**Jarra Dampha**

**21818413**

**BSc (Hons) Cyber Security**

**Year 2**

**Semester III**

**Open Sources Systems**

**CO 551**

**CW2**

**week 5**

**1**

**Class\_lib.php**

<?php

    class person {

        var $name;

        function set\_name($new\_name) {

            $this->name = $new\_name;

        }

        function get\_name() {

            return $this->name;

        }

    }

?>

**index.php**

<?php

include("class\_lib.php");

   $stefan = new person();

   $jimmy = new person;

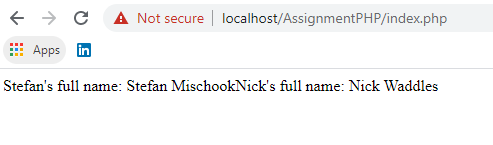
   $stefan->set\_name("Stefan Mischook");

   $jimmy->set\_name("Nick Waddles");

   echo "Stefan's full name: " . $stefan->get\_name();

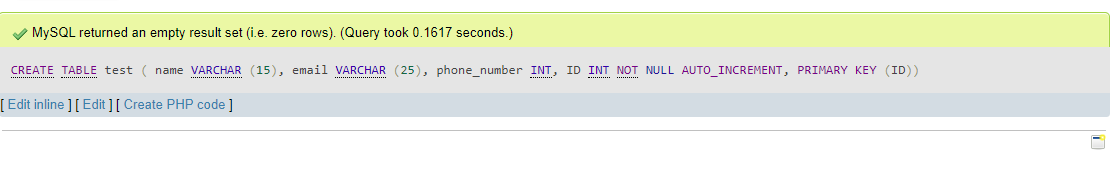
   echo "Nick's full name: " . $jimmy->get\_name();

?>



**2.**

CREATE TABLE test (  
name VARCHAR (15),  
email VARCHAR (25),  
phone\_number INT,  
ID INT NOT NULL AUTO\_INCREMENT,  
PRIMARY KEY (ID));

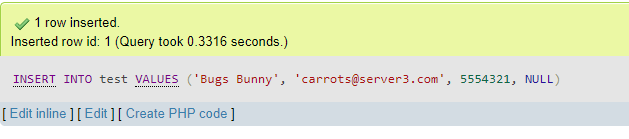


**3.**

INSERT INTO test VALUES

('Bugs Bunny', 'carrots@server3.com',

5554321, NULL);

****

**4.**

SELECT \* FROM test

WHERE (name = "Bugs Bunny");



**5.**

INSERT INTO test VALUES

('Bugs Bunny', 'peppers@server3.com',

5554331, NULL);

INSERT INTO test VALUES

('Bugs Bunny', 'lettuce@server3.com',

5554341, NULL);

INSERT INTO test VALUES

('Bugs Bunny', 'celery@server3.com',

5554351, NULL);

****

**6.**

SELECT \* FROM test

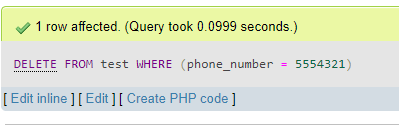
WHERE (name = "Bugs Bunny");

****

**7.**

DELETE FROM test

WHERE (phone\_number = 5554321);

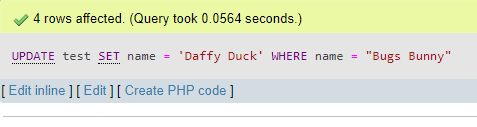
****

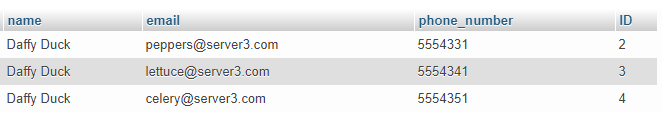
****

**8.**

UPDATE test SET name = 'Daffy Duck'

WHERE name = "Bugs Bunny";

****



**week 6**

## 1.

**wk6ex1.html**

<html>

<head></head>

<body>

    <form action='wk6ex1action.php' method='post'>

    Enter name :

    <input type='text' name='txtName' /><br/>

    Enter email :

    <input type='text' name='txtEmail'/><br/>

    Enter Tel number :

    <input type='text' name='txtPhoneNumber'/><br/><br/>

    <input type='submit' value='Save Data' />

    </form>

</body>

</html>

**wk6ex1action.php**

<?php

$sql ="INSERT INTO `test`(`name`, `email`, `phone\_number`) VALUES ('$\_POST[txtName]','$\_POST[txtEmail]','$\_POST[txtPhoneNumber]')";

    // Connect to server and select database

    define('HOST','localhost');

 define('USER','root');

 define('PASSWORD','');

 define('DB','db1\_gwalke01');

 $con = mysqli\_connect(HOST,USER,PASSWORD,DB) or die(mysqli\_connect\_error());

