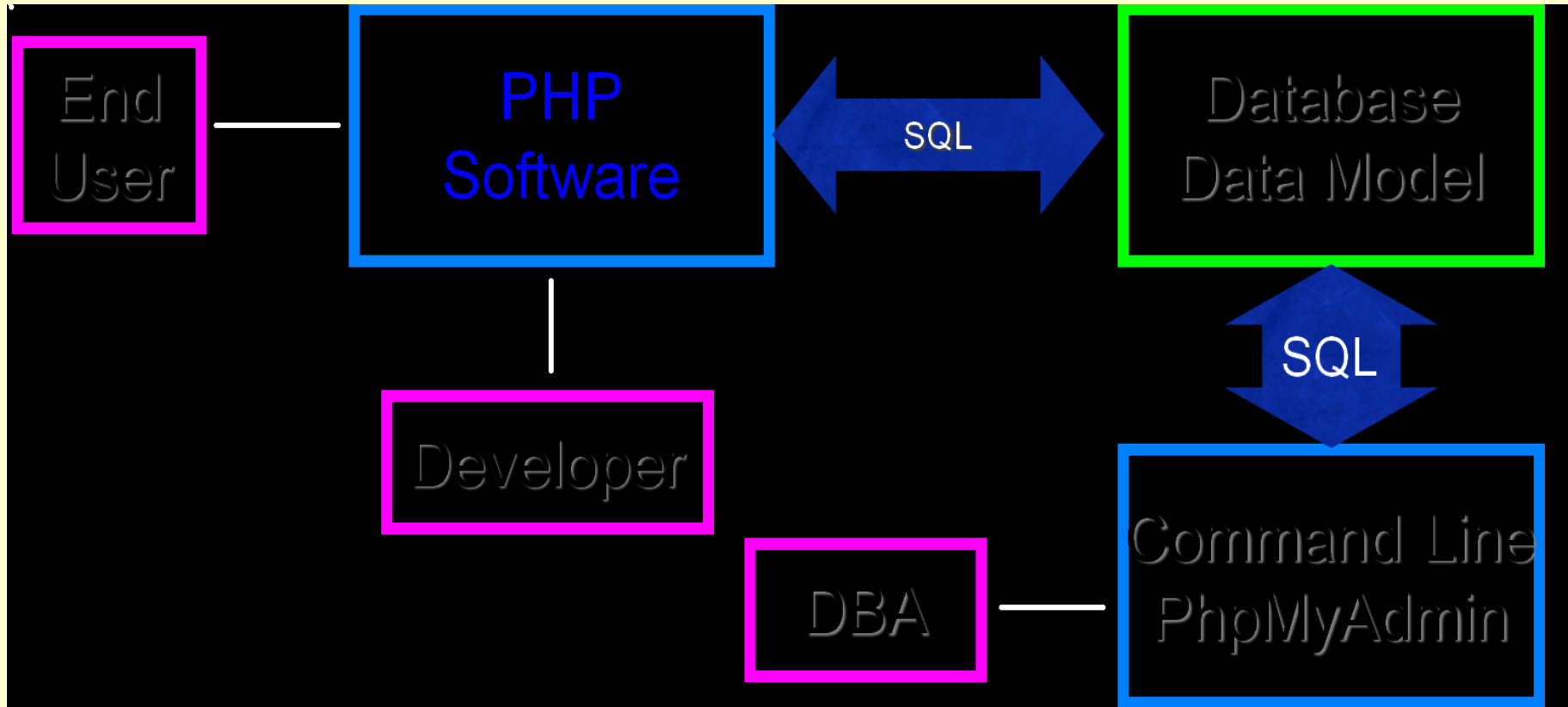# DT228/2 Web Development

Accessing MySQL Using PHP

Application Structure

Starting MySQL from the Windows Command Line

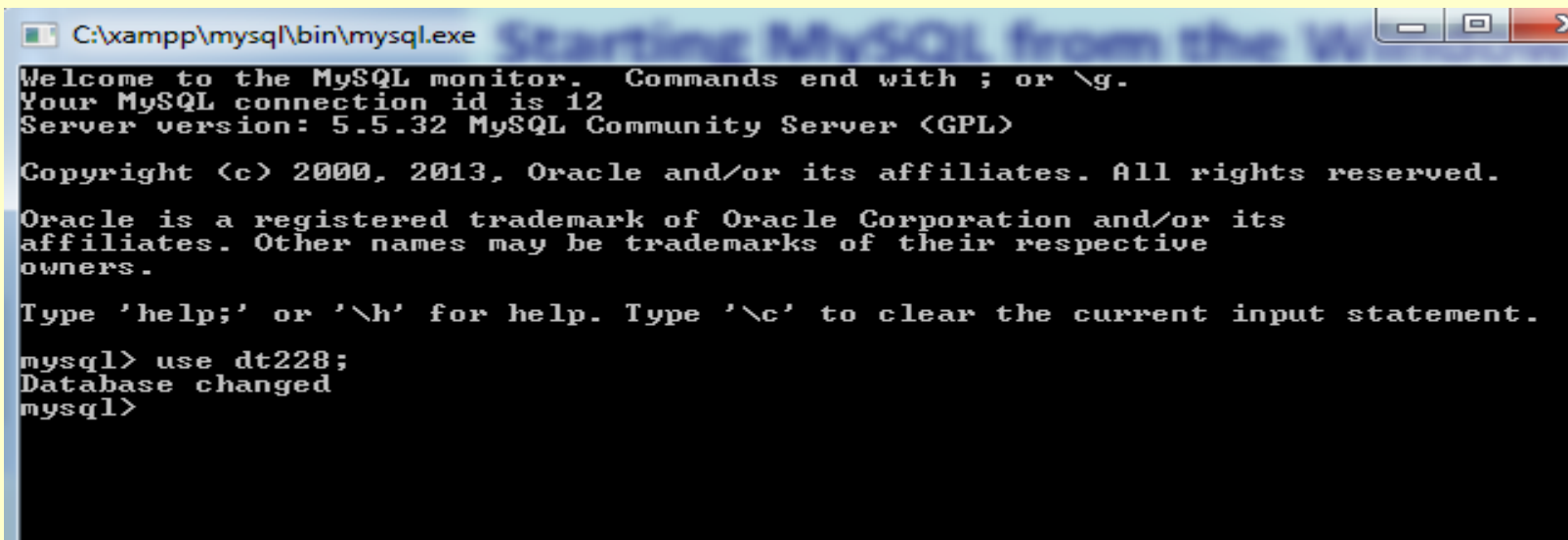To start the **mysqld** server from the command line, you should start a console window (or "DOS window") and enter this command:
shell> **"C:\Program Files\MySQL\MySQL Server 5.6\bin\mysqld"**
The path to **mysqld** may vary depending on the install location of MySQL on your system.
You can stop the MySQL server by executing this command:
shell> **"C:\Program Files\MySQL\MySQL Server 5.0\bin\mysqladmin" -u root shutdown**

