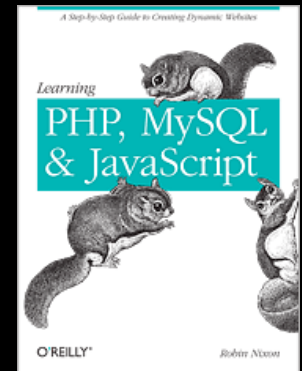


# Accessing MySQL Using PHP

Chapter 10

Dr. Charles Severance

To be used in association with the book:  
PHP, MySQL, and JavaScript by Robin Nixon



open.michigan

Unless otherwise noted, the content of this course material is licensed under a Creative Commons Attribution 3.0 License.

<http://creativecommons.org/licenses/by/3.0/>.

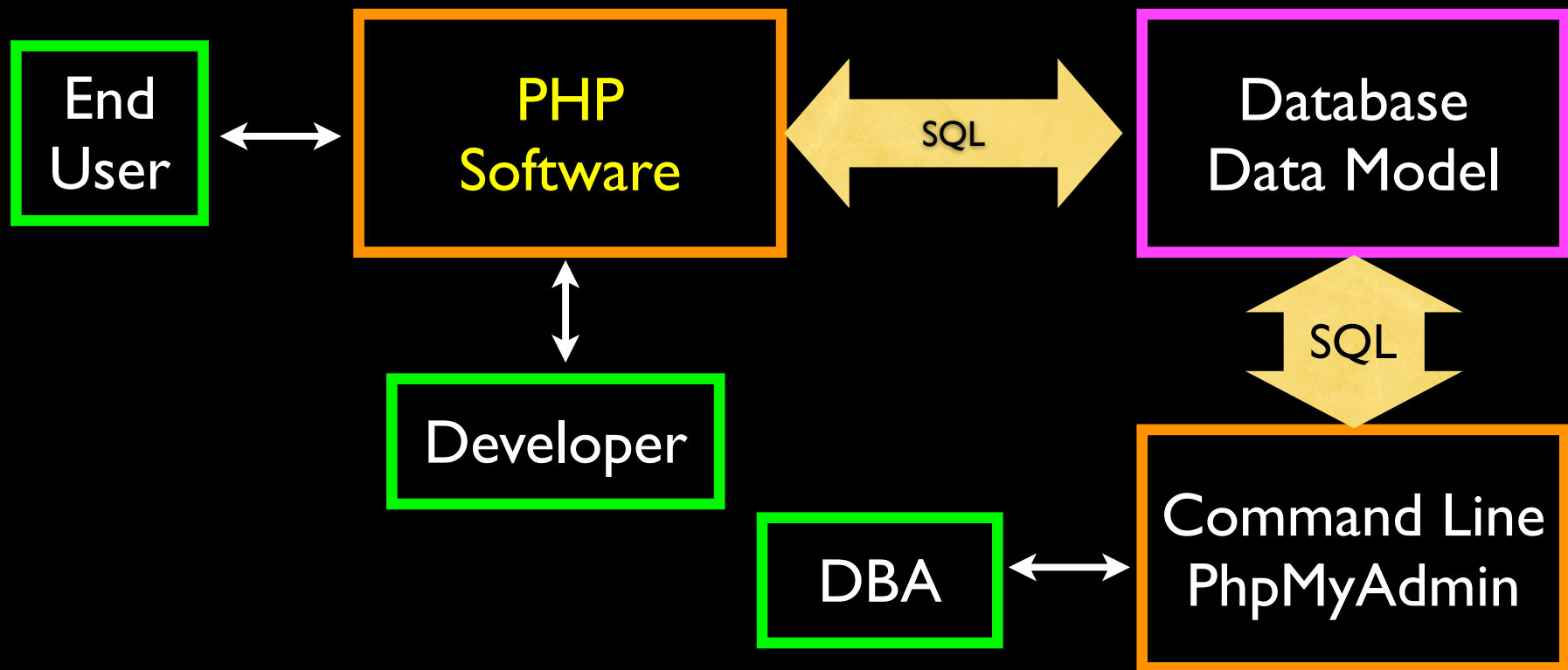
Copyright 2011, Charles Severance



# MySQL is Built Into PHP

- There are function calls to connect to a MySQL server, send SQL commands, and retrieve data from the server

# Application Structure



# Creating a Database and User

- `CREATE DATABASE misc;`
- `USE misc;`
- `GRANT ALL ON misc.* TO 'fred'@'localhost' IDENTIFIED BY 'zap';`
- `GRANT ALL ON misc.* TO 'fred'@'127.0.0.1' IDENTIFIED BY 'zap';`

`/Applications/xampp/xamppfiles/bin/mysql -uroot -p`

`c:\xampp\mysql\bin\mysql.exe`

# Creating a Table

```
CREATE TABLE users (  
  id INT UNSIGNED NOT NULL  
    AUTO_INCREMENT KEY,  
  name VARCHAR(128),  
  email VARCHAR(128),  
  password VARCHAR(128));
```

```
ALTER TABLE users ADD INDEX(email);
```

```
mysql> describe users;
```

Field	Type	Null	Key	Default	Extra
id	int(10) unsigned	NO	PRI	NULL	auto_increment
name	varchar(128)	YES		NULL	
email	varchar(128)	YES	MUL	NULL	
password	varchar(128)	YES		NULL	

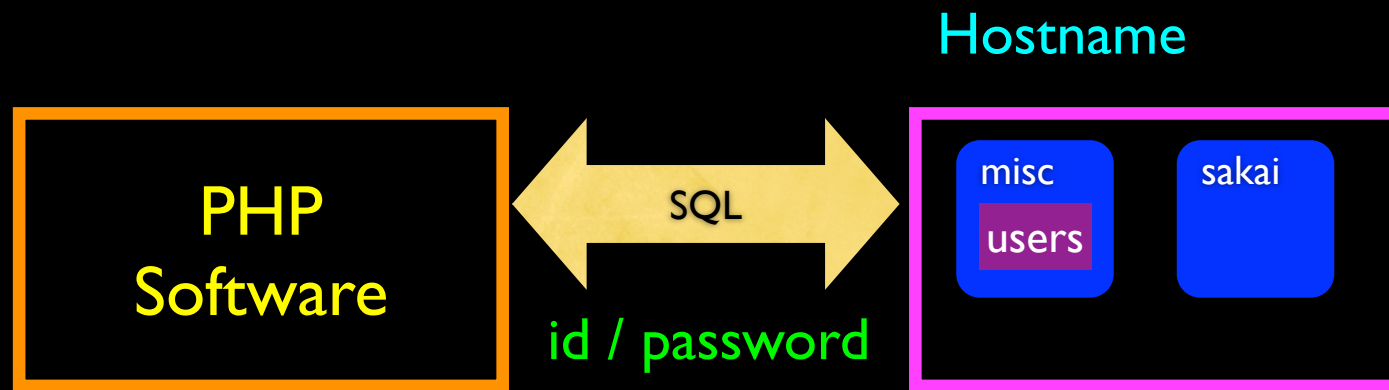
# Inserting a Few Records

```
INSERT INTO users (name,email,password) VALUES ('Chuck','csev@umich.edu','123');  
INSERT INTO users (name,email,password) VALUES ('Glenn','gg@umich.edu','456');
```

```
mysql> select * from users;
```

id	name	email	password
1	Chuck	csev@umich.edu	123
2	Glenn	gg@umich.edu	456

# Database Connection



```
$db = mysql_connect("localhost", "fred", "zap");  
mysql_select_db("misc");
```

```

<?php
echo "<pre>\n";
$db = mysql_connect("localhost", "fred", "zap");
mysql_select_db("misc");
$result = mysql_query("SELECT * FROM users");
while ( $row = mysql_fetch_row($result) ) {
    print_r($row);
}
echo "</pre>\n";
mysql_close($db);
?>

```

```
mysql> select * from users;
```

```

+-----+-----+-----+-----+
| id | name  | email          | password |
+-----+-----+-----+-----+
|  1 | Chuck | csev@umich.edu | 123      |
|  2 | Glenn | gg@umich.edu   | 456      |
+-----+-----+-----+-----+

```

```

Array
(
    [0] => 1
    [1] => Chuck
    [2] => csev@umich.edu
    [3] => 123
)
Array
(
    [0] => 2
    [1] => Glenn
    [2] => gg@umich.edu
    [3] => 456
)

