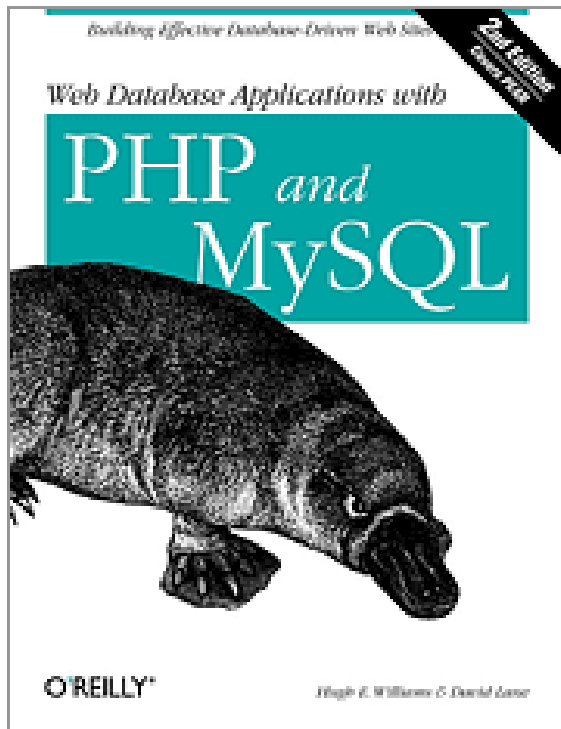


Database web interface

- User accounts
 - read/write restrictions
- 8 Web pages
 - account creation page/login page
 - at least one that allows (some) users to insert data
 - at least three predefined queries
 - at least three flexible/free form queries

Web accessible Databases PHP

Oct 25, 2007



Safari Online

www.php.net



Overview

- Data flow
 - html, php, sql, sessions
- HTML
- PHP
 - variables
 - control flow
 - connect to MySQL
 - HTML forms
 - Sessions
 - Authentication
 - binary data

Today's examples will be at:

<https://64.59.233.234/exampleFiles/>

`/opt/lampp/htdocs_secure/exampleFiles`

You have web space at:

`/opt/lampp/htdocs_secure/PUNetID`

Database Usage Scenario



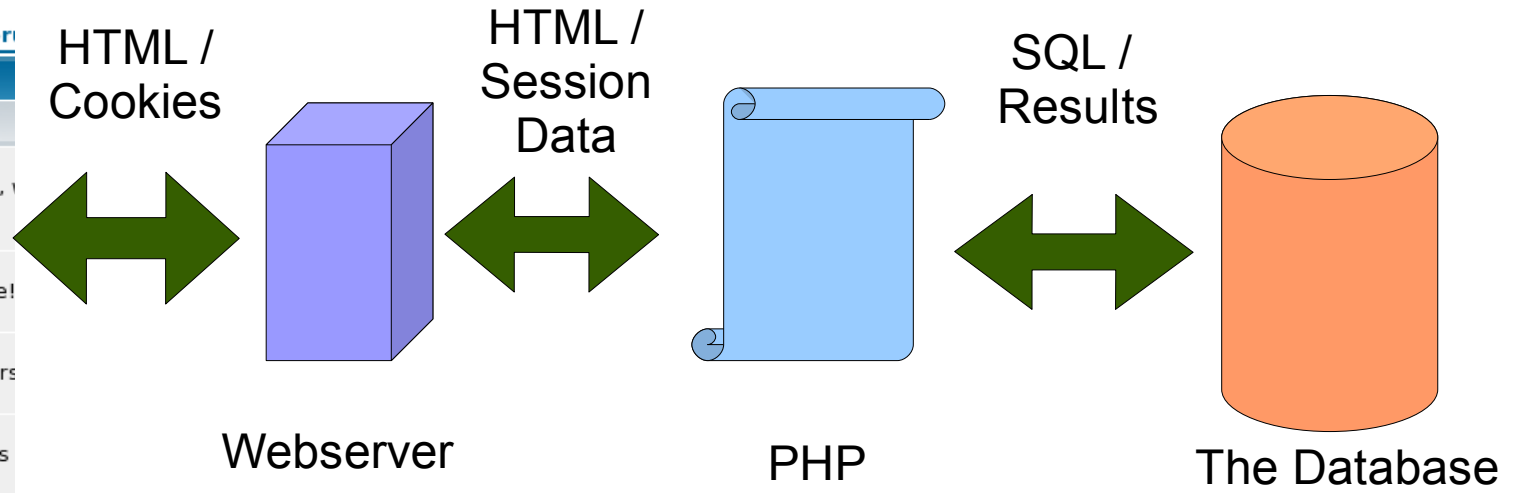
Pacific

The time now is Wed Jul 11, 2007 1:28 pm
Pacific University Computer Science For

Forum

Tools

- Linux**
Discuss your experiences with Linux, how do I do that?
- Eclipse**
Discuss your experience with Eclipse!
- Subversion**
Discuss your experience with Subvers
- Compilers/Make**
Discuss your experience with various
- Other**
All the other software tools you need!