    // Execute sql statement

    if (mysqli\_query($con, $sql) === TRUE) {

        echo "New record created successfully". "<br>" ;

    } else {

        echo "Error: " . $sql . "<br>" . mysqli\_error($con);

    }

    $sql = "SELECT \* from test";

    // Execute sql statement

   $result = mysqli\_query($con,$sql);

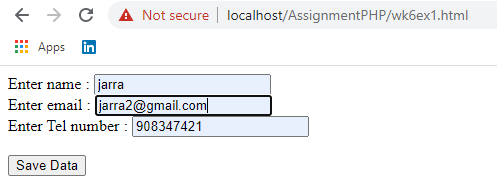
    while ($row = mysqli\_fetch\_assoc($result))

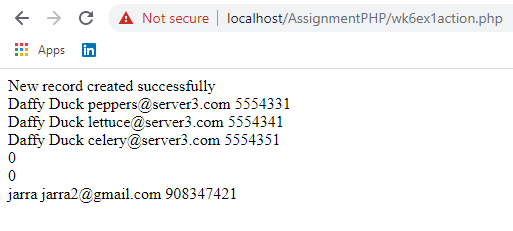
    {

        echo "$row[name]  $row[email]  $row[phone\_number] <br/>";

    }

?>



****

## 2.

**wk6ex2.php**

<?php

    // Connect to server and select database

 define('HOST','localhost');

 define('USER','root');

 define('PASSWORD','');

 define('DB','db1\_gwalke01');

 $con = mysqli\_connect(HOST,USER,PASSWORD,DB) or die(mysqli\_connect\_error());

    $sql = "SELECT \* from test";

    // Execute sql statement

    $result = mysqli\_query($con,$sql);

?>

<html>

<body>

<?php

while ($row = mysqli\_fetch\_assoc($result))

{

      echo "<a href=\"wk6ex2action.php?id=$row[name]\">$row[name]</a></br>";

}

?>

</body>

</html>

**wk6ex2action.php**

<?php

    // Connect to server and select database

    define('HOST','localhost');

    define('USER','root');

    define('PASSWORD','');

    define('DB','db1\_gwalke01');

    $con = mysqli\_connect(HOST,USER,PASSWORD,DB) or die(mysqli\_connect\_error());

    $sql = "SELECT \* from test where name = '$\_GET[id]' ";

    // Execute query

    $result = mysqli\_query($con,$sql);

    $row = mysqli\_fetch\_assoc($result);

?>

<html>

<body>

<form action="" method="post">

    Name :

    <input type=text name=txtname value="<?php echo $row['name'] ?>" />

    </br>

    Phone number :

    <input type=text name=txttelno value="<?php echo $row['phone\_number'] ?>" />

    </br>

    Email :

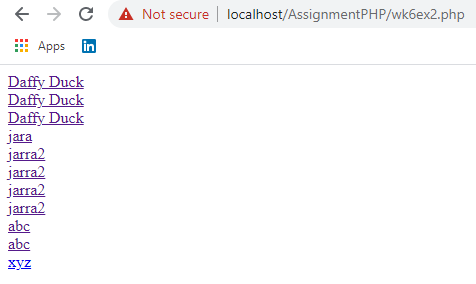
    <input type=text name=txtemail value="<?php echo $row['email'] ?>" />

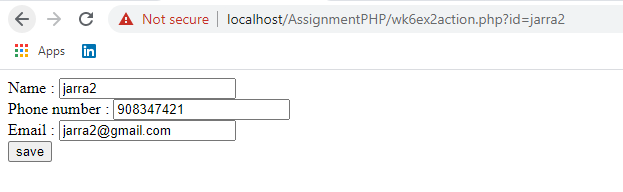
    </br>

    <input type=submit name=btnsubmit value="save"/>

</form>

</body>





**3.**

<?php

    // Connect to server and select database

    define('HOST','localhost');

    define('USER','root');

    define('PASSWORD','');

    define('DB','db1\_gwalke01');

    $con = mysqli\_connect(HOST,USER,PASSWORD,DB) or die(mysqli\_connect\_error());

    $sql = "SELECT \* from test where name = '$\_GET[id]' ";

    // Execute query

    $result = mysqli\_query($con,$sql);

    $row = mysqli\_fetch\_assoc($result);

?>

<html>

<body>

<form action="" method="post">

    Name :

    <input type=text name=txtname value="<?php echo $row['name'] ?>" />

    </br>

    Phone number :

    <input type=text name=txttelno value="<?php echo $row['phone\_number'] ?>" />

    </br>

    Email :

    <input type=text name=txtemail value="<?php echo $row['email'] ?>" />

    </br>

    <input type=submit name=btnsubmit value="save"/>

</form>

</body>

<?php

    if(isset($\_POST['btnsubmit'])){

        $name = $\_POST['txtname'];

        $email = $\_POST['txtemail'];

        $phone\_number = $\_POST['txttelno'];

