



**CHARUSAT
CSPIT, FTE**
*Smt. Kundanben Dinsha Patel Department of
Information Technology*



Practical No: 01

AIM:

Installation and configuration of Servers, Create PHP script for User's Profile registration form (Include the entire necessary HTML controls) and Display your information in HTML table format on new PHP page.

Take reference of first practical and apply validation using PHP to increase consistency of information submitted. (Validate Mobile No, Phone Number, email id, password with rules.)

Take reference of first practical and apply SQL injection on it. Create two different .php files to demonstrate importance of SQL injection (one without filters and second with filters).

Solution:

This practical has the following contents:

1.0 File Structure

- |— www/
- |— registration form/
- |— registration.php
- |— registration.css
- |— putdata.php
- |— login.php
- |— loginphp.php
- |— getdata.php
- |— persons.sql
- |— css/
- |— fonts/
- |— images/

2.0 Database

2.1 Database Tables

username	email	phone	password
rj15	rj@gamil.com	1234554400	123
saumil	saumil24@gmail.com	4567890123	4567
ram	ram13@gmail.com	2345678901	2345
ronak	ronak12@gmail.com	3456789012	3456

2.2 Database Schema

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
<input type="checkbox"/> 1	username	varchar(50)	latin1_swedish_ci		No	None			Change Drop More
<input type="checkbox"/> 2	email	varchar(50)	latin1_swedish_ci		No	None			Change Drop More
<input type="checkbox"/> 3	phone	varchar(50)	latin1_swedish_ci		No	None			Change Drop More
<input type="checkbox"/> 4	password	varchar(50)	latin1_swedish_ci		No	None			Change Drop More

3.0 Layout Files

registration.php

```

<link href="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/css/bootstrap.min.css" rel="stylesheet"
id="bootstrap-css">
<script src="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/js/bootstrap.min.js"></script>
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
<!-- Include the above in your HEAD tag -->
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
  <link rel="dns-prefetch" href="https://fonts.gstatic.com">
  <link href="https://fonts.googleapis.com/css?family=Raleway:300,400,600" rel="stylesheet"
type="text/css">
  <link rel="icon" href="Favicon.png">

```

```

    <link rel="stylesheet"
href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/bootstrap.min.css">
    <title>Laravel</title>
</head>
<body>
<?php
    session_start();
    $username = isset($_POST['username'])?$_POST['username']:"";
    $email = isset($_POST['email'])?$_POST['email']:"";
    $phone = isset($_POST['phone'])?$_POST['phone']:"";
    $password = isset($_POST['password'])?$_POST['password']:"";
    $confirm_password = isset($_POST['confirm_password'])?$_POST['confirm_password']:"";
    $error = "All the fields are required";
    if(!empty($_POST['Register'])){
        if(!preg_match('/^[a-zA-Z][a-zA-Z0-9-_.]{1,20}$/', $username)){
            $error = 'user name contain 2-20 characters';
        }
        elseif(!filter_var($email,FILTER_VALIDATE_EMAIL,FILTER_SANITIZE_EMAIL)){
            $error = 'entered email is invalide';
        }
        elseif(!preg_match('/^(?:0|(?\+33)\)?s?|0033?s?)[1-79](?:[\.\-\\s]?d\d){4}$/', $phone) &&
!filter_var($phone,FILTER_VALIDATE_INT)) {
            $error = 'entered phone number is invalide';
        }
        elseif($password != $confirm_password) {
            $error = 'entered password do not match';
        }
        else{
            $_SESSION['username'] = $username;
            $_SESSION['email'] = $email;
            $_SESSION['phone'] = $phone;
            $_SESSION['password'] = $password;
            $_SESSION['confirm_password'] = $confirm_password;
            header("Location: putdata.php");
        }
    }
?>
<nav class="navbar navbar-expand-lg navbar-light navbar-laravel">
    <div class="container">
        <button class="navbar-toggler" type="button" data-toggle="collapse" data-
target="#navbarSupportedContent" aria-controls="navbarSupportedContent" aria-expanded="false"
aria-label="Toggle navigation">
            <span class="navbar-toggler-icon"></span>
        </button>
    </div>
</nav>
<main class="my-form">

```

```

<div class="container">
  <div class="row justify-content-center">
    <div class="col-md-5">
      <div class="card">
        <div class="card-header"><center>Register</center></div>
        <div class="card-body">
          <form name="my-form" method="POST">
            <?php if(!empty($error)) { ?>
              <div class="form-group row col-form-label" style=" margin-left: 80px; width:
300px; align-items: center; color: red;"><?php if(isset($error)) echo $error; ?> </div>
              <?php } ?>
              <div class="form-group row">
                <label class="col-md-4 col-form-label text-md-right">Username</label>
                <div class="col-md-6">
                  <input type="text" class="form-control" name="username" required>
                </div>
              </div>
              <div class="form-group row">
                <label class="col-md-4 col-form-label text-md-right">E-Mail Address</label>
                <div class="col-md-6">
                  <input type="text" class="form-control" name="email" required>
                </div>
              </div>
              <div class="form-group row">
                <label class="col-md-4 col-form-label text-md-right">Phone Number</label>
                <div class="col-md-6">
                  <input type="text" class="form-control" name="phone" required>
                </div>
              </div>
              <div class="form-group row">
                <label class="col-md-4 col-form-label text-md-right">Password</label>
                <div class="col-md-6">
                  <input type="password" class="form-control" name="password" required>
                </div>
              </div>
              <div class="form-group row">
                <label class="col-md-4 col-form-label text-md-right">Confirm Password</label>
                <div class="col-md-6">
                  <input type="password" class="form-control" name="confirm_password"
required>
                </div>
              </div>
              <div class="col-md-6 offset-md-4">
                <input type="submit" class="btn btn-primary" value="Register"
name="Register" />
            </div>
          </form>
        </div>
      </div>
    </div>
  </div>
</div>