```

```

<?php
echo '<table border="1">'. "\n";
$db = mysql_connect("localhost", "fred", "zap");
mysql_select_db("misc");
$result = mysql_query("SELECT name, email, password FROM users");
while ( $row = mysql_fetch_row($result) ) {
    echo "<tr><td>";
    echo ($row[0]);
    echo("</td><td>");
    echo ($row[1]);
    echo("</td><td>");
    echo ($row[2]);
    echo("</tr>\n");
}
echo "</table>\n";
mysql_close($db);
?>

```

Chuck	csev@umich.edu	123
Glenn	gg@umich.edu	456

```

<table border="1">
<tr><td>Chuck</td><td>csev@umich.edu</td><td>123</td></tr>
<tr><td>Glenn</td><td>gg@umich.edu</td><td>456</td></tr>
</table>

```

# Some Idioms

- Put database connection information in a single file and include it in all your other files
  - Helps make sure to not mistakenly reveal id / pw
- Blah blah blah or die()

```
<?php
$db = mysql_connect("localhost","fred", "zap");
if ( $db === FALSE ) die('Fail message');
if ( mysql_select_db("misc") === FALSE ) die("Fail message");
?>
```

db.php

```
<?php
require_once "db.php";

echo "<pre>\n";
$result = mysql_query("SELECT * FROM users");
while ( $row = mysql_fetch_row($result) ) {
    print_r($row);
}
echo "</pre>\n";
mysql_close($db);
?>
```

misc3.php

```
Array
(
    [0] => 1
    [1] => Chuck
    [2] => csev@umich.edu
    [3] => 123
)
Array
(
    [0] => 2
    [1] => Glenn
    [2] => gg@umich.edu
    [3] => 456
)
```

db.php

```
<?php
$db = mysql_connect("localhost","fred", "zap");
if ( $db === FALSE ) die('Fail message');
if ( mysql_select_db("misc") === FALSE ) die("Fail message");
?>
```

```
<?php
$db = mysql_connect("localhost","fred", "zap")
    or die('Fail message');
mysql_select_db("misc") or die("Fail message");
?>
```

```
$db = mysql_connect("localhost","fred", "zap") or die('Fail message');  
($db = mysql_connect("localhost","fred", "zap")) or die('Fail message');
```

High precedence →

Very high precedence →

&&	Logical
	Logical
? :	Ternary
= += -= *= /= .= %= &= != ^= <<= >>=	Assignment
and	Logical
xor	Logical
or	Logical

# Assignments as Expressions

- While we seldom use the feature, **assignment statements** are also **expressions** that have values

```
<?php
```

```
$y = ($x = 3 * 4) + 200;
```

```
echo "X=$x Y=$y\n";
```

```
?>
```

```
X=12 Y=212
```

```
$y = ($x = 3 * 4) + 200;
```

```
$db = mysql_connect("localhost", "fred", "zap")  
      or die('Fail message');
```

```
( $db = mysql_connect("localhost", "fred", "zap") )  
      or die('Fail message');
```

# Forms and PHP

# Forms Submit Data

```
<p>Guessing game...</p>
```

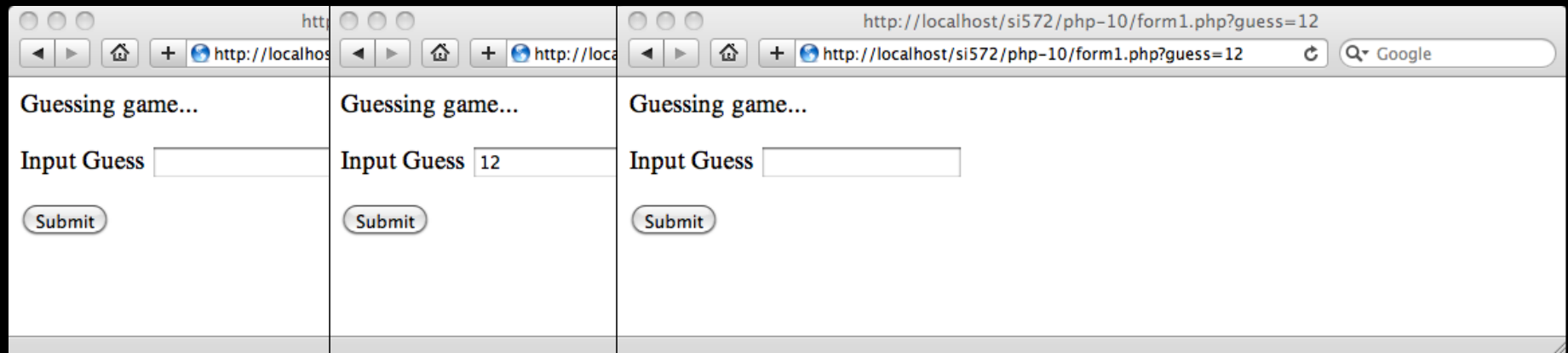
```
<form>
```

```
  <p><label for="guess">Input Guess</label>
```

```
  <input type="text" name="guess" id="guess" /></p>
```

```
  <input type="submit" />
```

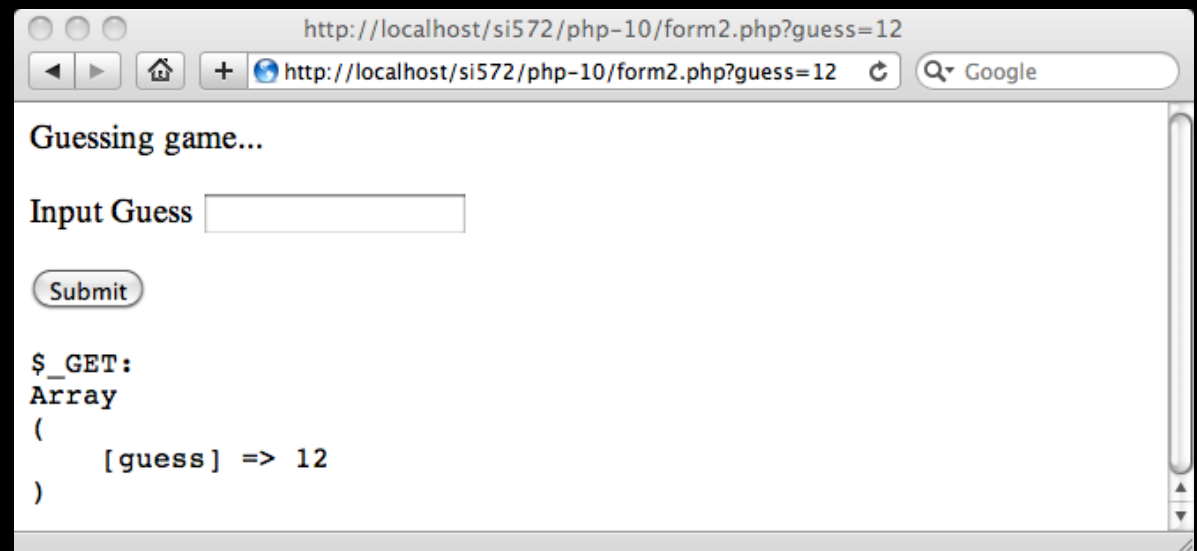
```
</form>
```



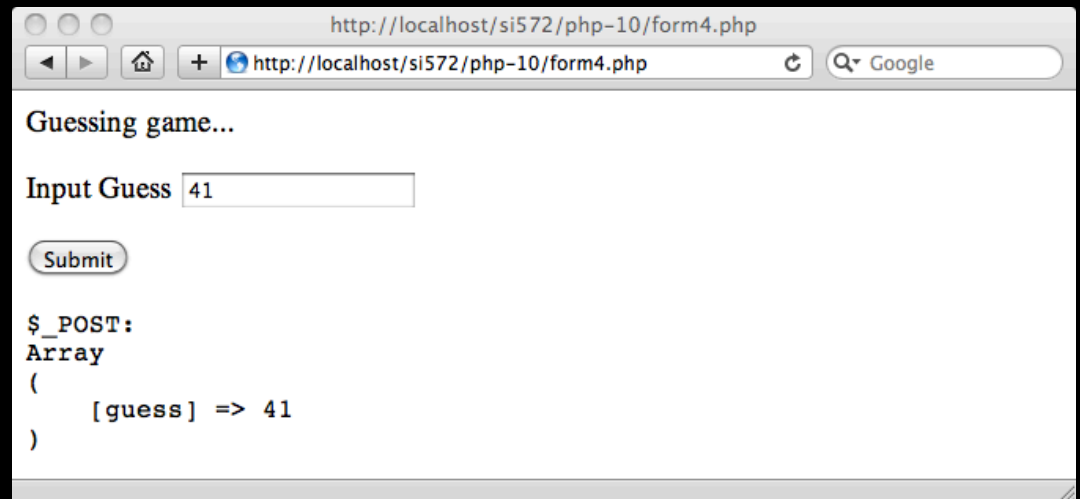
# `$_GET` and `$_POST`

- PHP loads the values for the URL parameters into an array called `$_GET` and the POST parameters into an array called `$_POST`

```
<p>Guessing game...</p>
<form>
  <p><label for="guess">Input Guess</label>
  <input type="text" name="guess" id="guess" /></p>
  <input type="submit" />
</form>
<pre>
$_GET:
<?php
  print_r($_GET);
?>
</pre>
```



```
<p>Guessing game...</p>
<form method="post">
  <p><label for="guess">Input Guess</label>
  <input type="text" name="guess" id="guess"
<?php
  echo 'value="' . $_POST['guess'] . '"';
?>
  /></p>
  <input type="submit"/>
</form>
<pre>
$_POST:
<?php
  print_r($_POST);
?>
</pre>
```



# Hygiene Alert!

- What happens when we use an HTML character in a form field value??

