Secure Programming
—— Introduction of the Web

胡天磊, Dr. HU Tianlei

Associate Professor

College of Computer Science, Zhejiang Univ.

htl@zju.edu.cn

Course Outline

- Introduction of Web Framework
- Introduction of Web Server Language
- Introduction of SQL & Database

Web Framework

A web application framework (WAF) is a software framework that is designed to support the development of dynamic websites, web applications, web services and web resources. The framework aims to alleviate the overhead associated with common activities performed in web development.

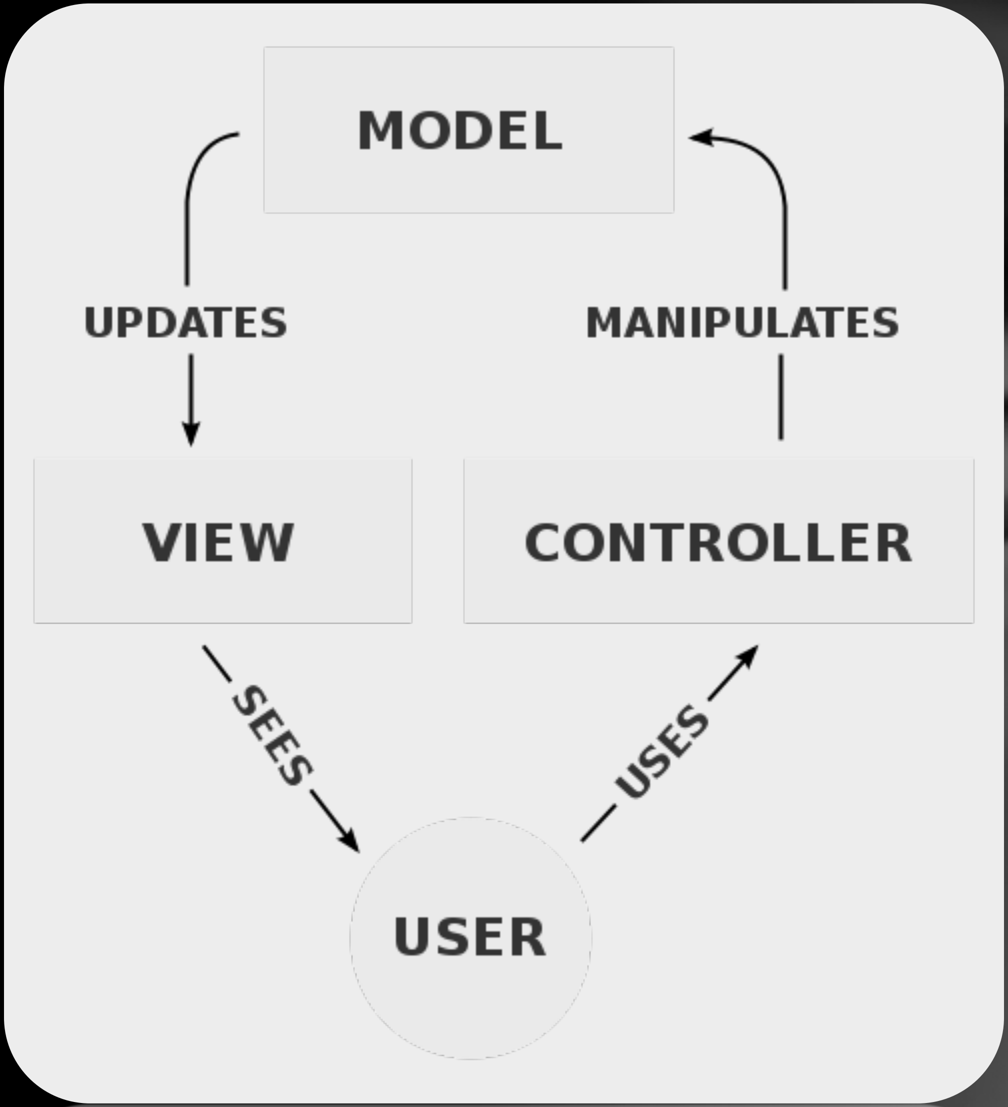
For example, many frameworks provide libraries for database access, templating frameworks and session management, and they often promote code reuse.

- **Model–view–controller (MVC)**
- **Three-tier organization**

Model–View–Controller (MVC)

Model–view–controller (MVC) is a software pattern for implementing user interfaces. It divides a given software application into three interconnected parts, so as to separate internal representations of information from the ways that information is presented to or accepted from the user.

