Easier Text Editing (Linux)

```
ssh -X 64.59.233.246
```

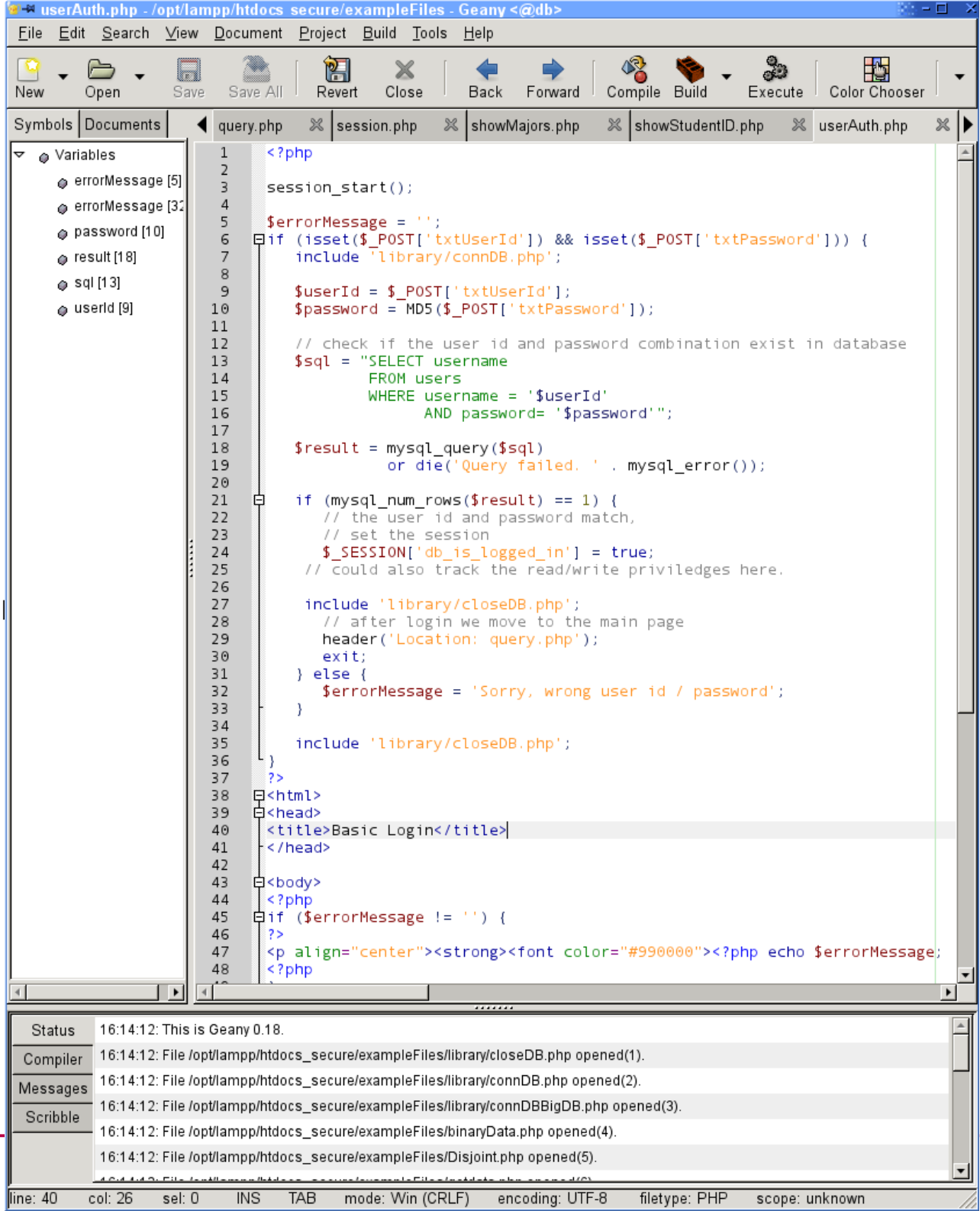
```
chadd@gray:~> geany &
```

Opens the Geany text editor so you ca
edit locally and save the files on the
remote (gray) machine!

