Forms and PHP

Forms Submit Data

```
<p>Guessing game...</p>                    FORM 1
<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

➢ There is another array called $_REQUEST which merges GET and

POST 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>
<pre>
$_GET:
<?php
print_r($_GET);
?>
</pre>
```
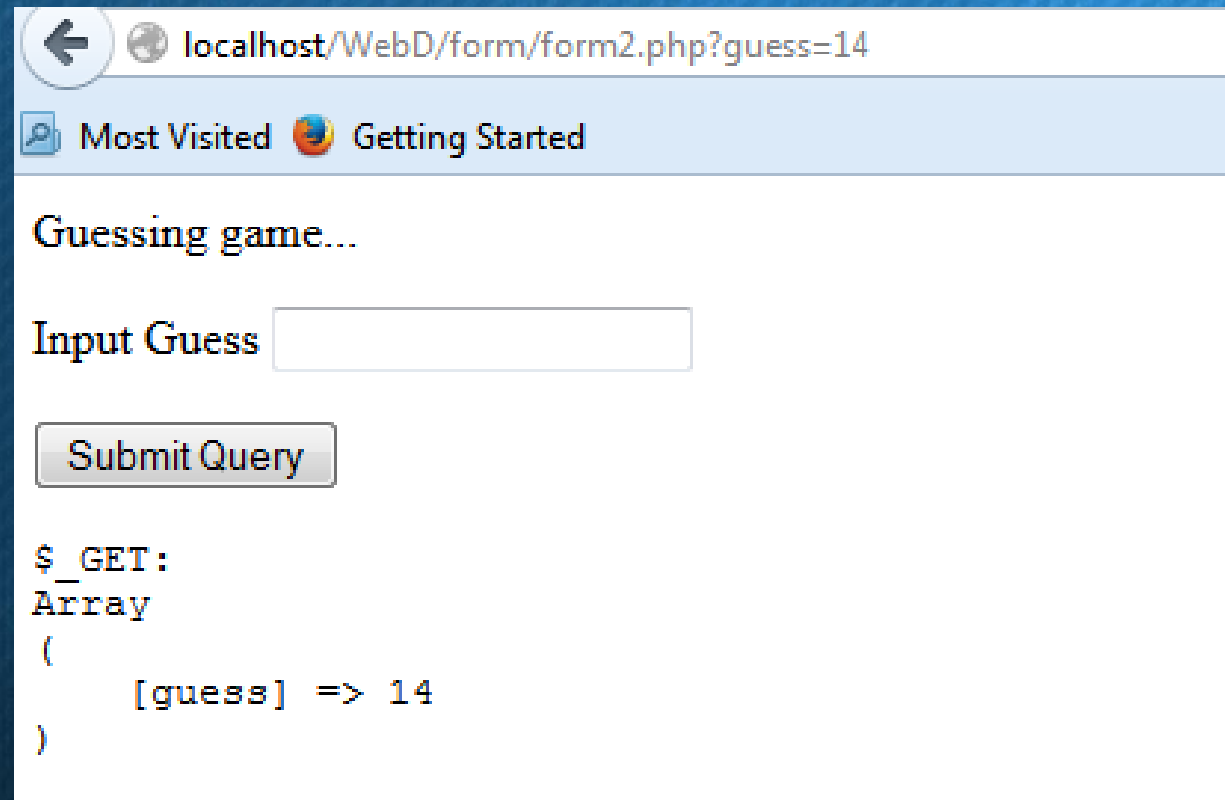
localhost/WebD/form/form2.php?guess=14

Most Visited Getting Started

Guessing game...

Input Guess [   ]

[Submit Query]

```
$_GET:
Array
(
    [guess] => 14
)
```

```html
<p>Guessing game...</p>
<form method="post">
<p><label for="guess">Input Guess</label>
<input type="text" name="guess" size="40" id="guess"/></p>
<input type="submit"/>
</form>
<pre>
$_POST:
<?php
print_r($_POST);
?>
$_GET:
<?php
print_r($_GET);
?>
</pre>
```


localhost/WebD/form/form3.php

Most Visited Getting Started

Guessing game...