- The central component, the model, consists of application data, business rules, logic, and functions.
- A view can be any output representation of information, such as a chart or a diagram. Multiple views of the same information are possible, such as a bar chart for management and a tabular view for accountants.
- The third part, the controller, accepts input and converts it to commands for the model or view.


MODEL
UPDATES
MANIPULATES
VIEW
CONTROLLER
SEES
USES
USER

Three-tier architecture

Presentation tier

This is the topmost level of the application. The presentation tier displays information related to such services as browsing merchandise, purchasing and shopping cart contents. It communicates with other tiers by which it puts out the results to the browser/client tier and all other tiers in the network. (In simple terms it is a layer which users can access directly such as a web page, or an operating systems GUI)

Three-tier architecture

Application tier

Also called business logic, logic tier, or middle tier

The logical tier is pulled out from the presentation tier and, as its own layer, it controls an application’s functionality by performing detailed processing.

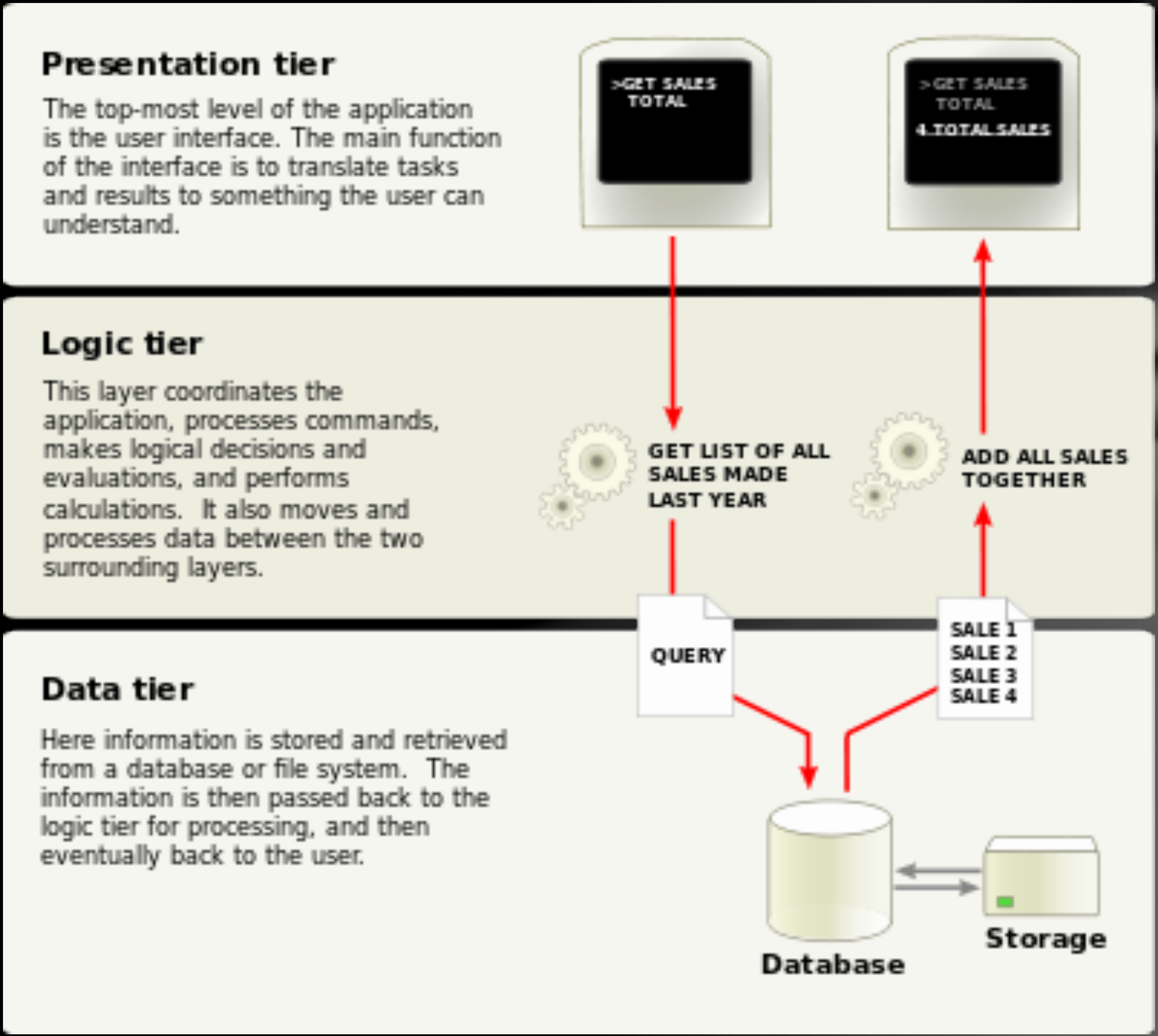
Three-tier architecture

Data tier

The data tier includes the data persistence mechanisms (database servers, file shares, etc.) and the data access layer that encapsulates the persistence mechanisms and exposes the data.