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);
```

```
Query OK, 0 rows affected (0.27 sec)
Records: 0  Duplicates: 0  Warnings: 0

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    |                |
+----------+------------------+------+-----+---------+----------------+
4 rows in set (0.08 sec)

mysql> _
```

Inserting a Few Records

```
INSERT INTO users (name,email,password) VALUES
('Liu','cindy.liu@dit.ie','123');
INSERT INTO users (name,email,password) VALUES
('Glenn','gg@gmail.com','456');
```

```
mysql> INSERT INTO users (name,email,password) VALUES ('Liu','cindy.liu@dit.ie',
'123');
Query OK, 1 row affected (0.08 sec)

mysql> INSERT INTO users (name,email,password) VALUES ('Glenn','gg@gmail.com','4
56');
Query OK, 1 row affected (0.03 sec)

mysql> select * from users;
+----+-------+------------------+----------+
| id | name  | email            | password |
+----+-------+------------------+----------+
|  1 | Liu   | cindy.liu@dit.ie | 123      |
|  2 | Glenn | gg@gmail.com     | 456      |
+----+-------+------------------+----------+
2 rows in set (0.00 sec)

mysql>
```
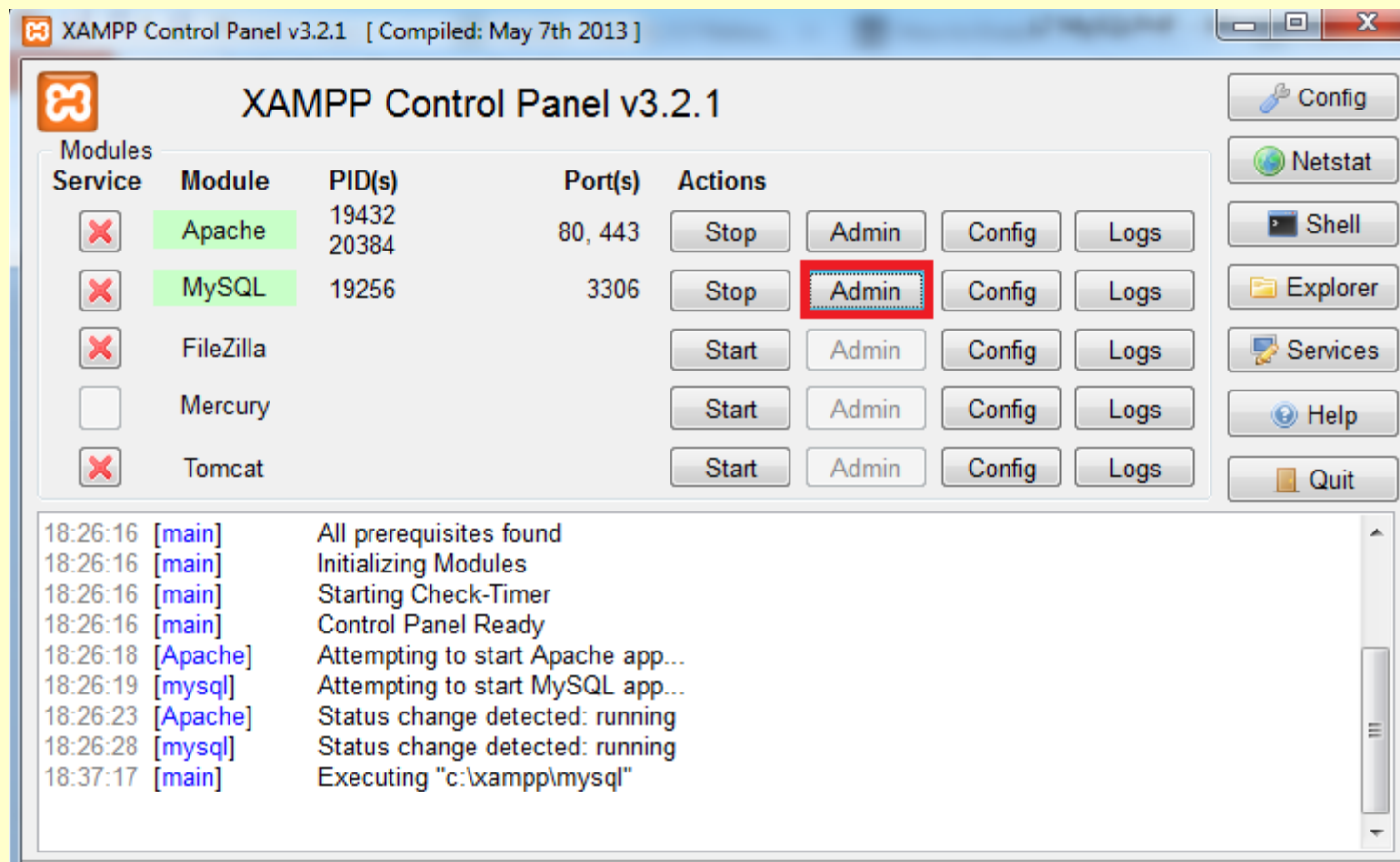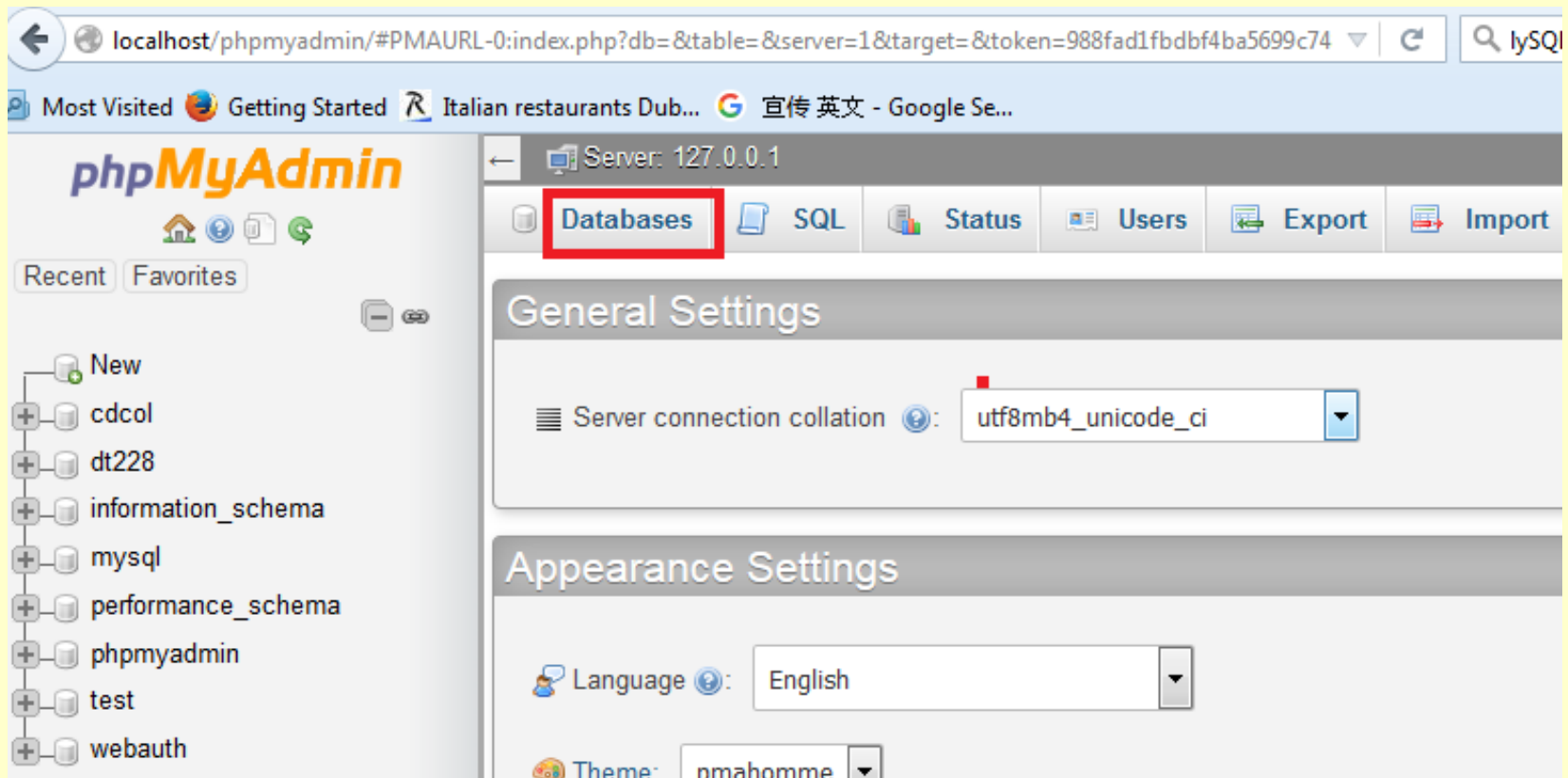
Starting MySQL from the XAMPP Control Panel

Click MySQL Admin button

Create database

Click the Database button

Create table

Click the Go button