```



```
.my-form .row
{
    margin-left: 0;
    margin-right: 0;
}
.login-form
{
    padding-top: 1.5rem;
    padding-bottom: 1.5rem;
}
.login-form .row
{
    margin-left: 0;
    margin-right: 0;
}
```

login.php

```
<!DOCTYPE html>
<html lang="en">
<head>
<title>Login V19</title>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="icon" type="image/png" href="images/icons/favicon.ico"/>
<link rel="stylesheet" type="text/css" href="vendor/bootstrap/css/bootstrap.min.css">
<link rel="stylesheet" type="text/css" href="fonts/font-awesome-4.7.0/css/font-awesome.min.css">
<link rel="stylesheet" type="text/css" href="fonts/Linearicons-Free-v1.0.0/icon-font.min.css">
<link rel="stylesheet" type="text/css" href="vendor/animate/animate.css">
<link rel="stylesheet" type="text/css" href="vendor/css-hamburgers/hamburgers.min.css">
<link rel="stylesheet" type="text/css" href="vendor/animstition/css/animstition.min.css">
<link rel="stylesheet" type="text/css" href="vendor/select2/select2.min.css">
<link rel="stylesheet" type="text/css" href="vendor/daterangepicker/daterangepicker.css">
<link rel="stylesheet" type="text/css" href="css/util.css">
<link rel="stylesheet" type="text/css" href="css/main.css">
</head>
<?php
session_start();
$error = isset($_GET['error'])?$_GET['error']:"";
?>
<body>
<div class="limiter">
    <div class="container-login100">
        <div class="wrap-login100 p-l-55 p-r-55 p-t-65 p-b-50">
            <form class="login100-form validate-form" method="POST"
action="loginphp.php">
                <span class="login100-form-title p-b-33" >
```

```

        Account Login
    </span>

    <div class="wrap-input100 validate-input" >
        <input class="input100" type="text" name="email"
placeholder="Email" required>
        <span class="focus-input100-1"></span>
        <span class="focus-input100-2"></span>
    </div>
    <br>

    <div class="wrap-input100 validate-input" >
        <input class="input100" type="password" name="password"
placeholder="Password" required>
        <span class="focus-input100-1"></span>
        <span class="focus-input100-2"></span>
    </div>
    <br>
    <?php if(!empty($error)) { ?>
        <div class="wrap-input100" style=" margin-left: 40px; width: 300px; color: red;"><?php
if(isset($error)) echo $error; ?>
        </div>
        <?php } ?>
        <div class="container-login100-form-btn m-t-20">
            <input type="submit" class="login100-form-btn" value="Sign in"
name="Sign in" />

            </div>
            <br>
            <div class="text-center">
                <span class="txt1">
                    Create an account?
                </span>

                <a href="registration.php" class="txt2 hov1">
                    Sign up
                </a>
            </div>
        </form>
    </div>
</div>
</body>
</html>

```

4.0 Processing Files

putdata.php

```
<?php
```

```
session_start();
$username = $_SESSION['username'];
$email = $_SESSION['email'];
$phone = $_SESSION['phone'];
$password = $_SESSION['password'];
$confirm_password = $_SESSION['confirm_password'];
$con = mysqli_connect("localhost", "root", "", "demo");

// Check connection
if($con === false){
    die("ERROR: Could not connect. " . mysqli_connect_error());
}

// Escape user inputs for security
echo $username." ".$email." ".$phone;
// Attempt insert query execution
$sql = "INSERT INTO persons (username, email, phone, password) VALUES ('$username', '$email', '$phone', '$password')";
if(mysqli_query($con, $sql)){
    echo "Records added successfully.";
    header("Location: login.php");
    exit($con);
} else{
    echo "ERROR: Could not able to execute $sql. " . mysqli_error($con);
}
mysqli_close($con);
?>
```

loginphp.php

```
<?php
```

```
$con = mysqli_connect("localhost", "root", "", "demo");
$email = $_POST['email'];
$password = $_POST['password'];
$error = "Please enter valide email and password";
if($con === false){
    die("ERROR: Could not connect. " . mysqli_connect_error());
}
$sql = "SELECT * FROM persons WHERE email = ".$email." AND password = ".$password."";
$res = mysqli_query($con,$sql);
if(mysqli_num_rows($res)>0){
    while($row=mysqli_fetch_assoc($res)){
        if($row["password"] == $password && $row["email"] == $email){
            header("Location: getdata.php"); $ser=1; break;}
    }
}
```



```

        }
    }
    if($er == 0){
        header("Location: login.php?error=$error");
    }
    mysqli_close($con);
    exit();
?>

```

getdata.php

```

<html>
<head>
<style>
table
{
border-style:solid;
border-width:2px;
border-color: black;
}
</style>
</head>
<body>
<?php
$con = mysqli_connect("localhost","root","","demo");
if($con === false){
    die("ERROR: Could not connect. " . mysqli_connect_error());
}
$sql = "SELECT * from persons";
$result = mysqli_query($con,$sql);
echo "<table border='1'>
<tr>
<th>name</th>
<th>email</th>
<th>phone</th>
</tr>";
while($row = mysqli_fetch_array($result))
{
    echo "<tr>";
    echo "<td>" . $row['username'] . "</td>";
    echo "<td>" . $row['email'] . "</td>";
    echo "<td>" . $row['phone'] . "</td>";
    echo "</tr>";
}
echo "</table>";
mysqli_close($con);
?>
<a href="login.php">back to login</a>