The data access layer should provide an API to the application tier that exposes methods of managing the stored data without exposing or creating dependencies on the data storage mechanisms.

Avoiding dependencies on the storage mechanisms allows them to be updated or changed without the application tier clients being affected by or even aware of the change.



Presentation tier

The top-most level of the application is the user interface. The main function of the interface is to translate tasks and results to something the user can understand.

Logic tier

This layer coordinates the application, processes commands, makes logical decisions and evaluations, and performs calculations. It also moves and processes data between the two surrounding layers.

Data tier

Here information is stored and retrieved from a database or file system. The information is then passed back to the user for processing, and then eventually back to the user.

SSH

What’s SSH

SSH is a integrated framework of struts + spring + hibernate, one of the very popular open-source Web application framework.

SSH framework is divided to four layers: presentation layer, logic layer, data persistence layer and domain module layer to help developers build a clear structure in the short term, can be a good reusability and easy maintenance of Web applications procedures.

- Struts infrastructure systems as a whole, is responsible for MVC separation, control the business logic;
- Hibernate is used to support to persistence.
- Spring in charge of management, manage struts and hibernate.

Web Server Language

Server Side Scripting

Many dynamically built web pages are mostly static. CGI, ISAPI and Servlets make you generate the entire page via your program, even though most of it is always the same.

Server-side scripting environments allow you to include server-side scripts in HTML documents (as well as client-side scripts).

- Server-side scripts are interpreted by the web server and translated into HTML before being sent to the client, so the client's browser doesn't even see the server side scripts.

Server-side scripts are like CGI programs in that they can access server-side resources such as databases, but they can't directly interact with the user.

- they can't for example, directly pop up a message box.

Like ISAPI and Servlets, server-side scripts are typically executed within the same process as the web server.

Web Server Scripting

Allows easy implementation of complex functionality (also for non-programmers)

- Think: Is this a good idea?
- Example scripting languages: ASP, JSP, PHP, Perl, Python

Scripts are installed on the Web server and return HTML as output that is then sent to the client