The image displays two browser windows side-by-side, illustrating the effect of an HTML injection into a form field. Both windows are titled 'http://localhost/si572/php-10/form4.php'.

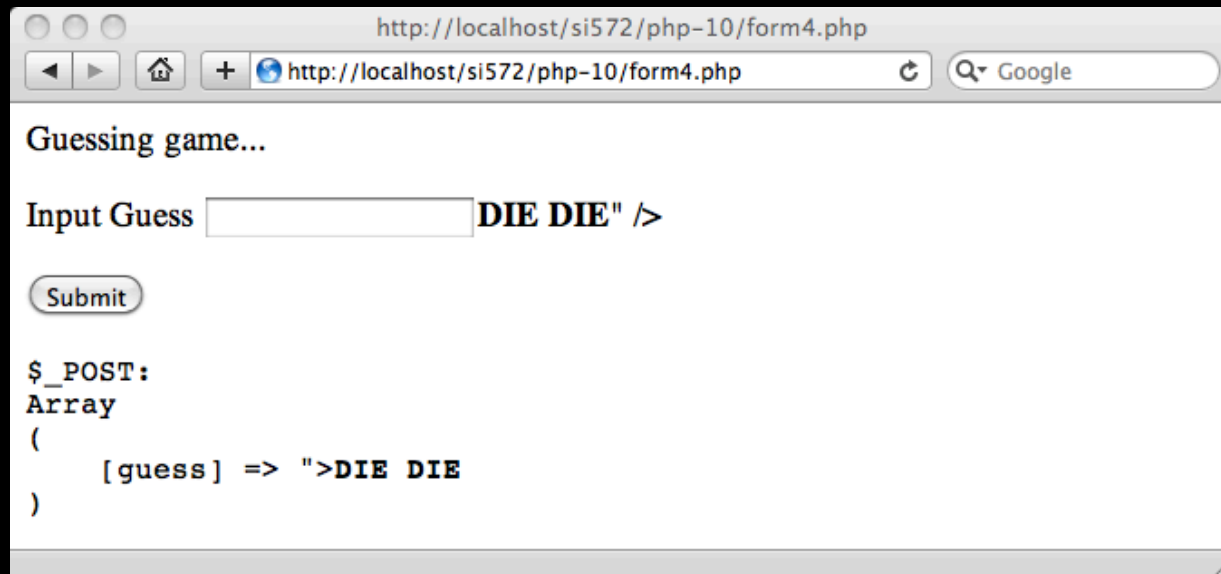
The left window shows the 'Guessing game...' page with an 'Input Guess' field containing the text '><b>DIE DIE</b>'. Below the field is a 'Submit' button. The output below the form shows the raw POST data: 

```
$_POST: Array ( )
```

The right window shows the same page after submission. The 'Input Guess' field now displays the rendered HTML: **DIE DIE**. Below the field is a 'Submit' button. The output below the form shows the raw POST data with the injected HTML: 

```
$_POST: Array ( [guess] => ">DIE DIE"
```

```
<form method="post">
  <p><label for="guess">Input Guess</label>
  <input type="text" name="guess" id="guess"
value=""><b>DIE DIE</b>" /></p>
  <input type="submit" />
</form>
```



The screenshot shows a web browser window with the URL `http://localhost/si572/php-10/form4.php`. The page title is "Guessing game...". The form contains a label "Input Guess" followed by a text input field containing the value `>DIE DIE" />`. Below the input field is a "Submit" button. At the bottom of the page, the PHP variable `$_POST` is displayed as an array with the following structure:

```
$_POST:
Array
(
    [guess] => ">DIE DIE"
)
```

# To The Rescue: htmlentities()

```
<form method="post">
  <p><label for="guess">Input Guess</label>
  <input type="text" name="guess" id="guess"
<?php
  echo 'value="' . htmlentities($_POST['guess']) . '"';
?>
  /></p>
  <input type="submit"/>
</form>
```

```
<form method="post">
  <p><label for="guess">Input Guess</label>
  <input type="text" name="guess" id="guess"
<?php
  echo 'value="' . htmlentities($_POST['guess']) . "'";
?>
  /></p>
  <input type="submit"/>
</form>
```

The screenshot shows a web browser window with the URL `http://localhost/si572/php-10/form5.php`. The page title is "Guessing game...". The form contains an "Input Guess" field with the value `<b>DIE DIE</b>` and a "Submit" button. Below the form, the `$_POST` array is displayed as follows:

```
$_POST:
Array
(
    [guess] => ">DIE DIE"
```

A callout box highlights the HTML output for the text input field:

```
<input type="text" name="guess" id="guess"
value="&quot;&gt;&lt;&b&gt;DIE DIE&lt;/b&gt;&quot; /></p>
```

To The Database HO!

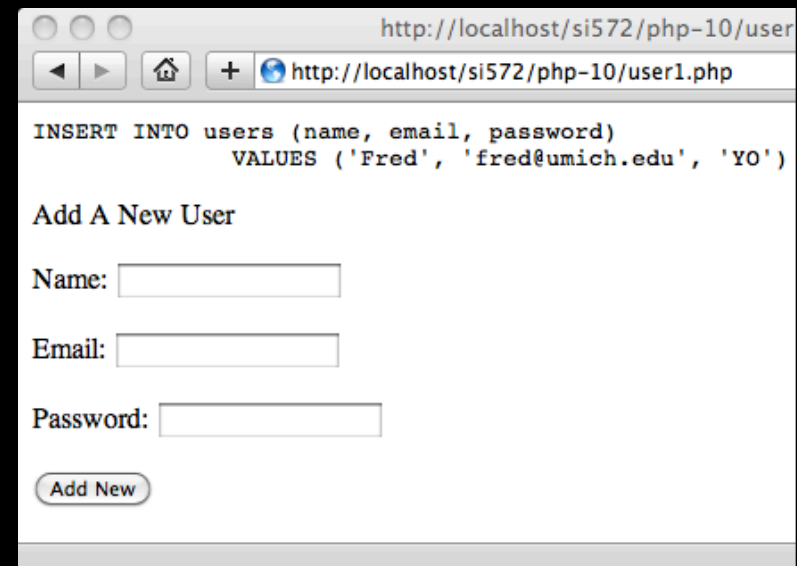
```

<?php
require_once "db.php";

if ( isset($_POST['name']) && isset($_POST['email'])
    && isset($_POST['password'])) {
    $n = $_POST['name'];
    $e = $_POST['email'];
    $p = $_POST['password'];
    $sql = "INSERT INTO users (name, email, password)
           VALUES ('$n', '$e', '$p')";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}

?>
<p>Add A New User</p>
<form method="post">
<p>Name:
<input type="text" name="name"></p>
<p>Email:
<input type="text" name="email"></p>
<p>Password:
<input type="password" name="password"></p>
<p><input type="submit" value="Add New"/></p>
</form>

```



http://localhost/si572/php-10/user1.php

http://localhost/si572/php-10/user1.php Google

```
INSERT INTO users (name, email, password)
VALUES ('Fred', 'fred@umich.edu', 'YO')
```

Add A New User

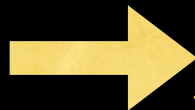
Name:

Email:

Password:

```
mysql> select * from users;
```

id	name	email	password
1	Chuck	csev@umich.edu	123
2	Glenn	gg@umich.edu	456
3	Chuck	csev@umich.edu	NULL
4	Sam	sam@umcih	pp
5	Fred	fred@umich.edu	YO



```

    $sql = "INSERT INTO users (name, email, password)
            VALUES ('$n', '$e', '$p)";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}

echo '<table border="1">'. "\n";
$result = mysql_query("SELECT name, email, password
FROM users");
while ( $row = mysql_fetch_row($result) ) {
    echo "<tr><td>";
    echo($row[0]);
    echo("</td><td>");
    echo($row[1]);
    echo("</td><td>");
    echo($row[2]);
    echo("</tr>\n");
}
?>
</table>
<p>Add A New User</p>

```

The screenshot shows a web browser window with the URL `http://localhost/si572/php-10/user2.php`. The browser's address bar also shows `http://localhost/si572/php-10` and a search bar with the text "Google".