Input Guess

Submit Query

```
$_POST:
Array
(
    [guess] => 42
)
$_GET:
Array
(
)
```
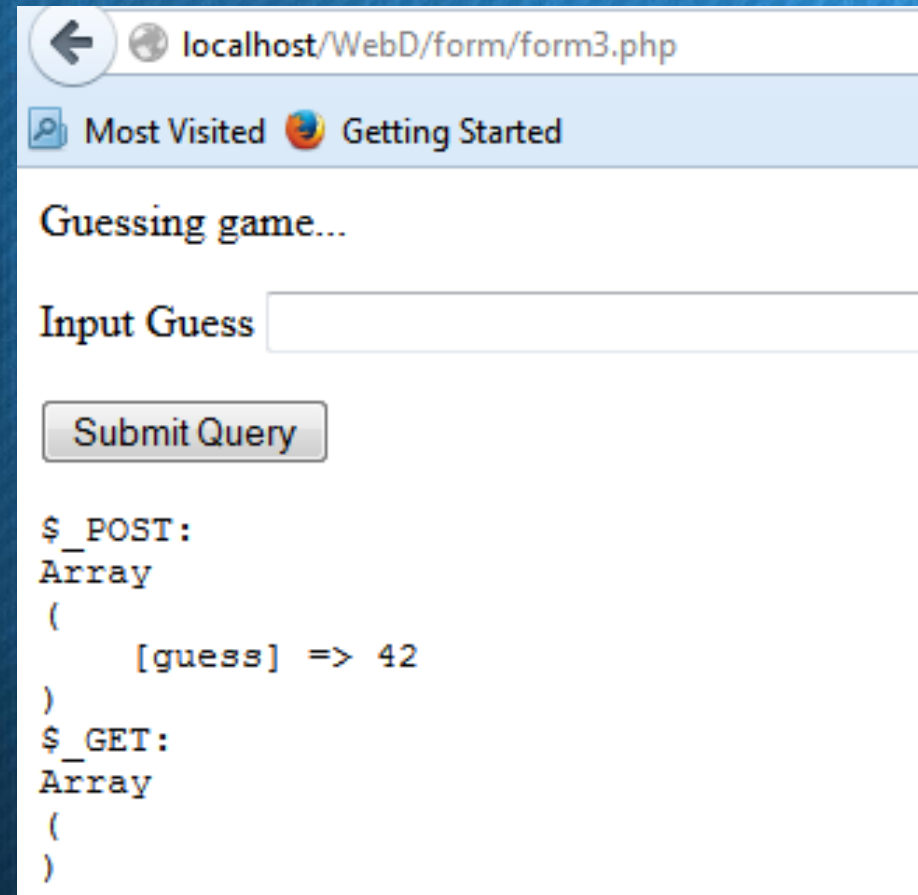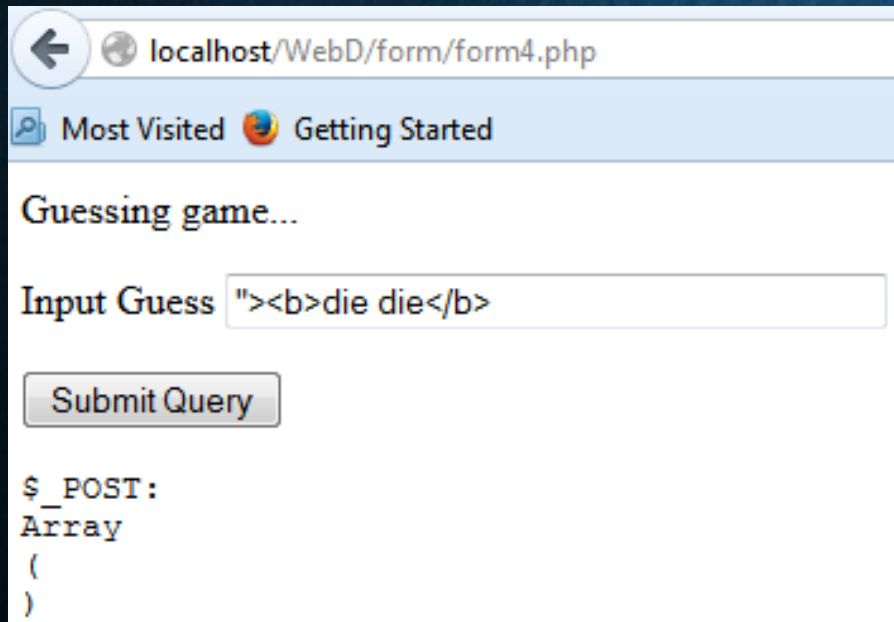
```php
<?php
$oldguess = isset($_POST['guess']) ?
$_POST['guess'] : '';
?>
<p>Guessing game...</p>
<form method="post">
<p><label for="guess">Input Guess</label>
<input type="text" name="guess" id="guess" size="40"
<?php
echo 'value="' .$oldguess. '"';
?>
/></p>
<input type="submit"/>
</form>
```

Hygiene Alert!

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

```
<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>
```