User

Simple HTML

```
<html>
  <head>
    <title>The Window Title
  </title>
</head>
<body>
  <h1>Hello everybody!</h1>
  <p>
    <table border=1>
      <tr><td>0,0</td><td>0,1</td></tr>
      <tr><td>1,0</td><td>1,1</td></tr>
    </table>
  <p>
    <a href="http://zeus.cs.pacificu.edu">Zeus!</a>
    
  </body>
</html>
```

Hello everybody!

0,0	0,1
1,0	1,1



Zeus!

HelloWorld.php

```
<html>
  <head>
    <title>The Window Title
  </title>
  </head>
  <body>

    <?php
      // HelloWorld.php
      print "Hello World!";
      print "<H1>Hello World!</H1>";
    ?>

  </body>
</html>
```

Danger! Quotation marks
do not copy and paste well!

VariablesIfs.php

```
<body>
  <H1>
  <?php
    $counter = 1; // create variable
    if( $counter == 0)
    {
      print "ZERO";
    }
    else
    {
      print $counter;
    }
  ?>
</H1>
</body>
```

Loops.php

<body>

<?php

```
$counter = 1; // create variable
while( $counter < 10)
{
    print $counter . " ". $counter*2;
    print "<p>";
    $counter += 1;
}
?>
```

</body>


```
<table border=1 cellpadding=4>
```

LoopsTable.php

```
<?php
```

```
    $rows = 1; // create variable
```

```
    while( $rows < 10)
```

```
    {
```

```
        print "<tr>";
```

```
        $columns = 1; // create variable
```

```
        while( $columns < 10)
```

```
        {
```

```
            print "<td>";
```

```
            print $rows . " , " . $columns;
```

```
            print "</td>";
```

```
            $columns += 1;
```

```
        }
```

```
        print "</tr>";
```

```
        $rows += 1;
```

```
    }
```

```
?>
```

```
</table>
```

```
<body>
  <?php
    print "<table border=1> <tr>";
    $columns = 1; // create variable
    while( $columns < 10)
    {
      print "<td>" . $columns . "</td>";
      $columns += 1;
    }
    print "</table>";
  ?>
  Hello out there
  <center> HI!</center>
  <?php
    print $columns; // retains value from above
  ?>
</body>
```

Connect to MySQL

Put this in library/connDB.php:

```
<?php
    // when we include this file we include
    // the variable $conn

    $conn = mysql_connect("127.0.0.1:3306",
        "yourlogin", "yourpassword")
    or print "Error connecting to mysql";

    mysql_select_db("PUNetID_gradebook");
?>
```

```
$ ls connDB.php
-rwxr-x--- 1 chadd nogroup 21:10 connDB.php
```

Connect to MySQL

Put this in `library/connDBBigProject.php`:

```
<?php
    // when we include this file we include
    // the variable $conn

    $conn = mysql_connect("127.0.0.1:3306",
        "yourlogin", "yourpassword")
    or print "Error connecting to mysql";

    mysql_select_db("PUNetID_BigProject");
?>
```

Close database connection

Put this in `library/closeDB.php`:

```
<?php
    mysql_close($conn) ;
?>
```

Include this file at the end of the php code

```
<?php
    include 'library/closeDB.php' ;
?>
```

php skeleton

```
<?php
    session_start();
    include 'library/connDB.php';
```

```
?>
```

```
<html>
    <head>
        <title></title>
    </head>
    <body>
        MIX OF PHP AND HTML
    </body>
</html>
```

```
<?php
    include 'library/closeDB.php';
```

```
?>
```

```
<body>
```

query.php

```
<?php
```

```
// don't forget to start_session() and  
// include connDB.php at the TOP of the file
```

```
$query = "SELECT FirstName, LastName  
from Students left join Majors on  
(Students.MajorID= Majors.MajorID)";
```

```
// run the query
```

```
$result = mysql_query($query);
```

```
// for each row in the result set
```

```
while( $row = mysql_fetch_array($result) )
```

```
{
```

```
    print "{$row['FirstName']} {$row['LastName']}";
```

```
    print "<p>";
```

```
}
```

```
include 'library/closeDB.php';
```

```
?>
```

```
</body>
```

input.html

```
<body>
  <form method="post" action="showMajors.php">
    Major:
    <select NAME="MajorID">
      <option VALUE="1">Computer Science</option>
      <option VALUE="2">Biology</option>
      <option VALUE="3">English</option>
    </select>
    Last Name:
    <input TYPE="text" NAME="LastName">
    <input TYPE="submit" NAME="Request" VALUE="Go" />
  </form>
</body>
```