The main content of the page is a table with the following data:

Chuck	csev@umich.edu	123
Glenn	gg@umich.edu	456
Chuck	csev@umich.edu	
Sam	sam@umcih	pp
Fred	fred@umich.edu	YO

Below the table is a section titled "Add A New User" with three input fields:

Name:

Email:

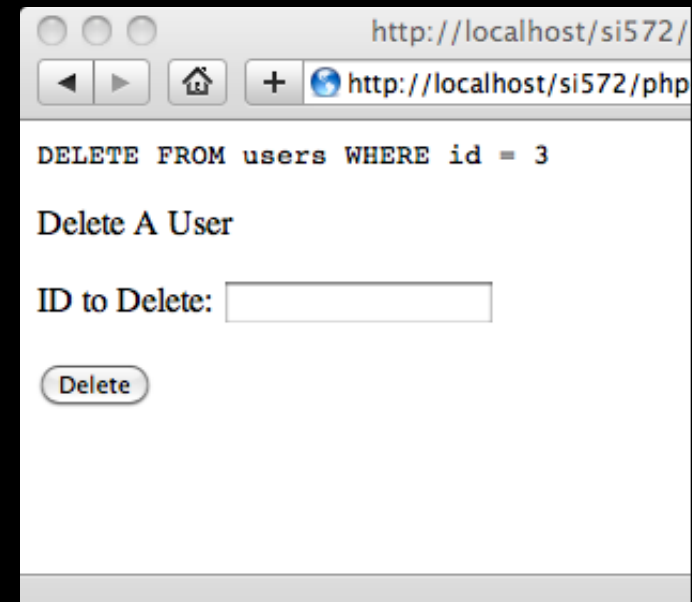
Password:

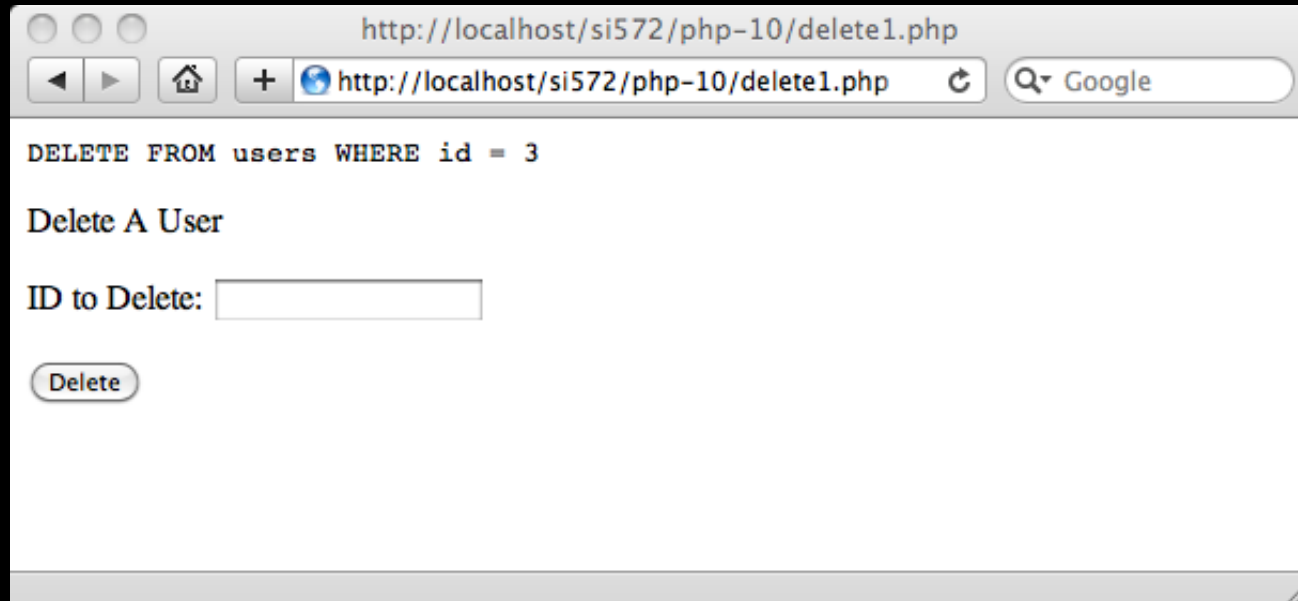
At the bottom of this section is a button labeled "Add New".

```
<?php
require_once "db.php";

if ( isset($_POST['id']) ) {
    $id = $_POST['id'];
    $sql = "DELETE FROM users WHERE id = $id";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}

?>
<p>Delete A User</p>
<form method="post">
<p>ID to Delete:
<input type="text" name="id"></p>
<p><input type="submit" value="Delete"/></p>
</form>
```





```
mysql> select * from users;
```

```
+-----+-----+-----+-----+
| id | name  | email          | password |
+-----+-----+-----+-----+
|  1 | Chuck | csev@umich.edu | 123      |
|  2 | Glenn | gg@umich.edu   | 456      |
|  4 | Sam   | sam@umcih     | pp       |
|  5 | Fred  | fred@umich.edu | YO       |
+-----+-----+-----+-----+
```

```

if ( isset($_POST['delete']) && isset($_POST['id'])
    && isset($_POST['password'])) {
    $id = $_POST['id'];
    $sql = "DELETE FROM users WHERE id = $id";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}

echo '<table border="1">'. "\n";
$result = mysql_query("SELECT name, email, password, id FROM users");
while ( $row = mysql_fetch_row($result) ) {
    echo "<tr><td>";
    echo(htmlentities($row[0]));
    echo("</td><td>");
    echo(htmlentities($row[1]));
    echo("</td><td>");
    echo(htmlentities($row[2]));
    echo("</td><td>\n");
    echo('<form method="post"><input type="hidden" name="id" value="' . $row[3] . '">');
    echo('<input type="submit" value="Del" name="delete">');
    echo("\n</form>\n");
    echo("</td></tr>\n");
}

```

http://localhost/si572/php-10/user3.php

Chuck	csev@umich.edu	123	Del
Glenn	gg@umich.edu	456	Del
Sam	sam@umich.edu	pp	Del
Fred	fred@umich.edu	YO	Del

Add A New User

Name:

Email:

Password:

```

echo('<form method="post"><input type="hidden" ');
echo('name="id" value="' . $row[3] . '">' . "\n");
echo('<input type="submit" value="Del" name="delete">');
echo("\n</form>\n");

```

http://localhost/si572/php-10/user3.php

Chuck	csev@umich.edu	123	Del
Glenn	gg@umich.edu	456	Del
Sam	sam@umcih	pp	Del
Fred	fred@umich.edu	YO	Del

Add A New User

Name:

Email:

Password:

```

<tr><td>Fred</td><td>fred@umich.edu</td>
<td>YO</td>

```

```

<td>

```

```

<form method="post">

```

```

<input type="hidden" name="id" value="5">

```

```

<input type="submit" value="Del" name="delete">

```

```

</form>

```

```

</td>

```

```

</tr>

```

```

if ( isset($_POST['delete']) && isset($_POST['id'])
    && isset($_POST['password'])) {
    $id = $_POST['id'];
    $sql = "DELETE FROM users WHERE id = $id";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}

```

http://localhost/si572/php-10/user3.php

DELETE FROM users WHERE id = 5

Chuck	csev@umich.edu	123	Del
Glenn	gg@umich.edu	456	Del
Sam	sam@umcih	pp	Del


Add A New User

Name:

Email:

Password:

```
if ( isset($_POST['delete']) && isset($_POST['id'])
    && isset($_POST['password'])) {
    $id = $_POST['id'];
    $sql = "DELETE FROM users WHERE id = $id";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}
```



