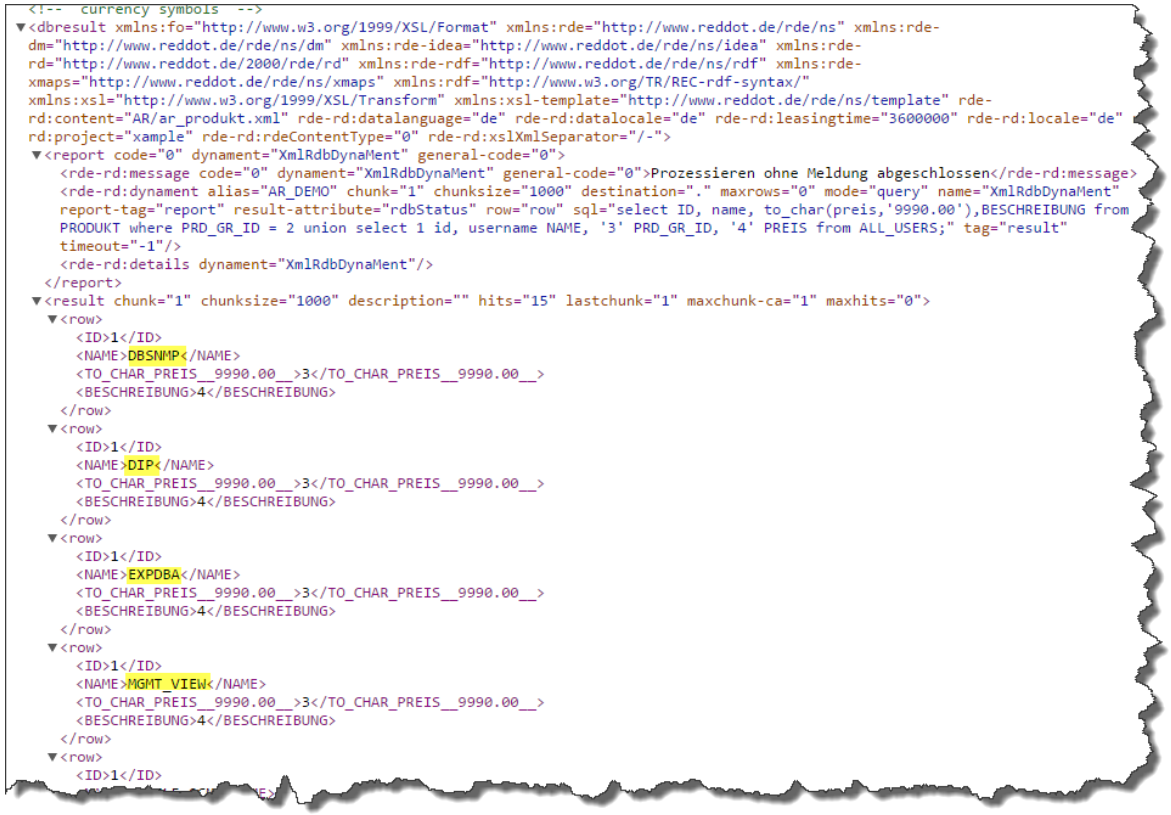
Vorgehen eines Angreifers
Ausnutzen der Schwachstellen (1)