Windows

Edit in the Putty Window

chadd@gray:~> nano

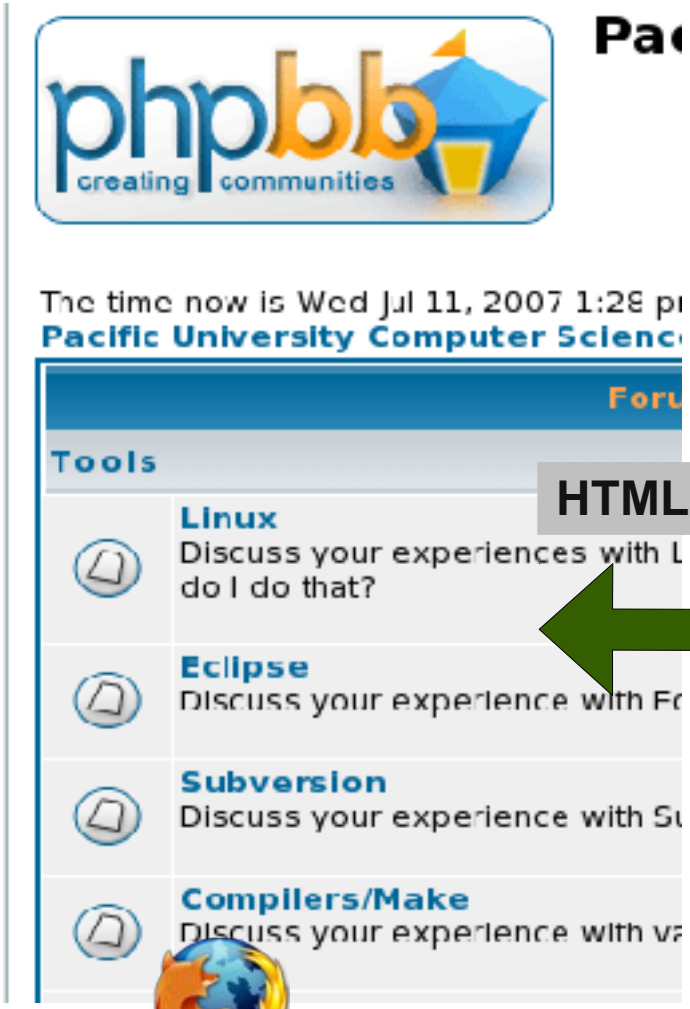


Web accessible Databases
PHP

Oct 24, 2011

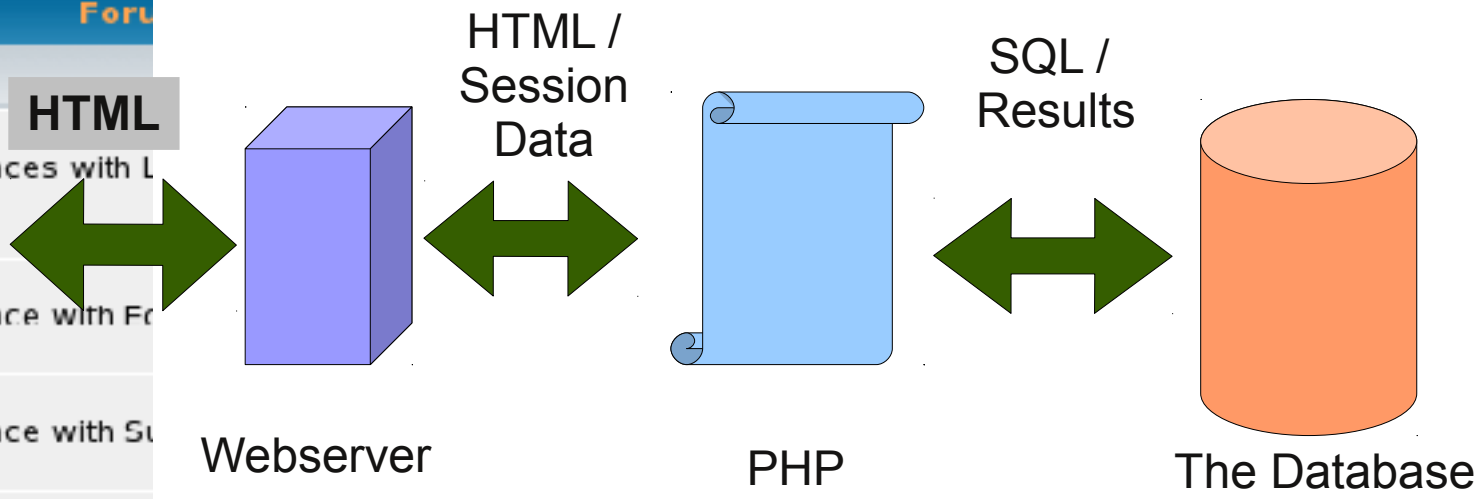
www.php.net

Database Usage Scenario



User

The PHP is used to generate HTML.



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://64.59.233.246/example/
https://64.59.233.246/chadd/

/space/https/example

You have web space at:
/space/https/PUNetID

https://gray.cs.pacificu.edu/PUnetID

https://gray/phpTest.php

Recommended Development Process

- ssh -X gray

  cd /space/https/PUNET

  geany &

  write code in Geany

You have a huge amount of screen space!

Use it!

- ssh gray

  mysql -u PUNET -p

If you are really ambitious, check out the PDT plugin for Eclipse.

- Test code on the gray command line

  php file.php OR press Execute in geany