# Program Outline

```
<?php
require_once "db.php";

if ( isset($_POST['name']) && isset($_POST['email'])
    && isset($_POST['password'])) {
    $n = $_POST['name'];
    $e = $_POST['email'];
    $p = $_POST['password'];
    $sql = "INSERT INTO users (name, email, password)
           VALUES ('$n', '$e', '$p)";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}

if ( isset($_POST['delete']) && isset($_POST['id']) ) {
    $id = $_POST['id'];
    $sql = "DELETE FROM users WHERE id = $id";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}
```

```
<?php
require_once "db.php";

if ( isset($_POST['name']) && isset($_POST['email'])
    && isset($_POST['password'])) {
    $n = $_POST['name'];
    $e = $_POST['email'];
    $p = $_POST['password'];
    $sql = "INSERT INTO users (name, email, password)
           VALUES ('$n', '$e', '$p)";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}

if ( isset($_POST['delete']) && isset($_POST['id']) ) {
    $id = $_POST['id'];
    $sql = "DELETE FROM users WHERE id = $id";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}

echo "<table border='1'>.\n";
$result = mysql_query("SELECT name, email, password, id FROM users");
while ( $row = mysql_fetch_row($result) ) {
    echo "<tr><td>";
    echo(htmlentities($row[0]));
    echo("</td><td>");
    echo(htmlentities($row[1]));
    echo("</td><td>");
    echo(htmlentities($row[2]));
    echo("</td><td>\n");
    echo("<form method='post'><input type='hidden' ");
    echo("name='id' value='".$row[3]."'>.\n");
    echo("<input type='submit' value='Del' name='delete'>");
    echo("</form>\n");
    echo("</td></tr>\n");
}
?>
</table>
<p>Add A New User</p>
<form method='post'>
<p>Name:
<input type='text' name='name'></p>
<p>Email:
<input type='text' name='email'></p>
<p>Password:
<input type='password' name='password'></p>
<p><input type='submit' value='Add New'></p>
</form>
```

```

echo '<table border="1">'. "\n";
$result = mysql_query("SELECT name, email, password, id FROM users");
while ( $row = mysql_fetch_row($result) ) {
    echo "<tr><td>";
    echo(htmlentities($row[0]));
    echo("</td><td>");
    echo(htmlentities($row[1]));
    echo("</td><td>");
    echo(htmlentities($row[2]));
    echo("</td><td>\n");
    echo('<form method="post"><input type="hidden" ');
    echo('name="id" value="' . $row[3] . '">'. "\n");
    echo('<input type="submit" value="Del" name="delete">');
    echo("\n</form>\n");
    echo("</td></tr>\n");
}
?>
</table>

```

```

<?php
require_once "db.php";

if ( !isset($_POST['name']) && !isset($_POST['email'])
    && !isset($_POST['password'])) {
    $n = $_POST['name'];
    $e = $_POST['email'];
    $p = $_POST['password'];
    $sql = "INSERT INTO users (name, email, password)
        VALUES ('$n', '$e', '$p)";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}

if ( !isset($_POST['delete']) && !isset($_POST['id']) ) {
    $id = $_POST['id'];
    $sql = "DELETE FROM users WHERE id = $id";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}

echo '<table border="1">'. "\n";
$result = mysql_query("SELECT name, email, password, id FROM users");
while ( $row = mysql_fetch_row($result) ) {
    echo "<td><td>";
    echo(htmlentities($row[0]));
    echo("</td><td>");
    echo(htmlentities($row[1]));
    echo("</td><td>");
    echo(htmlentities($row[2]));
    echo("</td><td>\n");
    echo('<form method="post"><input type="hidden" ');
    echo('name="id" value="' . $row[3] . '">'. "\n");
    echo('<input type="submit" value="Del" name="delete">');
    echo("\n</form>\n");
    echo("</td></tr>\n");
}
?>
</table>
<p>Add New User</p>
<form method="post">
<p>Name:
<input type="text" name="name"></p>
<p>Email:
<input type="text" name="email"></p>
<p>Password:
<input type="password" name="password"></p>
<p><input type="submit" value="Add New"/></p>
</form>

```

# Program Outline

```
<p>Add A New User</p>
<form method="post">
  <p>Name:
  <input type="text" name="name"></p>
  <p>Email:
  <input type="text" name="email"></p>
  <p>Password:
  <input type="password" name="password"></p>
  <p><input type="submit" value="Add New"/></p>
</form>
```

```
<?php
require_once "db.php";

if ( !isset($_POST['name']) && !isset($_POST['email'])
    && !isset($_POST['password'])) {
    $n = $_POST['name'];
    $e = $_POST['email'];
    $p = $_POST['password'];
    $sql = "INSERT INTO users (name, email, password)
            VALUES ('$n', '$e', '$p)";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}

if ( !isset($_POST['delete']) && !isset($_POST['id']) ) {
    $id = $_POST['id'];
    $sql = "DELETE FROM users WHERE id = $id";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}

echo "<table border='1'>.\n";
$result = mysql_query("SELECT name, email, password, id FROM users");
while ( $row = mysql_fetch_row($result) ) {
    echo "<tr><td>";
    echo(htmlentities($row[0]));
    echo("</td><td>");
    echo(htmlentities($row[1]));
    echo("</td><td>");
    echo(htmlentities($row[2]));
    echo("</td><td>\n");
    echo("<form method='post'><input type='hidden' ");
    echo("<name='id' value='". $row[3]. "'>.\n");
    echo("<input type='submit' value='Del' name='delete'>");
    echo("</form>\n");
    echo("</td></tr>\n");
}
?>
</table>
<p><input type="text" name="name"></p>
<p>Email:
<input type="text" name="email"></p>
<p>Password:
<input type="password" name="password"></p>
<p><input type="submit" value="Add New"/></p>
</form>
```

# Security Alert: SQL Injection

**SQL injection** or SQLi is a code injection technique that exploits a security vulnerability in some computer software. An injection occurs at the database level of an application (like queries). The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. Using well designed query language interpreters can prevent SQL injections.

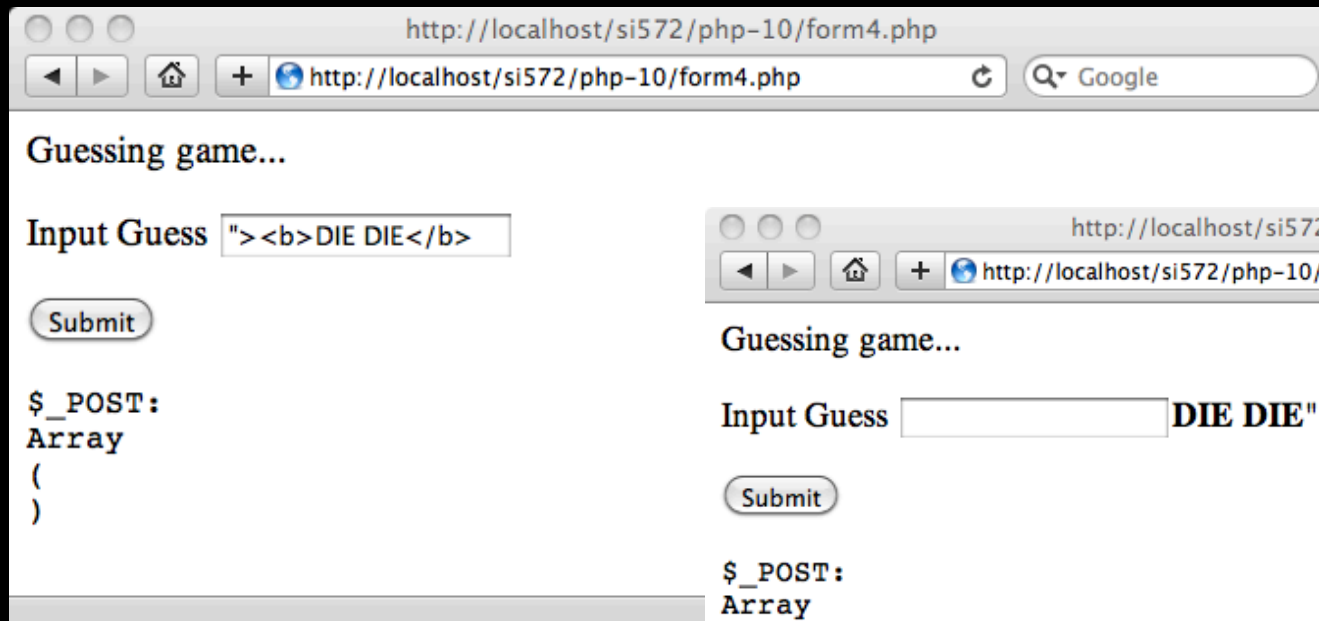
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

# Security Alert: SQL Injection

- This code is prone to SQL Injection - where?

```
if ( isset($_POST['name']) && isset($_POST['email'])
    && isset($_POST['password'])) {
    $n = $_POST['name'];
    $e = $_POST['email'];
    $p = $_POST['password'];
    $sql = "INSERT INTO users (name, email, password)
           VALUES ('$n', '$e', '$p')";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
}
```

# Recall



http://localhost/si572/php-10/form4.php

Guessing game...