Anhängen von weiteren Abfragen

→ Erkunden des DB-Designs

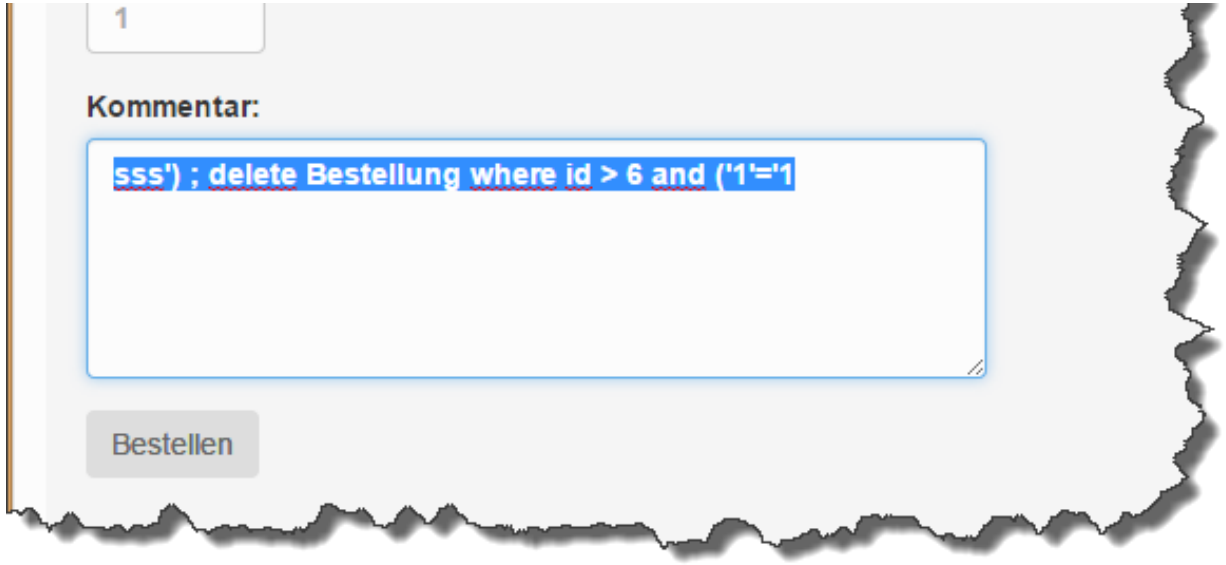
→ Ausspähen von Daten

http://www.xxx.de/cps/rde/xchg/xample/-/AR/ar_produkt.xml/-?gr_id=2 **union select 1 id, username NAME, '3' PRD_GR_ID, '4' PREIS from ALL_USERS**



Vorgehen eines Angreifers
Ausnutzen der Schwachstellen (2)

- Manipulieren von Daten



- Verändern der DB
  → z.B. Löschen von Tabellen

Härten der Seiten
Formular / Seitenaufruf

- Seitenaufruf
  - Seitenaufruf **ohne** Style verhindern, z.B. durch Apache-Regel
- Formular
  - Methode POST verwenden
  - Längenbegrenzung bei Eingabefelder
  - In HTML5 den Typ vorbelegen, z.B. auf Number
  - Nur benötigte Felder übergeben

Härten der Seiten
Nutzung von Parametern

- Vorbelegung der Parameter
- Nutzung von Inline-Funktionen
  - Daten-Konvertierung

✖
```
<dbresult>
  <rde-dm:rdb mode="query" tag="result" alias="AR_DEMO" sql="select ID, name,
  to_char(preis,'9990.00'),BESCHREIBUNG from PRODUKT where PRD_GR_ID = [#request:gr_id#];"
  row="row" report-tag="report" result-attribute="rdbStatus" />
</dbresult>
```

➤
```
<dbresult>
  <rde-dm:rdb mode="query" tag="result" alias="AR_DEMO" sql="select ID, name,
  to_char(preis,'9990.00'),BESCHREIBUNG from PRODUKT where PRD_GR_ID = [#request:gr_id#1#].asInteger();"
  row="row" report-tag="report" result-attribute="rdbStatus" />
</dbresult>
```

  - Entfernen von Sonderzeichen

✖
```
…… where name like '[#request:name#]%';…….
```

➤
```
…… where name like '[#request:name#xxx#].replace('\'','\'\'')%';…….
```

Härten der Seiten
Prepared operations oder Prepared statements

Nutzung der Parameter-Übergabe:

- Prepared statements

```
<dbresult>
  <rde-dm:rdb mode="query" tag="result" alias="AR_DEMO" sql="SELECT  ID, name,
to_char(preis,'9990.00'),BESCHREIBUNG  from PRODUKT WHERE name like ? " row="row" report-tag="report" result-
attribute="rdbStatus" >
    <rde-rd:param type="string">[#request:name#]%</rde-rd:param>
  </rde-dm:rdb>
</dbresult>
```

- Prepared operations

```
<dbresult>
  <rde-dm:rdb mode="query" tag="result" alias="AR_DEMO" operation="AR_Produkte"
  row="row" report-tag="report" result-attribute="rdbStatus">
  <rde-rd:param type="integer">[#request:gr_id#0#]</rde-rd:param>
</dbresult>
```

Anmerkung:
Es darf kein ; am Ende der Statements stehen!

