Advanced Web Technologies

Iosif Polenakis

PhD Candidate,
Department of Computer Science and Engineering,
University of Ioannina.

email: ipolenak@cs.uoi.gr, tel.: 2651008831

PHP Basics

- **PHP**: **P**HP **H**ypertext **P**reprocessor

PHP Basics

- **PHP**: **P**HP **H**ypertext **P**reprocessor
  - ✓ Used for Dynamic Modification of the content of a web page (dynamic web pages).

PHP Basics

- **PHP**: **P**HP **H**ypertext **P**reprocessor
  - ✓ Used for Dynamic Modification of the content of a web page (dynamic web pages).
  - ✓ Manipulation of data from HTML forms

PHP Basics

- **PHP**: **P**HP **H**ypertext **P**reprocessor
  - ✓ Used for Dynamic Modification of the content of a web page (dynamic web pages).
  - ✓ Manipulation of data from HTML forms
  - ✓ Accessing DataBases

PHP Basics

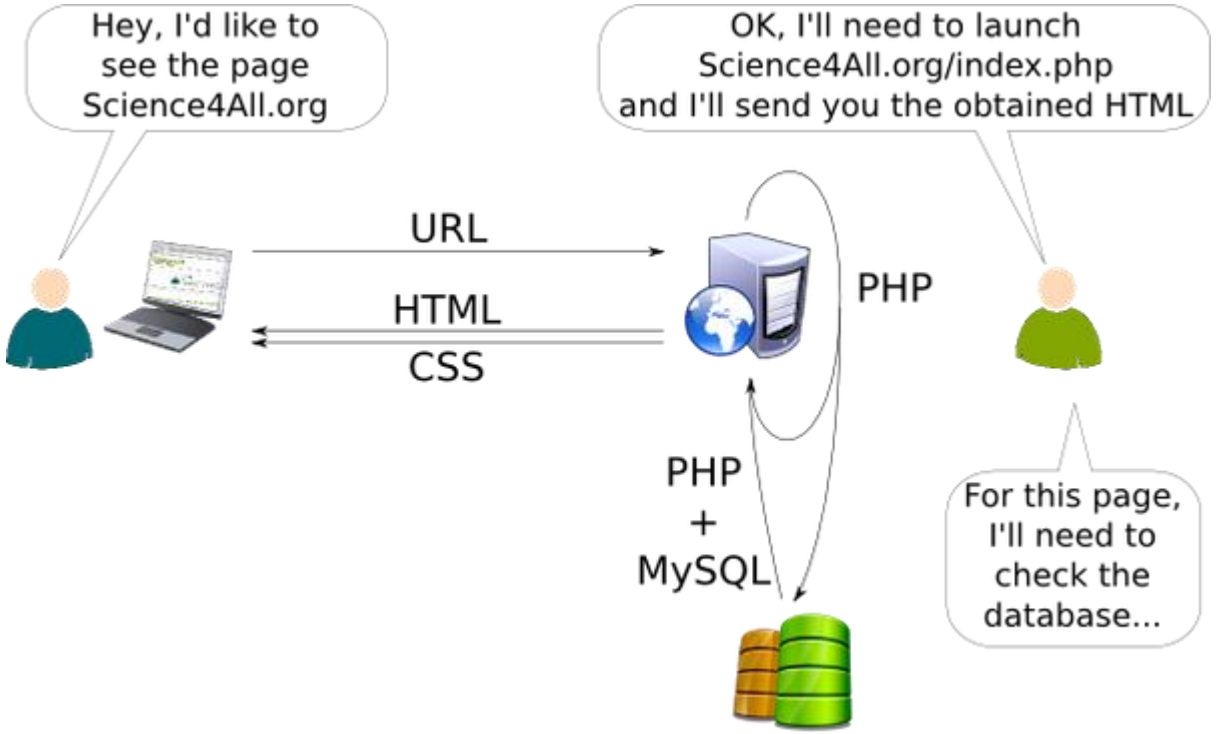
- **PHP**: **P**HP **H**ypertext **P**reprocessor
  - ✓ Used for Dynamic Modification of the content of a web page (dynamic web pages).
  - ✓ Manipulation of data from HTML forms
  - ✓ Accessing DataBases
  - ✓ Server-Side Scripting (non-visible source code)