Input Guess

```
$_POST:
Array
(
)
```



http://localhost/si572/php-10/form4.php

Guessing game...

Input Guess

```
$_POST:
Array
(
    [guess] => "><b>DIE DIE" />"
)
```



```
<form method="post">
  <p><label for="guess">Input Guess</label>
  <input type="text" name="guess" id="guess"
value=""><b>DIE DIE</b>" /></p>
  <input type="submit"/>
</form>
```

# What Could Go Wrong?



A screenshot of a web browser window. The address bar shows the URL `http://localhost/si572/php-10/user1.php`. The page content displays the following SQL statement:

```
INSERT INTO users (name, email, password)
VALUES ('Fred', 'fred@umich.edu', 'YO')
```

Below the SQL output is a section titled "Add A New User" containing three input fields:

Name:

Email:

Password:

At the bottom of the form is a button labeled "Add New".

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.



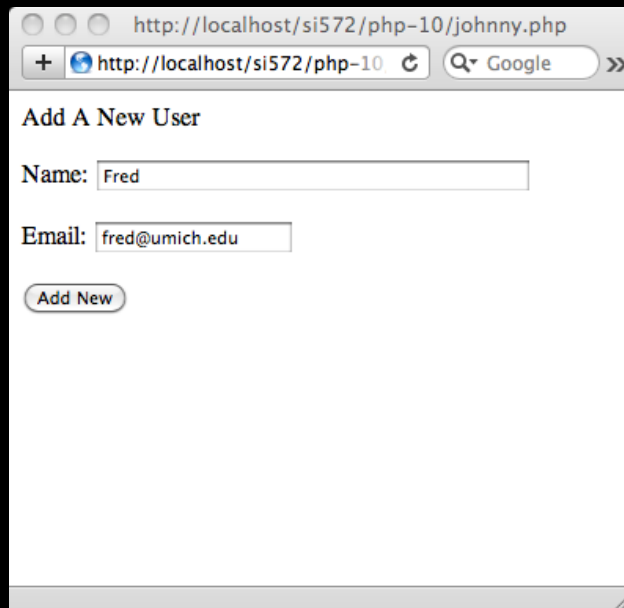
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

<http://xkcd.com/327/>

```
<?php
require_once "db.php";

if ( isset($_POST['name']) && isset($_POST['email'])) {
    $n = $_POST['name'];
    $e = $_POST['email'];
    $p = 'secret';
    $sql = "INSERT INTO users (email, name, password)
           VALUES ('$e', '$n', '$p')";
    echo "<p>\n$sql\n</p>\n";
    mysql_query($sql);
}
?>
<p>Add A New User</p>
<form method="post">
<p>Name:
<input type="text" name="name" size="50"></p>
<p>Email:
<input type="text" name="email"></p>
<p><input type="submit" value="Add New"/></p>
</form>
```

```
if ( isset($_POST['name']) && isset($_POST['email'])) {  
    $n = $_POST['name'];  
    $e = $_POST['email'];  
    $p = 'secret';  
    $sql = "INSERT INTO users (email, name, password)  
           VALUES ('$e', '$n', '$p')";  
    echo "<p>\n$sql\n</p>\n";  
    mysql_query($sql);  
}
```



http://localhost/si572/php-10/johnny.php

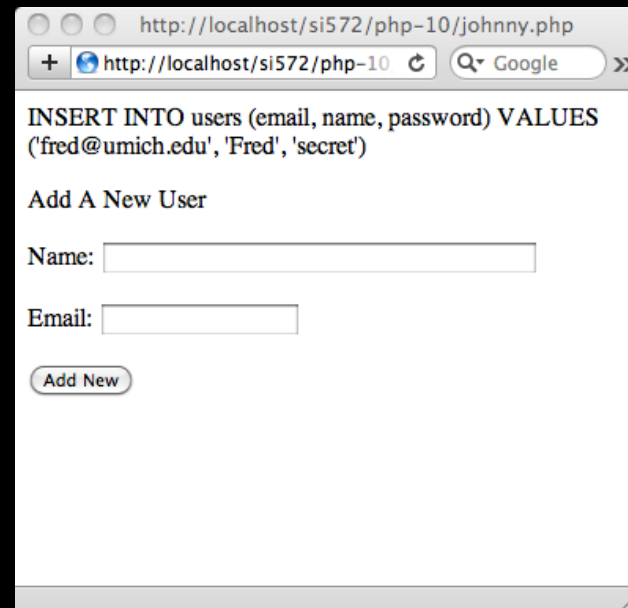
http://localhost/si572/php-10

Google

### Add A New User

Name:

Email:



http://localhost/si572/php-10/johnny.php

http://localhost/si572/php-10

Google

```
INSERT INTO users (email, name, password) VALUES  
( 'fred@umich.edu', 'Fred', 'secret')
```

### Add A New User

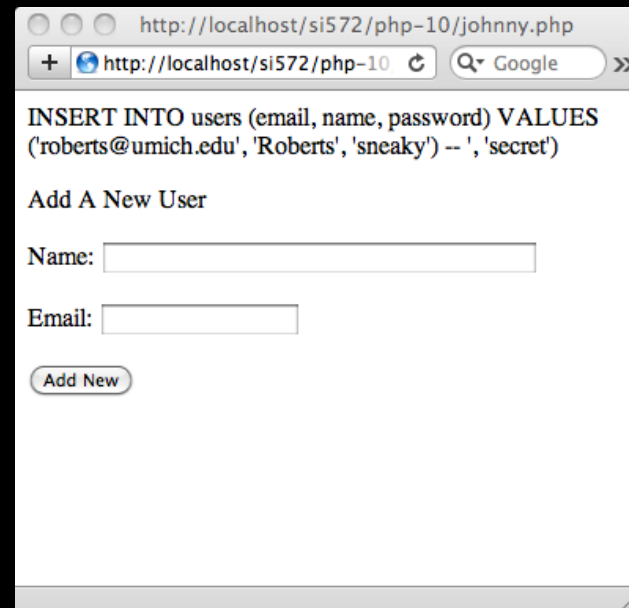
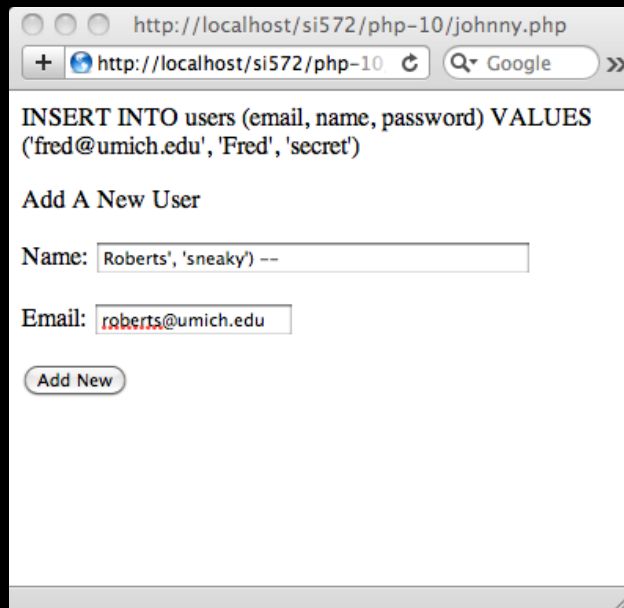
Name:

Email:

```

if ( isset($_POST['name']) && isset($_POST['email'])) {
    $n = $_POST['name'];
    $e = $_POST['email'];
    $p = 'secret';
    $sql = "INSERT INTO users (email, name, password)
            VALUES ('$e', '$n', '$p')";
    echo "<p>\n$sql\n</p>\n";
    mysql_query($sql);
}

```



```

if ( isset($_POST['name']) && isset($_POST['email'])) {
    $n = $_POST['name'];
    $e = $_POST['email'];
    $p = 'secret';
    $sql = "INSERT INTO users (email, name, password)
            VALUES ('$e', '$n', '$p')";
    echo "<p>\n$sql\n</p>\n";
    mysql_query($sql);
}

```

http://localhost/si572/php-10/johnny.php

INSERT INTO users (email, name, password) VALUES ('roberts@umich.edu', 'Roberts', 'sneaky') -- ', 'secret')

Add A New User

Name:

Email:

```

INSERT INTO users (email, name, password)
VALUES ('roberts@umich.edu',
        'Roberts', 'sneaky') -- ', 'secret')

```

```

INSERT INTO users (email, name, password)
VALUES ('roberts@umich.edu',
        'Roberts', 'sneaky') -- ', 'secret')