localhost/WebD/form/form4.php
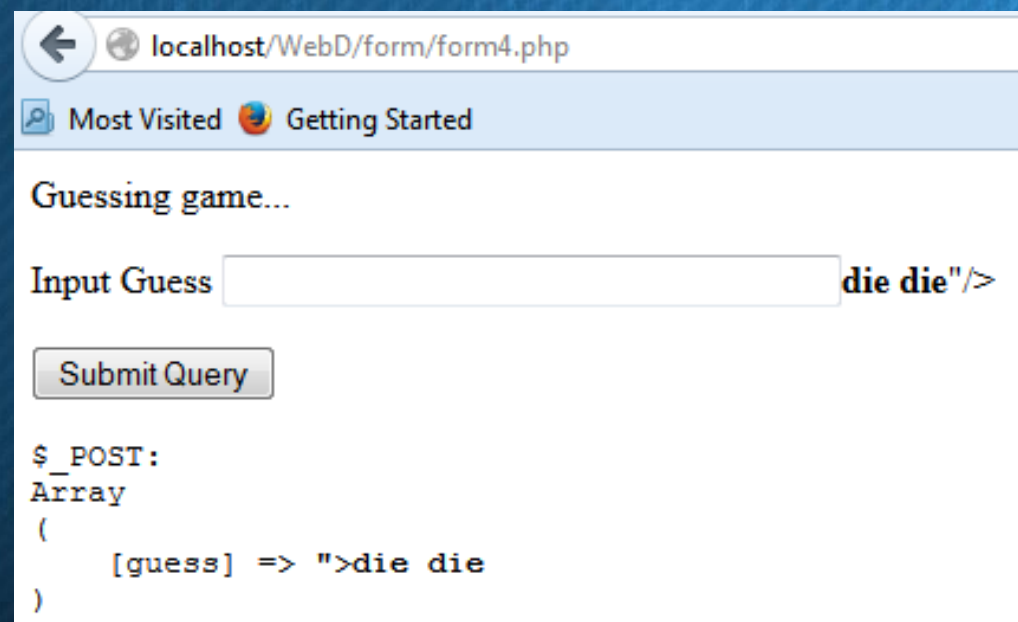
Most Visited   Getting Started
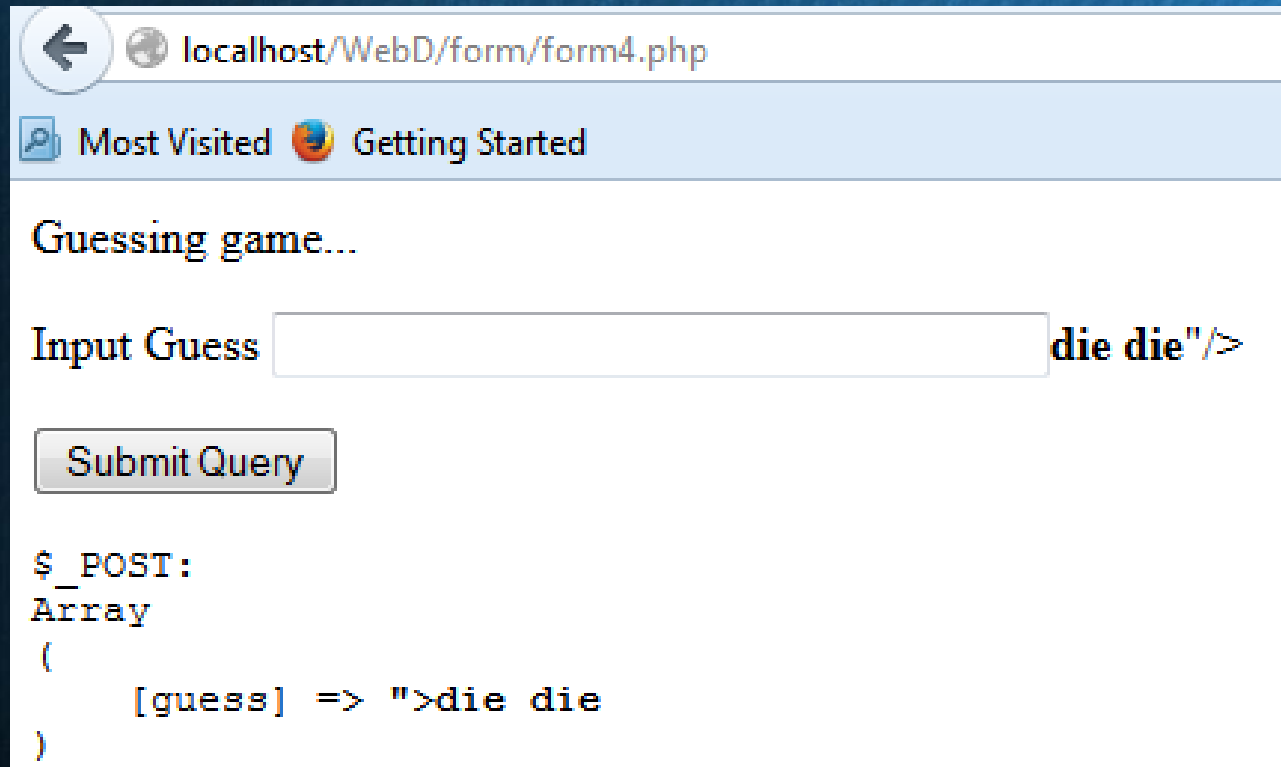
Guessing game...

Input Guess [   ] die die"/>

[Submit Query]

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

To The Rescue: htmlentities()

```
<form method="post">                FORM5
<p><label for="guess">Input Guess</label>
<input type="text" name="guess" id="guess" size="40"
<?php
echo 'value="'.htmlentities($oldguess).'"';
?>
/></p>
<input type="submit"/>
</form>
```

```
<form method="post">                    FORM4
<p><label for="guess">Input Guess</label>
<input type="text" name="guess" id="guess" size="40"
<?php
echo 'value="'.htmlentities($oldguess).'"';
?>
/></p>
<input type="submit"/>
</form>
```

localhost/WebD/form/form5.php

Most Visited 🌐 Getting Started

Guessing game...