        $sql = "UPDATE `test` SET name='$name',email='$email',phone\_number='$phone\_number' where name='$\_GET[id]' ";

// Execute query

if ($con->query($sql) === TRUE) {

    echo "Record updated successfully";

    $row = mysqli\_fetch\_assoc($result);

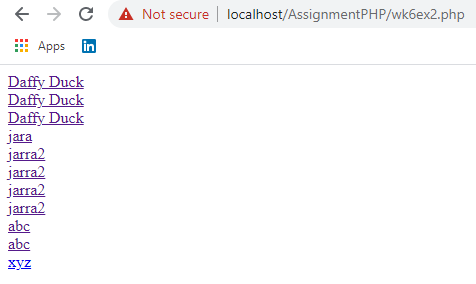
  } else {

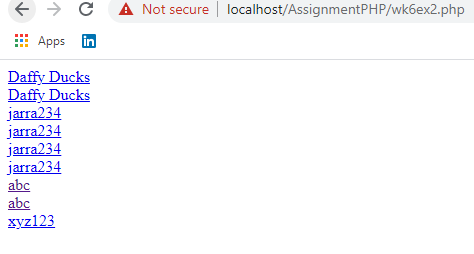
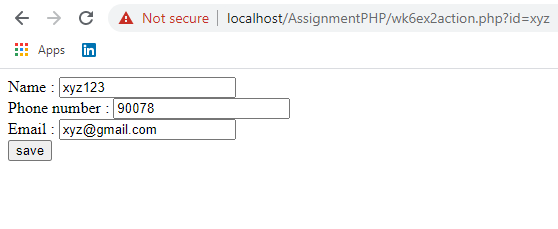
    echo "Error updating record: " . $con->error;

  }

    }

?>





**4.**

<?php

    // Connect to server and select database

    define('HOST','localhost');

    define('USER','root');

    define('PASSWORD','');

    define('DB','db1\_gwalke01');

    $con = mysqli\_connect(HOST,USER,PASSWORD,DB) or die(mysqli\_connect\_error());

    $id=$\_GET['id'];

    $sql = "SELECT \* from test where name = '$\_GET[id]' ";

    // Execute query

    $result = mysqli\_query($con,$sql);

    $row = mysqli\_fetch\_assoc($result);

?>

<html>

<body>

<form action="" method="post">

    Name :

    <input type=text name=txtname value="<?php echo $row['name'] ?>" />

    </br>

    Phone number :

    <input type=text name=txttelno value="<?php echo $row['phone\_number'] ?>" />

    </br>

    Email :

    <input type=text name=txtemail value="<?php echo $row['email'] ?>" />

    </br>

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

</form>

</body>

<?php

    if(isset($\_POST['delete'])){

       $sql="DELETE FROM `test` WHERE `test`.`name` = '$\_GET[id]' ";

// Execute query

if ($con->query($sql) === TRUE) {

    echo "Record deleted successfully";

  } else {

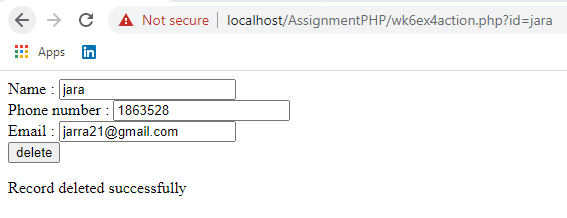
    echo "Error deleted record: " . $con->error;

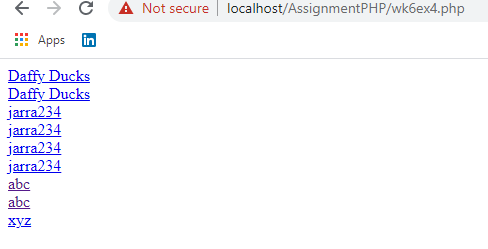
  }

  $con->close();

}

?>





## 5.

**myfunctions.inc**

<?php

function html\_header($pageTitle)

{

echo “<html><title> $pageTitle </title></head>”;

echo “<body>”;

}

function html\_h1($text)

{

echo “<h1> $text </h1>”;

}

function html\_footer()

{

echo “</body>”;

echo “</html>”;

}

?>

**wk6ex5.php**

<?php

    include("myfunctions.inc");

    html\_header("My first function demo");

    html\_h1("These functions are going to save me lots of time");

    html\_h2("passing some text as an argument");

    html\_footer();

?>



## 6.

function calculatetax($salary, $rate)

{

$tax = ($salary \* ($rate/100));

return $tax;

}

**wk6ex6.php**

<?php

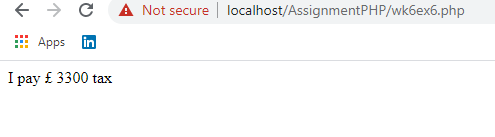
    include(“myfunctions.inc”);

    html\_header(“My second function demo”);

    echo “I pay £ “ . calculatetax(15000,22) . “ tax”;

    html\_footer();

