|  |  |
| --- | --- |
| **CS 335**  **Web Programming** | Midterm II **Wednesday November 30, 2022**  **Duration: 2h**  **Name: Ghazi Najeeb Al-Abbar**  **ID: 2181148914** |

**Link: http://ghazi-test.epizy.com/**

1. Write a PHP code to generate a password that contains N lowercase, M uppercase, K numeric, and W special characters. The length of the password should be at least 12 characters (N, M, K, and W are inputs from the user). [4 points]

Q1.php:

<!DOCTYPE html>

<html>

<head></head>

<body>

    <form method="post" action="page2.php">

        <p>

            <label>enter N</label>

            <input type="text" name="N">

        </p>

        <p>

            <label>enter M</label>

            <input type="text" name="M">

        </p>

        <p>

            <label>enter K</label>

            <input type="text" name="K">

        </p>

        <p>

            <label>enter W</label>

            <input type="text" name="W">

        </p>

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

    </form>

</body>

</html>

Page2.php:

<?php

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

    $N = (int) cleanData($\_POST["N"]);

    $M = (int) cleanData($\_POST["M"]);

    $K = (int) cleanData($\_POST["K"]);

    $W = (int) cleanData($\_POST["W"]);

    print<<<HERE

    <html>

        <body>

    HERE;

    if ($N + $M + $K + $W < 12) {

        print <<<HERE

        <h1>the password should be at least 12 character in length. Enter here to try again...</h1>

        <form method="post" action="q1.php">

            <input type="submit">

        </form>

        HERE;

    } else {

        $pass = "";

        $incr = 0;

        for ($i = 0; $i < $N; $i++) {

            if (97 + $incr >= 97 || 97 + $incr <= 122) {

                $pass .= chr(97 + $incr);

                $incr++;

            } else {

                $incr = 0;

            }

        }

        $incr = 0;

        for ($i = 0; $i < $M; $i++) {

            if (65 + $incr >= 65 || 65 + $incr <= 90) {

                $pass .= chr(65 + $incr);

                $incr++;

            } else {

                $incr = 0;

            }

        }

        $incr = 0;

        for ($i = 0; $i < $K; $i++) {

            if (48 + $incr >= 48 || 48 + $incr <= 57) {

                $pass .= chr(48 + $incr);

                $incr++;

            } else {

                $incr = 0;

            }

        }

        $incr = 0;

        for ($i = 0; $i < $K; $i++) {

            if (33 + $incr >= 33 || 33 + $incr <= 47) {

                $pass .= chr(33 + $incr);

                $incr++;

            } else {

                $incr = 0;

            }

        }

        print<<<HERE

        <h1>your new password:</h1>

        $pass

        HERE;

    }

    print<<<HERE

    </body></html>

    HERE;

}

function cleanData($data)

{

    $data = trim($data);

    $data = stripslashes($data);

    $data = trim($data);

    $data = htmlspecialchars($data);

    $data = strip\_tags($data);

    return $data;

}

?>



1. Write an HTML form that allows a user to enter his login and password. Once the information is submitted, a PHP code verifies, using regular expressions, that the password starts with a letter, includes at least a digit, a special character and its length is at least 11 characters. Then, it creates one cookie that includes both the login and password. The cookie expires in 1 day, 2 hours, and 35 minutes. [3 points]

Q2.php:

<!DOCTYPE html>

<html>

<body>

    <form method="post" action="cookie.php">

        <p>

            <label>login:</label>

            <input type="text" name="login">

        </p>

        <p>

            <label>password:</label>

            <input type="password" name="pass">

        </p>

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

    </form>

</body>

</html>

Cookie.php:

<?php

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

    print<<<HERE

    <html>

        <body>

    HERE;

    $login = cleanData($\_POST["login"]);

    $pass = cleanData($\_POST["pass"]);

