

# PHP/MySQL

- Some sample programs that deal with the `dbintro` database.
- List all users. Display as HTML table
- Account Creation, Login processing
- Viewing a shopping cart

# Table people

people :

userid	int
FirstName	varchar (30)
LastName	varchar (30)
DateOfBirth	date
Username	varchar (20)
Password	varchar (10)

# Show all users as an HTML table: create connection to database

```
<?php
/* Your MySQL username/password go here! */
$username="php";
$password="php";
$database="dbintro";

mysql_connect(localhost,$username,$password);
@mysql_select_db($database) or
    die("Unable to select database");
```

# Show all users as an HTML table: Send SQL command to database

```
// define the SQL command
$query = "SELECT * FROM people";

// submit the query to the database
$res=mysql_query($query);

// make sure it worked!
if (!$res) {
    echo mysql_error();
    exit;
}
```

# Show all users as an HTML table: Get records and output as a table

```
// find out how many records we got
$num = mysql_numrows($res);
echo "<table><tr><th>Name</th><th>Username</th></tr>\n";
// show all the records
for ($i=0;$i<$num;$i++) {
    $fname = mysql_result($res,$i,'FirstName');
    $lname = mysql_result($res,$i,'LastName');
    $username = mysql_result($res,$i,'Username');
    echo "<tr><td>$fname $lname</td>";
    echo "<td>$username</td></tr>\n";
}
echo "</table>\n";
```

# Account Creation

- We need a form the user can fill out
  - desired name/username/password, etc.
- The form should be submitted to a PHP program that:
  - makes sure the username is available (SQL)
  - creates the account if possible (SQL)

# Submission

- Assume we get the following from a form:
  - `firstname, lastname, username, password`
- We need to check to see if the username is already taken:

```
SELECT * FROM people WHERE Username=' $username '
```

If we get any resulting records, the username is already taken.

# Checking the username

```
$username = $_REQUEST['username'];  
  
// here we define the SQL command  
  
$query = "SELECT * FROM people WHERE Username='$username'";  
  
  
// submit the query to the database  
  
$res=mysql_query($query);  
  
if (!$res) { mysql_error(); exit; }  
  
$num = mysql_numrows($res);  
  
if ($num>0) {  
    echo "<h3>That username is already taken</h3>\n";  
    exit;  
}  
  
}
```

# Verify the submission

- In general, we need to make sure that the user fills in all fields with valid *stuff*.
- For now we can just make sure they enter *something* for each field.

```
$firstname = $_REQUEST['firstname'];
```

```
$lastname = $_REQUEST['lastname'];
```

```
$username = $_REQUEST['username'];
```

```
$password=$_REQUEST['password'];
```

```
if ($firstname && $lastname && $username && $password) {
```

# Creating the new record: INSERT

- To create a new record use the SQL INSERT command:

```
$query = "INSERT INTO people SET FirstName='$firstname',  
        LastName='$lastname', Username='$username',  
        Password='$password'";
```

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

```
// now make sure it worked (check $res)
```

# Quotes

- Whenever you are specifying the value of a non-numeric value in an SQL expression, you need to put the value in quotes:

```
SELECT * FROM people WHERE FirstName='Fred'
```

- This won't work:

```
SELECT * FROM people WHERE FirstName=Fred
```



Needs Quotes!

- You don't need to quote numbers.

# SQL-Injection

- What if someone enters the name:

```
Joe'; drop people
```

and we build a query like this:

```
$query="SELECT * FROM people WHERE FirstName='$firstname'"
```

which results in this:

```
SELECT * FROM people WHERE FirstName='Joe'; drop people
```

**This is an important security issue!**

# Avoid SQL injection trouble

- You need to *escape* all special characters in anything you put in an SQL query:

`Joe'; drop people` → `Joe\' ; drop people`

- There is a function that will do the work for you:

```
$firstname=mysql_real_escape_string($firstname);
```

# Login Processing

- Assumes we have a form with username and password fields.

```
SELECT * FROM people WHERE Username='$username'  
AND Password='$password'
```

- Need to make sure there is only one match!
- Create a session:

```
$_SESSION['userid'] = $userid;
```

# View the shopping cart

## **products :**

**productid: integer**

**Name: varchar (30)**

**Description: text**

**Price: float**

## **cartentries :**

**productid: integer**

**userid: integer**

**quantity: integer**

# viewcart.php

- Make sure there is a session:

```
if ( $_SESSION[ 'userid' ] )
```

- We could:
  - grab all entries in cartentries that match the userid
  - for each entry found, look up the product information.
- Or – use an SQL join
  - One query – grab everything we need

# Cart Query

```
$query = "SELECT * FROM cartentries,products  
WHERE cartentries.userid=$userid AND  
cartentries.productid=products.productid";
```

Each resulting record will have:

**productid**

**Name**

**Description**

**Price**

**userid**

**quantity**

# Sample Code

- Each of the functions described here is available (as a php file):
  - login.php
  - create.php
  - viewcart.php
- Get them and put them together as a *system*