Input Guess ">DIE DIE

Submit Q

```
<input type="text" name="guess" id="guess" size="40"
value="&quot;&gt;&lt;b&gt;DIE DIE&lt;/b&gt;"/></p>
$_POST:
Array
(
    [guess] => ">DIE DIE
)
```
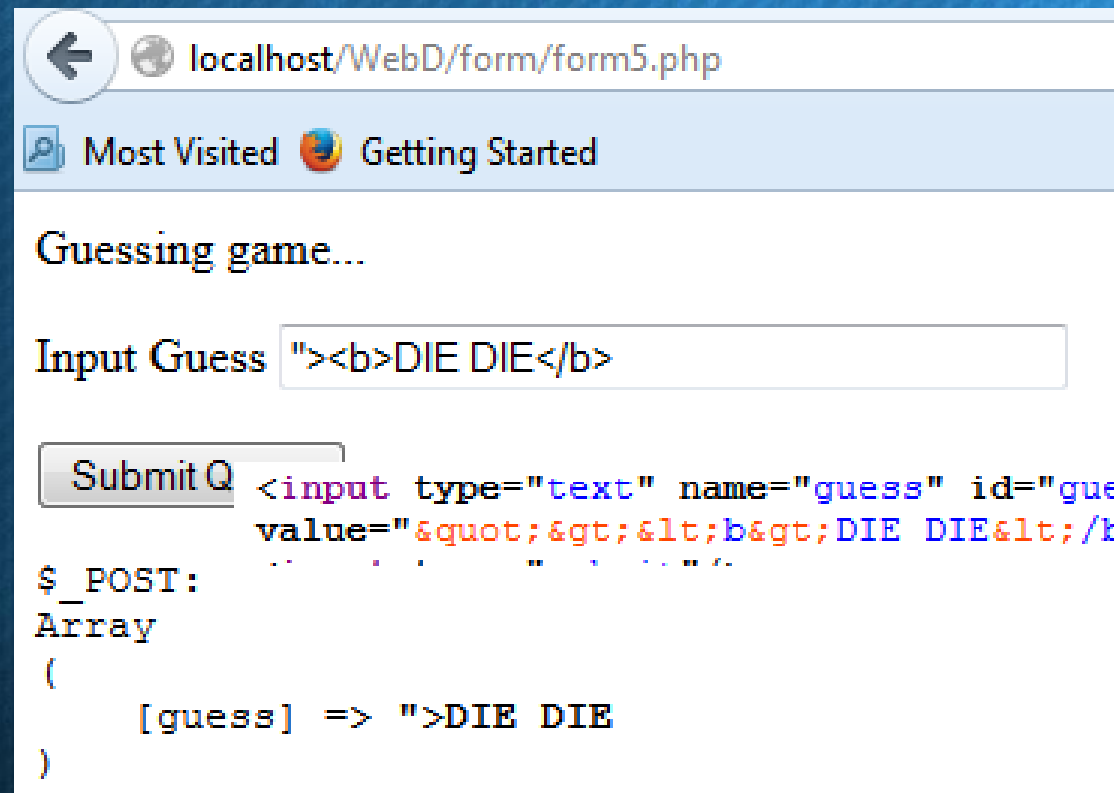
The $_POST Variable

- There are many patterns for handling POST data

- No "rules" just "suggestions"

```php
<?php
$guess = '';
$message = false;
if ( isset($_POST['guess']) ) {
// Trick for integer / numeric parameters
$guess = $_POST['guess'] + 0;
if ( $guess == 42 ) {
$message = "Great job!";
} else if ( $guess < 42 ) {
$message = "Too low";
} else {
$message = "Too high...";
}
}
?>

<html>
<head>
<title>A Guessing game</title>
</head>
<body style="font-family: sans-serif;">
<p>Guessing game...</p>
<?php
if ( $message !== false ) {
echo("<p>$message</p>\n");
}
?>
<form method="post">
<p><label for="guess">Input Guess</label>
<input type="text" name="guess" id="guess" size="40"
<?php
echo 'value="' . htmlentities($guess) . '"';
?>
/></p>
<input type="submit"/>
</form>
</body>
```

Completely process incoming POST data (if any) - produce no output.

Produce the page output.

```php
<?php
$guess = '';
$message = false;
if ( isset($_POST['guess']) ) {
// Trick for integer / numeric parameters
$guess = $_POST['guess'] + 0;
if ( $guess == 42 ) {
$message = "Great job!";
} else if ( $guess < 42 ) {
$message = "Too low";
} else {
$message = "Too high...";
}
}
?>
```

```html
<html>
<head>
<title>A Guessing game</title>
</head>
<body style="font-family: sans-serif;">
<p>Guessing game...</p>
<?php
if ( $message !== false ) {
echo("<p>$message</p>\n");
}
?>
<form method="post">
<p><label for="guess">Input Guess</label>
<input type="text" name="guess" id="guess"
size="40"
<?php
echo 'value="' . htmlentities($guess) . '"
?>
/></p>
<input type="submit"/>
</form>
</body>
```