    $pattern = "/^[a-zA-Z](?=.\* [0-9]{1,})(?=.\* [!@#$%^&\*\_-+=]{1,})[a-zA-Z0-9!@#$%^&\*\_-+=]{10,}/";

    if (!preg\_match($pattern, $pass)){

        print<<<HERE

        <h1>incorrect password</h1>

        <h1>the password starts with a letter, includes at least a digit, a special character and its length is at least 11 characters</h1>

        HERE;

    }

    else{

        $cookie\_name = "log&pass";

        $cookie\_val = "login=$login" . "&" . "pass=$pass";

        $time = time() + 24\*60\*60 + 2\*60\*60 + 35\*60;

        setcookie($cookie\_name, $cookie\_val, $time, "/");

    }

    print\_cookie();

    print<<<HERE

    </body></html>

    HERE;

}

function cleanData($data)

{

    $data = trim($data);

    $data = stripslashes($data);

    $data = trim($data);

    $data = htmlspecialchars($data);

    $data = strip\_tags($data);

    return $data;

}

function print\_cookie(){

    parse\_str($\_COOKIE["log&pass"]);

    print<<<HERE

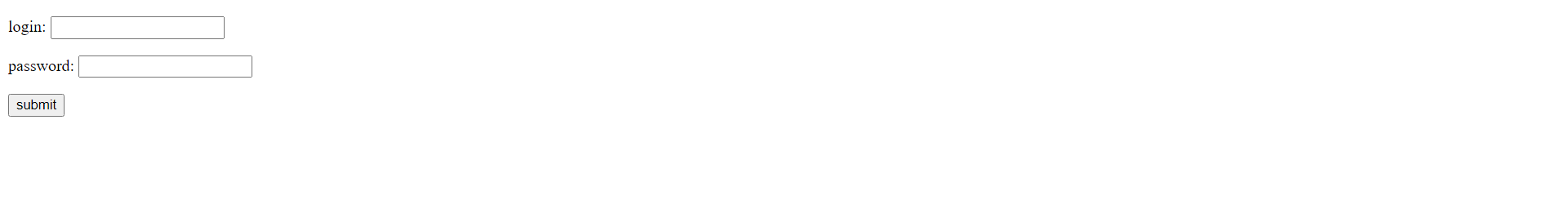
    name: $login <br />

    pass: $pass

    HERE;

}

?>



1. Create a Web page that includes links for your answers to the following questions: [8 points]
2. Create a database called *Construction* with the following two tables: [2 points]

*Projects* Table:

(Integer) (Text) (Integer) (Text) (Date) (Date)

Primary Key

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Project # | Description | Manager# | Type | Start Date | End Date |

*Managers* Table:

(Integer) (Text) (Integer) (Text) (Text)

Primary Key

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Manager# | Name | Experience | Nationality | Phone # |

1. Create two forms with their php/mysql codes to insert the following records with the consideration of the referential integrity constraint: [2 points]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Project# | Description | Manager# | Type | Start Date | End Date |
| 123 | Bridge construction | 35 | Public | 8/9/2023 | 4/15/2028 |
| 245 | Hospital extension | 70 | Private | 7/1/2022 | 3/12/2024 |
| 356 | Road extension | 35 | Public | 6/12/2023 | 7/25/2030 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Manager# | Name | Experience | Nationality | Phone # |
| 35 | Ahmed | 25 | Kuwaiti | 97983456 |
| 70 | Ali | 20 | Egyptian | 98703546 |

1. Write a php/mysql code that executes a query on the Managers table to show the following information: Manager#, Experience and Nationality. [2 points]
2. Write a php/mysql code that executes a query on both tables to show the following information: Manager name, Manager nationality, Project description, and Project type given that the project start date is after 1/1/2023 and its end date is before 12/31/2028. [2 points]

Addmanager.php:

<?php

//Checks if the submit button was entered in the right page and the right place

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

    /\* Data info \*/

    $manager\_no = cleanData($\_POST["manager\_no"]);

    $name = cleanData($\_POST["name"]);

    $exp = cleanData($\_POST["exp"]);