PHP Basics

- **PHP**: **P**HP **H**ypertext **P**reprocessor
  - ✓ Used for Dynamic Modification of the content of a web page (dynamic web pages).
  - ✓ Manipulation of data from HTML forms
  - ✓ Accessing DataBases
  - ✓ Server-Side Scripting (non-visible source code)
  - ✓ Results can be rendered to browser through HTML

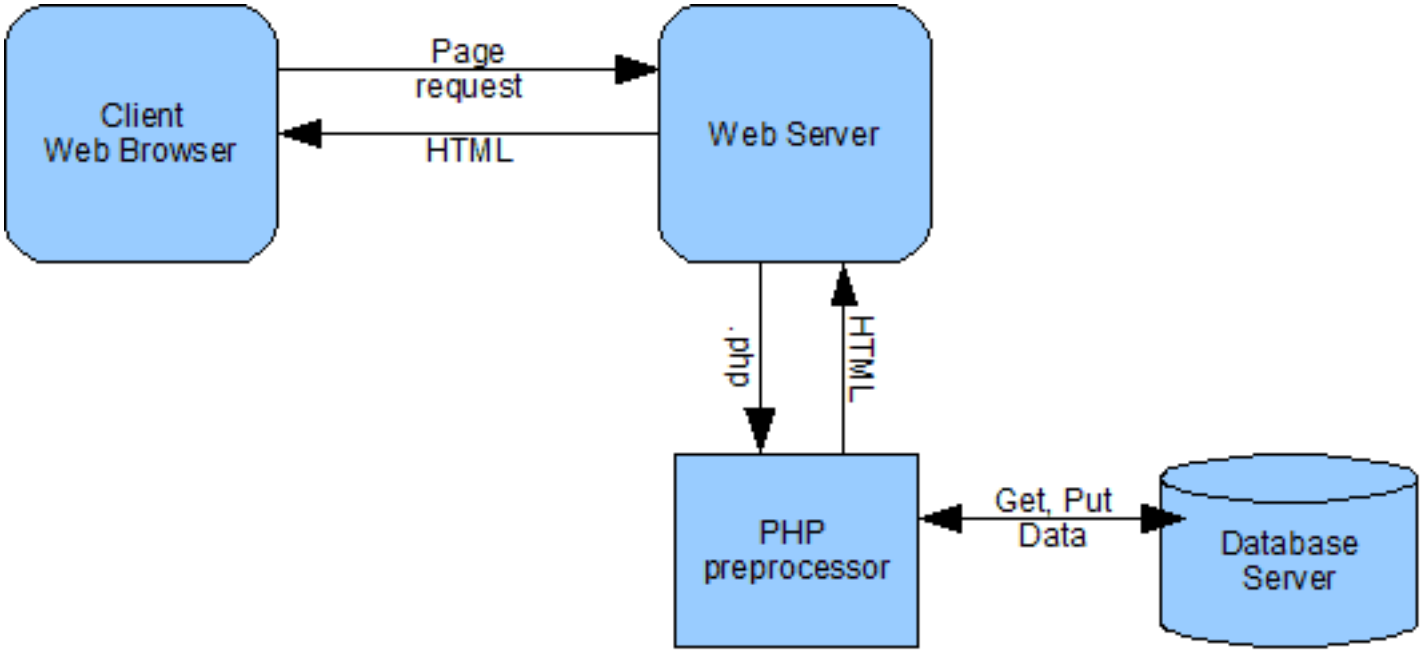
PHP Basics

- **PHP**: **P**HP **H**ypertext **P**reprocessor



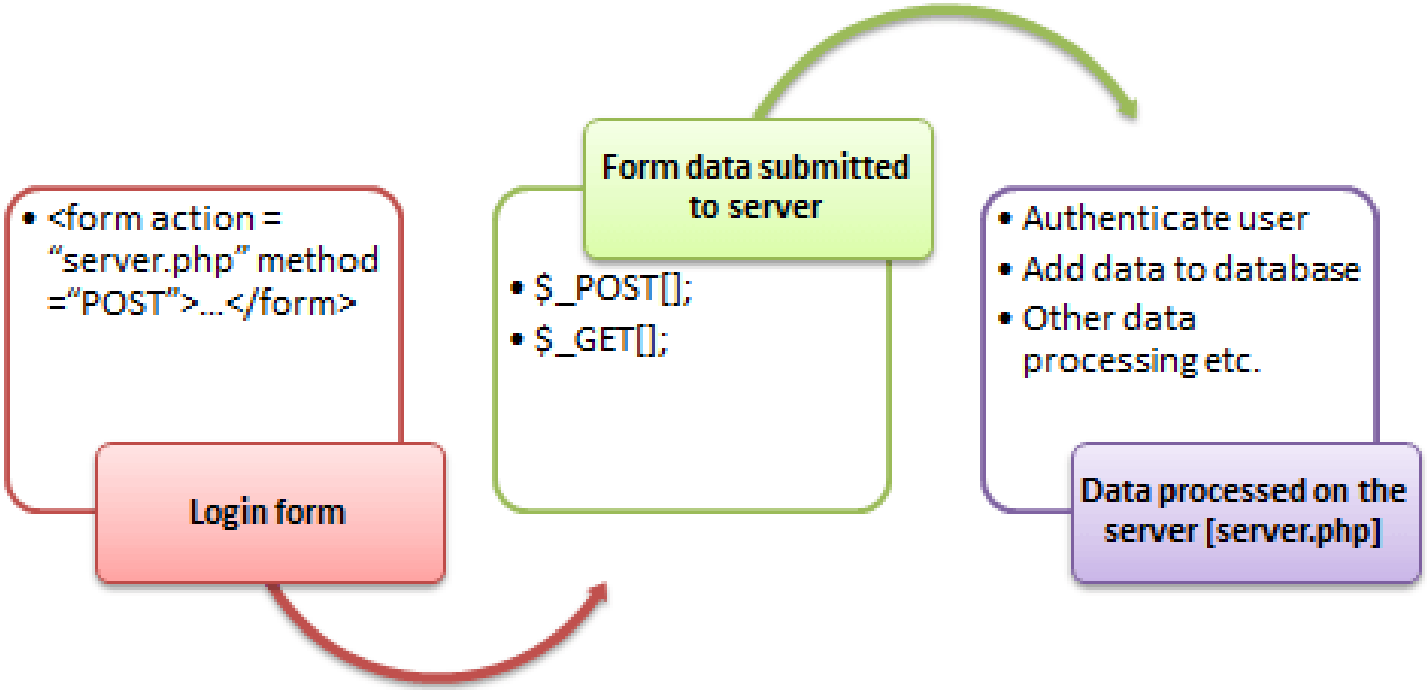
PHP Basics

- **PHP**: **P**HP **H**ypertext **P**reprocessor



PHP Basics

- **PHP**: **P**HP **H**ypertext **P**reprocessor



PHP Basics

- **PHP**: Programming Basics
  - ✓ **<?php** …place your code here… **?>**
  - ✓ Type declaration before using a variable is not prerequisite:

```
$my_num=3.14;
$my_alphanumeric="str123str"; etc...
```

  - ✓ Variables can be displayed through "echo":

```
echo "number: " .$my_num;
echo "string: " .$my_alphanumeric;
```

PHP Basics

- **PHP**: Programming Basics
  - ✓ `<?php …place your code here… ?>`
  - ✓ Every statement ends with semicolon:
    - `$a = 5;`
    - `$a = function();`
    - `$a = ($b = 5);`
    - `$a++; ++$a;`
    - `$a += 3;`

PHP Basics

- **PHP**: Programming Basics
  - ✓ **<?php** …place your code here… **?>**
  - ✓ Operators:
    - Arithmethic: +,-, * ,%
    - Setting variable: =
    - Bit: &, |, ^ , ~ , <>
    - Comparison: == , === , != , !== , <= , >=