guess.php

```php
<?php
$guess = '';
$message = false;
if ( isset($_POST['guess']) ) {
// Trick for integer / numeric parameters
$guess = $_POST['guess'] + 0;
if ( $guess == 42 ) {
$message = "Great job!";
} else if ( $guess < 42 ) {
$message = "Too low";
} else {
$message = "Too high...";
}
}
?>

<html>
<head>
<title>A Guessing game</title>
</head>
<body style="font-family: sans-serif;">
<p>Guessing game...</p>
<?php
if ( $message !== false ) {
echo("<p>$message</p>\n");
}
?>
<form method="post">
<p><label for="guess">Input Guess</label>
<input type="text" name="guess" id="guess" size="40"
<?php
echo 'value="' . htmlentities($guess) . '"';
?>
/></p>
<input type="submit"/>
</form>
</body>
```

```php
<?php
$guess = '';
$message = false;
if ( isset($_POST['guess']) ) {
// Trick for integer / numeric
parameters
$guess = $_POST['guess'] + 0;
if ( $guess == 42 ) {
$message = "Great job!";
} else if ( $guess < 42 ) {
$message = "Too low";
} else {
$message = "Too high...";
}
}
?>
<html>
......
```

```php
<?php
$guess = '';
$message = false;
if ( isset($_POST['guess']) ) {
// Trick for integer / numeric parameters
$guess = $_POST['guess'] + 0;
if ( $guess == 42 ) {
$message = "Great job!";
} else if ( $guess < 42 ) {
$message = "Too low";
} else {
$message = "Too high...";
}
}
?>

<html>
<head>
<title>A Guessing game</title>
</head>
<body style="font-family: sans-serif;">
<p>Guessing game...</p>
<?php
if ( $message !== false ) {
echo("<p>$message</p>\n");
}
?>
<form method="post">
<p><label for="guess">Input Guess</label>
<input type="text" name="guess" id="guess" size="40"
<?php
echo 'value="' . htmlentities($guess) . '"';
?>
/></p>
<input type="submit"/>
</form>
</body>
```

```
...?>
<html>
<head>
<title>A Guessing game</title>
</head>
<body style="font-family: sans-serif;">
<p>Guessing game...</p>
<?php
if ( $message !== false ) {
echo("<p>$message</p>\n");
}
?>
<form method="post">
<p><label for="guess">Input Guess</label>
<input type="text" name="guess" id="guess"
size="40"
<?php
echo 'value="' . htmlentities($guess) .
'"';
?>
/></p>
<input type="submit"/>
</form>
</body>
```

```php
<?php
$guess = '';
$message = false;
if ( isset($_POST['guess']) ) {
// Trick for integer / numeric parameters
$guess = $_POST['guess'] + 0;
if ( $guess == 42 ) {
$message = "Great job!";
} else if ( $guess < 42 ) {
$message = "Too low";
} else {
$message = "Too high...";
}
}
?>
<html>
......
```


Guessing game...

Too high...

Input Guess 101

Submit Query

localhost/WebD/form/guess.php

Most Visited 🦊 Getting Started

```php
...?>
<html>
<head>
<title>A Guessing game</title>
</head>
<body style="font-family: sans-serif;">
<p>Guessing game...</p>
<?php
if ( $message !== false ) {
echo("<p>$message</p>\n");
}
?>
<form method="post">
<p><label for="guess">Input Guess</label>
<input type="text" name="guess" id="guess"
size="40"
<?php
echo 'value="' . htmlentities($guess) .
'"';
?>
/></p>
<input type="submit"/>
</form>
</body>
```
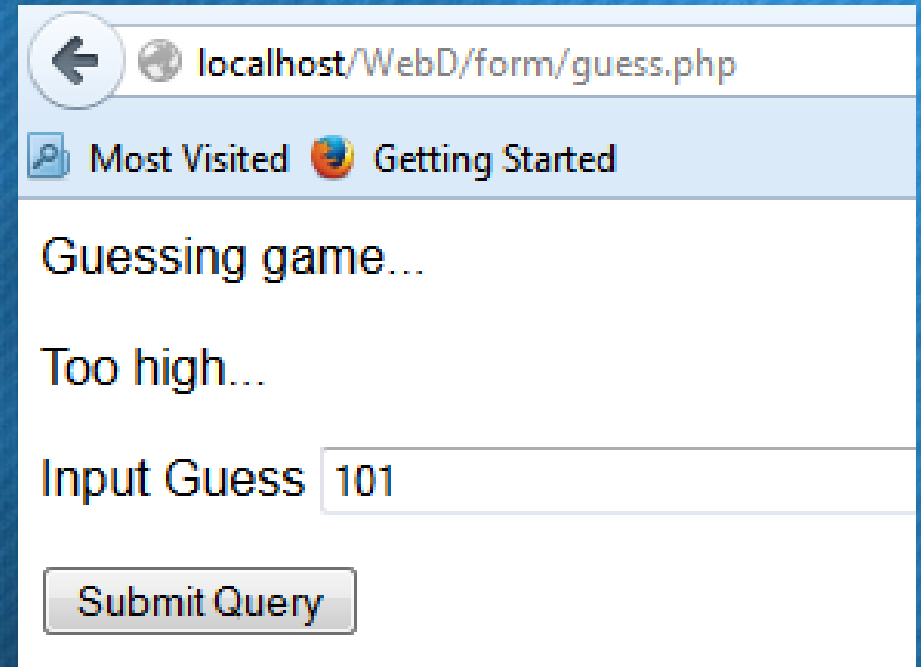
Guessing game...

Too low

Input Guess 41

Submit Query

localhost/WebD/form/guess.php

Most Visited   Getting Started

guess.php

Other Input Type

➢Text

➢Password

➢Radio Button

➢Check Box

➢Select / Drop-Down

➢TextArea

Many field types...