    $nat = cleanData($\_POST["nat"]);

    $pn = cleanData($\_POST["pn"]);

    addmanager($manager\_no, $name, $exp, $nat, $pn);

}

//cleans values from the user input

function cleanData($data)

{

    $data = trim($data);

    $data = stripslashes($data);

    $data = trim($data);

    $data = htmlspecialchars($data);

    $data = strip\_tags($data);

    return $data;

}

function addmanager($manager, $name, $exp, $nat, $pn){

    $PageTitle = "Add a Book";

    //Page header

    print<<<HERE

    <html>

        <body>

    HERE;

    include("myDB.php");

    include("PageFrame.php");

    $query = "SELECT \* FROM manager WHERE `manager#`='$manager'";

    $Rows = mysqli\_num\_rows(mysqli\_query($myDB, $query));

    if ($Rows > 0){

        print "<h1>The Book Already Exists..</h1>";

    }

    else{

        $query = "INSERT INTO manager (`managr#`, `name`, `experience`, `nationality`, `phone#`) VALUES('$manager', '$name', '$exp', '$nat', '$pn')";

        mysqli\_query($myDB, $query);

        print<<<HERE

        <h1>New manager Has Been Added!</h1>

        <table class="brdr">

            <tr class="brdr">

            <th class="brdr">ID</th>

                <th class="brdr">manager no</th>

                <th class="brdr">name</th>

                <th class="brdr">experience</th>

                <th class="brdr">nationality</th>

                <th class="brdr">phone number</th>

            </tr>

            <tr class="brdr">

                <td class="brdr">$manager</td>

                <td class="brdr">$name</td>

                <td class="brdr">$exp</td>

                <td class="brdr">$nat</td>

                <td class="brdr">$pn</td>

            </tr>

        </table>

        HERE;

    }

    print<<<HERE

    </body>

        </html>

    HERE;

}

?>

Addproject:

<?php

//Checks if the submit button was entered in the right page and the right place

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

    /\* Data info \*/

    $project\_no = cleanData($\_POST["project\_no"]);

    $desc = cleanData($\_POST["desc"]);

    $manager\_no = cleanData($\_POST["manager\_no"]);

    $type = cleanData($\_POST["type"]);

    $sd = cleanData($\_POST["sd"]);

    $ed = cleanData($\_POST["ed"]);

    //Calls the function to add the book to database

    addproject($project\_no, $desc, $manager\_no, $type, $sd, $ed);

}

//cleans values from the user input

function cleanData($data)

{

    $data = trim($data);

    $data = stripslashes($data);

    $data = trim($data);

    $data = htmlspecialchars($data);

    $data = strip\_tags($data);

    return $data;

}

function addproject($project, $desc, $manager, $type, $sd, $ed){

    $PageTitle = "Add a project";

    //Page header

    print<<<HERE

    <html>

        <body>

    HERE;

    include("myDB.php");

    include("PageFrame.php");

    $query = "SELECT \* FROM project WHERE `project#`='$project'";

    $row1 = mysqli\_num\_rows(mysqli\_query($myDB, $query));

    $query = "SELECT \* FROM manager WHERE `project#`='$project'";

    $row2 = mysqli\_num\_rows(mysqli\_query($myDB, $query));

    if ($row1 > 0 || $row1 != $row2){

        print "<h1>manager does not exist or already added..</h1>";

    }

    else{

        $query = "INSERT INTO project (`project#`, `description`, `manager#`, `type`, `Sdate`, `Edate`) VALUES ('$project', '$desc', '$manager', '$type', '$sd', '$ed')";

        mysqli\_query($myDB, $query);

        print<<<HERE

        <h1>New project Has Been Added!</h1>

        <table class="brdr">

            <tr class="brdr">

            <th class="brdr">project no</th>

            <th class="brdr">description</th>

            <th class="brdr">manager no</th>

            <th class="brdr">type</th>

            <th class="brdr">start date</th>

            <th class="brdr">end date</th>

            </tr>

            <tr class="brdr">

                <td class="brdr">$project</td>

                <td class="brdr">$desc</td>

                <td class="brdr">$manager</td>

                <td class="brdr">$type</td>

                <td class="brdr">$sd</td>

                <td class="brdr">$ed</td>

            </tr>

        </table>

        HERE;