PHP Basics

- **PHP**: Programming Basics
  - ✓ **<?php** …place your code here… **?>**
  - ✓ Control Sequence Statements:

```
<?php
  if ($a > $b){
      echo "a is bigger than b";
  }
  elseif($a == $b){
      echo "a is equal to b";
  }
  else{
      echo "a is smaller than b";
  }
?>
```

PHP Basics

- **PHP**: Programming Basics
  - ✓ **<?php** …place your code here… **?>**
  - ✓ Iteration Sequence Statements:

```
<?php
    //-------------- while loop -------------------
    $a=0;
    while($a<10){print $a; $a++;}




 ?>
```

PHP Basics

- **PHP**: Programming Basics
  - ✓ **<?php** …place your code here… **?>**
  - ✓ Iteration Sequence Statements:

```
<?php
    //-------------- while loop ------------------
    $a=0;
    while($a<10){print $a; $a++;}
    //-------------- do while loop ---------------
    $i = 0;
    do {print $i;} while ($i > 0);



 ?>
```

PHP Basics

- **PHP**: Programming Basics
  - ✓ **<?php** …place your code here… **?>**
  - ✓ Iteration Sequence Statements:

```
<?php
    //-------------- while loop ------------------
    $a=0;
    while($a<10){print $a; $a++;}
    //-------------- do while loop ---------------
    $i = 0;
    do {print $i;} while ($i > 0);
    //---------------- for loop ------------------
    for($i = 1; $i <= 10; $i++){print $i;}


 ?>
```

PHP Basics

- **PHP**: Programming Basics
  - ✓ **<?php** …place your code here… **?>**
  - ✓ Iteration Sequence Statements:

```
<?php
    //-------------- while loop ------------------
    $a=0;
    while($a<10){print $a; $a++;}
    //-------------- do while loop ---------------
    $i = 0;
    do {print $i;} while ($i > 0);
    //---------------- for loop ------------------
    for($i = 1; $i <= 10; $i++){print $i;}
    //-------------- foreach loop ----------------
    $arr = array(1, 2, 3, 4);
    foreach($arr as $value){echo $value;}
 ?>
```

PHP Basics

- **PHP**: Programming Basics
  - ✓ **<?php** …place your code here… **?>**
  - ✓ Iteration Sequence Statements:

```
<?php
    //-------------- while loop ------------------
    $a=0;
    while($a<10){print $a; $a++;}
    //-------------- do while loop ---------------
    $i = 0;
    do {print $i;} while ($i > 0);
    //---------------- for loop ------------------
    for($i = 1; $i <= 10; $i++){print $i;}
    //-------------- foreach loop ----------------
    $arr = array(1, 2, 3, 4);
    foreach($arr as $value){echo $value;}
 ?>
```

PHP Basics

- **PHP**: Programming Basics
  - ✓ **<?php** …place your code here… **?>**
  - ✓ Functions:

```
<?php
  $name="joe";
  $target="prof";
  $str= "what Joe wanna be? <br>".strcnt($name,$target);

 function strcnt($x,$y){
          print "-->".$x."wanna be a".$y."<br>";
 }
?>
```

PHP Basics

- **PHP**: Programming Basics
  - ✓ **<?php** …place your code here… **?>**

Communication with forms:

index.html

```
<html>
<head></head>
<body>
<form action="form_receiver.php" method="get">

        Name: <input type="text" name="name" />

        Surname: <input type="text" name="surname" />

        <input type="submit" value="say hello"/>

</form>
</body>
</html>
```

PHP Basics

- **PHP**: Programming Basics
  - ✓ **<?php** …place your code here… **?>**

Communication with forms:

form_receiver.php

```
<?php
  $name_from_form=$_GET['name'];
  $surname_from_form=$_GET['surname'];
  echo "Nice to meet you Mr ".$name_from_form."-".$surname_from_form;
 ?>
```