Account: [   ]

Password: [   ]

Nick Name: [   ]

Preferred Time:
○ AM
● PM

Classes taken:
☑ CMPU2022 - Web Development2
☐ CMPU2007 - Database1
☐ CMPU2012 - Mathematics

Which drink: [-- Please Select -- ▼]

Which snack: [-- Please Select -- ▼]

Tell us about yourself:
```
I love building web sites in PHP and
MySQL.
```

Which are awesome?
```
Python
CSS
HTML
PHP
```

[Submit] [Escape]

```
<p><label for="inp01">Account:</label>
<input type="text" name="account" id="inp01" size="40" ></p>
<p><label for="inp02">Password:</label>
<input type="password" name="pw" id="inp02" size="40" ></p>
<p><label for="inp03">Nick Name:</label>
<input type="text" name="nick" id="inp03" size="40" ></p>
```

Many field types...

Account: Xiaoling

Password: •••••

Nick Name: Cindy

```
$_POST:
Array
(
[account] => Xiaoling
[pw] => 12345
[nick] => Cindy
[when] => pm
...
)
```

moreform.php

```
<p>Preferred Time:<br/>
<input type="radio" name="when" value="am">AM<br>
<input type="radio" name="when" value="pm" checked>PM</p>
```

Preferred Time:
○ AM
◉ PM

```
$_POST:
Array
(
…
[nick] => Cindy
[when] => pm
[class] => CMPU2022

...
)
```

moreform.php

```
<p>Classes taken:<br/>
<input type="checkbox" name="class" value="CMPU2022" checked>
CMPU2022 - Web Development2<br>
<input type="checkbox" name="class" value="CMPU2007">
CMPU2007 - Database1<br>
<input type="checkbox" name="class" value="CMPU2012">
CMPU2012 - Mathematics<br></p>
```

Classes taken:
☑ CMPU2022 - Web Development2
☐ CMPU2007 - Database1
☐ CMPU2012 - Mathematics

```
$_POST:
Array
(
…
[when] => pm
[class] => CMPU2022
[drink] => 0

...
)
```

moreform.php

```
<p><label for="inp06">Which drink:
<select name="drink" id="inp06">
<option value="0">-- Please Select --</option>
<option value="1">Coke</option>
<option value="2">Pepsi</option>
<option value="3">Mountain Dew</option>
<option value="4">Orange Juice</option>
<option value="5">Lemonade</option>
</select>
</p>
```
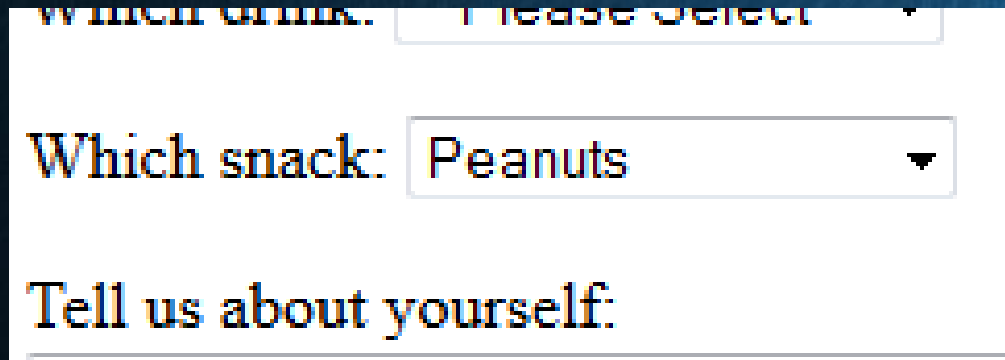
Which drink: -- Please Select -- ▼

```
$_POST:
Array
(
…
[class] => CMPU2022
[drink] => 0
[snack] => peanuts

...
)
```

```
<p><label for="inp07">Which snack:
<select name="snack" id="inp07">
<option value="">-- Please Select --</option>
<option value="crisps">Crisps</option>
<option value="peanuts" selected>Peanuts</option>
<option value="cookie">Cookie</option>
</select></p>
```

Which snack: Peanuts

Tell us about yourself:

```
$_POST:
Array
(
…
[drink] => 0
[snack] => peanuts
...
)
```

moreform.php

```
<p><label for="inp08">Tell us about yourself:<br/>
<textarea rows="5" cols="40" id="inp08" name="about">
I love building web sites in PHP and MySQL.
</textarea></p>
```
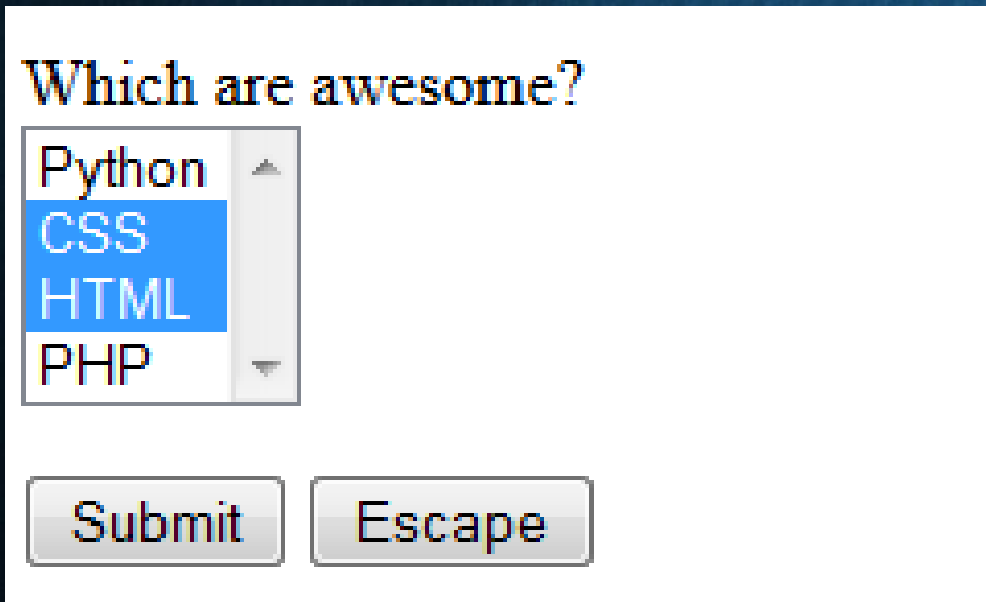
Tell us about yourself:

I love building web sites in PHP and
MySQL.

$_POST:
Array
(
…
[about] => I love
building web sites in
PHP and MySQL.
...
)

```
<p><label for="inp09">Which are awesome?<br/>
<select multiple="multiple" name="code[]" id="inp09">
<option value="python">Python</option>
<option value="css">CSS</option>
<option value="html">HTML</option>
<option value="php">PHP</option>
</select>
```



```
$_POST:
Array
(
…
[code] => Array
        (0) => css
        (1) => html
)
[dopost] => Submit
...
)
```

moreform.php

```
<p>
<input type="submit" name="dopost" value="Submit"/>
<input type="button" onclick="location.href='http://www.php-intro.com/';
return false;"value="Escape">
</p>
```



```
$_POST:
Array
(
…
[dopost] => Submit
...
)
```

moreform.php

HTML5 Input Types

- HTML5 defines new input types

- Not all browsers support all input types

- The fall back to type="text"

- http://www.w3schools.com/html/html5_form_input_types.asp

Summary

➢ Forms, $_GET and $_POST

➢ Sanitizing HTML

➢ Form fields

➢ New form fields in HTML5

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

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

Name
- add.php
- db.php
- delete.php
- edit.php
- index.php
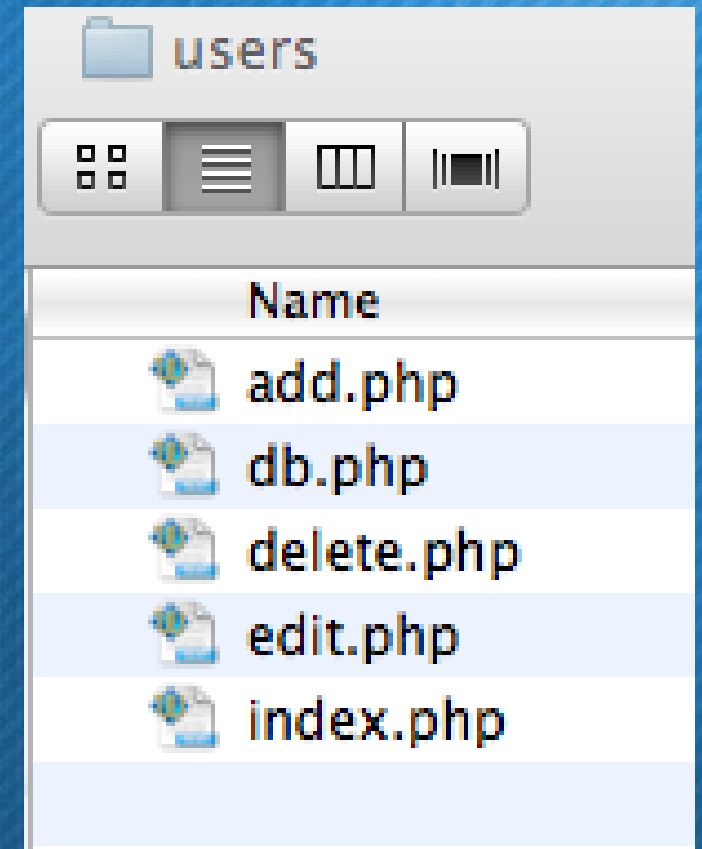
index.php

```php
<?php
require_once "database.php";
$sql = "SELECT UserID, Username, Password, email FROM user";
$result = $conn->query($sql);
if ($result->num_rows > 0) {
    // output data of each row in a table
echo "<table border='1'>";
while($row = $result->fetch_assoc()) {
echo "<tr><td>";
echo(htmlentities($row["Username"]));
echo("</td><td>");
echo(htmlentities($row["Password"]));
echo("</td><td>");
echo(htmlentities($row["email"]));
echo("</td><td>\n");
echo('<a href="edit.php?id='.htmlentities($row["UserID"]).'">Edit</a> / ');
echo('<a href="delete.php?id='.htmlentities($row["UserID"]).'">Delete</a>');
echo("</td></tr>\n");
} }else {
    echo "0 results";
}
$conn->close();
?>
</table>
<a href="add.php">Add New</a>
```