    }

    print<<<HERE

    </body>

        </html>

    HERE;

}

?>

Managerform.php:

<?php

$PageTitle = "Add manager";

include("PageFrame.php");

?>

<html>

<body>

    <!-- Form to add a new book -->

    <form method="post" action="addmanager.php">

        <h1>Add a new manager</h1>

        <table>

            <tr>

                <td>manager no</td>

                <td><input type="text" name="manager\_no"></td>

            </tr>

            <tr>

                <td>name</td>

                <td><input type="text" name="name"></td>

            </tr>

            <tr>

                <td>experience</td>

                <td><input type="text" name="exp"></td>

            </tr>

            <tr>

                <td>nationality</td>

                <td><input type="text" name="nat"></td>

            </tr>

            <tr>

                <td>phone number</td>

                <td><input type="text" name="pn"></td>

            </tr>

            <tr>

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

            </tr>

        </table>

    </form>

</body>

</html>

Projectform.php:

<?php

$PageTitle = "Add manager";

include("PageFrame.php");

?>

<html>

<body>

    <!-- Form to add a new book -->

    <form method="post" action="AddBook.php">

        <h1>Add a new manager</h1>

        <table>

            <tr>

                <td>project no</td>

                <td><input type="text" name="project\_no"></td>

            </tr>

            <tr>

                <td>description</td>

                <td><input type="text" name="desc"></td>

            </tr>

            <tr>

                <td>manager\_no</td>

                <td><input type="text" name="manager\_no"></td>

            </tr>

            <tr>

                <td>type</td>

                <td><input type="text" name="type"></td>

            </tr>

            <tr>

                <td>start date</td>

                <td><input type="text" name="sd"></td>

            </tr>

            <tr>

                <td>end date</td>

                <td><input type="text" name="ed"></td>

            </tr>

            <tr>

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

            </tr>

        </table>

    </form>

</body>

</html>

Index\_1.php:

<?php

$PageTitle = "Home Page";

include("PageFrame.php");

include("myDB.php");

$query = "SELECT \* FROM manager";

$Result = mysqli\_query($myDB, $query); //executes the query in the mysql server

print <<<HERE

<html>

<body>

<h1>manager table</h1>

<table class="brdr">

    <tr class="brdr">

        <th class="brdr">manager no</th>

        <th class="brdr">name</th>

        <th class="brdr">experience</th>

        <th class="brdr">nationality</th>

        <th class="brdr">phone number</th>

    </tr>

HERE;

while ($Row = mysqli\_fetch\_assoc($Result)){

    $manager = $Row["manager#"];

    $name = $Row["name"];

    $exp = $Row["experience"];

    $nat = $Row["nationality"];

    $pn = $Row["phone#"];

    print<<<HERE

    <tr class="brdr">

        <td class="brdr">$manager</td>

        <td class="brdr">$name</td>

        <td class="brdr">$exp</td>

        <td class="brdr">$nat</td>

        <td class="brdr">$pn</td>

    </tr>

    HERE;

}

print <<<HERE

</table>

<h1>project table</h1>

<table class="brdr">

    <tr class="brdr">

        <th class="brdr"></th>

        <th class="brdr"></th>

        <th class="brdr"></th>

        <th class="brdr"></th>

        <th class="brdr"></th>

    </tr>

HERE;

$query = "SELECT \* FROM project";

$Result = mysqli\_query($myDB, $query);

while ($Row = mysqli\_fetch\_assoc($Result)){

    $project = $Row["project#"];

    $manager = $Row["manager#"];

    $desc = $Row["description"];

    $type = $Row["type"];

    $sd = $Row["Sdate"];

