

FIT2094-FIT3171 Databases
Week 12 Tutorial Suggested Solution
DB Connectivity, Web Technology
FIT Database Teaching Team

FIT2094-FIT3171 2021 S2

FIT2094-FIT3171 Databases

Author: FIT Database Teaching Team

License: Copyright © Monash University, unless otherwise stated. All Rights Reserved.

COPYRIGHT WARNING

Warning

This material is protected by copyright. For use within Monash University only. NOT FOR RESALE.

Do not remove this notice.

12.1 Database Connectivity

Discuss following terms:

1. Data layer → the data management application (DBMS)
2. Application layer → the external interface, mostly in the form of an Application Programming Interface (API)
3. Database middleware → software that manages connectivity and data transformation issues between applications and DBMSs
 - a. ODBC → Microsoft based database middleware which provides functionality for Windows based applications to access the database
 - b. JDBC → provides functionality for Java based applications to access the database
 - c. OLE-DB → Microsoft based database middleware which provides functionality for Windows based applications to access both relational and non-relational databases
4. Web server → the web server is software and underlying hardware which receives requests from the client's browsers and sends the responses back to the browsers via the internet/network. In the database query scenario, the web server generates the webpage contents (in html format) based on data retrieved from the web to database middleware then sends it to the client web browser.
5. Web to database middleware → a database server-side extension that sends/retrieves data to/from databases and passes them to the web server, which in turn sends the data to the client's browser for display.

12.2 Web-Database Connectivity using PHP

There is no sample solution for this section. The required files are provided on Moodle.

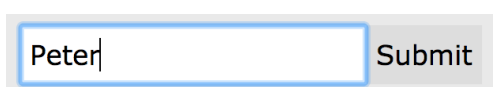
12.3 Web Frameworks and Security Consideration

12.3.1 Web Frameworks

1. Name some other popular web frameworks that can utilise Oracle as a database back-end.
 - Django
 - Node.js
 - CakePHP
 - Symfony
2. A common programming technique used in many frameworks (including Oracle) is Object-Relational Mapping (ORM). Briefly describe what it means.
 - It is a technique that lets you query and manipulate data from a database using an object-oriented paradigm.

12.3.2 SQL Injection

To understand how serious the issue is, let's assume you have a website which lets you enter a first name as a search query:



A screenshot of a web form. It consists of a text input field with a blue border and a light gray background. The text 'Peter' is entered into the field, followed by a vertical cursor. To the right of the input field is a button labeled 'Submit' in a light gray box.

The website then uses your search string (e.g. "Peter") and places it in a SQL SELECT statement so that it can show you results, using the following SQL query.
(Your search string is highlighted).

```
SELECT * FROM users WHERE first_name = 'Peter';
```

1. Discuss what SQL Injection means. In the example above, how can a malicious user craft a special search string in order to, say, view everything in another table they're not supposed to view?

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. The client may insert 'Peter' followed by 'or 1=1'. Since the second condition will always return true value, the output of the query shows all users details.

2. How can you prevent these from happening to your own application?

- Sanitise and check your input
- Use views, procedures and packages
- Manage the privileges of the users (e.g. not giving all users the admin privilege)
- Further reference:
https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.md

12.4 Web Modification Exercise

Sample solution is provided in week12_samplesolution.zip