Overview

- Database review
  - Database server

- Database web interface
  - Combine markup and query languages
  - Server side scripting
  - SQL injection

Database Server

- Accepts requests to access database
  - Requests in query language (e.g., SQL)

- MySQL
  - Multithreaded
  - Multiuser
  - SQL database management system (DBMS)
  - Open source
    - Free download of Community Edition

Database Web Interface

- Requires
  - Database server (MySQL)
  - Web server (Apache)
  - Method of connecting two (scripts)
    - CGI, Javascript, PHP, Ruby on Rails
PHP – PHP: Hypertext Preprocessor

Scripting language
• Designed to produce web pages
• Can also be used from command line, in GUIs

Characteristics
• Paradigm
  ➢ Imperative, object-oriented
• Type system
  ➢ Dynamic, weak
• Application domain
  ➢ Server side scripting

Server-side Scripting

Steps
1. Browser requests PHP document from server
2. Server reads the PHP document and
   ➢ Runs the PHP code
   ➢ Generates HTML document
   ➢ Returns HTML document to browser
3. Browser displays HTML document

Other server-side scripting languages
• ASP.NET, JavaServer Pages, mod_perl, eRuby

PHP Documents

PHP document
• Filename ends in .php or .phtml
• PHP code enclosed in (non-html) tags
  ➢ <?php PHP code ?>
  ➢ <script language="php"> PHP code </script>
• Everything outside of PHP tags is unchanged
  ➢ Usually standard HTML
• PHP output is standard HTML document

PHP Document Example

test2.php
<?php
function hello() { return 'Hello'; }
function world() { return 'World!\n'; }
$fn1 = 'hello';
$fn2 = 'world';
echo $fn1 . ' ' . $fn2();
?>
PHP Functions

- Connect to database server
  - `mysql_connect($hostName, $userName, $password)` or die("Unable to connect to host $hostName");
- Modify database
  - `mysql_select_db($dbName)` or die("Unable to select database $dbName");
- Disconnect from database server
  - `mysql_close();`

Manage Tables Through Queries

- Basic information searches
  - `$SQL = "SELECT FirstName, LastName, DOB, Gender FROM Patients WHERE Gender = '$Gender' ORDER BY FirstName DESC";`;
  - `$Patients = mysql_query($SQL);`
- Editing, adding, and deleting records and tables
  - `$SQL = "INSERT INTO Patients (FirstName, LastName) VALUES('$firstName', '$lastName')";`;
  - `$Patients = mysql_query($SQL);`
- Potential problem...

SQL Injection

- Users may inject malicious commands to query
  - Through intentionally misformed fields
- Example
  - Query code
    - `$SQL = "SELECT ... WHERE Gender = '$Gender' ...";`;
    - `$Patients = mysql_query($SQL);`
  - User enters for Gender
    - "M"; DROP TABLE Patients;" instead of "M"
  - Query becomes
    - `mysql_query("SELECT...WHERE Gender = 'M'; DROP TABLE patients;...";`;
  - Causing patient database to be deleted!
- Prevention
  - User input must be filtered / escaped / parameterized

Ruby On Rails

- Web application development framework
  - Written in Ruby
  - Supports web database applications
  - Uses Javascript libraries, AJAX for GUI
- Model-view-controller model
  - Used to organize web DB applications
  - Separates database from GUI
- Generates "scaffolding" code
  - Scripts generate code from specifications
  - Gets web database up and running quickly
**AJAX**

- Asynchronous JavaScript and XML
- Group of interrelated web development techniques
  - Used for creating interactive web application
  - Can update portions of page without browser refresh
  - Retrieves data using XMLHttpRequest from browser

**Examples**
- Google Maps
- Gmail
- Flickr

**eRuby**

- Rails uses eRuby
  - Template system to embed Ruby in text document
  - Needs interpreter to process eRuby and output HTML
  - Filename ends in `.rhtml` or `.erb`

**eRuby tags**

- `<% Ruby code %>`
- `% Ruby code`
- `<%= Ruby expression %>`
  - Evaluates expression and replaces with result
  - Example: `<%= 2+3 %>` → `5`

**eRuby Examples**

- Generate 3 list items
  `<ul>
  <% 3.times do %>
  <li>list item</li>
  <% end %>
  </ul>`

- Alternative version
  `<ul>
  % 3.times do
  % list item
  % end
  </ul>`

- Return current time
  `<p>Date: <%= Time.now %></p>`