CSCI-UA:0060-02

Database Design & Web Implementation

Professor Evan Sandhaus
sandhaus@cs.nyu.edu
evan@nytimes.com

Lecture #19: PHP: The PHP Hypertext Preprocessor
Adminstrivia

- Homework
  - Homework 6 due TODAY

- Do Some Reading
  - Chapters 1-3 PHP & MYSQL Book

- Extra Credit!
  - PHP Extra Credit Assignment
On The Menu

- HTML Forms + PHP = Recap
- PHP - Selective Blocks
- PHP And MySQL
  - Syntax
  - Examples
<form
  action="cms.php"
  method="post"
>
</form>
Inputs

<input type="text" name='headline'/>

<select name='issue'>
  <option value='winter'>Winter</option>
  <option value='spring'>Spring</option>
  <option value='summer'>Summer</option>
  <option value='fall'>Fall</option>
</select>
<input type='radio' name='content_type' value='news'>News</input>
<input type='radio' name='content_type' value='opinion'>Opinion</input>

<textarea rows=10 cols=60 name='article_body'></textarea>

<input type="checkbox" name="tag[]" value="us">United States<br>
<input type="checkbox" name="tag[]" value="world">World<br>
<input type="checkbox" name="tag[]" value="sports">Sports<br>
<input type="checkbox" name="tag[]" value="entertainment">Entertainment<br>
Submit

<input type="submit" value="Submit">
<!DOCTYPE html>
<html>
<head>
    <title>Fake CMS Form</title>
</head>
<body>
<form name="cms_input" action="cms.php" method="post" class='pretty_form'>
    <p>Headline:<br>
        <input type="text" name='headline'/>
    </p>
    <p>Byline:<br>
        <input type="text" name='byline'/>
    </p>
    <p>Issue:<br>
        <select name='issue'>
            <option value='winter'>Winter</option>
            <option value='spring'>Spring</option>
            <option value='summer'>Summer</option>
            <option value='fall'>Fall</option>
        </select>
    </p>
    <p>Content Type:<br>
        <input type='radio' name='content_type' value='news'>News
        <input type='radio' name='content_type' value='opinion'>Opinion
    </p>
    <p>Article Text:<br>
        <textarea rows="10" cols="60" name='article_body'>
        </textarea>
    </p>
    <p>Tags:<br>
        <input type='checkbox' name='tag[]' value='us'>United States<br>
        <input type='checkbox' name='tag[]' value='world'>World<br>
        <input type='checkbox' name='tag[]' value='sports'>Sports<br>
        <input type='checkbox' name='tag[]' value='entertainment'>Entertainment<br>
    </p>
</form>
</body>
</html>
Handling Forms in PHP

- **$_REQUEST** - Variable where all the request parameters get stored
- **$_GET & $_POST** alternatives based on HTTP method used to request form
- **var_dump / print_r** : EXTREMELY USEFUL methods for printing out the values of complex objects.
- Let's submit our forms and lookup the values.
What Is Truth

When converting to boolean, the following values are considered FALSE:

- the boolean FALSE itself
- the integer 0 (zero)
- the float 0.0 (zero)
- the empty string, and the string "0"
- an array with zero elements
- an object with zero member variables (PHP 4 only)
- the special type NULL (including unset variables)
== vs ===

- $x == y$
  - Checks if $x$ and $y$ evaluate to the same value
- $x === y$
  - Checks if $x$ and $y$ evaluate to the same value AND have the same type.

E.G.
- $0 == \text{false} \ // \ True$
- $0 === \text{false} \ // \ False$
PHP Selective Blocks

```php
<html>
<head>
    <title>Insert Demo</title>
</head>
<body>
    <?php if ($condition) : ?>
    <!-- Printed iff $condition is true -->
    <?php elseif($condition_2): ?>
    <!-- Printed iff $condition is false and $condition_2 is true -->
    <?php else: ?>
    <!-- Printed if both $condition and $condition_2 are false. -->
    <?php endif; ?>
</body>
</html>
```
**PHP & MySQL**

- `connect`
  - `$database_connection = mysqli_connect($host, $username, $password, $database_name);`
PHP Security

- Don't put sensitive (e.g. passwords) information in web-accessible folders
- PHP on i6 can include files from non-web-accessible folders, put sensitive information there.
PHP Mysql

- Query
  - $results = mysqli_query($database_connection, $sql);

Tuesday, April 16, 13
**PHP Mysql**

- **Handle Results**
  - while ($row = $result-&gt;fetch_assoc()) {
    ...
  }

  - Iterates over all rows returned by the database as an associative array between column names and values.
PHP Query Security

- PHP Will often take user inputs and place those inputs into a query.
- Malicious actors (bad hackers) can embed MySQL commands into their inputs that can affect the underlying database and inadvertently expose your private data.
PHP Query Security

- Suppose you have a form that takes a user name and then queries the database for the username.
- "SELECT * FROM user WHERE user_name ='".$user_name.";";
- What would happen if a bad actor submitted this as a user name: 
  - '; DROP TABLES;
- Official Name: SQL Injection attack
PHP SQL Injection

HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.

OH, DEAR - DID HE BREAK SOMETHING? IN A WAY-

DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;--?

OH, YES. LITTLE BOBBY TABLES, WE CALL HIM.

WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.

AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.
Protecting Against SQL Injection

- Use the `mysqli_real_escape_string` on ALL database inputs.
- E.G.
  ```
  $sql = "SELECT * FROM x WHERE y ="'. mysqli_real_escape_string($z).'"";
  ```
Let's Build

- PHP Script That queries mysql to display a table containing all professors and all classes.
- PHP Script That Submits a professor name through a `<select>` drop-down pre-populated with all valid professor names.
- (If Time) PHP Script That Allows Us to add new professors, classes and associations between them.