FIT2094-FIT3171 2019 S1 -- Week 12 eBook

Credits and Copyrights:
Authors: FIT3171 2018 S2 UG Databases
FIT Database Teaching Team
Maria Indrawan, Manoj Kathpalia, Lindsay Smith, et al

Change Log:

- Formatted and Imported from Alexandria MAY 2019.

12.0. Database Web Interfaces - Role of PHP

Now that you are familiar with designing, creating and managing tables we will look at the manner in which such data can be accessed.

To date you have been using SQL Developer; clearly, in practice, your users will not have access to/use this item of software. Access to your created tables by normal users will be via an application or web front end.

PHP (recursive acronym for PHP: Hypertext Preprocessor) is one of the most widely used programming languages, especially for web development.

In this section, we will study how, as an example, PHP code can be used to access an Oracle database and present results of queries to an end-user. (Monash offers several advanced units in which you can further advance your understanding of PHP, and PHP is often used in final year industrial projects within a course).

PHP enables the mixing of PHP code (marked between **<?php** and **?>**) and standard HTML code within a single file. When accessed via the web server the PHP code is handled via the PHP processor on the web server and replaced with appropriate output.

For this unit we are not expecting you to become PHP experts, this is simply an exercise to increase your awareness of how a database can be accessed via the web. If you wish to delve further into PHP immediately there are a large number of good tutorials available on the web. A good starting point is https://www.w3schools.com/php/

The steps in using PHP to access table data are:

1. connect to the database
2. define a SQL query string

3. parse the SQL query against the database
4. execute the statement
5. fetch and display the data, and finally
6. free the resources being used and close the connection.

For Step 1, please refer sample code on Moodle called connection.php.

This is a file containing Oracle connection details, we will include this into PHP scripts we create to access the database.

For Steps 2 to 6, please refer sample code on Moodle called sampleStudentTable.php.

This file actually contains PHP code, interspersed with actual HTML code. The sample PHP script will access and display the student data in the student table of the UNIVERSITY database that you are familiar with: it has all the required material (in the PHP language) to carry out a SELECT of the student table and display the results in an HTML table. You should look through the code and understand the details of what has been coded.

12.0.1. Discussion Questions - PHP

NB: You are not expected to know how to code in PHP (writing code, correct syntax, etc) for the exam, but you are expected to know some basic theory of how to develop an interface for databases.

Use the following questions to guide your knowledge.

1. What is OCI, and the role of oci… functions in the PHP files?
2. From the PHP code samples given on Moodle, can you identify which parts are PHP code, and which parts are HTML code?
3. Why do you think connection details need to be extracted into a connection.php file rather than hard coding it in the sampleStudentTable.php file?
    a. Hint 1: Security?
    b. Hint 2: Consistency?

12.1. Database Web Interfaces - Practical Considerations and Security

12.1.1. Discussion Questions - Use of Frameworks

Nowadays, the use of frameworks are quite popular to develop entire interfaces and web applications (e.g. a Customer-Relationship Management / CRM app, using a database backend).

1. Name some other popular web frameworks that can utilise Oracle as a database back-end. (We have discussed Symfony as one good example).
2. A common programming technique used in many frameworks (including Oracle) is Object-Relational Mapping (ORM). Briefly describe what it means.

12.1.2. Discussion Questions - Security Considerations

SQL Injection is a very common vulnerability when it comes to building web frontends (e.g. in PHP) for databases. 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:

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?
2. How can you, as a Database Developer, prevent these from happening to your own database apps?

12.2. Exam Revision

Finally, please spend some time looking over the sample exam paper on Moodle with your tutor and classmates.

You may also want to brush up on your SQL using the SQL Revision Questions on Moodle.

NB: As the lecture focuses on trends in databases as well as exam revision, there will be NO pre-lecture notes.

That's the end of the tutorial series! Thank you very much :-)

EOF.