    $ed = $Row["Edate"];

    print<<<HERE

    <tr class="brdr">

        <td class="brdr">$project</td>

        <td class="brdr">$desc</td>

        <td class="brdr">$manager</td>

        <td class="brdr">$type</td>

        <td class="brdr">$sd</td>

        <td class="brdr">$ed</td>

    </tr>

    HERE;

}

print <<<HERE

        </table>

    </body>

</html>

HERE;

?>

myDB.php:

<?php

/\* my DB information \*/

$DB\_NAME = "epiz\_33048164\_construction";

$USERNAME = "epiz\_33048164";

$PASSWORD = "fD3cwdZr34";

$HOST = "sql305.epizy.com";

$myDB = mysqli\_connect($HOST, $USERNAME, $PASSWORD, $DB\_NAME); //Connect to the DB

//Checks if there is an error with connecting to the DB

if (mysqli\_connect\_errno()) {

    echo "Connection Failed: " . mysqli\_connect\_error();

    exit(1);

}

?>

Pageframe.php:

<?php

//Name: Ghazi Najeeb Al-Abbar

//ID: 2181148914

//Assignment 4

//Filename: PageFrame.php

?>

<!DOCTYPE html>

<html>

<head>

    <meta charset='utf-8'>

    <title>

        <?php print $PageTitle ?>

    </title>

    <?php

    include("Styles.php");

    ?>

</head>

<!-- Page header for all pages -->

<body style="margin-bottom: 50px">

    <nav>

        <ul>

            <li><a href="index\_1.php">Home</a></li>

            <li><a href="addmanager.php">Add manager</a></li>

            <li><a href="addproject.php">add project</a></li>

            <li><a href="question\_c.php">question c</a></li>

            <li><a href="question\_d.php">question d</a></li>

        </ul>

    </nav>

</body>

</html>

Question\_c.php:

<?php

include("PageFrame.php");

$query = "SELECT Employee\_No, Role, Nationality FROM Employee";

$Result = mysqli\_query($myDB, $query);

?>

<body>

    <h1> Employee Number, Role and Nationality from the Employee Table</h1>

    <table>

        <tr>

            <th>manager#</th>

            <th>experience</th>

            <th>Nationality</th>

        </tr>

        <?php

                while ($Rows = mysqli\_fetch\_assoc($Result)){

                    $manager = $Rows["manager#"];

                    $exp = $Rows["experience"];

                    $Nationality = $Rows["nationality"];

                    print<<<HERE

                    <tr>

                        <td>$manager</td>

                        <td>$exp</td>

                        <td>$Nationality</td>

                    </tr>

                    HERE;

                }

            ?>

    </table>

</body>

</html>

Question\_d.php:

<?php

include("PageFrame.php");

include("myDataBase.php");

$query = "SELECT

manager.name,

manager.nationality,

project.type,

project.description,

project.Sdate,

project.Edate

FROM

manager

INNER JOIN project ON `manager.manager#`=`project.manager#`

WHERE

project.Sdate > '1-1-2023'

AND project.Edate < '12-31-2028'";

$Result = mysqli\_query($myDB, $query);

?>

<table>

    <tr>

        <th>name</th>

        <th>Nationality</th>

        <th>Description</th>

        <th>type</th>

        <th>start date</th>

        <th>end date</th>

    </tr>

    <?php

                while ($Rows = mysqli\_fetch\_assoc($Result)){

                    $Name = $Rows["name"];

                    $Nationality = $Rows["nationality"];

                    $Desc = $Rows["Description"];

                    $type = $Rows["type"];

                    $sd = $Rows["Sdate"];

                    $ed = $Rows["Edate"];

                    print<<<HERE

                    <tr>

                        <td>$Name</td>

                        <td>$Nationality</td>

                        <td>$Desc</td>

                        <td>$type</td>

                        <td>$sd</td>

                        <td>$ed</td>

                    </tr>

                    HERE;

                }

            ?>

</table>

</body>

</html>