?>



## 7.

function calculatetax($salary, $rate=40)

{

$tax = ($salary \* ($rate/100));

return $tax;

}

**wk6ex6.php**

<?php

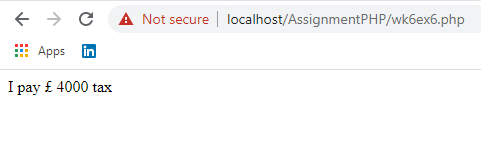
    include("myfunctions.inc");

    html\_header("My second function demo");

    echo "I pay " . calculatetax(10000) . " tax";

    html\_footer();

?>

****

## 8.

function calculatetax($salary, $rate=40,$taxallowance)

{

$tax = ($salary \* ($rate/100)\*$taxallowance);

return $tax;

}

**wk6ex6.php**

<?php

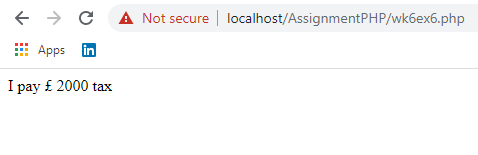
    include("myfunctions.inc");

    html\_header("My second function demo");

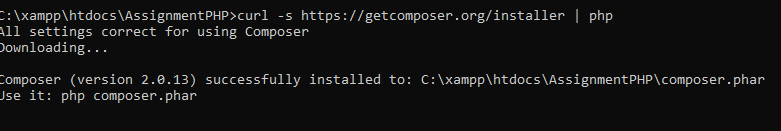
    echo "I pay £ " . calculatetax(10000,20,10) . " tax";

    html\_footer();

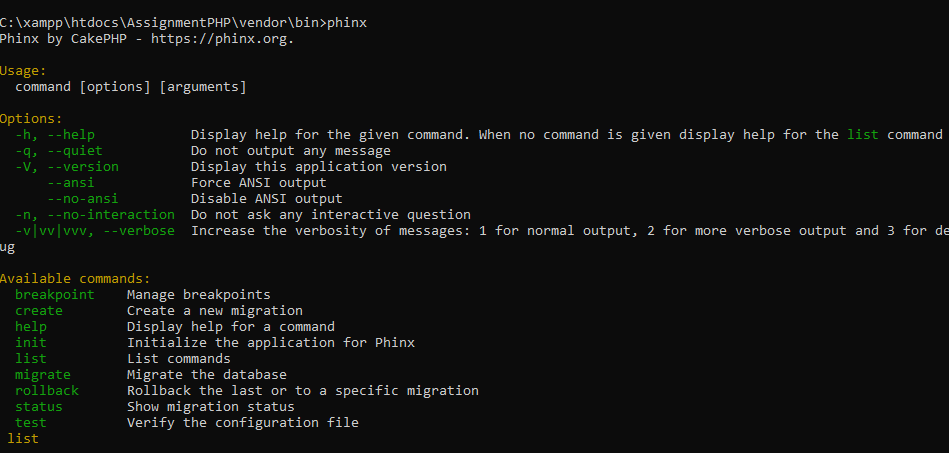
?>



**9.**



**10.**



**11.**

public function change(): void

    {

        $users = $this->table('test1');

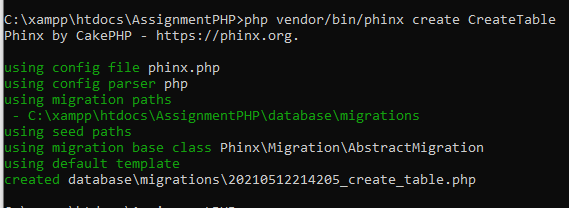
        $users->addColumn('name', 'string', ['null' => false], ['limit' => 15],'primarykey')

              ->addColumn('email', 'string', ['limit' => 25], ['null' => false])

              ->addColumn('phone\_number', 'integer', ['null' => false])

              ->create();

    }



**12.**

public function up(){

       $users = $this->table('test1');

        $users->addColumn('name', 'string', ['null' => false], ['limit' => 15],'primarykey')

              ->addColumn('email', 'string', ['limit' => 25], ['null' => false])

              ->addColumn('phone\_number', 'integer', ['null' => false])

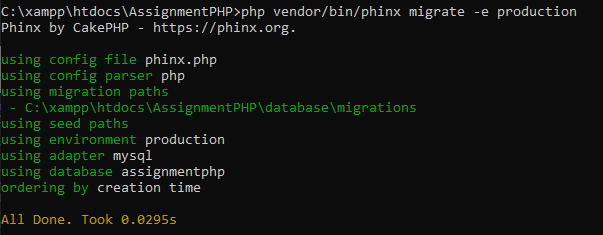
              ->save();