```php
<?php
echo "<pre>\n";
$db = mysqli_connect('localhost', 'root', '') or
die(mysqli_error());
mysqli_select_db("DT228") or die(mysqli_error());
$result = mysql_query("SELECT * FROM users");
while ( $row = mysqli_fetch_row($result) ) {
print_r($row);
}
echo "</pre>\n";
mysqli_close($db);
```
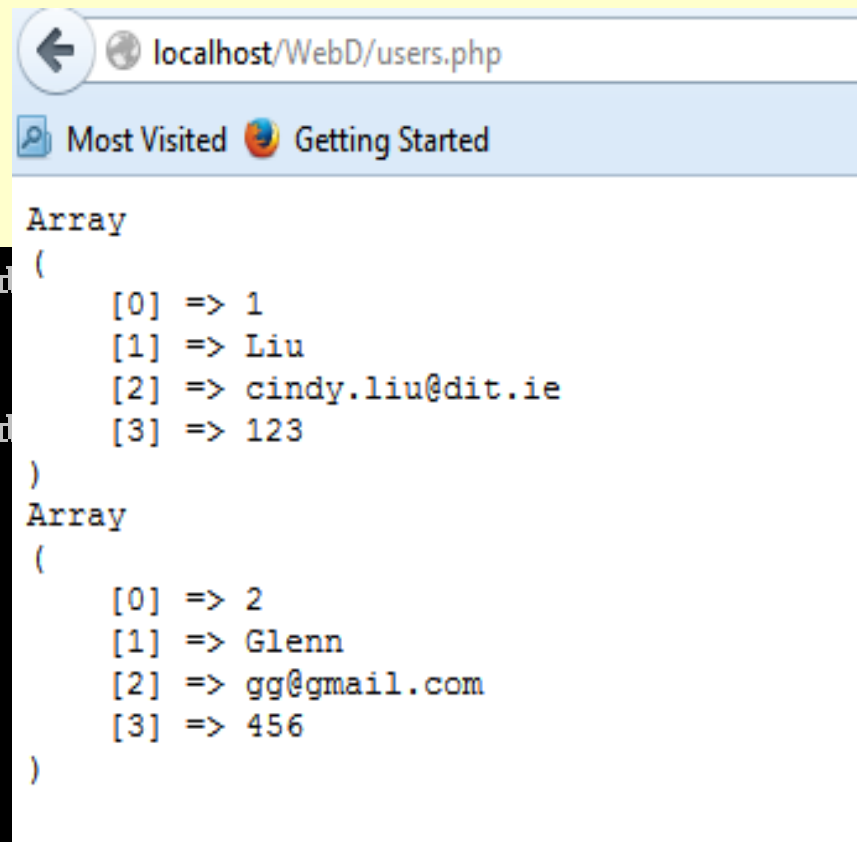
```
mysql> INSERT INTO users (name,email,password
'123');
Query OK, 1 row affected (0.08 sec)

mysql> INSERT INTO users (name,email,password
56');
Query OK, 1 row affected (0.03 sec)

mysql> select * from users;
+----+-------+-------------------+----------+
| id | name  | email             | password |
+----+-------+-------------------+----------+
|  1 | Liu   | cindy.liu@dit.ie  | 123      |
|  2 | Glenn | gg@gmail.com      | 456      |
+----+-------+-------------------+----------+
2 rows in set (0.00 sec)