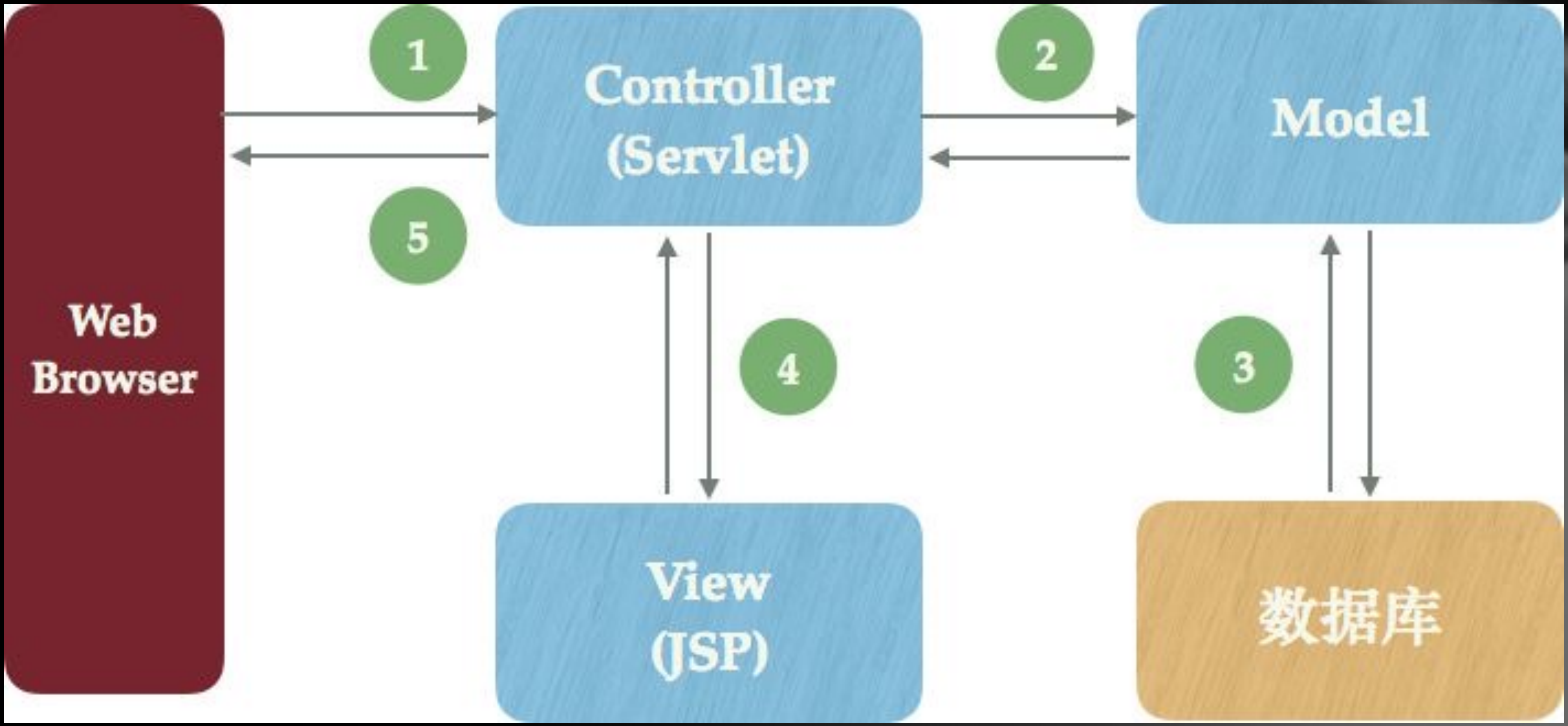
Java Servlet / JSP

What's JSP

The JavaServer Pages is a technology for inserting dynamic content into a HTML or XML page using a Java servlet container.

- In other word, instead of sending HTML pages to web clients that are always the same for every one, you can send HTML pages that can be different for each client and each time they receive it (using database data for instance).

Data Flow



Syntax

JSP pages use several delimiters for scripting functions.

- <% … %>, scriptlet, is a fragment of Java code that is run when the user requests the page.
- <%= … %>, expressions, places an expression to be evaluated inside the java servlet class. Expressions should not be terminated with a semi-colon.
- <%@ … %>, comment, does nothing. It is ignored. It lets you document the file. It is different from a HTML comment as a HTML comment (<!-- -->) will appear in the generated HTML file.

Example

```
<p>Counting to three:</p>
<% for (int i=1; i<4; i++) { %>
   <p>This number is <%= i %>.</p>
<% } %>
<p>OK.</p>
```

The output displayed in the user's web browser would be:

```
Counting to three:

This number is 1.

This number is 2.

This number is 3.

OK.
```

Directives

JSP directives are added at the top of a JSP page. These directives control how the JSP compiler generates the servlet.

include

The include directive informs the JSP compiler to include a complete file into the current file. It is as if the contents of the included file were pasted directly into the original file. This functionality is similar to the one provided by the C preprocessor. Included files generally have the extension "jspf" (for JSP Fragment)

```
<%@ include file="somefile.jspf" %>
```

Directives

page

```
<%@ page import="java.util.*" %> <%-- example import --%>
<%@ page contentType="text/html" %> <%-- example contentType --%>
<%@ page isErrorPage="false" %> <%-- example for non error page --%>
<%@ page isThreadSafe="true" %> <%-- example for a thread safe JSP --%>
<%@ page session="true" %> <%-- example for using session binding --%>
<%@ page autoFlush="true" %> <%-- example for setting autoFlush --%>
<%@ page buffer="20kb" %> <%-- example for setting Buffer Size --%>
```

Note: Only the "import" page directive can be used multiple times in the same JSP.

Directives

taglib

The taglib directive indicates that a JSP tag library is to be used. The directive requires a prefix (much like a namespace in C++) and the URI for the tag library description.

```
<%@ taglib prefix="myprefix" uri="taglib/mytag.tld" %>
```

Implicit objects

t

w
a
c

Object	Description
out	The JspWriter used to write the data to the response stream.
page	The servlet itself.
pageContext	A PageContext instance that contains data associated with the whole page. A given HTML page may be passed among multiple JSPs.
request	The HttpServletRequest object that provides HTTP request information.
response	The HttpServletResponse object that can be used to send data back to the client.
session	The HttpSession object that can be used to track information about a user from one request to another.
config	Provides servlet configuration data.
application	Data shared by all JSPs and servlets in the application.
exception	Exceptions not caught by application code.