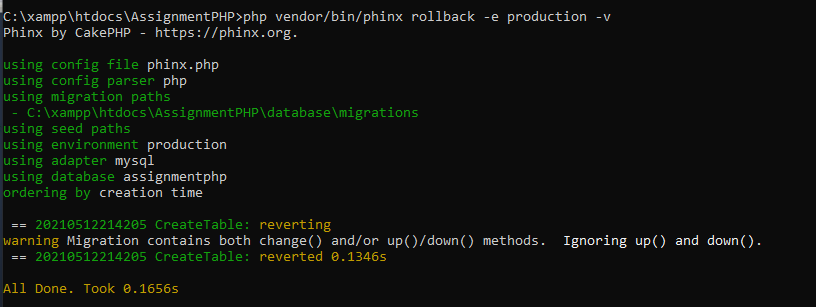
    }

    public function down(){

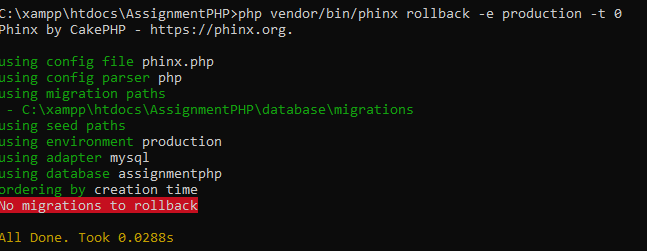
         $this->dropTable('test1');

    }





**13.**



**Session 7**

**1a.**

Create table monster

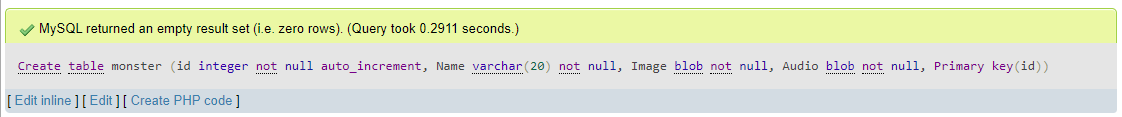
(id integer not null auto\_increment,

Name varchar(20) not null,

Image blob not null,

Audio blob not null,

Primary key(id));



**1b.**

<?php

use Phinx\Migration\AbstractMigration;

class MyNewMigration extends AbstractMigration

{

    public function change()

    {

        $users = $this->table('monster');

        $users->addColumn('id', 'integer', ['null' => false],'primarykey')

              ->addColumn('Name', 'varchar', ['limit' => 20], ['null' => false])

              ->addColumn('Image', 'blob', ['null' => false])

              ->addColumn('Audio', 'blob', ['null' => false])

              ->create();

    }

public function up(){

       $users->addColumn('id', 'integer', ['null' => false],'primarykey')

              ->addColumn('Name', 'varchar', ['limit' => 20], ['null' => false])

              ->addColumn('Image', 'blob', ['null' => false])

              ->addColumn('Audio', 'blob', ['null' => false])

              ->save();

    }

    public function down(){

         $this->dropTable(' monster ');

    }

}

**2.**

<html>

<head>

<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-BVYiiSIFeK1dGmJRAkycuHAHRg32OmUcww7on3RYdg4Va+PmSTsz/K68vbdEjh4u" crossorigin="anonymous">

<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js" integrity="sha384-Tc5IQib027qvyjSMfHjOMaLkfuWVxZxUPnCJA7l2mCWNIpG9mGCD8wGNIcPD7Txa" crossorigin="anonymous"></script>

</head>

<body>

<h2>Monster Details</h2>

<form enctype="multipart/form-data" action="savemonster.php" method="post">

 Monster name :

 <input type="text" name="txtname" size="15" class="form-control" />

 </br></br>

 Monster image :

 <input  type="file" name="monsterimage" accept="image/jpeg" class="form-control" />

 </br></br>

 Monster Sound :

 <input  type="file" name="monsteraudio" accept="audio/basic" class="form-control"  />

 </br></br>

 <input type="submit" class="btn btn-default" value="Save" />

</form>

</body>

</html>

**savemonster.php**

<?php

  define('HOST','localhost');

  define('USER','root');

  define('PASSWORD','');

  define('DB','db1\_gwalke01');

  $con = mysqli\_connect(HOST,USER,PASSWORD,DB) or die(mysqli\_connect\_error());

// Obtain the file sent to the server within the response.