- Open a web browser
  - https://gray/PUNET/file.php
  - https://gray/example/simple.html

Accept the self-signed certificate!

You can trust me!

Backups

- gray is not backed up!
- Subversion is installed
- OR

```
tar czf backup.tar.gz *.php *.html
scp backup.tar.gz punet@zeus:
```

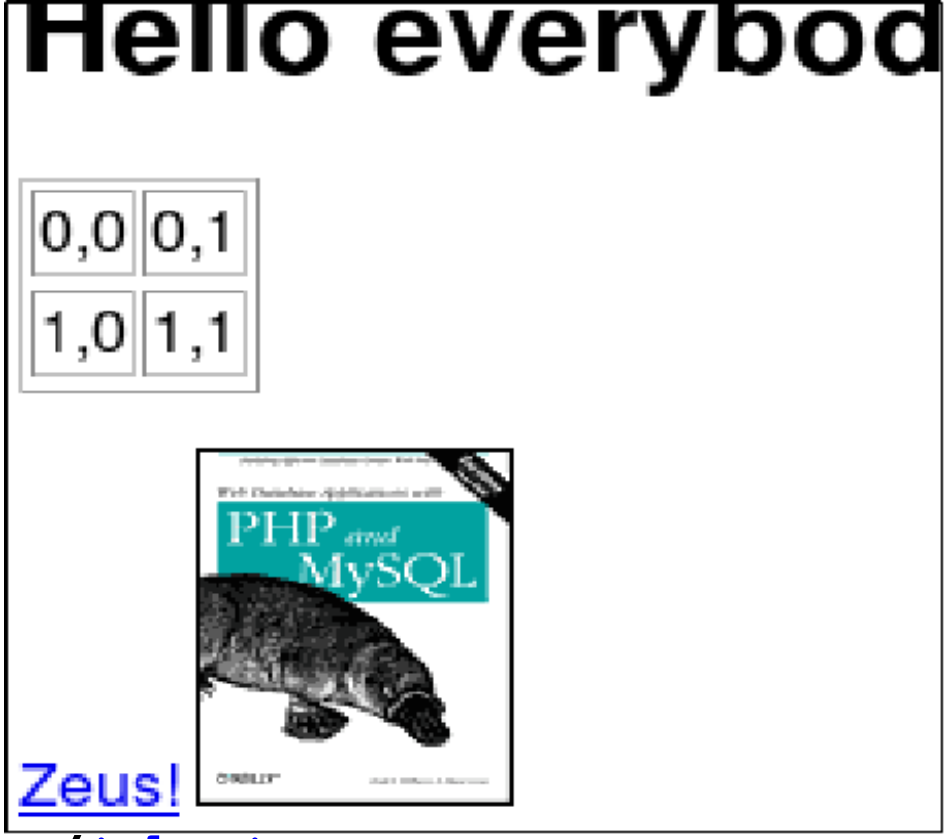
- Coding Standards
  - use file and function header comments as defined for C
  - two spaces for a tab
  - break the line at 78 characters

```
/*****************************************************************************
 Function:        getAllSoftwareProducts
 Description:     Get all software name, versions, and manager
 Parameters:      $DBConn - the database connection
 Returned:        An array containing the results.
*****************************************************************************/
```