mysql>
```

localhost/WebD/users.php

Most Visited Getting Started

```
Array
(
    [0] => 1
    [1] => Liu
    [2] => cindy.liu@dit.ie
    [3] => 123
)
Array
(
    [0] => 2
    [1] => Glenn
    [2] => gg@gmail.com
    [3] => 456
)
```
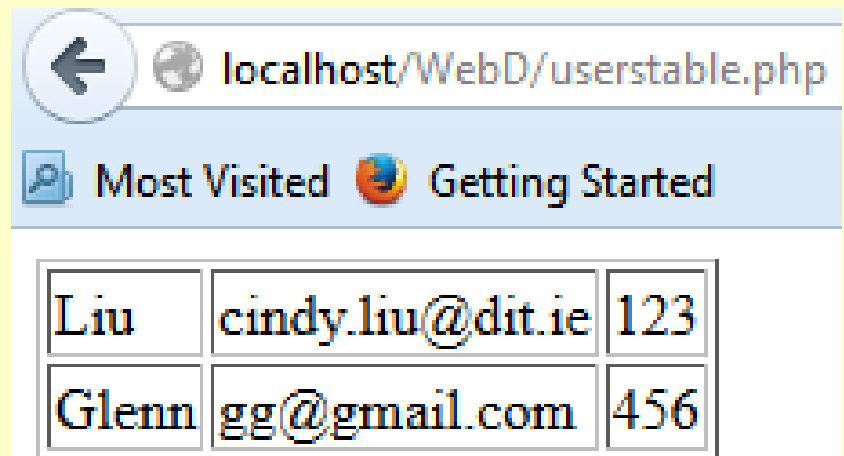
```php
<?php
echo '<table border="1">'."\n";
$db = mysqli_connect('localhost', 'root', '') or
die(mysqli_error());
mysqli_select_db("DT228") or die(mysqli_error());
$result = mysqli_query("SELECT name, email, password
FROM users");
while ( $row = mysqli_fetch_row($result) ) {
echo "<tr><td>";
echo($row[0]);
echo("</td><td>");
echo($row[1]);
echo("</td><td>");
echo($row[2]);
echo("</tr>\n");
}
echo "</table>\n";
mysqli_close($db);
?>
```

localhost/WebD/userstable.php

Most Visited   Getting Started

| Liu | cindy.liu@dit.ie | 123 |
| Glenn | gg@gmail.com | 456 |

```html
<table border="1">
<tr><td>Liu</td><td>cindy.liu@dit.ie</td><td>123</tr>
<tr><td>Glenn</td><td>gg@gmail.com</td><td>456</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
<?php
$db = mysqli_connect('localhost', 'root', '');
if ( $db === FALSE ) die('Fail message');
if ( mysqli_select_db("dt228") === FALSE ) die("Fail
message");
?>
```
db.php

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

echo "<pre>\n";
$result = mysqli_query($db,"SELECT * FROM use
while ( $row = mysql_fetch_row($result) ) {
print_r($row);
}
echo "</pre>\n";
mysqli_close($db);
?>
```
users2.php

```php
<?php
$db = mysqli_connect('localhost', 'root', '');
if ( $db === FALSE ) die('Fail message');
if ( mysqli_select_db("dt228") === FALSE ) die("Fail
message");
?>
```

db.php

```php
<?php
$db = mysqli_connect('localhost', 'root', '') or
die('Fail message');
mysqli_select_db("dt228") or die("Fail message");
?>
```
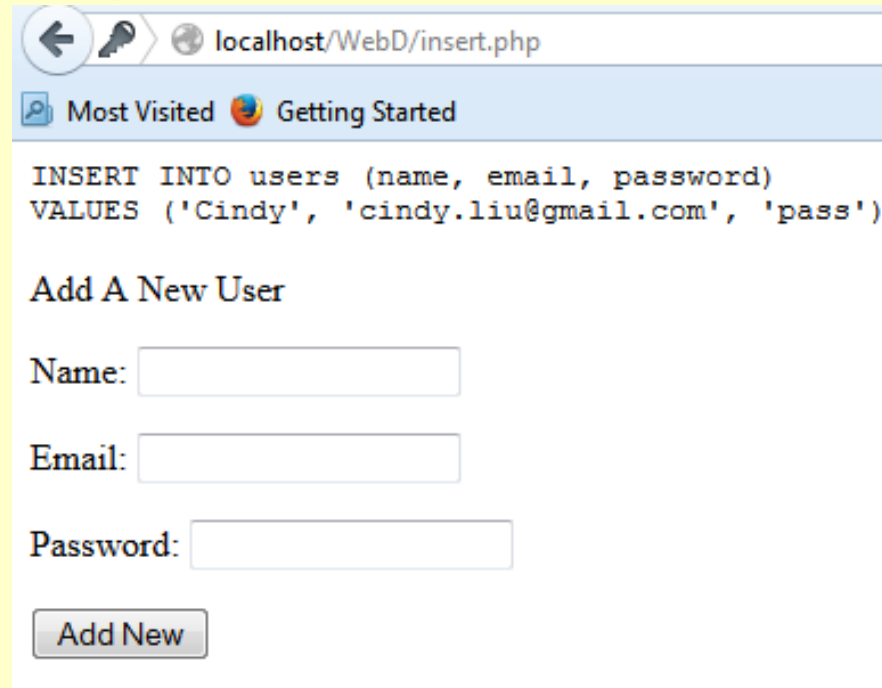
db2.php

```php
<?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$sql\n</pre>\n";
mysqli_query($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>
```


Browser window showing localhost/WebD/insert.php:

```
INSERT INTO users (name, email, password)
VALUES ('Cindy', 'cindy.liu@gmail.com', 'pass')
```

Add A New User

Name: [   ]

Email: [   ]

Password: [   ]

[Add New]

```
localhost/WebD/insert.php

Most Visited    Getting Started

INSERT INTO users (name, email, password)
VALUES ('Cindy', 'cindy.liu@gmail.com', 'pass')

Add A New User

Name:    [                    ]

Email:   [                    ]

Password: [                    ]

[ Add New ]
```

```
mysql> select * from users;
+----+-------+---------------------+----------+
| id | name  | email               | password |
+----+-------+---------------------+----------+
|  1 | Liu   | cindy.liu@dit.ie    | 123      |
|  2 | Glenn | gg@gmail.com        | 456      |
|  3 | Cindy | cindy.liu@gmail.com | pass     |
+----+-------+---------------------+----------+
3 rows in set (0.00 sec)

mysql>
```

```php
  $sql = "INSERT INTO users (name, email, password)
VALUES ('$n', '$e', '$p')";
echo "<pre>\n$sql\n</pre>\n";
mysqli_query($sql);
}
echo '<table border="1">'."\n";
$result = mysqli_query("SELECT name, email, password
FROM users");
while ( $row = mysqli_fetch_row($result) ) {
echo "<tr><td>";
echo(htmlentities($row[0]));
echo("</td><td>");
echo(htmlentities($row[1]));
echo("</td><td>");
echo(htmlentities($row[2]));
echo("</tr>\n");
}
?>
</table>
<p>Add A New User</p>
```
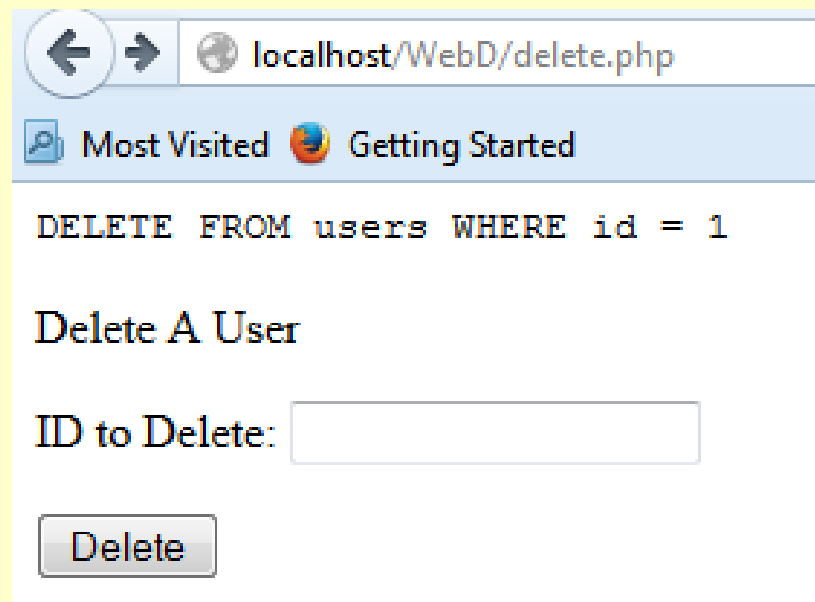
```php
<?php
require_once "db.php";
if ( isset($_POST['id']) ) {
$id = $_POST['id'];
$sql = "DELETE FROM users WHERE id = $id";
echo "<pre>\n$sql\n</pre>\n";
mysqli_query($sql);
}
?>
<p>Delete A User</p>
<form method="post">
<p>ID to Delete:
<input type="text" name="id"></p>
<p><input type="submit" value="Delete"/></p>
</form>
```