JSP actions

jsp:include

Includes a specified jsp into the returned HTML page but it works differently. The Java servlet temporarily hands the request and response off to the specified JavaServer Page. Control will then return to the current JSP, once the other JSP has finished. Using this, JSP code will be shared between multiple other JSPs, rather than duplicated.

```
<html>
 <head></head>
 <body>
  <jsp:include page="mycommon.jsp" >
   <jsp:param name="extraparam" value="myvalue" />
  </jsp:include>
  name:<%=request.getParameter("extraparam")%>
 </body>
</html>
```

JSP actions

jsp:param

Can be used inside a jsp:include, jsp:forward or jsp:params block. Specifies a parameter that will be added to the request's current parameters.

jsp:forward

Used to hand off the request and response to another JSP or servlet. Control will never return to the current JSP.

```
<jsp:forward page="subpage.jsp" >
  <jsp:param name="forwardedFrom" value="this.jsp" />
</jsp:forward>
```

In this forwarding example, the request is forwarded to subpage.jsp

JSP actions

jsp:plugin

Older versions of Netscape Navigator and Internet Explorer used different tags to embed an applet. This action generates the browser specific tag needed to include an applet. The plugin example illustrates an HTML uniform way of embedding applets in a web page.

```
<jsp:plugin type=applet height="100%" width="100%"
  archive="myjarfile.jar, myotherjar.jar"
  codebase="/applets"
  code="com.foo.MyApplet" >
  <jsp:params>
    <jsp:param name="enableDebug" value="true" />
  </jsp:params>
  <jsp:fallback>
   Your browser does not support applets.
  </jsp:fallback>
</jsp:plugin>
```

JSP References

Tutorials:

http://www.apl.jhu.edu/~hall/java/Servlet-Tutorial/

http://www.coreservlets.com/

Specification:

http://java.sun.com/products/jsp/download.html

PHP

What’s PHP

- PHP is an acronym for "PHP Hypertext Preprocessor"
- PHP is a widely-used, open source scripting language
- PHP scripts are executed on the server
- PHP costs nothing, it is free to download and use

PHP (Hypertext Pre-Processor)

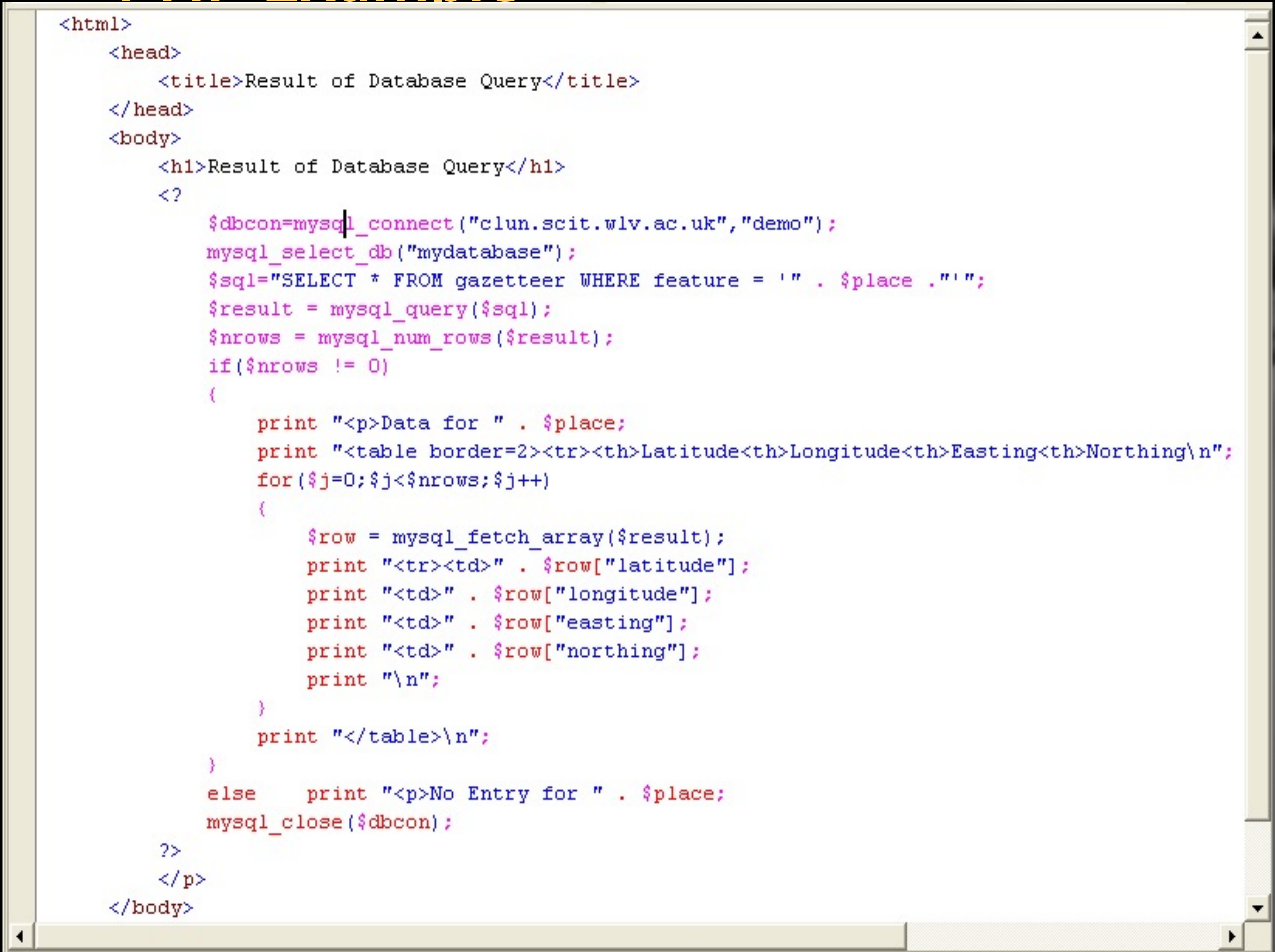
Advantages:

- Cross-platform support (PWS, IIS and Apache web servers)
- Open Source, developed by Rasmus Lerdorf in 1994.
- Language specifically designed for the web.
- Typically runs in process.
- Excellent string processing capabilities (like Perl)
- Tight integration with MySQL (fast)
- Zend optimizing compiler (available commercially)

Disadvantages:

- Quick and dirty ("stubborn function-over-form approach").
- Poor error handling
- "Tedious" objected-oriented programming support.
- Normally interpreted

PHP Example



```
<html>
    <head>
        <title>Result of Database Query</title>
    </head>
    <body>
        <h1>Result of Database Query</h1>
        <?
            $dbcon=mysql_connect("clun.scit.wlv.ac.uk","demo");
            mysql_select_db("mydatabase");
            $sql="SELECT * FROM gazetteer WHERE feature = '" . $place ."'";
            $result = mysql_query($sql);
            $nrows = mysql_num_rows($result);
            if($nrows != 0)
            {
                print "<p>Data for " . $place;
                print "<table border=2><tr><th>Latitude<th>Longitude<th>Easting<th>Northing\n";
                for($j=0;$j<$nrows;$j++)
                {
                    $row = mysql_fetch_array($result);
                    print "<tr><td>" . $row["latitude"];
                    print "<td>" . $row["longitude"];
                    print "<td>" . $row["easting"];
                    print "<td>" . $row["northing"];
                    print "\n";
                }
                print "</table>\n";
            }
            else    print "<p>No Entry for " . $place;
            mysql_close($dbcon);
        ?>
        </p>
    </body>
```

Introduction of SQL Language

SQL

What's SQL

- SQL stands for Structured Query Language
- SQL lets you access and manipulate databases
- SQL is an ANSI (American National Standards Institute) standard

RDBMS

- RDBMS stands for Relational Database Management System.
- RDBMS is the basis for SQL, and for all modern database systems such as MS SQL Server, IBM DB2, Oracle, MySQL, and Microsoft Access.
- The data in RDBMS is stored in database objects called tables.
- A table is a collection of related data entries and it consists of columns and rows.

A Table in RDBMS

Id	Name	Age	Grade	Comment
1	Alice	18	A	…
2	Bob	20	B	?
3	Calvin	16	F	

Table: Students

Columns: Id, Name, Age, Grade, Comment

Rows: Id = 1, Id = 2 …

SQL Statements

- Most of the actions you need to perform on a database are done with SQL statements.
- The following SQL statement selects all the records in the "Customers" table:

```
SELECT * FROM Customers;
```

Keep in Mind That ...

- SQL is NOT case sensitive: select is the same as SELECT.