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>
     <img src="image/php.gif">
  </body>

</html>
```



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,...)

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!

Comment!

The web browser only sees the HTML, not the PHP.
View | Page Source

A file that contains ANY php MUST have a .php extension!

VariablesIfs.php

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

String concatenation is done with a dot .

LoopsTable.php

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

Disjoint.php

```
<body>
    <?php
       print "<table border=1> <tr>";
       $columns = 1; // create variable
       while( $columns < 10)
       {
          print "<td>" . $columns . "</td>";
          $columns += 1;
       }
       print "</tr> </table>";
    ?>

    Hello out there
    <center> HI!</center>

    <?php
       print $columns; // retains value from above
    ?>
 </body>
```

```php
<?php          // sessionTest.php
  session_start();
  $_SESSION['PID']=2; // global associative array
                      // acts like a hash table
  header('Location: showPID.php');

?>
```

IMPORTANT:
There must be no blank lines or HTML before the **header**() function call!

```php
<?php          // showPID.php
  session_start();
  if( isset($_SESSION['PID']))
  {
    print $_SESSION['PID'];
  }

?>
```

Exercises

- Write a php file to display the first 100 odd integers in a table

- Write a php file to set a session variable (SESS_TEST) to 42 and redirect to another php page which prints all the integers 1 to SESS_TEST. Be sure to use isset() to determine if SESS_TEST is set.

- BONUS: Have the table in either of the above pages alternate colors for rows.

Connect to MySQL

Put this in connDB.php:

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

   $conn = mysql_connect("127.0.0.1:3306",
   "yourDBlogin", "yourDBpassword")
   or print "Error connecting to mysql";
      mysql_select_db("PUNetID_AssignmentOne");
?>
```

Close database connection

Put this in closeDB.php:

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

Connect to MySQL

Put this in connDBBigDB.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_DBProject");
?>
```

Good Coding

- We want to separate the data access from the presentation as much as we can
  - query files
  - presentation files
  - all are .php files
- Query files: write data access functions.
  - many presentations files can access the same query
  - may have many functions per file
- skeleton.php is an example of a presentation file
  - lots of HTML and PHP function calls to get/present data

Presentation file skeleton.php

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

?>

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

</html>


<?php
  include 'closeDB.php';

?>
```

Rather than **print** every line of HTML, you can inline HTML outside of the **<?php ?>** tags and it is automatically printed

php functions

```
<?php  // print.php

  function printData ($data1, $data2)
  {

    $lString = $data1 . " " . $data2;

    print $lString;
    return $lString;

  }

?>
```

```
<?php   //testPrint.php
  include 'print.php';
  $result = printData("hello","World");

  print $result;

?>
```

This code could be in the <body> of the skeleton.php!

You might collect all the includes at the top.

php functions

```
<?php  // passByReference.php
  function printDataRef (&$data1, &$data2)
  {
    $lString = $data1 . " " . $data2;

    print $lString;
    return $lString;
  }

?>
```

```
<?php   //globalVariables.php
   $gValue = 1;
   function printDataGlobal($data)
   {
     global $gValue;  // this attaches the name
                      // to the global variable.
     print $gValue . ' ' . $data;
   }

?>
```