Härten der Seiten
Vermeiden von Informationen für Angreifer (1)

- Der Parameter **report-tag** gehört in **nicht** Live-Systeme
- Wird kein Ergebnis zur Anzeige erwartet (in der Regel DML-Anweisungen), so sollte man **process-mode="execute"** nutzen
- Man sollte den Parameter **result-attribute** auswerten und eine Fehlerseite aufrufen

```
<rde-dm:rdb mode="update" alias="AR_DEMO" process-mode="execute" row="notag" result-attribute="rdbStatus"
sql="INSERT INTO bestellung (id,NAME,VORNAME,PROD_ID,MENGE,KOMMENTAR) VALUES (SEQ_BESCH.nextval,
substr(?,1,30),substr(?,1,30),?, ?, substr(?,1,1000))">
  <rde-rd:param type="string">[#request:nachname#]</rde-rd:param>
  <rde-rd:param type="string">[#request:vorname#]</rde-rd:param>
  <rde-rd:param type="integer">[#request:prod_id#0#]</rde-rd:param>
  <rde-rd:param type="integer">[#request:menge#0#]</rde-rd:param>
  <rde-rd:param type="string">[#request:kommentar#]</rde-rd:param>
</rde-dm:rdb>
<rde-dm:attribute mode="condition" source="request" attribute="rdbStatus" op="lt" value="0">
  <rde-dm:if>
      <script>
       window.location.href="#RDE-URL:/html/arDBerror.htm/#"
      </script>
      <noscript>
       An dieser Stelle ist ein Fehler in der Anwendung aufgetreten. Bitte klicken Sie <a href="#RDE-
URL:/html/arDBerror.htm/#">hier</a> für die Fehlermeldung
      </noscript>
  </rde-dm:if>
</rde-dm:attribute>
```

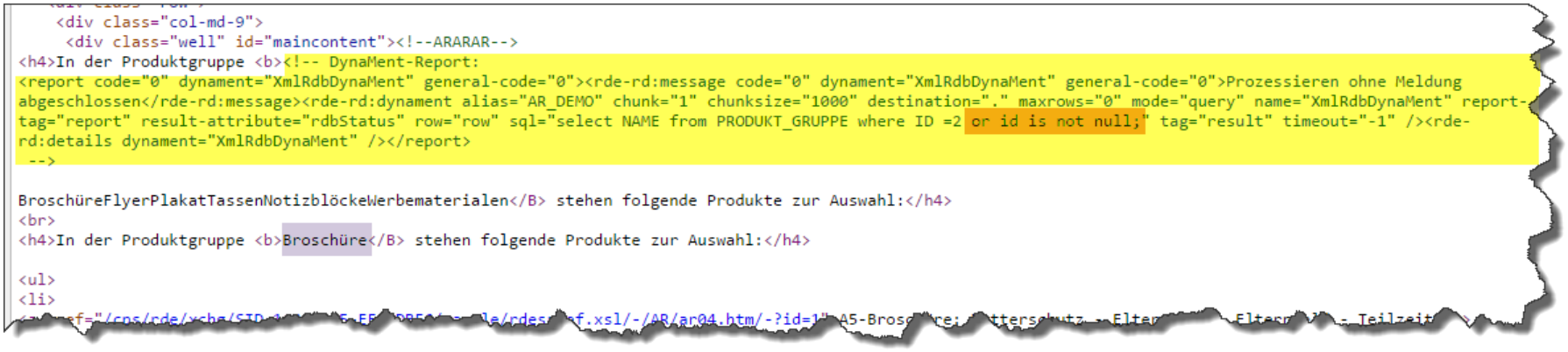
Härten der Seiten
Vermeiden von Informationen für Angreifer (2)