SQL Commands

Some of The Most Important SQL Commands

- SELECT - extracts data from a database
- UPDATE - updates data in a database
- DELETE - deletes data from a database
- INSERT INTO - inserts new data into a database
- CREATE DATABASE - creates a new database
- ALTER DATABASE - modifies a database
- CREATE TABLE - creates a new table
- ALTER TABLE - modifies a table
- DROP TABLE - deletes a table
- CREATE INDEX - creates an index (search key)
- DROP INDEX - deletes an index.

SQL-Select

The SELECT statement is used to select data from a database.

- The result is stored in a result table, called the result-set.

SQL SELECT Syntax

```
SELECT column_name,column_name
FROM table_name;
WHERE column_name = value
```

And

```
SELECT * FROM table_name;
```

Navigation in a Result-set

Most database software systems allow navigation in the result-set with programming functions, like: Move-To-First-Record, Get-Record-Content, Move-To-Next-Record, etc.

SQL-Insert Into

The INSERT INTO statement is used to insert new records in a table.

SQL Insert Into Syntax

It is possible to write the INSERT INTO statement in two forms.

The first form does not specify the column names where the data will be inserted, only their values:

```
INSERT INTO table_name
VALUES (value1,value2,value3,...);
```

The second form specifies both the column names and the values to be inserted:

```
INSERT INTO table_name (column1,column2,column3,...)
VALUES (value1,value2,value3,...);
```

SQL-Update

The UPDATE statement is used to update existing records in a table.

SQL Update Syntax

```
UPDATE table_name
SET column1=value1,column2=value2,...
WHERE some_column=some_value;
```

Notice

The WHERE clause specifies which record or records that should be updated. If you omit the WHERE clause, all records will be updated!

SQL - Delete

The DELETE statement is used to delete rows in a table.

SQL Delete Syntax

```
DELETE FROM table_name
WHERE some_column=some_value;
```

Notice

The WHERE clause specifies which record or records that should be updated. If you omit the WHERE clause, all records will be updated!

Delete All Data

```
DELETE FROM table_name;
or
DELETE * FROM table_name;
```

More Info

Reference: http://www.w3schools.com/sql/default.asp

Introduction of SQL Database

What's Database

A database is an organized collection of data. The data are typically organized to model relevant aspects of reality in a way that supports processes requiring this information.

Database management systems (DBMSs) are specially designed software applications that interact with the user, other applications, and the database itself to capture and analyze data.

A general-purpose DBMS is a software system designed to allow the definition, creation, querying, update, and administration of databases.

Well-known DBMSs : MySQL, SQL Server, Access, Oracle, Sybase, DB2.