Query Syntax

```
$query = "SELECT name, VersionMajor, ".
         "VersionMinor1, VersionMinor2, Manager " .
         "FROM Software";

// run the query
$result = mysql_query($query, $conn);

$row = mysql_fetch_array($result);

print "{$row['name']} {$row['Manager']}";
```

queryFunction.php

```
function getAllSoftwareProducts($DBconn)

{

  $rows = array();

  $query = "SELECT name, VersionMajor,  " .
           "VersionMinor1, VersionMinor2, Manager " .
           "FROM Software "; // no ; inside the " " ;


  $result = mysql_query($query, $DBconn);


  while (false != ($row = mysql_fetch_array($result))
  {
    $rows[] = $row;
   }
   return $rows; //alt: return $result;
}
```

queryFunctionCall.php

```
<?php

include 'connDB.php';
include 'queryFunction.php';

$data = getAllSoftwareProducts($conn);

foreach ( $data as $row )
{
  print $row['name'] . ' ' . $row['VersionMajor'].
        ' ' .$row['VersionMinor1']. ' ' .
        $row['VersionMinor2']. ' ' . $row['Manager'].
        ' <br/> ';

}


?>
```

queryFunctionParams.php

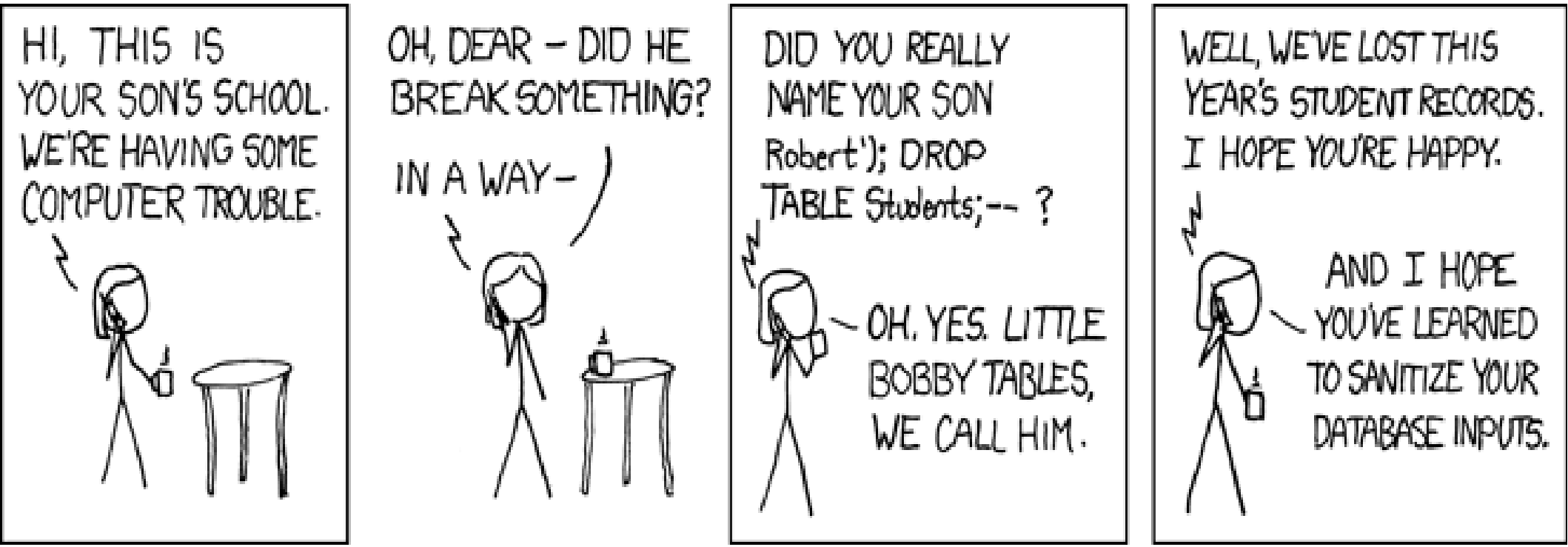
```
function getAllSoftwareProductsParamMangID
        ($DBconn, $MangID)

{
  $rows = array();

  $query = sprintf("SELECT name, VersionMajor,  " .
     "VersionMinor1, VersionMinor2, Manager ".
     "FROM Software " .
     "WHERE Manager = %s",
     mysql_real_escape_string($MangID));


  $result = mysql_query($query, $DBconn);
  while (false != ($row = mysql_fetch_array($result))
  {
    $rows[] = $row;
   }
   return $rows;
}
```