PHP Basics

- **PHP**: Programming Basics
  - ✓ **<?php** …place your code here… **?>**

Data Sanitization

Example: stripslashes ()

```
$str = "Is your name O\'reilly?";

// Outputs: Is your name O'reilly?

echo stripslashes($str);
```

http://php.net/manual/en/function.stripslashes.php

PHP Basics

- **PHP**: Programming Basics
  - ✓ **<?php** …place your code here… **?>**

Data Sanitization

Example: addslashes()

```
$str = "O'Reilly?";

eval("echo '" . addslashes($str) . "';");
```

http://php.net/manual/en/function.addslashes.php

PHP Basics

- **PHP**: Programming Basics
  - ✓ **<?php** …place your code here… **?>**

Data Sanitization

Example: get_magic_quotes_gpc()

```
if (get_magic_quotes_gpc()) {
    $data = stripslashes($_POST['data']);

}

else {

      $data = $_POST['data'];

}
```

http://php.net/manual/en/function.get-magic-quotes-gpc.php

PHP Basics

- **PHP**: Cookies…
  - ✓ An HTTP cookie (also called web cookie, Internet cookie, browser cookie, or simply cookie) is a small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing.
  - ✓ Cookies are byte-streams sent from server to client over each HTTP-request, in order to manage its state.

PHP Basics

- **PHP**: Cookies… (Authentication)
  - ✓ Authentication cookies are the most common method used by web servers to know whether the user is logged in or not, and which account they are logged in with.
  - ✓ Without such a mechanism, the site would not know whether to send a page containing sensitive information, or require the user to authenticate themselves by logging in.

PHP Basics

- **PHP**: Cookies… (Authentication)
  - ✓ The security of an authentication cookie generally depends on the security of the issuing website and the user's web browser, and on whether the cookie data is encrypted.
  - ✓ Security vulnerabilities may allow a cookie's data to be read and, used to gain access to user data, or used to gain access to the website to which the cookie belongs.

PHP Basics

- **PHP**: Sessions…
  - ✓ Session variables (session objects) are used to personalize the content regarding user's status.
  - ✓ Server stores temporary informative data (name, ID, etc.) for each user, according to a uniquely assigned ID.
  - ✓ Session data are available to server throughout the entire length of the application (i.e. pages used) .
  - ✓ Functions:
    session_start(), session_destroy(), unset(), etc…

PHP Basics

PHP: Authenticating User Account

```
<html>
<head>
<title>LogIn As Administrator</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
</head>
<body>

<form align=left name="theform" method="post" action="em_intro_page.htm">
<input type="submit" value="BACK"></form>

<h2 align=center><b><i>Administration</i></b></h2>

<body background=img24.jpg>
<body text=white>
<br><br><br><br><br><br><br>
<div align="center">
    <form  name="form" method="POST" action="em_admin_auth.php">
    <table width="200" border="0">
      <tr>
        <td><b>USERNAME:</b></td>
        <td><input type="text" name="adminUsername"/></td>
      </tr>
      <tr>
        <td><b>PASSWORD:</b></td>
        <td><input type="password" name="adminPassword"/></td>
      </tr>
      <tr>
        <td> </td>
        <td><label>
          <input type="submit" name="Submit" value="LogIn" />
        </label></td>
      </tr>
    </table>
    </form>
</div>
</body>
</html>
```

PHP Basics

❑ PHP: Authenticating User Account

```
<html>
<head><title>USER AUTHENTICATION</title></head>
<body text=black></body>
</html>

<?php

if (empty($_POST['adminUsername']) || empty($_POST['adminPassword']))
{
    echo "test1";
    echo "<script language=\"JavaScript\" type=\"text/javascript\"> alert('Submit both username and password'); </script>";
    echo "<meta http-equiv='refresh' content='0; url=em_admin_auth.htm'>";
    exit();
}
else
{
    echo "test2";
    $username_from_form = $_POST['adminUsername'];
    $password_from_form = $_POST['adminPassword'];

    $hashed_username_usr = sha1($username_from_form);
    $hashed_password_usr = sha1($password_from_form);

    $dbusnm='12dea96fec20593566ab75692c9949596833adc9';//user
    $dbpswd='9d4e1e23bd5b727046a9e3b4b7db57bd8d6ee684';//polenakis

    if (strcmp($hashed_username_usr, $dbusnm) != 0 || strcmp($hashed_password_usr, $dbpswd) != 0)
    {
        echo "<script language=\"JavaScript\" type=\"text/javascript\"> alert('the combination of username and password is not correct'); </script>";
        echo "<meta http-equiv='refresh' content='0; url=em_admin_auth.htm'>";
        exit();
    }
    else
    {
        echo "Mr/s ".$username_from_form."Welcome";
        session_start();

        $_SESSION['is_administrator_logged_in'] = true;
        echo "<meta http-equiv='refresh' content='0; url=index.html'>";
    }
}
?>
```