```

```
</body>
</html>
<?php
?>
```

5.0 Output

Register

All the fields are required

Username

E-Mail Address

Phone Number

Password

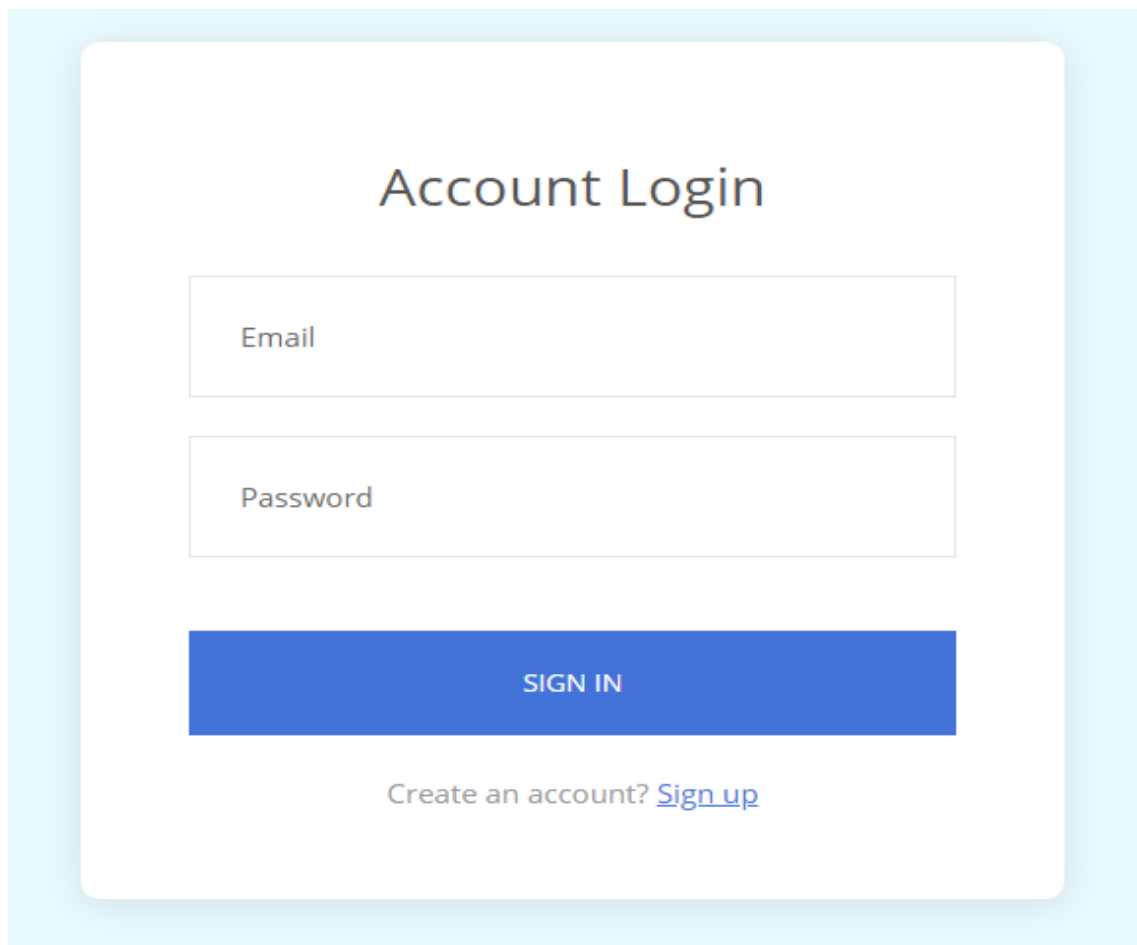
Confirm Password

Register

Go to account? [Login](#)

Description:

First new user needs to enter his/her detail into the registration form for to create his/her account. For all field there is apply validation using PHP to increase consistency of information submitted. (Validate Mobile No, Phone Number, email id, password with rules.)

A screenshot of a web form titled "Account Login". The form is centered on a light blue background. It contains two input fields: "Email" and "Password", both with placeholder text. Below these fields is a blue button labeled "SIGN IN". At the bottom of the form, there is a link that says "Create an account? [Sign up](#)".

Account Login

SIGN IN

Create an account? [Sign up](#)

Description:

After creation of new account user need to login into his account to enter the next page if user have already account then he/she need to directly login into his/her account. For given fields there is applied SQL injection on it.

name	email	phone
rj15	rj@gamil.com	1234554400
saumil	saumil24@gmail.com	4567890123
ram	ram13@gmail.com	2345678901
ronak	ronak12@gmail.com	3456789012

[back to login](#)

Description:

Here when user login successfully then there is all data will fetch from the database to show him.

Practical No: 02

AIM:

Create small application of PHP shopping cart using SESSIONS and MySQL database. (Use provided reference tutorial file).

Solution:

This practical has the following contents:

1.0 File Structure

```

|— www/
|— tblproduct/
|——index.php
|——style.css
|——dbcontroller.php
|——shopping_cart.php
|——tblproduct.sql
|—— product-images/
  
```

2.0 Database

2.1 Database Tables

				id	name	code	image	price
<input type="checkbox"/>				1	Pro 3D Camera	3DcAM01	product-images/camera.jpg	20000.00
<input type="checkbox"/>				2	Portable Hard Drive	USB02	product-images/external-hard-drive.jpg	2000.00
<input type="checkbox"/>				3	Wrist Watch	wristWear03	product-images/watch.jpg	5000.00
<input type="checkbox"/>				4	Intel Core Laptop	LPN45	product-images/laptop.jpg	80000.00
<input type="checkbox"/>				5	Laptop Bag	BAG406LP	product-images/bag.jpg	800.00
<input type="checkbox"/>				6	EPSON Printer	EP2S400	product-images/printer.jpg	15000.00
<input type="checkbox"/>				7	hp Desktop	HP3455DS	product-images/computer.jpg	50000.00
<input type="checkbox"/>				8	MI Smart Watch	MI400SMW	product-images/smartwatch.jpg	7000.00
<input type="checkbox"/>				9	Apple Smart Phone	I804PN	product-images/smartphone.jpg	70000.00

2.2 Database Schema

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id	int(8)			No	None		AUTO_INCREMENT	Change Drop More
2	name	varchar(255)	latin1_swedish_ci		No	None			Change Drop More
3	code	varchar(255)	latin1_swedish_ci		No	None			Change Drop More
4	image	text	latin1_swedish_ci		No	None			Change Drop More
5	price	double(10,2)			No	None			Change Drop More