$image = $\_FILES['monsterimage']['tmp\_name'];

$audio = $\_FILES['monsteraudio']['tmp\_name'];

  // Get the file binary data

  $imagedata = addslashes(fread(fopen($image, "r"), filesize($image)));

  $audiodata = addslashes(fread(fopen($audio, "r"), filesize($audio)));

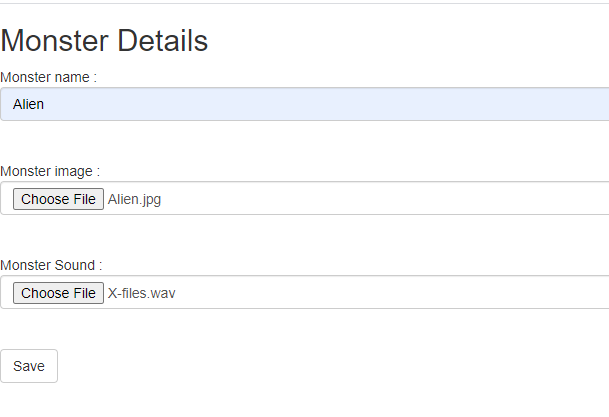
  $sql = "INSERT INTO monster";

  $sql .= "(Name, Image, Audio) ";

  $sql .= "VALUES ('$\_POST[txtname]', '$imagedata','$audiodata')";

  $result = mysqli\_query( $con,$sql);

?>



**3.**

**getjpg.php**

<?php

  header("Content-type: image/jpeg");

  $conn = mysqli\_connect("localhost", "root","", "db1\_gwalke01");

  $sql = "SELECT image FROM monster WHERE id='" . $\_GET[id] ."';";

  $result = mysqli\_query($sql, $conn);

  $row = mysqli\_fetch\_array($result);

  $jpg = $row["image"];

  echo $jpg;

?>

**getwav.php**

<?php

  header("Content-type: audio/wav");

  $conn = mysqli\_connect("localhost", "root","", "db1\_gwalke01");

  $sql = "SELECT audio FROM monster WHERE id='" . $\_GET[id] ."';";

  $result = mysqli\_query($sql, $conn);

  $row = mysqli\_fetch\_array($result);

  $audio = $row["audio"];

  echo $audio;

?>

**displaymonster.php**

<html>

<head></head>

<body>

<?php

  define('HOST','localhost');

  define('USER','root');

  define('PASSWORD','');

  define('DB','db1\_gwalke01');

  $con = mysqli\_connect(HOST,USER,PASSWORD,DB) or die(mysqli\_connect\_error());

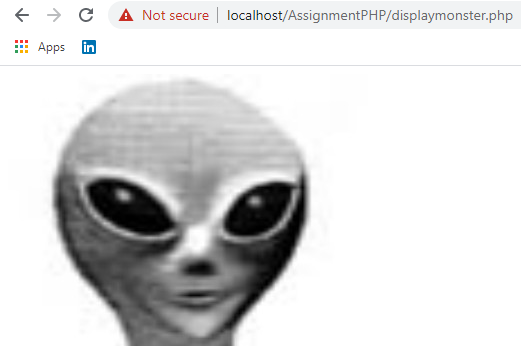
$sql = "select id from monster;";

$result = mysqli\_query($con,$sql);

$row = mysqli\_fetch\_array($result);

echo "<img src='getjpg.php?id=" . $row['id']. "'/>";

?>



**4.**

**displaymonster.php**

<html>

<head></head>

<body>

<?php

  define('HOST','localhost');

 define('USER','root');

 define('PASSWORD','');

 define('DB','db1\_gwalke01');

 $con = mysqli\_connect(HOST,USER,PASSWORD,DB) or die(mysqli\_connect\_error());

//$sql = "SELECT \* from `monster`";

$sql = "select id,Name,Image from `monster`;";

echo "<table align='center' border='1'>";

echo "<tr><th width='200' align='left'>ID</th><th width='200' align='left'>Name</th><th>Audio</th><th>Image</th></tr>";

$result = mysqli\_query( $con,$sql);

while($row = mysqli\_fetch\_assoc($result)){

  echo "<tr>";

  echo "<td>" . $row['id'] . "</td>";

  echo "<td>" . $row['Name'] . "</td>";

  echo "<td><a href='getwav.php?id=" .$row['id']. "'>Click to play</a></td>";