What’s MySQL

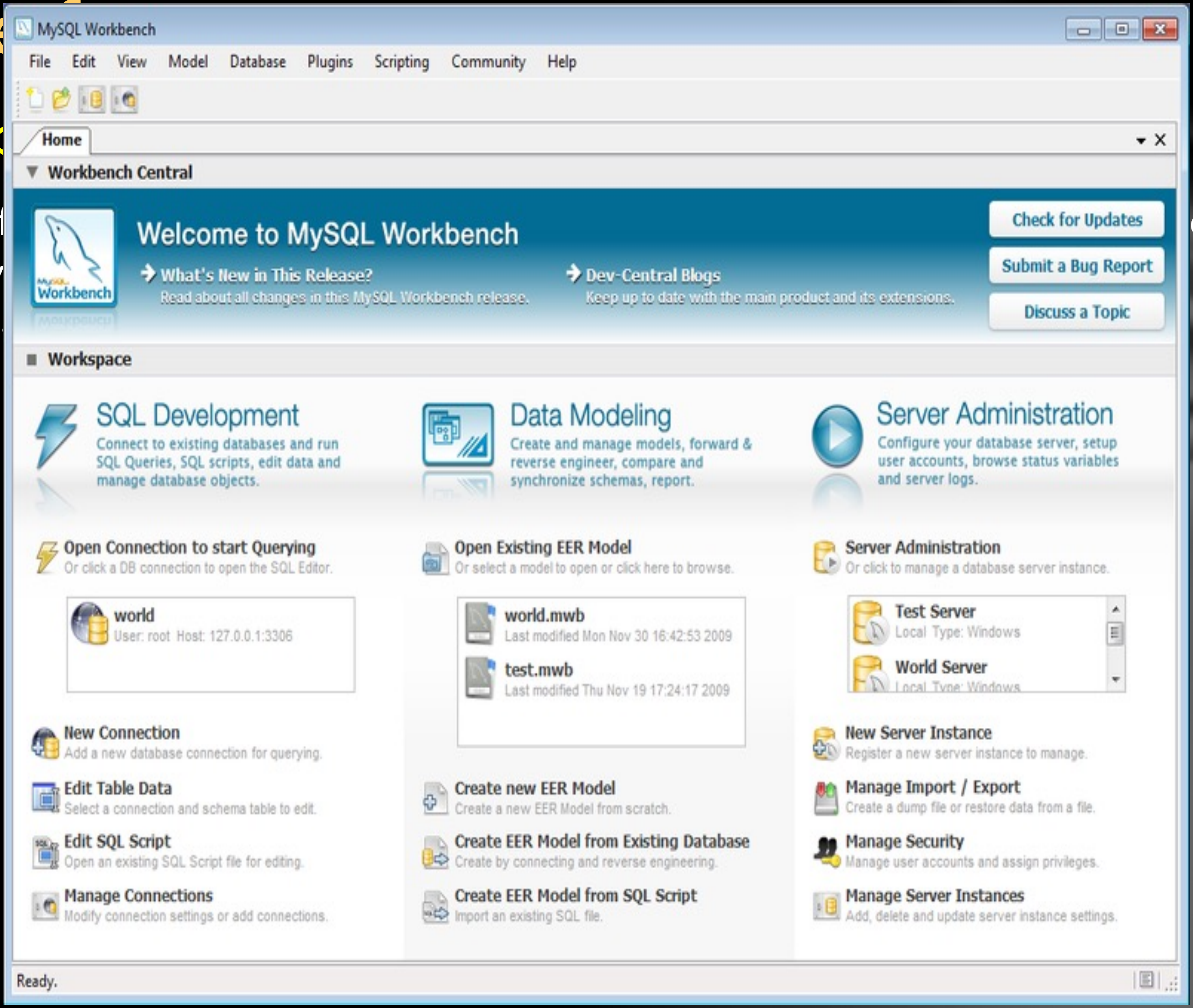
MySQL is the world's most widely used open-source relational database management system (RDBMS).

It is named after co-founder Michael Widenius's daughter, My. The SQL phrase stands for Structured Query Language.

Inte

Grap

The of ed
by My
datab



MySQL Workbench

File Edit View Model Database Plugins Scripting Community Help

Home

Workbench Central

Welcome to MySQL Workbench

What's New in This Release?
Read about all changes in this MySQL Workbench release.

Dev-Central Blogs
Keep up to date with the main product and its extensions.

Check for Updates

Submit a Bug Report

Discuss a Topic

Workspace

SQL Development
Connect to existing databases and run SQL Queries, SQL scripts, edit data and manage database objects.

Data Modeling
Create and manage models, forward & reverse engineer, compare and synchronize schemas, report.

Server Administration
Configure your database server, setup user accounts, browse status variables and server logs.

Open Connection to start Querying
Or click a DB connection to open the SQL Editor.

world
User: root Host: 127.0.0.1:3306

New Connection
Add a new database connection for querying.

Edit Table Data
Select a connection and schema table to edit.

Edit SQL Script
Open an existing SQL Script file for editing.

Manage Connections
Modify connection settings or add connections.

Open Existing EER Model
Or select a model to open or click here to browse.

world.mwb
Last modified Mon Nov 30 16:42:53 2009

test.mwb
Last modified Thu Nov 19 17:24:17 2009

Create new EER Model
Create a new EER Model from scratch.

Create EER Model from Existing Database
Create by connecting and reverse engineering.

Create EER Model from SQL Script
Import an existing SQL file.

Server Administration
Or click to manage a database server instance.

Test Server
Local Type: Windows

World Server
Local Type: Windows

New Server Instance
Register a new server instance to manage.

Manage Import / Export
Create a dump file or restore data from a file.

Manage Security
Manage user accounts and assign privileges.

Manage Server Instances
Add, delete and update server instance settings.

Ready.

Interfaces

Command line

MySQL ships with many command line tools, from which the main interface is 'MySQL' client.

Programming

Open Source LAMP software

Linux	http://www.linux.org
Apache	http://www.apache.org
MySQL	http://www.mysql.com
PHP	http://www.php.net

Review

- **Introduction of Web Framework**
  - MVC
  - Three-tier architecture
  - SSH
- **Introduction of Web Server Language**
  - Java / JSP
  - PHP
- **Introduction of Database & SQL**
  - Select / Insert-Into / Update / Delete
  - MySQL