3.0 Layout Files

index.php

```

<?php
session_start();
require_once("dbcontroller.php");
$db_handle = new DBController();
if(!empty($_GET["action"])) {
switch($_GET["action"]) {
    case "add":
        if(!empty($_POST["quantity"])) {
            $productByCode = $db_handle->runQuery("SELECT * FROM tblproduct WHERE
code=" . $_GET["code"] . "");
            $itemArray =
array($productByCode[0]["code"]=>array('name'=>$productByCode[0]["name"],
'code'=>$productByCode[0]["code"], 'quantity'=>$_POST["quantity"],
'price'=>$productByCode[0]["price"], 'image'=>$productByCode[0]["image"]));

            if(!empty($_SESSION["cart_item"])) {
                if(in_array($productByCode[0]["code"],array_keys($_SESSION["cart_item"]))) {
                    foreach($_SESSION["cart_item"] as $k => $v) {
                        if($productByCode[0]["code"] == $k) {

                            if(empty($_SESSION["cart_item"][$k]["quantity"])) {
                                $_SESSION["cart_item"][$k]["quantity"] = 0;
                            }
                            $_SESSION["cart_item"][$k]["quantity"]+=

```

```

    }
        }
    } else {
        $_SESSION["cart_item"] =
array_merge($_SESSION["cart_item"], $itemArray);
    }
    } else {
        $_SESSION["cart_item"] = $itemArray;
    }
    }
    break;
    case "remove":
        if(!empty($_SESSION["cart_item"])) {
            foreach($_SESSION["cart_item"] as $k => $v) {
                if($_GET["code"] == $k)
                    unset($_SESSION["cart_item"][$k]);

                if(empty($_SESSION["cart_item"]))
                    unset($_SESSION["cart_item"]);
            }
        }
        break;

    case "empty":
        unset($_SESSION["cart_item"]);
        break;
    }
}
?>
<HTML>
<HEAD>
<TITLE>Simple PHP Shopping Cart</TITLE>
<link href="style.css" type="text/css" rel="stylesheet" />
<style>
#btnlink {
    background-color: #ffffff;
    border: #00b2e9 1px solid;
    padding: 5px 10px;
    color: #00b2e9;
    float: right;
    text-decoration: none;
    border-radius: 3px;
    margin: 10px 0px;
}
#btnlink:hover {

```

```

background-color: #00b2e9;
border: #00b2e9 1px solid;
padding: 5px 10px;
color: #ffffff;
float: right;
text-decoration: none;
border-radius: 3px;
margin: 10px 0px;
}

.txt-heading {
color: #211a1a;
border-bottom: 3px solid #E0E0E0;
overflow: auto;
font-weight: 600;
font-size: 20px;
}

.product-item {
float: left;
background: #ffffff;
margin: 30px 20px 0px 30px;
border: #E0E0E0 1px solid;
}
</style>
</HEAD>
<BODY>

<div id="shopping-cart">
<a id="btnlink" href="shopping_cart.php">Go to Cart</a>
</div>
<br>

<div id="product-grid">
<div class="txt-heading">Products</div>
<?php
$product_array = $db_handle->runQuery("SELECT * FROM tblproduct ORDER BY id ASC");
if (!empty($product_array)) {
    foreach($product_array as $key=>$value){
        ?>
        <div class="product-item">
            <form method="post" action="index.php?action=add&code=<?php echo
$product_array[$key]["code"]; ?>">

```

```

?>"></div>
    <div class="product-image">
    <div class="product-title"><?php echo $product_array[$key]["name"]; ?></div>
    <div class="product-price"><?php echo "$".$product_array[$key]["price"]; ?></div>
    <div class="cart-action">
        <input type="text" class="product-quantity" name="quantity" value="1"
size="2" />
        <input type="submit" value="Add to Cart" class="btnAddAction" ></div>
    </div>
    </form>
</div>
<?php
    }
}
?>
</div>
</BODY>
</HTML>

```

style.css

```

body {
    font-family: Arial;
    color: #211a1a;
    font-size: 0.9em;
}
#shopping-cart {
    margin: 40px;
}
#product-grid {
    margin: 40px;
}
#shopping-cart table {
    width: 100%;
    background-color: #F0F0F0;
    background-color: rgb(145, 145, 145);
}
#shopping-cart table td {
    background-color: #FFFFFF;
}
.txt-heading {
    color: #211a1a;
    border-bottom: 1px solid #E0E0E0;
    overflow: auto;
}

```



```
    font-size: 60px;
}
#btnEmpty {
    background-color: #ffffff;
    border: #d00000 1px solid;
    padding: 5px 10px;
    color: #d00000;
    float: right;
    text-decoration: none;
    border-radius: 3px;
    margin: 10px 0px;
}
.btnAddAction {
    padding: 5px 10px;
    margin-left: 5px;
    background-color: #efefef;
    border: #E0E0E0 1px solid;
    color: #211a1a;
    float: right;
    text-decoration: none;
    border-radius: 3px;
    cursor: pointer;
}
#product-grid .txt-heading {
    margin-bottom: 18px;
}
.product-item {
    float: left;
    background: #ffffff;
    margin: 30px 30px 0px 0px;
    border: #E0E0E0 1px solid;
}
.product-image {
    height: 155px;
    width: 250px;
    background-color: #FFF;
}
.clear-float {
    clear: both;
}
.demo-input-box {
    border-radius: 2px;
    border: #CCC 1px solid;
    padding: 2px 1px;
```

```
}
.tbl-cart {
    font-size: 0.9em;
}
.tbl-cart th {
    font-weight: normal;
}
.product-title {
    margin-bottom: 20px;
}
.product-price {
    float:left;
}
.cart-action {
    float: right;
}
.product-quantity {
    padding: 5px 10px;
    border-radius: 3px;
    border: #E0E0E0 1px solid;
}
.product-tile-footer {
    padding: 15px 15px 0px 15px;
    overflow: auto;
}
.cart-item-image {
    width: 30px;
    height: 30px;
    border-radius: 50%;
    border: #E0E0E0 1px solid;
    padding: 5px;
    vertical-align: middle;
    margin-right: 15px;
}
.no-records {
    text-align: center;
    clear: both;
    margin: 38px 0px;
}
```