localhost/WebD/delete.php

Most Visited   Getting Started

```
DELETE FROM users WHERE id = 1
```

Delete A User

ID to Delete: [   ]

[Delete]

localhost/WebD/delete.php

Most Visited   Getting Started

```
DELETE FROM users WHERE id = 1
```

Delete A User

ID to Delete: [   ]

[Delete]

```
Current database: dt228

+------+--------+------------------------+----------+
| id   | name   | email                  | password |
+------+--------+------------------------+----------+
|    2 | Glenn  | gg@gmail.com           | 456      |
|    3 | Cindy  | cindy.liu@gmail.com    | pass     |
|    4 | dt228  | dt228@dit.ie           | dt228    |
+------+--------+------------------------+----------+
3 rows in set (1.06 sec)

mysql> _
```

```php
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";
mysqli_query($sql);
}
echo '<table border="1">'."\n";
$result = mysqli_query("SELECT name, email, passwo
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");
}
```


localhost/WebD/users3.php

Most Visited   Getting Started

Glenn	gg@gmail.com	456	Del
Cindy	cindy.liu@gmail.com	pass	Del
dt228	dt228@dit.ie	dt228	Del
Cindy	cindy.liu@dit.ie	123	Del

Add A New User

Name:

Email:

Password:

Add New

```php
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");
```

```html
<tr><td>Cindy</td><td>cindy.liu@dit.ie</td>
<td>123</td>
<td><form method="post">
<input type="hidden" name="id" value="5">
<input type="Submit" value="Del" name="delete">
</form>
</td>
</tr>
```

```php
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";
mysqli_query($sql);
}
```

localhost/WebD/users3.php

Most Visited Getting Started

Glenn	gg@gmail.com	456	Del
Cindy	cindy.liu@gmail.com	pass	Del
dt228	dt228@dit.ie	dt228	Del
Cindy	cindy.liu@dit.ie	123	Del

Add A New User

Name:

Email:

Password:

Add New

```
localhost/WebD/users4.php

Most Visited  Getting Started

DELETE FROM users WHERE id = 6
```

Glenn	gg@gmail.com	456	Del
Cindy	cindy.liu@gmail.com	pass	Del
dt228	dt228@dit.ie	dt228	Del

Add A New User

Name: [   ]

Email: [   ]

Password: [   ]

[Add New]

```php
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";
mysqli_query($sql);
}
```

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

Security Alert: SQL Injection

- This code is prone to SQL Injection - where?

```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$sql\n</pre>\n";
    mysqli_query($sql);
}
```

An Example


```
<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>
```

Another Example

```
<?PHP
$query = "Select news_title, news_text ";
$query .= "FROM news";
$query .= "Where news_id=". $_GET['id'];

mysqli_query($query);
?>
```
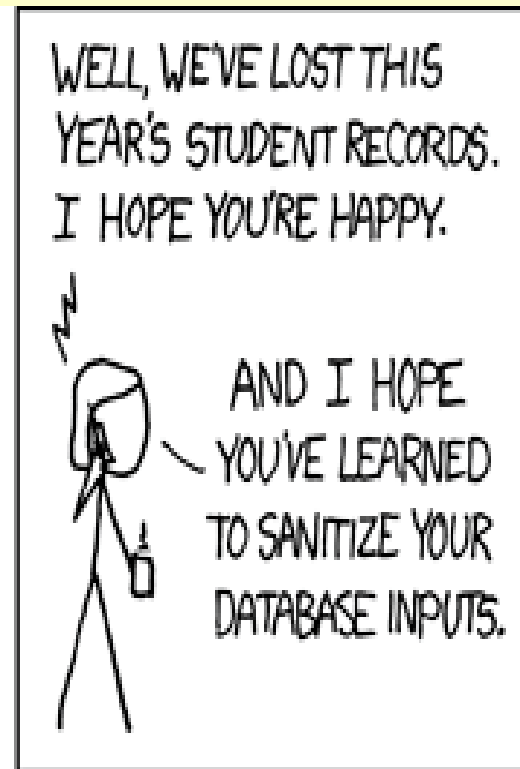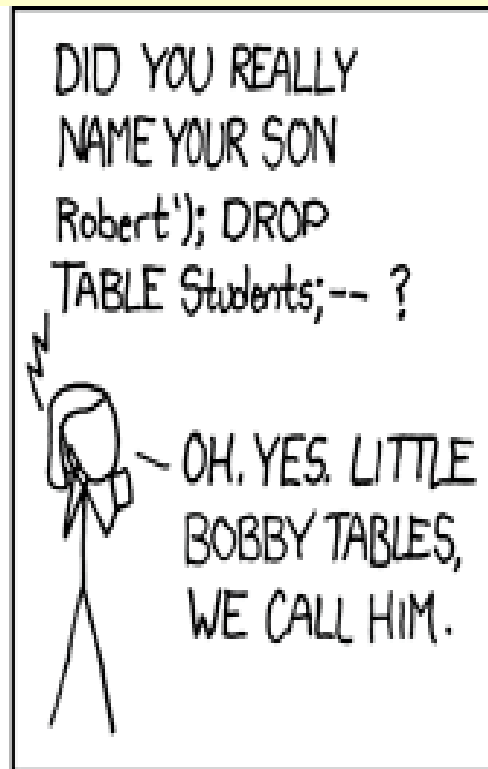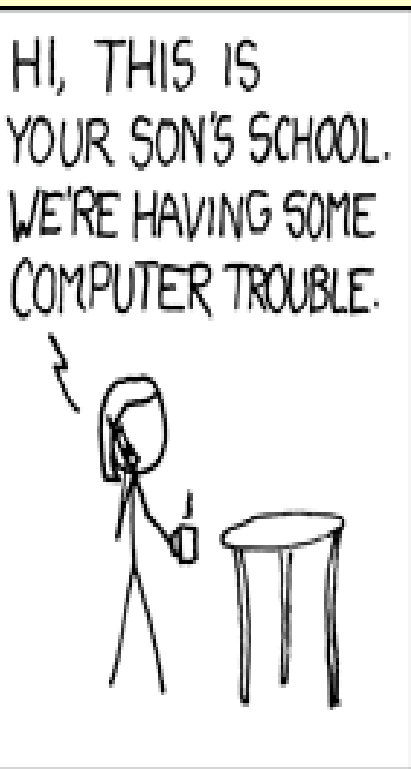
What if the valuse of $_GET['id'] is "0; Delete FROM news;" ?