Why we use mysql_real_escape_string()




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

$userId = ' bob'); Drop Table Students; --”

mysql_real_escape_string(): $userId = ' bob\\\');
Drop Table Students; --”
```

SQL Injection

queryFunctionCallParams.php

```
<?php

include 'connDB.php';
include 'queryFunction.php';

$data = getAllSoftwareProductsParamMangID($conn, 3);

foreach ( $data as $row )
{
  print $row['name'] . ' ' . $row['VersionMajor'].
        ' ' .$row['VersionMinor1']. ' ' .
        $row['VersionMinor2']. ' ' . $row['Manager'].
        ' <br/> ';

}


?>
```

runQueryTable.php

Software	FName	LName	Email	Salary
Stellar Teller	Aline	Maddox	elementum.purus.accumsan@parturient.edu	153308
Word Precise	Quintessa	Frederick	et@Curae;Donectincidunt.ca	167687
Anodize	Carissa	Ford	Quisque@elitpellentesquea.ca	23308
ATM Buddy	Odette	Espinoza	non.sollicitudin@variusorciin.org	153903
Where Am I? GPS App	Ursula	Stewart	condimentum@a.edu	49855
Speller	Tyrone	Wong	lacus.Quisque@DonecnibhQuisque.edu	31763
SpellerLite	Wyatt	Figueroa	ullamcorper@montesnascetur.ca	73617
StoryTeller	Michael	Atkinson	laoreet.lectus@necorciDonec.com	63376
Stone Tablet	Oscar	Cox	Vivamus.rhoncus@Suspendissealiquet.org	61079
Vi	Quail	Crawford	convallis.in.cursus@orci.ca	77551
mauris id	Martin	Mccarthy	ipsum@nec.edu	178511
Vivamus nibh	Palmer	Albert	euismod.in@perconubia.edu	46726

```
SELECT Name, FName, LName, Email, Salary
FROM Software, Employees
WHERE Manager =  Employees.id;
```

Exercises

- Build a web page that displays the FName, LName, of each employee and the FName, LName of that employee's Manager.

- Build a web page the displays the total salary earned by all the employees who work on each software product (One row per software product).

```
<form method="post" action="showWorksOn.php">
    Manager:
    <select NAME="EmpID">
      <option VALUE="9">Wyatt Figueroa</option>
      <option VALUE="8">Tyrone Wong</option>
      <option VALUE="7">Ursula Stewart</option>
      <option VALUE="6">Odette Espinoza</option>
    </select>
    <input TYPE="submit" NAME="Request" VALUE="Go" />
</form>
```

showWorksOn.php

```
<?php

  include 'connDB.php';
  include 'queryWorksOnByEmpID.php';

  if( !isset ($_POST['EmpID']) )
  {
     die("ERROR: No EmpID");
  }

  $EmpID = $_POST['EmpID'];

  $data = getWorksOnByEmpID($conn, $EmpID);