shopping_cart.php

```
<?php
session_start();
require_once("dbcontroller.php");
```

```

$db_handle = new DBController();
if(!empty($_GET["action"])) {
switch($_GET["action"]) {
    case "add":
        if(!empty($_POST["quantity"])) {
            $productByCode = $db_handle->runQuery("SELECT * FROM tblproduct WHERE
code=" . $_GET["code"] . "");
            $itemArray =
array($productByCode[0]["code"]=>array('name'=>$productByCode[0]["name"],
'code'=>$productByCode[0]["code"], 'quantity'=>$_POST["quantity"],
'price'=>$productByCode[0]["price"], 'image'=>$productByCode[0]["image"]));

            if(!empty($_SESSION["cart_item"])) {
                if(in_array($productByCode[0]["code"],array_keys($_SESSION["cart_item"]))) {
                    foreach($_SESSION["cart_item"] as $k => $v) {
                        if($productByCode[0]["code"] == $k) {

                            if(empty($_SESSION["cart_item"][$k]["quantity"])) {

                                $_SESSION["cart_item"][$k]["quantity"] = 0;
                            }
                            $_SESSION["cart_item"][$k]["quantity"] +=
$_POST["quantity"];

                        }
                    }
                } else {
                    $_SESSION["cart_item"] =
array_merge($_SESSION["cart_item"],$itemArray);
                }
            } else {
                $_SESSION["cart_item"] = $itemArray;
            }
        }
        break;
    case "remove":
        if(!empty($_SESSION["cart_item"])) {
            foreach($_SESSION["cart_item"] as $k => $v) {
                if($_GET["code"] == $k)
                    unset($_SESSION["cart_item"][$k]);
                if(empty($_SESSION["cart_item"]))
                    unset($_SESSION["cart_item"]);
            }
        }
        break;
}
}

```

```
        case "empty":
            unset($_SESSION["cart_item"]);
        break;
    }
}
?>
<HTML>
<HEAD>
<TITLE>Simple PHP Shopping Cart</TITLE>
<link href="style.css" type="text/css" rel="stylesheet" />
<style>
#btnlink {
    background-color: #ffffff;
    border: #00b2e9 1px solid;
    padding: 5px 10px;
    color: #00b2e9;
    float: right;
    text-decoration: none;
    border-radius: 3px;
    margin: 10px 0px;
}
#btnlink:hover {
    background-color: #00b2e9;
    border: #00b2e9 1px solid;
    padding: 5px 10px;
    color: #ffffff;
    float: right;
    text-decoration: none;
    border-radius: 3px;
    margin: 10px 0px;
}
#shopping-cart table {
    width: 100%;
    background-color: rgb(145, 145, 145);
}
#shopping-cart table tr {
    background-color: rgb(145, 145, 145);
    color: #ffffff;
}
#shopping-cart table td {
    background-color: #FFFFFF;
    color: #000000;
}
#btnEmpty:hover {
```

```

background-color: #d00000;
border: #d00000 1px solid;
padding: 5px 10px;
color: #ffffff;
float: right;
text-decoration: none;
border-radius: 3px;
margin: 10px 0px;
}
.txt-heading {
color: #211a1a;
border-bottom: 3px solid #E0E0E0;
overflow: auto;
font-weight: 600;
font-size: 20px;
}
</style>
</HEAD>
<BODY>
<div id="shopping-cart">
<a id="btnlink" href="index.php">Back to Products</a>
</div>
<br>

<div id="shopping-cart">
<div class="txt-heading">Shopping Cart</div>

<a id="btnEmpty" href="shopping_cart.php?action=empty">Empty Cart</a>
<?php
if(isset($_SESSION["cart_item"])){
    $total_quantity = 0;
    $total_price = 0;
?>
<table cellpadding="10" cellspacing="1">
<tbody>
<tr>
<th style="text-align:center;">Name</th>
<th style="text-align:center;">Code</th>
<th style="text-align:center;" width="5%">Quantity</th>
<th style="text-align:center;" width="10%">Unit Price</th>
<th style="text-align:center;" width="10%">Price</th>
<th style="text-align:center;" width="5%">Remove</th>
</tr>
<?php

```

```

foreach ($_SESSION["cart_item"] as $item){
    $item_price = $item["quantity"]*$item["price"];
    ?>

        <tr>
        <td style="text-align:center;"><?php echo $item["name"]; ?></td>
        <td style="text-align:center;"><?php echo $item["code"]; ?></td>
        <td style="text-align:right;"><?php echo $item["quantity"]; ?></td>
        <td style="text-align:right;"><?php echo " ". $item["price"]; ?></td>
        <td style="text-align:right;"><?php echo " ". number_format($item_price,2);
?></td>

        <td style="text-align:center;"><a
href="shopping_cart.php?action=remove&code=<?php echo $item["code"]; ?>"
class="btnRemoveAction" id="btnEmpty">Remove</a></td>
        </tr>
        <?php
        $total_quantity += $item["quantity"];
        $total_price += ($item["price"]*$item["quantity"]);
    }
    ?>

<tr>
<td colspan="2" align="right">Total:</td>
<td align="right"><?php echo $total_quantity; ?></td>
<td align="right" colspan="2"><strong><?php echo " ".number_format($total_price, 2);
?></strong></td>
<td></td>
</tr>
</tbody>
</table>
    <?php
    } else {
    ?>
    <div class="no-records">Your Cart is Empty</div>
    <?php
    }
    ?>
    </div>
</BODY>
</HTML>

```

4.0 Processing Files

dbcontroller.php

```

<?php
class DBController {
    private $host = "localhost";

```

```









private $user = "root";
private $password = "";
private $database = "blog_samples";
private $conn;
function __construct() {
    $this->conn = $this->connectDB();
}
function connectDB() {
    $conn = mysqli_connect($this->host,$this->user,$this->password,$this->database);
    return $conn;
}
function runQuery($query) {
    $result = mysqli_query($this->conn,$query);
    while($row=mysqli_fetch_assoc($result)) {
        $resultset[] = $row;
    }
    if(!empty($resultset))
        return $resultset;
}
function numRows($query) {
    $result = mysqli_query($this->conn,$query);
    $rowcount = mysqli_num_rows($result);
    return $rowcount;
}
}
?>