Select news_title, news_text FROM news Where news_id=0; Delete FROM news;

This is not Funny

http://xkcd.com/327/

```php
<?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$sql\n</p>\n";
mysqli_query($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>
```

```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$sql\n</p>\n";
mysqli_query($sql);
}
```

localhost/WebD/insertw

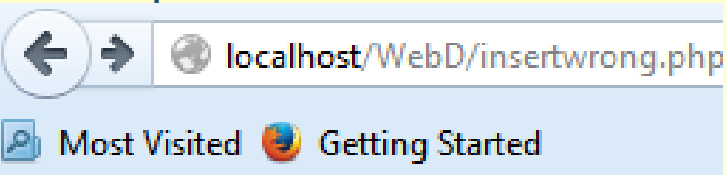Most Visited Getting Started

Add A New User

Name: test

Email: test

[Add New]

---

localhost/WebD/insertwrong.php

Most Visited Getting Started

INSERT INTO users (email, name, password) VALUES ('test', 'test', 'secret')
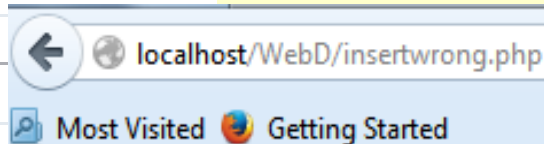
Add A New User

Name:

Email:

[Add New]

```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$sql\n</p>\n";
mysqli_query($sql);
```

localhost/WebD/insertwrong.php

Most Visited   Getting Started

Add A New User

Name: Roberts', 'sneaky') --

Email: test

[Add New]

localhost/WebD/insertwrong.php

Most Visited   Getting Started

INSERT INTO users (email, name, password) VALUES ('test', 'Roberts', 'sneaky') -- ', 'secret')

Add A New User

Name: [   ]

Email: [   ]

[Add New]

```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$sql\n</p>\n";
mysqli_query($sql);
```

localhost/WebD/insertwrong.php
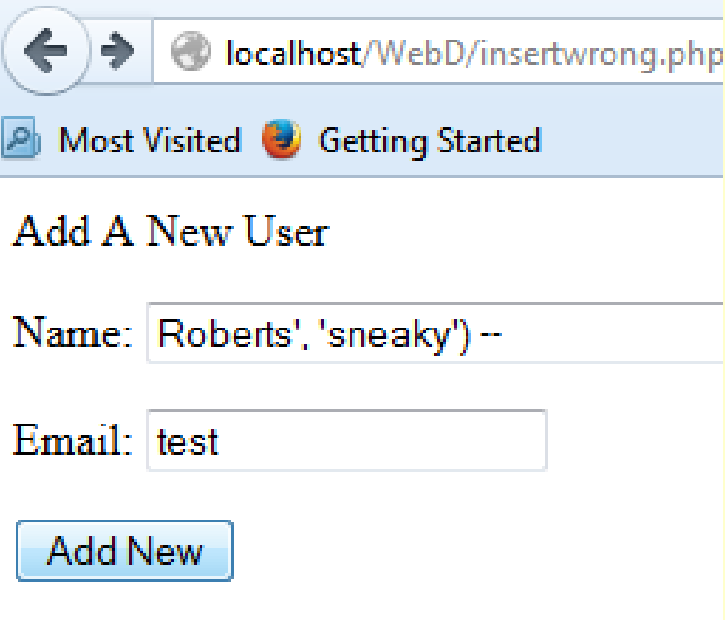
Most Visited 🔴 Getting Started

Add A New User

Name: Roberts','sneaky') --

Email: test

Add New

INSERT INTO users (email, name, password)
VALUES ('test','Roberts', 'sneaky') --
', 'secret')

INSERT INTO users (email, name, password)
VALUES ('test','Roberts', 'sneaky')--
', 'secret')

```
mysql> select * from users;
+----+---------+-----------------------+----------+
| id | name    | email                 | password |
+----+---------+-----------------------+----------+
|  2 | Glenn   | gg@gmail.com          | 456      |
|  3 | Cindy   | cindy.liu@gmail.com   | pass     |
|  4 | dt228   | dt228@dit.ie          | dt228    |
|  7 | test    | test                  | secret   |
|  8 | Roberts | test                  | sneaky   |
+----+---------+-----------------------+----------+
5 rows in set (0.00 sec)

mysql>
```

localhost/WebD/inse

Most Visited Getting Started

Add A New User

Name: Roberts', 'sneaky') --

Email: test

Add New

---

localhost/WebD/insertwrong.php

Most Visited Getting Started

INSERT INTO users (email, name, password) VALUES ('test', 'Roberts', 'sneaky') -- ', 'secre

Add A New User

Name:

Email:

Add New

Rescue: mysql_real_escape_string()

```php
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

```
mysql> select * from users;
+----+-----------------------------+-----------------------+----------+
| id | name                        | email                 | password |
+----+-----------------------------+-----------------------+----------+
|  2 | Glenn                       | gg@gmail.com          | 456      |
|  3 | Cindy                       | cindy.liu@gmail.com   | pass     |
|  4 | dt228                       | dt228@dit.ie          | dt228    |
|  7 | test                        | test                  | secret   |
|  8 | Roberts                     | test                  | sneaky   |
|  9 | Roberts', 'sneaky') --      | correct               | secret   |
+----+-----------------------------+-----------------------+----------+
6 rows in set (0.00 sec)

mysql>
```


localhost/WebD/insertcorre

Most Visited Getting Started

Add A New User

Name: Roberts', 'sneaky') --

Email: correct

Add New

localhost/WebD/insertcorrect.php

Most Visited Getting Started

INSERT INTO users (email, name, password) VALUES ('correct', 'Roberts\', \'sneaky\') -- ', '

Add A New User

Name:

Email:

Add New

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()**

CRUD

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

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)

users

add.php
db.php
delete.php
edit.php
index.php

index.php