- Das SQL-Statement sollte inkl. der Standardwerte so formuliert sein, dass es lieber kein Ergebnis liefert, als dass eine Fehlermeldung kommt bzw. Daten beschnitten werden

```
<dbresult>
  <rde-dm:rdb mode="query" tag="result" alias="AR_DEMO" sql="SELECT  ID, name,
to_char(preis,'9990.00'),BESCHREIBUNG  from PRODUKT WHERE id = ? " row="row" result-attribute="rdbStatus" >
    <rde-rd:param type="integer">[#request:id#0#]%</rde-rd:param>
  </rde-dm:rdb>
</dbresult>
```

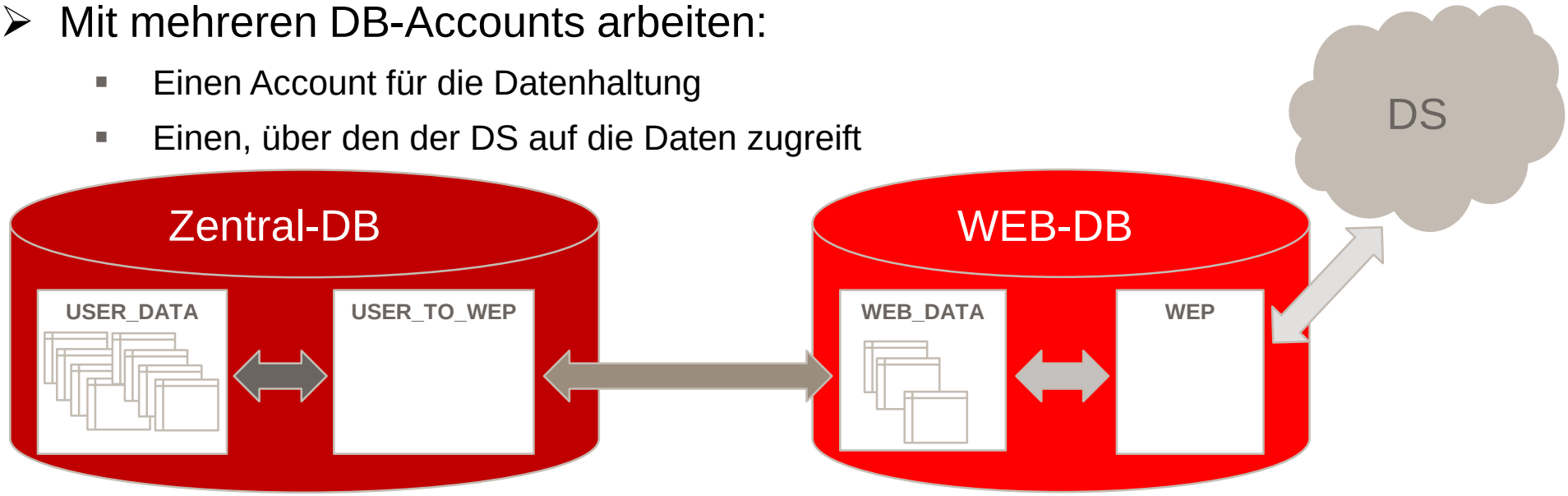
- Wird nur 1 Datensatz als Antwort erwartet, sollte man die **maxrows** auch auf 1 begrenzen

- Nutzung von **tag="notag"**



Was kann/sollte man beim Design der Datenbank beachten?

- Nur die Daten in der DB halten, die für die Web-Site benötigt werden
- Mit mehreren DB-Accounts arbeiten:
  - Einen Account für die Datenhaltung
  - Einen, über den der DS auf die Daten zugreift



- Den zugreifenden Account mit Minimalrechten ausstatten
- Mit Synonymen arbeiten, um den Account der Datenhaltung nicht preis zu geben
- Bei Oracle die Abfrage auf All_Views verhindern

Fragen & Antworten