```

5.0 Output

[Go to Cart](#)

Products

 <p>Pro 3D Camera</p> <p>\$20000.00 <input type="text" value="1"/> Add to Cart</p>	 <p>Portable Hard Drive</p> <p>\$2000.00 <input type="text" value="1"/> Add to Cart</p>	 <p>Wrist Watch</p> <p>\$5000.00 <input type="text" value="1"/> Add to Cart</p>	 <p>Intel Core Laptop</p> <p>\$80000.00 <input type="text" value="1"/> Add to Cart</p>
 <p>Laptop Bag</p> <p>\$800.00 <input type="text" value="1"/> Add to Cart</p>	 <p>EPSON Printer</p> <p>\$15000.00 <input type="text" value="1"/> Add to Cart</p>	 <p>hp Desktop</p> <p>\$50000.00 <input type="text" value="1"/> Add to Cart</p>	 <p>MI Smart Watch</p> <p>\$7000.00 <input type="text" value="1"/> Add to Cart</p>

Description:

Here is the Shopping cart module with session in this above is the first part of application which is product selection.

[Back to Products](#)
Shopping Cart
[Empty Cart](#)

Name	Code	Quantity	Unit Price	Price	Remove
Pro 3D Camera	3DcAM01	1	20000.00	20,000.00	Remove
Portable Hard Drive	USB02	2	2000.00	4,000.00	Remove
Wrist Watch	wristWear03	3	5000.00	15,000.00	Remove
Intel Core Laptop	LPN45	1	80000.00	80,000.00	Remove
MI Smart Watch	MI400SMW	2	7000.00	14,000.00	Remove
Total:		9		133,000.00	

Description:

Here is the Shopping cart application with session in this above is the second part of application which is cart of selected items with price and total cost of the all products.

Practical No: 03

AIM :

Take reference of first practical and apply validation using PHP to increase consistency of information submitted. (Validate Mobile No, Phone Number, email id, password with rules.)

Registration validation :

<?php

```
$nameErr=$userErr=$emailErr=$pwordErr=$cwordErr=$connoErr="";
$name=$user=$email=$pword=$cword=$conno="";

if($_SERVER["REQUEST_METHOD"]=="POST"){
    if(empty($_POST["name"])){
        $nameErr = "*Enter Name.<br>";
    }
    else{
        $name = test_input($_POST["name"]);
        if(!preg_match("/^[a-zA-Z ]+$/",$name)){
            $nameErr = "*Only letters allowed.<br>";
        }
    }

    if(empty($_POST["user"])){
        $userErr = "*Enter Username.<br>";
    }
    else{
        $user = test_input($_POST["user"]);
        if(!preg_match("/^[a-zA-Z0-9_-]{3,15}$/",$user)){
            $userErr = "*Only letters, numbers and special characters('_-') allowed.<br>";
        }
    }

    if(empty($_POST["email"])){
        $emailErr = "*Enter Email Id.<br>";
    }
    else{
        $email = test_input($_POST["email"]);
        if(filter_var($email, FILTER_VALIDATE_EMAIL) === false){
            $emailErr = "*Enter Valid Email Id.<br>";
        }
    }

    if(empty($_POST["pword"])){
        $pwordErr = "*Enter Password.<br>";
    }
    else{
        $pword = test_input($_POST["pword"]);
        if(!preg_match("/^[a-zA-Z0-9_@-]{8,15}$/",$pword)){
            $pwordErr = "*Only letters, numbers and special characters('@_-') allowed.<br>";
        }
    }
}
```

```

    }
}

if(empty($_POST["cword"])){
    $swordErr = "*Enter Password.<br>";
}
else{
    $sword = test_input($_POST["cword"]);
}

if($_POST["pword"]!= $_POST["cword"]){
    $swordErr = "*Password don't match.<br>";
}

if(empty($_POST["conno"])){
    $connoErr = "*Enter Contact Number.<br>";
}
else{
    $conno = test_input($_POST["conno"]);
    if(!preg_match("/^[0-9]{10}$/", $conno)){
        $connoErr = "*Only 10 Digits Allowed.<br>";
    }
}

if($nameErr==" && $userErr==" && $emailErr==" && $pwordErr==" && $swordErr==" &&
$connoErr==""){
    include 'dbinsert.php';
}

function test_input($data) {
    $data = trim($data);
    $data = stripslashes($data);
    $data = htmlspecialchars($data);
    return $data;
}

?>

```

Registration Page

Name:

Username:

Email Id:

*Enter Valid Email Id.

Password:

*Enter Password.

Confirm Password:

*Enter Password.

Contact Number:

Description

Practical No: 04

AIM:

Take reference of first practical and apply SQL injection on it. Create two different .php files to demonstrate importance of SQL injection (one without filters and second with filters).

Solution:

2.0 Database

2.1 Database Tables

| | | | | id | username | email | password | | | |
|--------------------------|--|------|--|------|----------|--------|----------|----------|-------------------------|----------------------------------|
| <input type="checkbox"/> | | Edit | | Copy | | Delete | 1 | Hetul | 17it107@charusat.edu.in | 912ec803b2ce49e4a541068d495ab570 |
| <input type="checkbox"/> | | Edit | | Copy | | Delete | 2 | anushree | 17it104@charusat.edu.in | 912ec803b2ce49e4a541068d495ab570 |
| <input type="checkbox"/> | | Edit | | Copy | | Delete | 3 | japan | 17it105@charusat.edu.in | 912ec803b2ce49e4a541068d495ab570 |
| <input type="checkbox"/> | | Edit | | Copy | | Delete | 4 | kunj | 17it106@charusat.edu.in | 912ec803b2ce49e4a541068d495ab570 |
| <input type="checkbox"/> | | Edit | | Copy | | Delete | 5 | aradhi | 17it099@charusat.edu.in | 912ec803b2ce49e4a541068d495ab570 |