Major: Last Name:

Computer Science
Biology
English

showMajors.php

```
<?php
```

```
// this could easily be an insert SQL statement
```

```
$query = "SELECT StudentID, FirstName,  
LastName from Students where MajorID = "
```

```
addslashes($_POST['MajorID']) .
```

```
" and LastName = ' " .
```

```
addslashes($_POST['LastName']) . "'";
```

```
print "The Query we ran: $query <p>";
```

```
$result = mysql_query($query);
```

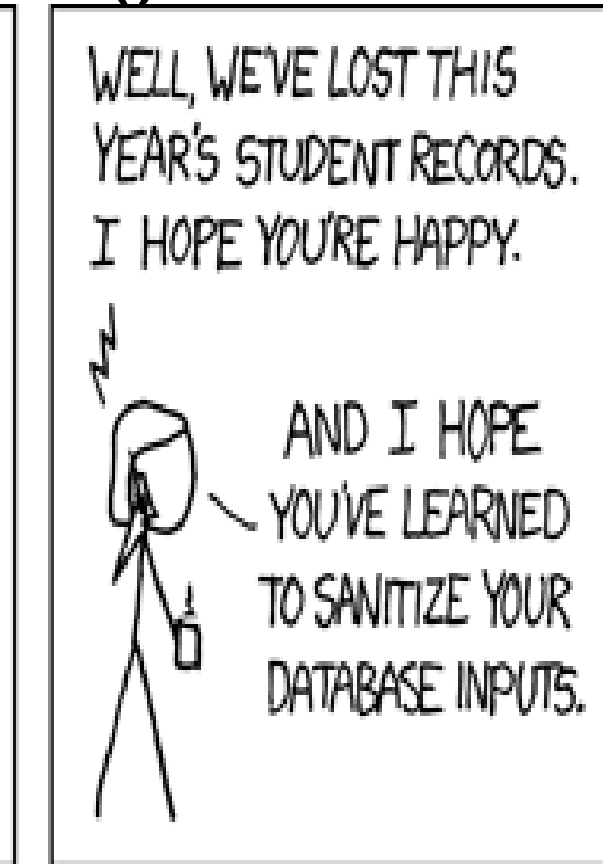
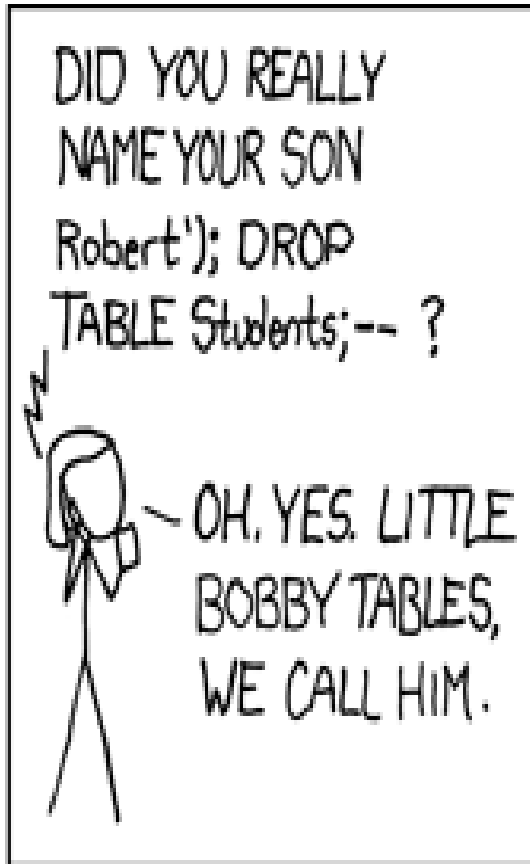
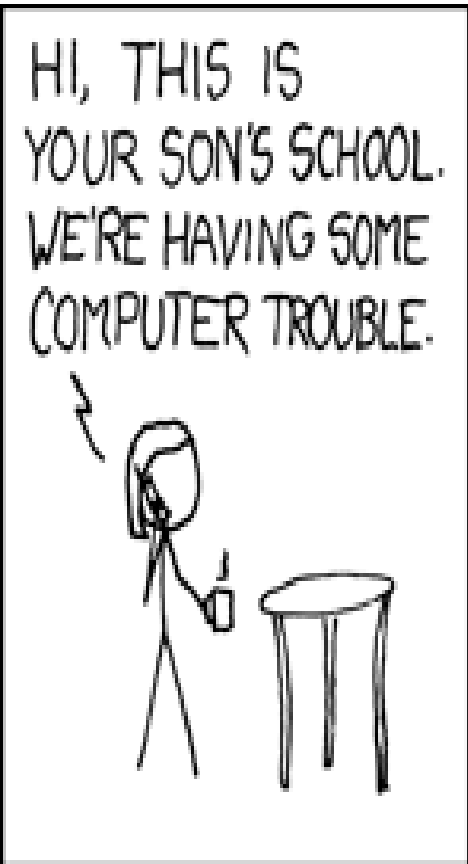
```
while($row = mysql_fetch_array($result))
```

```
{  
    print "$row[0] $row[1]<p>";
```

```
}
```

```
?>
```