  // display data in table

?>
```

Other Input Types

```
<input TYPE="submit" NAME="Request" VALUE="Go" />
```

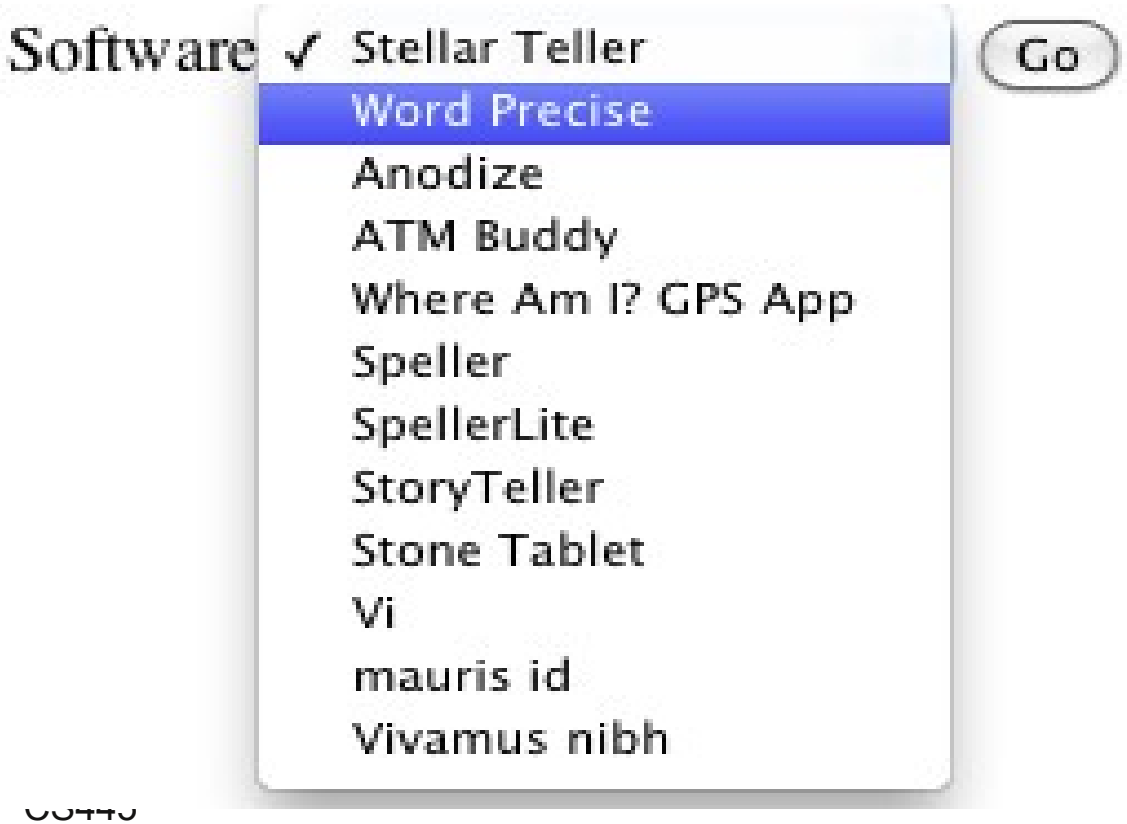
- **TYPE=”text”**
- **TYPE=”password”**
- **TYPE=”radio”**
- **TYPE=”checkbox”**
- **TYPE=”textarea”**

http://www.w3schools.com/html/html_forms.asp

Exercises

- Build a page to show all client information

- Build a page to auto-populate a select box with software and then show all the software the chosen software directly depends on.



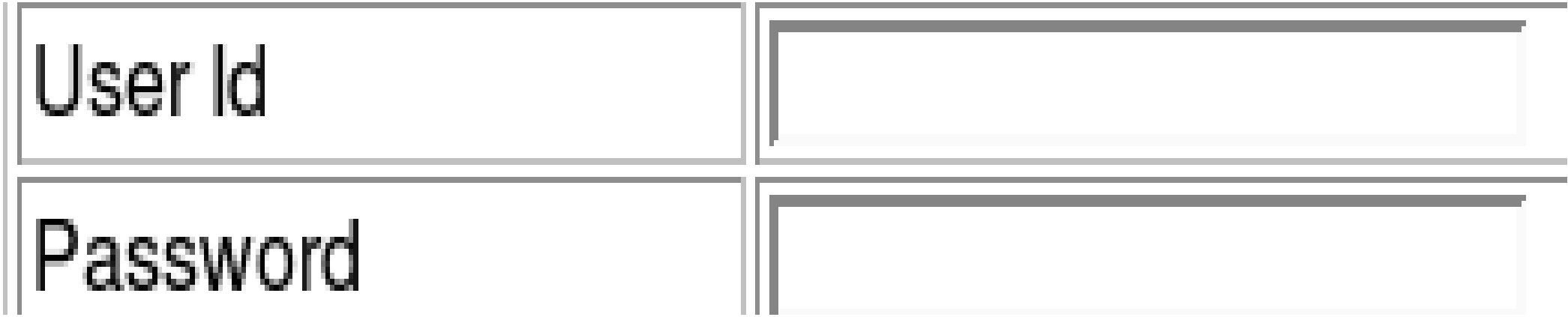
User Authentication

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