2.2 Database Schema

| # | Name | Type | Collation | Attributes | Null | Default | Comments | Extra | Action |
|--------------------------|------|----------|--------------|-------------------|------|---------|----------|----------------|--------------------|
| <input type="checkbox"/> | 1 | id | int(11) | | No | None | | AUTO_INCREMENT | Change Drop More |
| <input type="checkbox"/> | 2 | username | varchar(100) | latin1_swedish_ci | No | None | | | Change Drop More |
| <input type="checkbox"/> | 3 | email | varchar(100) | latin1_swedish_ci | No | None | | | Change Drop More |
| <input type="checkbox"/> | 4 | password | varchar(100) | latin1_swedish_ci | No | None | | | Change Drop More |

3.0 Layout Files

login.php

```
<?php include('server.php') ?>
<!DOCTYPE html>
<html>
<head>
<title>Registration system PHP and MySQL</title>
<link rel="stylesheet" type="text/css" href="style.css">
</head>
<body>
<div class="header">
<h2>Login</h2>
</div>
```

```
<form method="post" action="login.php">
  <?php include('errors.php'); ?>
  <div class="input-group">
    <label>Username</label>
    <input type="text" name="username" >
  </div>
  <div class="input-group">
    <label>Password</label>
    <input type="text" name="password">
  </div>
  <div class="input-group">
    <button type="submit" class="btn" name="login_user">Login</button>
  </div>
  <p>
    Not yet a member? <a href="register.php">Sign up</a>
  </p>
</form>
</body>
</html>
```

register.php

```
<?php include('server.php') ?>
<!DOCTYPE html>
<html>
<head>
  <title>Registration system PHP and MySQL</title>
  <link rel="stylesheet" type="text/css" href="style.css">
</head>
<body>
  <div class="header">
    <h2>Register</h2>
  </div>
```

```
<form method="post" action="register.php">

    <?php include('errors.php'); ?>

    <div class="input-group">

        <label>Username</label>

        <input type="text" name="username" value="<?php echo $username; ?>">

    </div>

    <div class="input-group">

        <label>Email</label>

        <input type="email" name="email" value="<?php echo $email; ?>">

    </div>

    <div class="input-group">

        <label>Password</label>

        <input type="password" name="password_1">

    </div>

    <div class="input-group">

        <label>Confirm password</label>

        <input type="password" name="password_2">

    </div>

    <div class="input-group">

        <button type="submit" class="btn" name="reg_user">Register</button>

    </div>

    <p>

        Already a member? <a href="login.php">Sign in</a>

    </p>

</form>

</body>

</html>
```

error.php

```

<?php if (count($errors) > 0) : ?>

<div class="error">

    <?php foreach ($errors as $error) : ?>

        <p><?php echo $error ?></p>

    <?php endforeach ?>

</div>

<?php endif ?>

```

4.0 Processing Files

index.php

```

<?php

session_start();

if (!isset($_SESSION['username'])) {

    $_SESSION['msg'] = "You must log in first";

    header('location: login.php');

}

if (isset($_GET['logout'])) {

    session_destroy();

    unset($_SESSION['username']);

    header("location: login.php");

}

?>

<!DOCTYPE html>

<html>

<head>

<title>Home</title>

<link rel="stylesheet" type="text/css" href="style.css">

```

```
</head>

<body>

<div class="header">

  <h2>Home Page</h2>

</div>

<div class="content">

  <!-- notification message -->

  <?php if (isset($_SESSION['success'])) : ?>

    <div class="error success" >

      <h3>

        <?php
          echo $_SESSION['success'];
          unset($_SESSION['success']);
        ?>

      </h3>

    </div>

    <?php endif ?>

  <!-- logged in user information -->

  <?php if (isset($_SESSION['username'])) : ?>

    <p>Welcome <strong><?php echo $_SESSION['username']; ?></strong></p>

    <p> <a href="index.php?logout=1" style="color: red;">logout</a> </p>

    <?php endif ?>

  </div>

</body>

</html>
```


server.php

```
<?php

session_start();

// initializing variables

$username = "";
$email = "";
$errors = array();

// connect to the database

$db = mysqli_connect('localhost', 'root', '', 'registration');

// REGISTER USER
if (isset($_POST['reg_user'])) {
    // receive all input values from the form
    $username = mysqli_real_escape_string($db, $_POST['username']);
    $email = mysqli_real_escape_string($db, $_POST['email']);
    $password_1 = mysqli_real_escape_string($db, $_POST['password_1']);
    $password_2 = mysqli_real_escape_string($db, $_POST['password_2']);

    // form validation: ensure that the form is correctly filled ...
    // by adding (array_push()) corresponding error unto $errors array
    if (empty($username)) { array_push($errors, "Username is required"); }
    if (empty($email)) { array_push($errors, "Email is required"); }
    if (empty($password_1)) { array_push($errors, "Password is required"); }
    if ($password_1 != $password_2) {
        array_push($errors, "The two passwords do not match");
    }
}
```

```
// first check the database to make sure

// a user does not already exist with the same username and/or email

$user_check_query = "SELECT * FROM users WHERE username='$username' OR email='$email'
LIMIT 1";

$result = mysqli_query($db, $user_check_query);

$user = mysqli_fetch_assoc($result);

if ($user) { // if user exists

    if ($user['username'] === $username) {

        array_push($errors, "Username already exists");

    }

    if ($user['email'] === $email) {

        array_push($errors, "email already exists");

    }

}

// Finally, register user if there are no errors in the form

if (count($errors) == 0) {

    $password = md5($password_1);//encrypt the password before saving in the database

    $query = "INSERT INTO users (username, email, password)

        VALUES('$username', '$email', '$password)";

    mysqli_query($db, $query);

    $_SESSION['username'] = $username;

    $_SESSION['success'] = "You are now logged in";

    header('location: index.php');

}
```

```
}

// LOGIN USER

if (isset($_POST['login_user'])) {

    $username = mysqli_real_escape_string($db, $_POST['username']);

    $password = $_POST['password'];

    echo $password;


    if (empty($username)) {

        array_push($errors, "Username is required");

    }

    if (empty($password)) {

        array_push($errors, "Password is required");

    }


    if (count($errors) == 0) {

        //$password = md5($password);

        $query = "SELECT * FROM users WHERE username='$username' AND password='$password' ";

        echo $query;

        $results = mysqli_query($db, $query);

        echo gettype($results);

        if (mysqli_num_rows($results) > 0) {

            $_SESSION['username'] = $username;

            $_SESSION['success'] = "You are now logged in";

            header('location: index.php');

        }else {

            array_push($errors, "Wrong username/password combination");

        }

    }

}
```

```
}
```

```
?>
```