```php
<?php
require_once "db.php";
echo '<table border="1">'."\n";
$result = mysqli_query("SELECT name, email, password, id FROM
users");
while ( $row = mysqli_fetch_row($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>
```
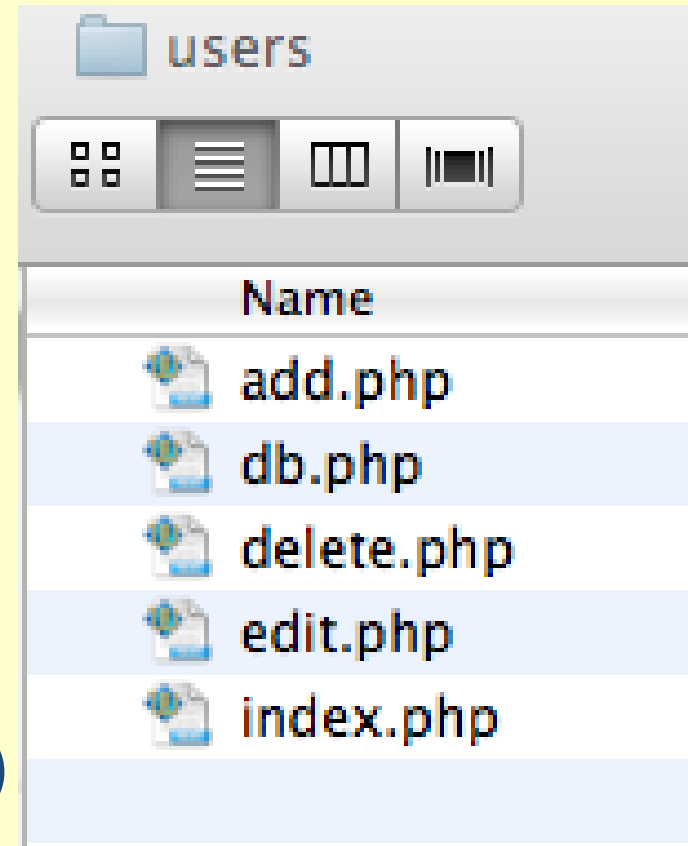
Glenn	gg@gmail.com	456	Edit / Delete
Cindy	cindy.liu@gmail.com	pass	Edit / Delete
dt228	dt228@dit.ie	dt228	Edit / Delete
test	test	secret	Edit / Delete
Roberts	test	sneaky	Edit / Delete
Roberts', 'sneaky') --	correct	secret	Edit / Delete

Add New
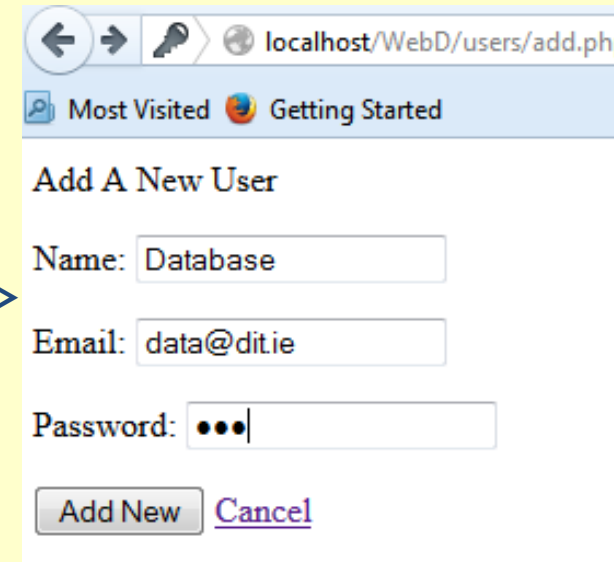
```
<tr><td>Glenn</td><td>gg@gmail.com</td><td>456</td><td>
<a href="edit.php?id=2">Edit</a> / <a
href="delete.php?id=2">Delete</a></td></tr>
<tr><td>Cindy</td><td>cindy.liu@gmail.com</td><td>pass</td><td>
<a href="edit.php?id=3">Edit</a> / <a
href="delete.php?id=3">Delete</a></td></tr>
<tr><td>dt228</td><td>dt228@dit.ie</td><td>dt228</td><td>
<a href="edit.php?id=4">Edit</a> / <a
href="delete.php?id=4">Delete</a></td></tr>
<tr><td>test</td><td>test</td><td>secret</td><td>
<a href="edit.php?id=7">Edit</a> / <a
href="delete.php?id=7">Delete</a></td></tr>
<tr><td>Roberts</td><td>test</td><td>sneaky</td><td>
```

add.php

```php
<?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$sql\n</pre>\n";
mysqli_query($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>
```

Glenn	gg@gmail.com	456	Edit / Delete
Cindy	cindy.liu@gmail.com	pass	Edit / Delete
dt228	dt228@dit.ie	dt228	Edit / Delete
test	test	secret	Edit / Delete
Roberts	test	sneaky	Edit / Delete
Roberts', 'sneaky') --	correct	secret	Edit / Delete

Add New

Add A New User

Name: Database

Email: data@dit.ie

Password: •••

Add New   Cancel

```
INSERT INTO users (name, email, password)
VALUES ('Database', 'data@dit.ie', '123')
```

Success - Continue...

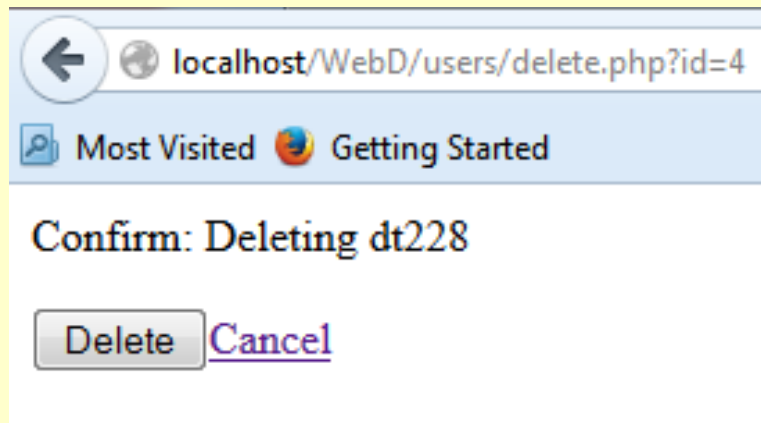| Glenn | gg@gmail.com | 456 | Edit / Delet |
Cindy	cindy.liu@gmail.com	pass	Edit / Delet
dt228	dt228@dit.ie	dt228	Edit / Delet
test	test	secret	Edit / Delet
Roberts	test	sneaky	Edit / Delet
Roberts', 'sneaky') --	correct	secret	Edit / Delet
Database	data@dit.ie	123	Edit / Delet

Add New

delete.php