add.php

```php
<?php
require_once "database.php";
if ( isset($_POST['name']) && isset($_POST['email'])
&& isset($_POST['password'])) {
$n = $conn -> real_escape_string($_POST['name']);
$e = $conn -> real_escape_string($_POST['email']);
$p = $conn -> real_escape_string($_POST['password']);
$sql = "INSERT INTO user (Username, Password, email)
VALUES ('$n', '$p', '$e')";
echo "<pre>\n$sql\n</pre>\n";
$conn->query($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>
```

localhost/WebD/users/add.php

Add A New User

Name: Xiaoling Liu

Email: cindy.liu@tudublin.ie

Password: •••••

Add New   Cancel

add.php

```php
<?php
require_once "database.php";
if ( isset($_POST['name']) && isset($_POST['email'])
&& isset($_POST['password'])) {
$n = $conn -> real_escape_string($_POST['name']);
$e = $conn -> real_escape_string($_POST['email']);
$p = $conn -> real_escape_string($_POST['password']);
$sql = "INSERT INTO user (Username, Password, email)
VALUES ('$n', '$p', '$e')";
echo "<pre>\n$sql\n</pre>\n";
$conn->query($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>
```

localhost/WebD/users/add.php

```
INSERT INTO user (Username, Password, email)
VALUES ('php', 'php', 'php@tudublin.ie')
```

Success - Continue...

localhost/WebD/users/index.php

Cindy	letmein	cindy.liu@tudublin.ie	Edit	Delete
somethingelse	pass	s@s.ie	Edit	Delete
Jade	jade	jade@gmail.com	Edit	Delete
test	test	test@test.ie	Edit	Delete
test	test	test@test.ie	Edit	Delete
dt211	dt211	dt211@tudublin.ie	Edit	Delete
Xiaoling Liu	cindy	cindy.liu@tudublin.ie	Edit	Delete
php	php	php@tudublin.ie	Edit	Delete

Add New

delete.php

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

localhost/WebD/users/index.php

Cindy	letmein	cindy.liu@tudublin.ie	Edit / Delete
somethingelse	pass	s@s.ie	Edit / Delete
Jade	jade	jade@gmail.com	Edit / Delete
test	test	test@test.ie	Edit / Delete
test	test	test@test.ie	Edit / Delete
dt211	dt211	dt211@tudublin.ie	Edit / Delete
Xiaoling Liu	cindy	cindy.liu@tudublin.ie	Edit / Delete
php	php	php@tudublin.ie	Edit / Delete

Add New

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

Confirm: Deleting test

Delete Cancel

delete.php


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

edit.php

```php
<?php
require_once "database.php";
if ( isset($_POST['name']) && isset($_POST['email'])
&& isset($_POST['password']) && isset($_POST['id']) ) {
$n = $conn -> real_escape_string($_POST['name']);
$e = $conn -> real_escape_string($_POST['email']);
$p = $conn -> real_escape_string($_POST['password']);
$id = $conn -> real_escape_string($_POST['id']);
$sql = "UPDATE user SET Username='$n', email='$e',
Password='$p' WHERE UserID='$id'";
echo "<pre>\n$sql\n</pre>\n";
$conn->query($sql);
echo 'Updated - <a href="index.php">Continue...</a>';
return;
}
$id = $conn -> real_escape_string($_GET['id']);
$sql = "SELECT Username,Password, email, UserID FROM user WHERE UserID='$id'";
$result = $conn->query($sql);
$row = $result->fetch_assoc();
$n = htmlentities($row["Username"]);
$e = htmlentities($row["email"]);
$p = htmlentities($row["Password"]);
$id = htmlentities($row["UserID"]);
```

edit.php

```php
18  $result = $conn->query($sql);
19  $row = $result->fetch_assoc();
20  $n = htmlentities($row["Username"]);
21  $e = htmlentities($row["email"]);
22  $p = htmlentities($row["Password"]);
23  $id = htmlentities($row["UserID"]);
24
25  echo <<< _END
26  <p>Edit User</p>
27  <form method="post">
28  <p>Name:
29  <input type="text" name="name" value="$n"></p>
30  <p>Email:
31  <input type="text" name="email" value="$e"></p>
32  <p>Password:
33  <input type="password" name="password" value="$p"></p>
34  <input type="hidden" name="id" value="$id">
35  <p><input type="submit" value="Update"/>
36  <a href="index.php">Cancel</a></p>
37  </form>
38  _END
39  ?>
```

edit.php

Edit User

Name: php

Email: php@tudublin.ie

Password: ••••••

Update   Cancel

localhost/WebD/users/index.php

Cindy	letmein	cindy.liu@tudublin.ie	Edit / Delete
somethingelse	pass	s@s.ie	Edit / Delete
Jade	jade	jade@gmail.com	Edit / Delete
test	test	test@test.ie	Edit / Delete
dt211	dt211	dt211@tudublin.ie	Edit / Delete
Xiaoling Liu	cindy	cindy.liu@tudublin.ie	Edit / Delete
php	phpphp	php@tudublin.ie	Edit / Delete

Add New

localhost/WebD/users/edit.php?id=11

UPDATE user SET Username='php', email='php@tudublin.ie', Password='phpphp' WHERE UserID='11'

Updated - Continue...

Summery

➤ Making database connections

➤ Sanitizing HTML

➤ Inserting and Deleting

➤ Security: Sanitizing SQL

➤ A multi-file CRUD application