```

```
mysql> select * from users;
```

id	name	email	password
1	Chuck	csev@umich.edu	123
2	Glenn	gg@umich.edu	456
4	Sam	sam@umcih	pp
14	Roberts	roberts@umich.edu	sneaky
13	Fred	fred@umich.edu	secret

http://localhost/si572/php-10/johnny.php

INSERT INTO users (email, name, password) VALUES ('fred@umich.edu', 'Fred', 'secret')

Add A New User

Name:

Email:

http://localhost/si572/php-10/johnny.php

INSERT INTO users (email, name, password) VALUES ('roberts@umich.edu', 'Roberts', 'sneaky') -- ', 'secret')

Add A New User

Name:

Email:

# Rescue: mysql\_real\_escape\_string()

```
if ( isset($_POST['name']) && isset($_POST['email'])) {  
    $n = mysql_real_escape_string($_POST['name']);  
    $e = mysql_real_escape_string($_POST['email']);  
    $p = 'secret';  
    $sql = "INSERT INTO users (email, name, password)  
           VALUES ('$e', '$n', '$p)";  
    echo "<p>\n$sql\n</p>\n";  
    mysql_query($sql);  
}
```

Escapes special characters in the string, taking into account the current character set of the connection so that it is safe to place it in a `mysql_query()`. If binary data is to be inserted, this function must be used.

<http://php.net/manual/en/function.mysql-real-escape-string.php>

id	name	email	password
1	Chuck	csev@umich.edu	123
2	Glenn	gg@umich.edu	456
4	Sam	sam@umcih	pp
15	Smith', 'sneaky') --	smith@umich.edu	secret
14	Roberts	roberts@umich.edu	sneaky
13	Fred	fred@umich.edu	secret

http://localhost/si5.../php-10/johnny2.php

http://localhost/si572/php-10

Add A New User

Name:

Email:

http://localhost/si5.../php-10/johnny2.php

http://localhost/si572/php-10

INSERT INTO users (email, name, password) VALUES ('smith@umich.edu', 'Smith', 'sneaky') -- ', 'secret')

Add A New User

Name:

Email:

# Security Lesson: SQL Injection

- **NEVER EVER EVER** take values from the outside world and put them in an SQL string without using
- `mysql_real_escape_string()`

```
if ( isset($_POST['name']) && isset($_POST['email'])) {
    $n = mysql_real_escape_string($_POST['name']);
    $e = mysql_real_escape_string($_POST['email']);
    $p = 'secret';
    $sql = "INSERT INTO users (email, name, password)
           VALUES ('$e', '$n', '$p)";
    echo "<p>\n$sql\n</p>\n";
    mysql_query($sql);
}
```

CRUD!

# CRUD Pattern

- When we store things in database tables we generally need
  - **Create** - Insert a new row
  - **Read** - Read existing row(s)
  - **Update** - Change some values of a record
  - **Delete** - Delete a record
- So far we have done 3/4

# Our Program is a little Ugly

- Usually we create several screens
  - Add new row
  - View all rows (paging)
  - View single row
  - Edit single row
  - Delete a row

Chuck	csev@umich.edu	123	Del
Glenn	gg@umich.edu	456	Del
Sam	sam@umcih	pp	Del
Fred	fred@umich.edu	YO	Del

Add A New User

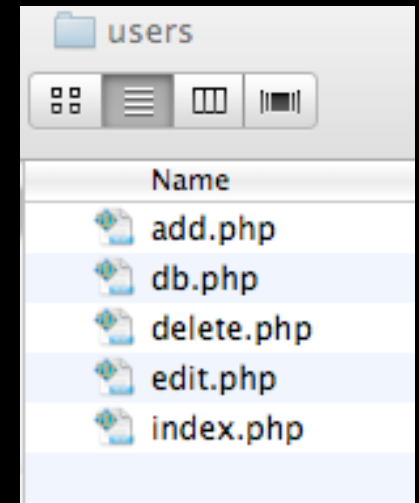
Name:

Email:

Password:

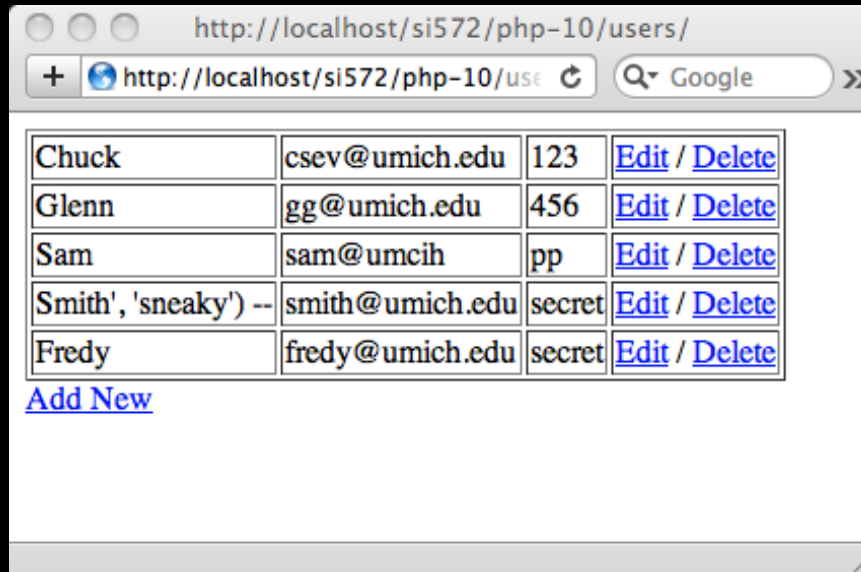
# Five Separate Files

- **index.php** - Main list and links to other files
- **add.php** - Add a new entry
- **delete.php** - Delete an entry
- **edit.php** - Edit existing
- **view.php** (if index.php needed a detail view)



index.php

```
<?php
require_once "db.php";
echo '<table border="1">'. "\n";
$result = mysql_query("SELECT name, email, password, id FROM users");
while ( $row = mysql_fetch_row($result) ) {
    echo "<tr><td>";
    echo(htmlentities($row[0]));
    echo("</td><td>");
    echo(htmlentities($row[1]));
    echo("</td><td>");
    echo(htmlentities($row[2]));
    echo("</td><td>\n");
    echo('<a href="edit.php?id=' .htmlentities($row[3]).'">Edit</a> / ');
    echo('<a href="delete.php?id=' .htmlentities($row[3]).'">Delete</a>');
    echo("</td></tr>\n");
}
?>
</table>
<a href="add.php">Add New</a>
```



```
<tr><td>Chuck</td><td>csev@umich.edu</td><td>123</td><td>  
<a href="edit.php?id=1">Edit</a> /  
<a href="delete.php?id=1">Delete</a></td></tr>  
  
<tr><td>Glenn</td><td>gg@umich.edu</td><td>456</td><td>  
<a href="edit.php?id=2">Edit</a> /  
<a href="delete.php?id=2">Delete</a></td></tr>
```

```

<?php
require_once "db.php";

if ( isset($_POST['name']) && isset($_POST['email'])
    && isset($_POST['password'])) {
    $n = mysql_real_escape_string($_POST['name']);
    $e = mysql_real_escape_string($_POST['email']);
    $p = mysql_real_escape_string($_POST['password']);
    $sql = "INSERT INTO users (name, email, password)
        VALUES ('$n', '$e', '$p')";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
    echo 'Success - <a href="index.php">Continue...</a>';
    return;
}
?>
<p>Add A New User</p>
<form method="post">
<p>Name:
<input type="text" name="name"></p>
<p>Email:
<input type="text" name="email"></p>
<p>Password:
<input type="password" name="password"></p>
<p><input type="submit" value="Add New" />
<a href="index.php">Cancel</a></p>
</form>

```

add.php

http://localhost/si572/php-10/users/add.php

http://localhost/si572/php-10/use

Google

Add A New User

Name: Sarah

Email: sarah@umich.edu

Password: ...