PHP Basics

PHP: Connection to Database

```
<form name='registration' action="insert_into_db_A.php" method="POST" onSubmit="return formValidation();">
<table border=20 align =center>
<tr><td align="right">User id:</td>
    <td><input type="text" name="userid" size="30" /></td></tr>
<tr><td align="right">Password:</td>
    <td><input type="password" name="passid" size="30" /></td></tr>
<tr><td align="right">Name:</td>
    <td><input type="text" name="username" size="30" /></td></tr>
<tr><td align="right">Address:</td>
    <td><input type="text" name="address" size="30" /></td></tr>
<tr><td align="right">Country:</td>
    <td><select name="country">
        <option selected="" value="Default">(Please select a country)</option>
        <option value="GR">Greece</option>
        <option value="DE">Germany</option>
        <option value="IT">Italy</option>
        <option value="FR">France</option>
        <option value="SP">Spain</option>
        <option value="EN">England</option>
        <option value="IR">Ireland</option>
        <option value="SW">Sweden</option>
        <option value="FI">Finland</option>
        <option value="NO">Norway</option>
        </select></td></tr>
<tr><td align="right">ZIP Code:</td>
    <td><input type="text" name="zip" size="30" /></td></tr>
<tr><td align="right">Email:</td>
    <td><input type="text" name="email" size="30" /></td></tr>
<tr><td align="right">About:</td>
    <td><textarea name="desc" id="desc" rows="1" cols="10" id="myTextArea"></textarea></td></tr>
<tr><td><input type="reset" name="reset" value="Reset" /></td><td><input type="submit" name="submit" value="Submit" /></td>
</tr>
</table>
</form>
```

Registration.html

PHP Basics

❑ **PHP**: Connection to Database

```
<form name='registration' action="insert_into_db_A.php" method="POST" onSubmit="return formValidation();">
<table border=20 align =center>
<tr><td align="right">User id:</td>
    <td><input type="text" name="userid" size="30" /></td></tr>
<tr><td align="right">Password:</td>
    <td><input type="password" name="passid" size="30" /></td></tr>
<tr><td align="right">Name:</td>
    <td><input type="text" name="username" size="30" /></td></tr>
<tr><td align="right">Address:</td>
    <td><input type="text" name="address" size="30" /></td></tr>
<tr><td align="right">Country:</td>
    <td><select name="country">
        <option selected="" value="Default">(Please select a country)</option>
        <option value="GR">Greece</option>
        <option value="DE">Germany</option>
        <option value="IT">Italy</option>
        <option value="FR">France</option>
        <option value="SP">Spain</option>
        <option value="EN">England</option>
        <option value="IR">Ireland</option>
        <option value="SW">Sweden</option>
        <option value="FI">Finland</option>
        <option value="NO">Norway</option>
        </select></td></tr>
<tr><td align="right">ZIP Code:</td>
    <td><input type="text" name="zip" size="30" /></td></tr>
<tr><td align="right">Email:</td>
    <td><input type="text" name="email" size="30" /></td></tr>
<tr><td align="right">About:</td>
    <td><textarea name="desc" id="desc" rows="1" cols="10" id="myTextArea"></textarea></td></tr>
<tr><td><input type="reset" name="reset" value="Reset" /></td><td><input type="submit" name="submit" value="Submit" /></td>
</tr>
</table>
</form>
```