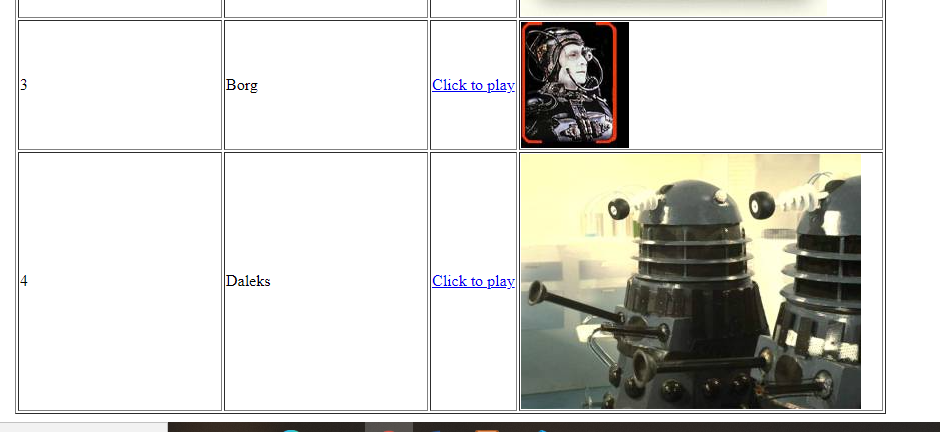
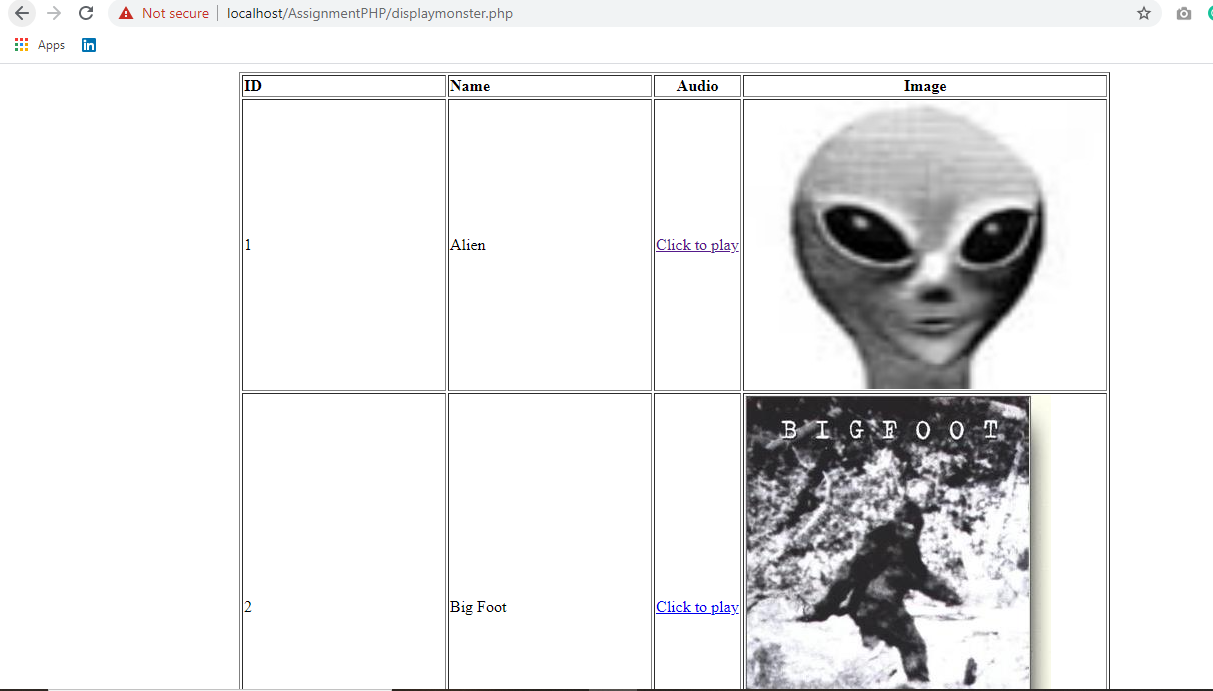
  echo '<td><img src="data:image/jpeg;base64,'.base64\_encode($row['Image']) .' " style=" height=100 width=100" </td>';

  echo "</tr>";

}

echo "</table>";

?>



**5.**

<html>

<head>

<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-BVYiiSIFeK1dGmJRAkycuHAHRg32OmUcww7on3RYdg4Va+PmSTsz/K68vbdEjh4u" crossorigin="anonymous">

<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js" integrity="sha384-Tc5IQib027qvyjSMfHjOMaLkfuWVxZxUPnCJA7l2mCWNIpG9mGCD8wGNIcPD7Txa" crossorigin="anonymous"></script>

</head>

<body>

<h2>Monster Details</h2>

<form enctype="multipart/form-data" method="post">

 Monster name :

 <input type="text" name="txtname" size="15" class="form-control" />

 </br></br>

 Monster image :

 <input  type="file" name="monsterimage" accept="image/jpeg" class="form-control" />

 </br></br>

 Monster Sound :

 <input  type="file" name="monsteraudio" accept="audio/basic" class="form-control"  />

 </br></br>

 <button type="submit" class="btn btn-default" value="Save" name="submit" >Save</button>

</form>

</body>

</html>

<?php

if(isset($\_POST['submit'])){

    function InsertInTable($table,&$fields){

    define('HOST','localhost');

    define('USER','root');

    define('PASSWORD','');

    define('DB','assignmentphp');

    $con = mysqli\_connect(HOST,USER,PASSWORD,DB) or die(mysqli\_connect\_error());

        $col = "insert into $table (`".implode("` , `",array\_keys($fields))."`)";

        $val = " values('";

        foreach($fields as $key => $value) {

          $fields[$key] = mysqli\_real\_escape\_string($con,$value);

        }

        $val .= implode("' , '",array\_values($fields))."');";