```
create table users (username varbinary(25),
                    passwd varbinary(64),
                    Primary Key (username));

insert into users ('bobby',
   sha2( concat('passwd', substr('bobby',0,4)), 256));
```

  - PHP: hash("sha256" , password)
    - creates a 64 byte hash



Other Resources

http://phpsec.org/articles/2005/password-hashing.html

http://www.php.net/manual/en/faq.passwords.php

http://www.w3schools.com/php/func_string_crypt.asp

http://www.ibm.com/developerworks/opensource/library/os-php-encrypt/

Use a secure hash to store the passwords

Also add a **salt**, unique to each user, to each password so that if two users have the same password each user ends up with a different hash.

userAuth.php

```
<?php
$_SESSION['VALID'] = 0;

if(  isset($_POST['txtUser']) &&
     isset($_POST['txtPassword']))
{
   $userID =
      mysql_real_escape_string($_POST['txtUser']);
   $passwd = $_POST['txtPassword'];

   $result = queryValidUser($conn, $userID, $passwd);

   if( TRUE == $result )
   {
      $_SESSION['VALID'] = 1;
      header('Location: loggedIn.php');
   }
   else
   {
      header('Location: login.html');
```

queryValidateuser.php

```
<?php // queryValidateUser.php

  function queryValidateUser($DBConn, $user, $passwd)
  {
     $retVal = FALSE;
     $user = mysql_real_escape_string($user);
     $salt = substr($userID, 0, 4);

     $hashedPW = hash("sha256", $passwd.$salt);

     $query = sprintf("SELECT * FROM users WHERE
          username = %s and passwd = %s",
          $user, $hashedPW);
     $result = mysql_query($query, $DBConn);
     if( mysql_num_rows($result) > 0 )
     {
        $retVal = TRUE;
     }
     return $retVal;
  }
```

login.html

```
<body>

  <form method="post" name="frmLogin" action=
  "authUser.php">

  Username:
  <input name="txtUserId" type="text" >

  Password:
  <input name="txtPassword" type="password">

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

  </form>

</body>
```

authHelper.php

```
<?php
   // include this code at the top of each
   // php file that requires the user to
   // have already been authenticated

   if( !isset($_SESSION['VALID']) ||
       $_SESSION['VALID'] != 1 )
   {
      header('Location: login.html');
   }

?>
```

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=binaryDataInput.php
      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="datafile"  size="40">

     <p>
      <input type="submit" name="submit"
        value="submit">
    </form>
</body>
```

binaryDataInput.php

```
<?php
if(isset($_POST['submit']) ) {

  $filename = $_FILES['datafile']['tmp_name'];
  $filesize = $_FILES['datafile']['size'];
  $filetype = $_FILES['datafile']['type'];

  $data = mysql_real_escape_string(
                fread( fopen($filename, "r"),
                     filesize($filename)));

  $result=mysql_query("INSERT INTO pictures ".
              "VALUES (null, '$data' , '$filetype')")
            or print mysql_error();

  print "We just added PicID:".mysql_insert_id();
  print "{$filetype} {$_FILES['datafile']['name']}";

}

?>
```

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

getData.php

```
<?php
  if( isset($_GET['id']) ) {
    include 'library/connDB.php';
    $id = mysql_real_escape_string($_GET['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;
    include 'library/closeDB.php';
  }else{
     print "FILE NOT FOUND";
  }
?>
```

showImage.html

https://64.59.233.246/chadd/getData.php?id=1

```
<html>
   <body>
      Image: <img src="getData.php?id=24">
   </body>
</html>
```

```
<html>
   <body>
      Image: <img src="getData.php?id=
   <?php $_SESSION['PicID'] ?>">
   </body>
</html>
```