Insert Data from HTML Form

PHP Basics

❑ **PHP**: Connection to Database (MySQL)

insert

insert_into_db_A.php

```php
<?php

  $user=$_POST['userid'];
  $usn=$_POST['username'];
  $pswd=$_POST['passid'];
  $adr=$_POST['address'];
  $cntr=$_POST['country'];
  $zip=$_POST['zip'];
  $email=$_POST['email'];
  $about=$_POST['desc'];


  $con = mysql_connect("localhost", "user", "admin");
  if (!$con){
     die('Could not connect: '.mysql_error());
  }
  echo "Successfully Connected to DataBase";

  $sql="INSERT INTO person (userid,username,password,address,country,zip_code,mail,description) VALUES
                           (".$user.",".$usn.",".$pswd.",".$adr.",". $cntr.",".$zip.",".$email.",".$about.")";
  if (!mysql_query($sql,$con)){
      die('Error: ' . mysql_error());
  }
  echo "User Registered Successfully";
  mysql_close($con);
?>
```

PHP Basics

❑ **PHP**: Connection to Database (MySQL)

```php
<?php
    $con = mysql_connect("localhost", "user", "admin");
    if (!$con) {
        die('Could not connect: ' . mysql_error());
    }
    mysql_select_db("project_db", $con);

    $select_data = mysql_query("SELECT userid,username,password,address,country,zip_code,mail,description
                                FROM accounts");
    echo "<table border='1'> <tr> <th>USERNAME</th><th>PASSWORD</th><th>ADDRESS</th><th>COUNTRY</th>
                               <th>ZIP</th><th>MAIL</th><th>ABOUT</th></tr>";
    while ($tuple = mysql_fetch_array($select_data)) {
      echo "<tr>";
      echo "<td>".$tuple['username']."</td>";

      echo "<td>".$tuple['password']."</td>";
      echo "<td>".$tuple['address']."</td>";
      echo "<td>".$tuple['country']."</td>";
      echo "<td>".$tuple['zip_code']."</td>";
      echo "<td>".$tuple['mail']."</td>";
      echo "<td>".$tuple['description']."</td>";
      echo "</tr>";
    }
    echo "</table>";
    mysql_close($con);
  ?>
```

retrieve

Select_from_db_A.php

PHP Basics

❑ **PHP**: Connection to Database (MySQL)

```php
<?php
    $con = mysql_connect("localhost", "user", "admin");
    if (!$con) {
        die('Could not connect: ' . mysql_error());
    }
    mysql_select_db("project_db", $con);

    $select_data = mysql_query("SELECT userid,username,password,address,country,zip_code,mail,description
                                FROM accounts");
    echo "<table border='1'> <tr> <th>USERNAME</th><th>PASSWORD</th><th>ADDRESS</th><th>COUNTRY</th>
                               <th>ZIP</th><th>MAIL</th><th>ABOUT</th></tr>";
    while ($tuple = mysql_fetch_array($select_data)) {
      echo "<tr>";
      echo "<td>".$tuple['username']."</td>";

      echo "<td>".$tuple['password']."</td>";
      echo "<td>".$tuple['address']."</td>";
      echo "<td>".$tuple['country']."</td>";
      echo "<td>".$tuple['zip_code']."</td>";
      echo "<td>".$tuple['mail']."</td>";
      echo "<td>".$tuple['description']."</td>";
      echo "</tr>";
    }
    echo "</table>";
    mysql_close($con);
?>
```

retrieve

Select_from_db_A.php

Inject HTML

PHP Basics

❑ PHP: Connection to Database (MySQLi)

Instruction		
connect to DB	`$con = new mysqli('localhost', 'user','admin','project_db');`	`$con = mysqli_connect('localhost', 'user', 'admin', 'project_db');`
select DB	`$con->select_db(project_db);`	`mysqli_select_db($con,'project_db');`
query execution	`$select_data= $con->query(…);`	`$select_data= mysqli_query($con,query);`
fetch results	`$tuple= $result->fetch_array() ;`	`$tuple=mysqli_fetch_array($select_data);`
close connection	`$con->close();`	`mysqli_close();`