        $fields = array();

        return;

      }

      $image = $\_FILES['monsterimage']['tmp\_name'];

      $audio = $\_FILES['monsteraudio']['tmp\_name'];

      // Get the file binary data

      $imagedata = addslashes(fread(fopen($image, "r"), filesize($image)));

      $audiodata = addslashes(fread(fopen($audio, "r"), filesize($audio)));

      $field['Name'] = '$\_POST[txtname]';

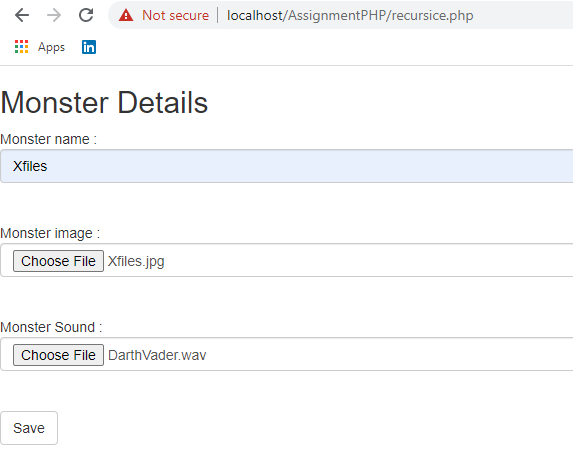
      $field['Image'] = '$imagedata';

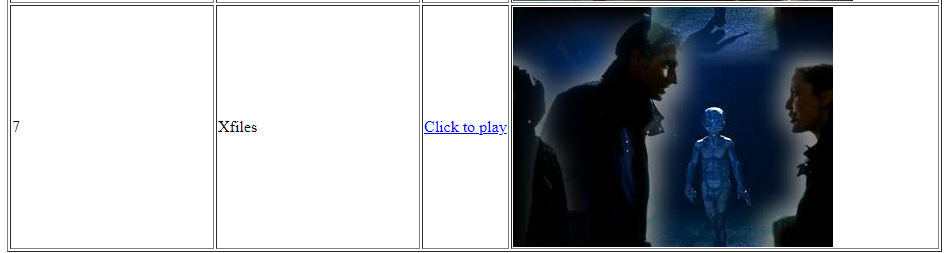
      $field['Audio'] = '$audiodata';

      InsertInTable("monster",$field);

}

?>





**6.**



**WEEK 8**

**2 different server-side approaches to development**

**1, PHP**

‘According to Szklarczyk, R. (2013) notes’, PHP (Hypertext Pre-Process) commonly known for embedded HTML and mainly for website development. PHP enable and control constraint logical programming aid. PHP is an application that is basically responsible the GUI. The server scripting languages interprets script to the server-side rather than the client side. It can contain only simple GUI and socket communication, or it could be large enterprise solution, that must support for example some scheduling process.

The socket communication from the side of PHP operates according to the model:

1) Establish socket connection.

2) Send command (and parameter).

3) Read server response from the socket.

4) Close the socket.

**2, ASP.NET**

ASP.NET been a very important and indeed a very powerful platform for programming with visualization. It enables dynamic architect established with web applications, its also well recommended web application in networking programming for engineering. But .NET is not good at some applications, such as signal analysis, matrix calculation, and other complex mathematical calculations, which has been a bottleneck for .NET to be applied to the engineering field. To realize complex mathematical calculation, shorten software developing cycle, and reduce development costs, it is necessary to adopts other technology to .NET platform.

**2 Important security concerns**

**1, Code Injection**

“Code injection protection: The user input data must be ensured that it does not contain any SQL injection, OS commands, any code injection patterns or any malicious scripts. Malicious SQL statements can be introduced into a vulnerable application using many different input mechanisms including user inputs, cookies, and server variables. More details can be found in the survey entirely dedicated to SQL injections” (Halfond et al. 2006).

**2, Input Protection and Validations**

‘As mentioned in the OWASP (2013). Notes’, Form input protection or input validations: Administrators can be given detailed rules to regulate the user input like validating user input data, checking input size, checking input characters and other type of input forms. Nowadays, input validation attacks are seen as the most dangerous and popular attacks against web application security, Which manifest as the top two security risks (i.e., injections, cross-site scripting)

**References**

Halfong, W. G., Viegas, J., and Orso, A. (2006). A Classification of SQL-Injection Attacks and Countermeasures. In Proc. of the International Symposium on Secure Software Engineering. Delectable Publications.

OWASP Top Ten, OWASP: <http://www.owasp.org/documentation/topten.html> [Accessed 18 May 2021].

Rao, H., Zhou, X. and Zhao, Q. (2009). Remote Signal Analysis Based on the Hybrid-Programming between ASP.NET and MATLAB: Delectable Publications.

Szklarczyk, R. (2013). GNU Prolog-PHP multi-tier integration, 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Delectable Publications.