Why we use **addslashes()**



```
SELECT username FROM users WHERE username = '$userId';
```

```
$userId = " bob' ); Drop Table Students; --"
```

```
after addslashes(): $userId = " bob\\\ '); Drop Table Students; --"
```

```
<?php
```

```
    $_SESSION['StudentID']=2;  
    header('Location: showStudentID.php');
```

```
?>
```

```
<?php           // showStudentID.php
```

```
    print $_SESSION['StudentID'];
```

```
?>
```

User Authentication

- Store usernames and passwords in the DB
 - Don't make a MySQL account for every user!

```
create table users (username varbinary(25) ,  
                    passwd varbinary(16) ,  
                    Primary Key (username)) ;
```

```
insert into users Values ('bob' , MD5('bobsPassword')) ;
```

- We will use MD5() to securely store our password
 - creates a 16 byte hash
- Form and PHP in the same file

User Id	<input type="text"/>
Password	<input type="password"/>
	<input type="button" value="Login"/>

```
if (isset($_POST['txtUserID'] &&
isset($_POST['txtPassword'])))
{
    $userID = addslashes($_POST['txtUserId']);
    $passwd = MD5($_POST['txtPassword']);

    // query the users table in the db.
    $sql = " SELECT username
            FROM users
            WHERE username = '$userId'
            AND password= '$passwd'";

    $result = mysql_query($sql);
    if (mysql_num_rows($result) == 1) {
        // redirect using header()
    }
}
```

userAuth.php

```
<body>
```

```
<form method="post" name="frmLogin" action=  
"<?php echo $_SERVER['PHP_SELF'] ?>">
```

Username:

```
<input name="txtUserId" type="text" >
```

Password:

```
<input name="txtPassword" type="password">
```

```
<input type="submit" name="btnLogin" value="Login">
```

```
</form>
```

```
</body>
```

Binary Data

```
CREATE TABLE pictures (  
  `PicID` int(11) NOT NULL auto_increment,  
  `image` mediumblob NOT NULL,  
  `type` varchar(255) NOT NULL,  
  PRIMARY KEY (`PicID`)) ENGINE=InnoDB;
```

For binary data, we need to track the type of data we have stored.

Usually the MIME type.

image/gif

image/png

binaryDataInput.php

```
<body>
```

```
<form method="post"
  action="<?php echo $PHP_SELF; ?>"
  enctype="multipart/form-data">
```

```
<input type="hidden" name="MAX_FILE_SIZE"
  value="1000000">
```

```
<br>File to upload/store in database:<br>
```

```
<input type="file" name="form_data" size="40">
```

```
<p>
```

```
<input type="submit" name="submit"
  value="submit">
```

```
</form>
```

```
</body>
```

File to upload/store in database:

Browse...

submit


```
<?php
```

binaryDataInput.php

```
$data = addslashes (
    fread(
        fopen($form_data, "r"),
        filesize($form_data)
    )
);

$result=mysql_query("INSERT INTO pictures ".
    "VALUES (null, '$data' ,
    '{$_FILES['form_data']['type']}')")
or print mysql_error();

print "We just added PicID:". mysql_insert_id();
print $_FILES['form_data']['type'];
print $_FILES['form_data']['name'];
include 'library/closeDB.php';
```

```
?>
```

<http://www.phpbuilder.com/columns/florian19991014.php3?page=2>

<?php

getData.php

```
include 'library/connDB.php';

$id = addslashes($id);

$query = "select image, type from pictures where
PicID=$id";

$result = mysql_query($query);

$data = mysql_result($result, 0, "image");
$type = mysql_result($result, 0, "type");

Header("Content-type: $type");

print $data;
```

?>

Practice Exercise

- Add an Editor field to the user table
 - only allow people marked as editors to insert data in the queries below
- Build a webpage to create a new user
- Build a webpage that allows a user to enter a new Student
 - provide a drop down box listing all majors
- Build a webpage that allows the user to search for Students that received a specific final grade
 - provide a drop down box listing grades (A,A-,B+,B,...)