APEX – play it save

DOAG regio Stuttgart

Carola Berzl
Consultant

Who Am I

- Consultant and course instructor at Trivadis GmbH in Munich
- Focus:
  - Oracle APEX:
    - Infrastructure
    - Application Development
    - Security
- Course instructor for the following Trivadis courses
  - Oracle Application Express (O-OAE)
  - Introduction to Oracle SQL (O-SQL)

Agenda

1. Introduction
2. Kinds of Attacks
3. SQL Injection
4. Cross Site Scripting (XSS)

Introduction

Introduction

A secure environment for confidential and secret data requires that **all** components fulfill the security-requirements

- Webserver
- Database-Server
- Database
- APEX instance (= workspace internal)
- Individual APEX workspace
- **APEX application**
  => Kinds of attacks
  => Countermeasures

Kinds of Attacks

Kinds of Attacks to Applications

- **SQL Injection**
- **Cross Site Scripting (XSS)**
  - Reflexive Attack
  - Persistent Attack
  - Measures against XSS

SQL Injection

SQL Injection

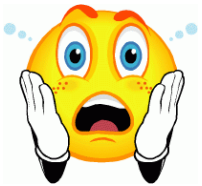
- General definition: A piece of SQL-Code is inserted into a form
  -> the SQL statement is changed

SQL Injection

Demo

SQL Injection

- SQL Injection with dynamic SQL
  - The SQL-statement is concatenated dynamically
  - e.g.: `l_sql := l_sql || ' WHERE deptno = ' || :P1_DEPTNO;`
  - If an attacker inserts certain strings (e.g. 50 or 1=1)
    -> a different statement will be executed
    -> all records are shown
  - The statement with the malicious code is concatenated **before** the PL/SQL block is parsed



SQL Injection

- Countermeasure:
  - **Embed** the variable **in** the bind-variable syntax into the string
  - e.g.: `l_sql := l_sql || ' WHERE deptno = :P1_DEPTNO';`
  - The PL/SQL block is parsed as a whole
    -> an error message appears

SQL Injection - Countermeasure

Demo

SQL Injection

- Practical tip:
  - Show SQL-statement in an item
  - Use the debug-view
  - Use select list if possible

SQL Injection in APEX 5

Demo

SQL Injection in APEX 5

- The imported application works the same as with APEX 4
- Attempt to save changes: error message ORA-01008 not all variables bound
- We can‘t insert „weak“ PL/SQL code

- Side-effect: Bind-Variable-Syntax in if-clause has to be changed

Cross Site Scripting (=XSS)

Cross site Scripting (=XSS)

- General definition:
  - Execution of JavaScript code is the aim of the attack
- Reflexive attack
  - Malicious code is excuted by the browser -> **one user** is affected
- Persistent attack
  - Malicious code is stored in the database -> is executed at **every call**

Cross Site Scripting (XSS) - reflexive

Demo (Wines)

Cross Site Scripting (XSS) - persistent

Demo (Customers)

Cross Site Scripting (XSS) – PL/SQL-Region

Demo (Grapes)

Countermeasure against XSS

- Mask the displayed characters (Escape special characters = YES)
- “Restricted Characters” allows blacklist
- Use APEX_ESCAPE with PL/SQL-regions

Show Pictures in Report Columns

Show Pictures in Report Columns

- Initial position:

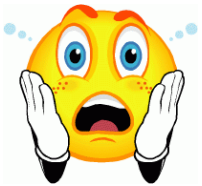
  Show an image in a report column dependent of an other column

Demo (Wine Categories)

Show Pictures in Report Columns

- Default attribute for column is „Display as text (escape special characters, does not save state)“
- **But** attribute „Standard Report Column“ must be used in order to show picture

  =>Exposure for XSS-Attacks



Show Pictures in Report Columns

- Countermeasures
  - If „Standard Report Column“ must be used
  - Don‘t use HTML in the query
  - Use HTML expression in column attribute

Questions and answers…

Carola Berzl
Consultant