```php
<?php
require_once "db.php";
if ( isset($_POST['delete']) && isset($_POST['id']) ) {
$id = mysqli_real_escape_string($_POST['id']);
$sql = "DELETE FROM users WHERE id = $id";
echo "<pre>\n$sql\n</pre>\n";
mysqli_query($sql);
echo 'Success - <a href="index.php">Continue...</a>';
return;
}
$id = mysqli_real_escape_string($_GET['id']);
$result = mysqli_query("SELECT name,id FROM users WHERE id='$id'");
$row = mysql_fetch_row($result);
echo "<p>Confirm: Deleting $row[0]</p>\n";
echo('<form method="post"><input type="hidden" ');
echo('name="id" value="'.htmlentities($row[1]).'">'."\n");
echo('<input type="submit" value="Delete" name="delete">');
echo('<a href="index.php">Cancel</a>');
echo("\n</form>\n");
?>
```

localhost/WebD/users/delete.php?id=4

Most Visited   Getting Started

Confirm: Deleting dt228

Delete Cancel

Most Visited Getting Started

Glenn	gg@gmail.com	456	Edit / Delete
Cindy	cindy.liu@gmail.com	pass	Edit / Delete
dt228	dt228@dit.ie	dt228	Edit / Delete
test	test	secret	Edit / Delete
Roberts	test	sneaky	Edit / Delete
Roberts', 'sneaky') --	correct	secret	Edit / Delete

Add New

localhost/WebD/users/delete.php

Most Visited Getting Started

Confirm: Deleting dt228

Delete Cancel

localhost/WebD/users/delete.php?id=

Most Visited Getting Started

DELETE FROM users WHERE id = 4
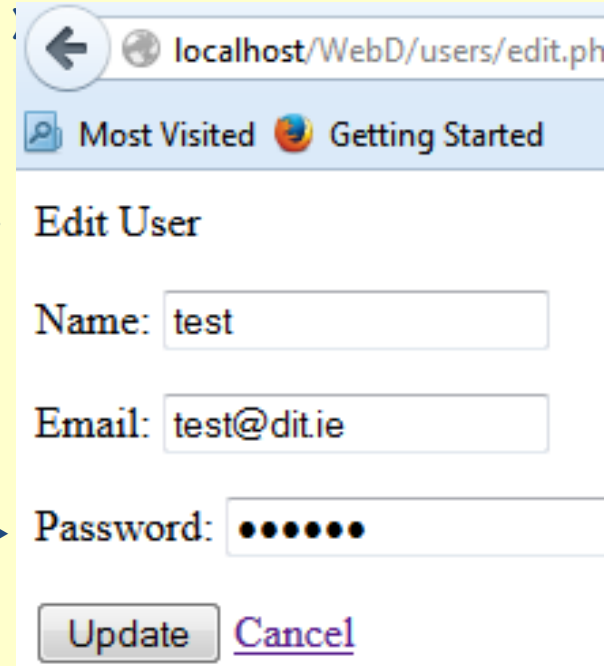
Success - Continue...

localhost/WebD/users/index.php

Most Visited Getting Started

Glenn	gg@gmail.com	456	Edit / Delete
Cindy	cindy.liu@gmail.com	pass	Edit / Delete
test	test	secret	Edit / Delete
Roberts	test	sneaky	Edit / Delete
Roberts', 'sneaky') --	correct	secret	Edit / Delete
Database	data@dit.ie	123	Edit / Delete

Add New

edit.php

```php
<?php
require_once "db.php";
if ( isset($_POST['name']) && isset($_POST['email'])
&& isset($_POST['password']) && isset($_POST['id'])
$n = mysqli_real_escape_string($_POST['name']);
$e = mysqli_real_escape_string($_POST['email']);
$p = mysqli_real_escape_string($_POST['password']);
$id = mysqli_real_escape_string($_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;
}
$id = mysqli_real_escape_string($_GET['id']);
$result = mysqli_query("SELECT name, email, password, id
FROM users WHERE id='$id'");
$row = mysql_fetch_row($result);
$n = htmlentities($row[0]);
$e = htmlentities($row[1]);
$p = htmlentities($row[2]);
$id = htmlentities($row[3]);
```

localhost/WebD/users/edit.ph
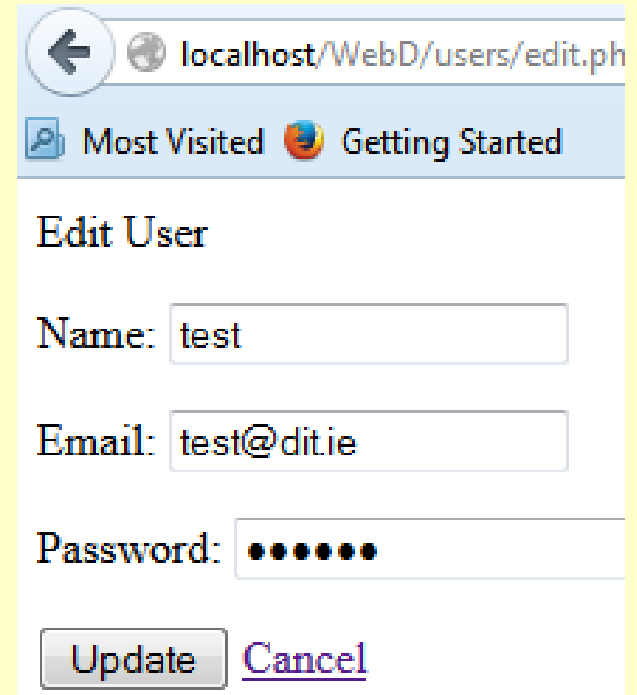
Most Visited Getting Started

Edit User

Name: test

Email: test@dit.ie

Password: ••••••

Update Cancel

edit.php

```php
$id = $_GET['id'];
$result = mysqli_query("SELECT name, email, password, id
FROM users WHERE id='$id'");
$row = mysqli_fetch_row($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
?>
```

Most Visited 🦊 Getting Started

Glenn	gg@gmail.com	456	Edit / Delete
Cindy	cindy.liu@gmail.com	pass	Edit / Delete
dt228	dt228@dit.ie	dt228	Edit / Delete
test	test	secret	Edit / Delete
Roberts	test	sneaky	Edit / Delete
Roberts', 'sneaky') --	correct	secret	Edit / Delete

Add New

Most Visited 🦊 Getting Started

Edit User

Name: test

Email: test@dit.ie

Password: ••••••

Update   Cancel

Most Visited 🦊 Getting Started

```
UPDATE users SET name='test', email='test@dit.ie',
password='secret' WHERE id='7'
```

Updated - Continue...

Most Visited 🦊 Getting Started

Glenn	gg@gmail.com	456	Edit / Delete
Cindy	cindy.liu@gmail.com	pass	Edit / Delete
test	test@dit.ie	secret	Edit / Delete
Roberts	test	sneaky	Edit / Delete
Roberts', 'sneaky') --	correct	secret	Edit / Delete
Database	data@dit.ie	123	Edit / Delete

Add New

Summary

- Making database connections

- Sanitizing HTML

- Inserting and Deleting

- Security: Sanitizing SQL

- A multi-file CRUD application