Add New Cancel

http://localhost/si572/php-10/users/

Chuck	csev@umich.edu	123	<a href="#">Edit / Delete</a>
Glenn	gg@umich.edu	456	<a href="#">Edit / Delete</a>
Sam	sam@umcih	pp	<a href="#">Edit / Delete</a>
Smith', 'sneaky') --	smith@umich.edu	secret	<a href="#">Edit / Delete</a>
Fredy	fredy@umich.edu	secret	<a href="#">Edit / Delete</a>

[Add New](#)

http://localhost/si572/php-10/users/add.php

Add A New User

Name:

Email:

Password:

[Cancel](#)

http://localhost/si572/php-10/users/add.php

```
INSERT INTO users (name, email, password)
VALUES ('Sarah', 'sarah@umich.edu', '123')
```

Success - [Continue...](#)

http://localhost/si572/php-10/users/index.php

Chuck	csev@umich.edu	123	<a href="#">Edit / Delete</a>
Glenn	gg@umich.edu	456	<a href="#">Edit / Delete</a>
Sam	sam@umcih	pp	<a href="#">Edit / Delete</a>
Smith', 'sneaky') --	smith@umich.edu	secret	<a href="#">Edit / Delete</a>
Sarah	sarah@umich.edu	123	<a href="#">Edit / Delete</a>
Fredy	fredy@umich.edu	secret	<a href="#">Edit / Delete</a>

[Add New](#)

## delete.php

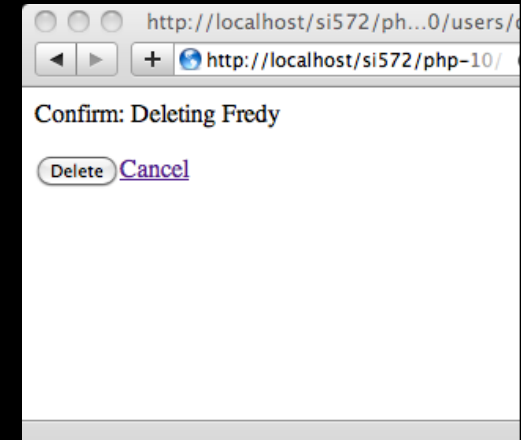
```
<?php
require_once "db.php";

if ( isset($_POST['delete']) && isset($_POST['id']) ) {
    $id = $_POST['id'];
    $sql = "DELETE FROM users WHERE id = $id";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
    echo 'Success - <a href="index.php">Continue...</a>';
    return;
}

$id = $_GET['id'];
$result = mysql_query("SELECT name,id FROM users WHERE id='$id'");
$row = mysql_fetch_row($result);

echo "<p>Confirm: Deleting $row[0]</p>\n";

echo('<form method="post"><input type="hidden" ');
echo('name="id" value="' . $row[1] . '">');
echo('<input type="submit" value="Delete" name="delete">');
echo('<a href="index.php">Cancel</a>');
echo("\n</form>\n");
?>
```



http://localhost/si572/php-10/users/index.php

Chuck	csev@umich.edu	123	<a href="#">Edit</a> / <a href="#">Delete</a>
Glenn	gg@umich.edu	456	<a href="#">Edit</a> / <a href="#">Delete</a>
Sam	sam@umcuh	pp	<a href="#">Edit</a> / <a href="#">Delete</a>
Smith', 'sneaky') --	smith@umich.edu	secret	<a href="#">Edit</a> / <a href="#">Delete</a>
Sarah	sarah@umich.edu	123	<a href="#">Edit</a> / <a href="#">Delete</a>
Fredy	fredy@umich.edu	secret	<a href="#">Edit</a> / <a href="#">Delete</a>

[Add New](#)

http://localhost/si572/ph...0/users/delete.php?id=13

Confirm: Deleting Fredy

[Cancel](#)

http://localhost/si572/ph...0/users/delete.php?id=13

```
DELETE FROM users WHERE id = 13
```

Success - [Continue...](#)

http://localhost/si572/php-10/users/index.php

Chuck	csev@umich.edu	123	<a href="#">Edit</a> / <a href="#">Delete</a>
Glenn	gg@umich.edu	456	<a href="#">Edit</a> / <a href="#">Delete</a>
Sam	sam@umcuh	pp	<a href="#">Edit</a> / <a href="#">Delete</a>
Smith', 'sneaky') --	smith@umich.edu	secret	<a href="#">Edit</a> / <a href="#">Delete</a>
Sarah	sarah@umich.edu	123	<a href="#">Edit</a> / <a href="#">Delete</a>

[Add New](#)

```

<?php
require_once "db.php";

if ( isset($_POST['name']) && isset($_POST['email'])
    && isset($_POST['password']) && isset($_POST['id']) ) {
    $n = mysql_real_escape_string($_POST['name']);
    $e = mysql_real_escape_string($_POST['email']);
    $p = mysql_real_escape_string($_POST['password']);
    $id = mysql_real_escape_string($_POST['id']);
    $sql = "UPDATE users SET name='$n', email='$e',
        password='$p' WHERE id='$id'";
    echo "<pre>\n$sql\n</pre>\n";
    mysql_query($sql);
    echo 'Updated - <a href="index.php">Continue...</a>';
    return;
}

$id = $_GET['id'];
$result = mysql_query("SELECT name, email, password, id
    FROM users WHERE id='$id'");
$row = mysql_fetch_row($result);

$n = htmlentities($row[0]);
$e = htmlentities($row[1]);
$p = htmlentities($row[2]);
$id = htmlentities($row[3]);

```

edit.php

http://localhost/si572/php-10/users/edit.php?id=4

http://localhost/si572/php-10/ Google

Edit User

Name:

Email:

Password:

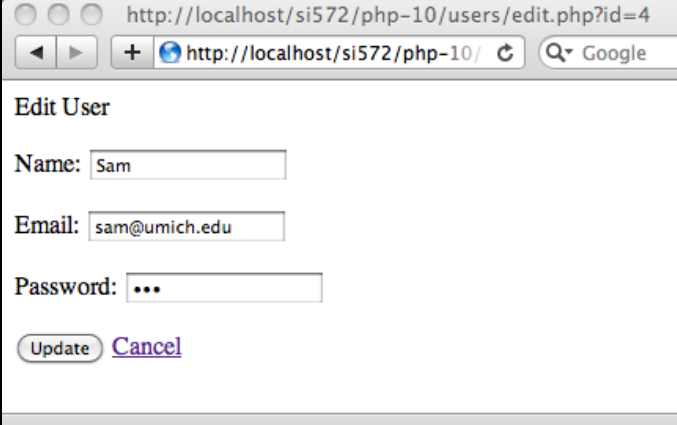
[Cancel](#)

## edit.php

```
$id = $_GET['id'];
$result = mysql_query("SELECT name, email, password, id
    FROM users WHERE id='$id'");
$row = mysql_fetch_row($result);

$n = htmlentities($row[0]);
$e = htmlentities($row[1]);
$p = htmlentities($row[2]);
$id = htmlentities($row[3]);

echo <<< _END
<p>Edit User</p>
<form method="post">
<p>Name:
<input type="text" name="name" value="$n"></p>
<p>Email:
<input type="text" name="email" value="$e"></p>
<p>Password:
<input type="password" name="password" value="$p"></p>
<input type="hidden" name="id" value="$id">
<p><input type="submit" value="Update"/>
<a href="index.php">Cancel</a></p>
</form>
_END
?>
```



http://localhost/si572/php-10/users/edit.php?id=4

http://localhost/si572/php-10/ Google

Edit User

Name:

Email:

Password:

[Cancel](#)

http://localhost/si572/php-10/users/index.php

Chuck	csev@umich.edu	123	<a href="#">Edit</a> / <a href="#">Delete</a>
Glenn	gg@umich.edu	456	<a href="#">Edit</a> / <a href="#">Delete</a>
Sam	sam@umcih	pp	<a href="#">Edit</a> / <a href="#">Delete</a>
Smith', 'sneaky') --	smith@umich.edu	secret	<a href="#">Edit</a> / <a href="#">Delete</a>
Sarah	sarah@umich.edu	123	<a href="#">Edit</a> / <a href="#">Delete</a>

[Add New](#)

http://localhost/si572/php-10/users/edit.php?id=4

Edit User

Name:

Email:

Password:

[Cancel](#)

http://localhost/si572/php-10/users/edit.php?id=4

```
UPDATE users SET name='Sam', email='sam@umich.edu',
password='zzz' WHERE id='4'
```

Updated - [Continue...](#)

http://localhost/si572/php-10/users/index.php

Chuck	csev@umich.edu	123	<a href="#">Edit</a> / <a href="#">Delete</a>
Glenn	gg@umich.edu	456	<a href="#">Edit</a> / <a href="#">Delete</a>
Sam	sam@umich.edu	zzz	<a href="#">Edit</a> / <a href="#">Delete</a>
Smith', 'sneaky') --	smith@umich.edu	secret	<a href="#">Edit</a> / <a href="#">Delete</a>
Sarah	sarah@umich.edu	123	<a href="#">Edit</a> / <a href="#">Delete</a>

[Add New](#)

# Summary

- Making database connections
- Forms, `$_GET` and `$_POST`
- Sanitizing HTML
- Inserting and Deleting
- Security: Sanitizing SQL
- A multi-file CRUD application