search.php

```
<?php
```

```
mysqli_connect("localhost", "root", "") or die("Error connecting to database: ".mysql_error());
```

```
/*
```

localhost - it's location of the mysql server, usually localhost

root - your username

third is your password

if connection fails it will stop loading the page and display an error

```
*/
```

```
mysqli_select_db("registration") or die(mysql_error());
```

```
/* tutorial_search is the name of database we've created */
```

```
?>
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

```
<html xmlns="http://www.w3.org/1999/xhtml">
```

```
<head>
```

```
<title>Search results</title>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
```

```
<link rel="stylesheet" type="text/css" href="style.css"/>
```

```
</head>
```

```
<body>
```

```
<?php
```

```
$query = $_GET['query'];
```

```
// gets value sent over search form

$min_length = 3;

// you can set minimum length of the query if you want

if(strlen($query) >= $min_length){ // if query length is more or equal minimum length then

    $query = htmlspecialchars($query);
    // changes characters used in html to their equivalents, for example: < to &lt;

    $query = mysql_real_escape_string($query);
    // makes sure nobody uses SQL injection

    $raw_results = mysql_query("SELECT * FROM users
        WHERE (`username` LIKE '%".$query."%') OR (`email` LIKE '%".$query."%')") or
    die(mysql_error());

    // * means that it selects all fields, you can also write: `id`, `title`, `text`

    // articles is the name of our table

    // '%$query%' is what we're looking for, % means anything, for example if $query is Hello
    // it will match "hello", "Hello man", "gogohello", if you want exact match use `title`='$query'
    // or if you want to match just full word so "gogohello" is out use '% $query %' ...OR ... '$query
    %' ... OR ... '% $query'

    if(mysql_num_rows($raw_results) > 0){ // if one or more rows are returned do following

        while($results = mysql_fetch_array($raw_results)){
            // $results = mysql_fetch_array($raw_results) puts data from database into array, while it's
```

valid it does the loop

```
        echo "<p><h3>".$results['title'].</h3>".$results['text'].</p>";
        // posts results gotten from database(title and text) you can also show id ($results['id'])
    }

}

else{ // if there is no matching rows do following
    echo "No results";
}

}

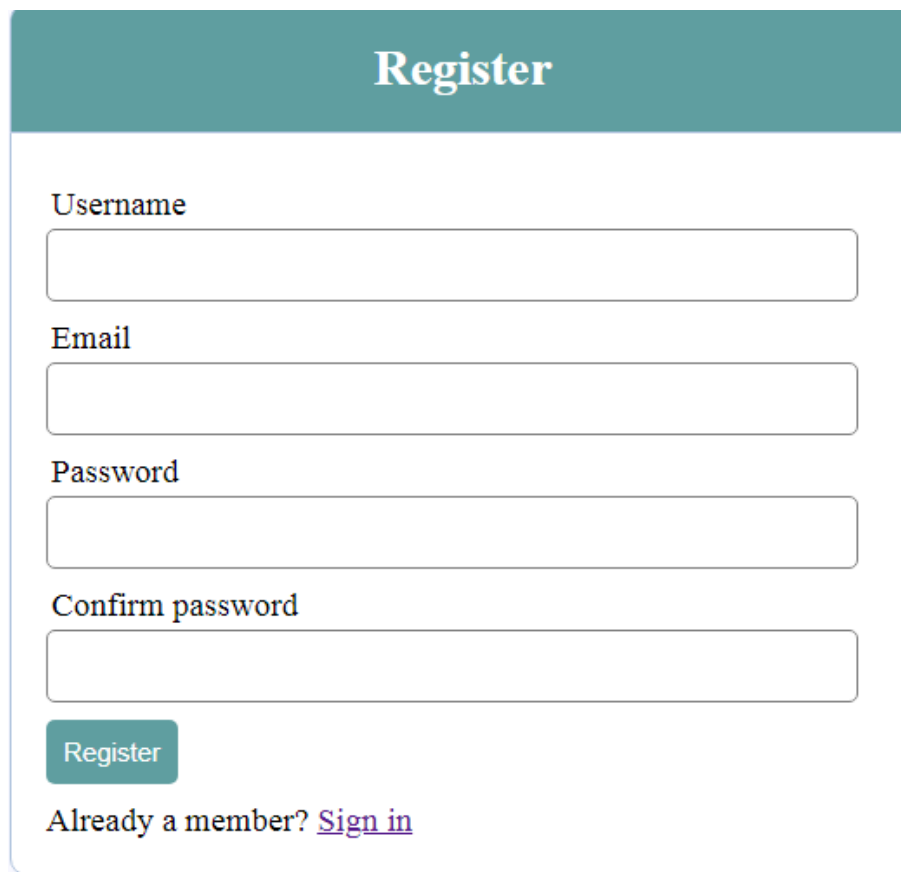
else{ // if query length is less than minimum
    echo "Minimum length is ".$min_length;
}

?>

</body>

</html>
```

5.0 Output



The Register form features a teal header with the title 'Register' in white. Below the header, there are four input fields: 'Username', 'Email', 'Password', and 'Confirm password'. Each field is a simple white rectangle with a thin grey border. At the bottom left of the form is a teal 'Register' button. To the right of the button, the text 'Already a member?' is followed by a purple underlined link 'Sign in'.

Register

Username

Email

Password

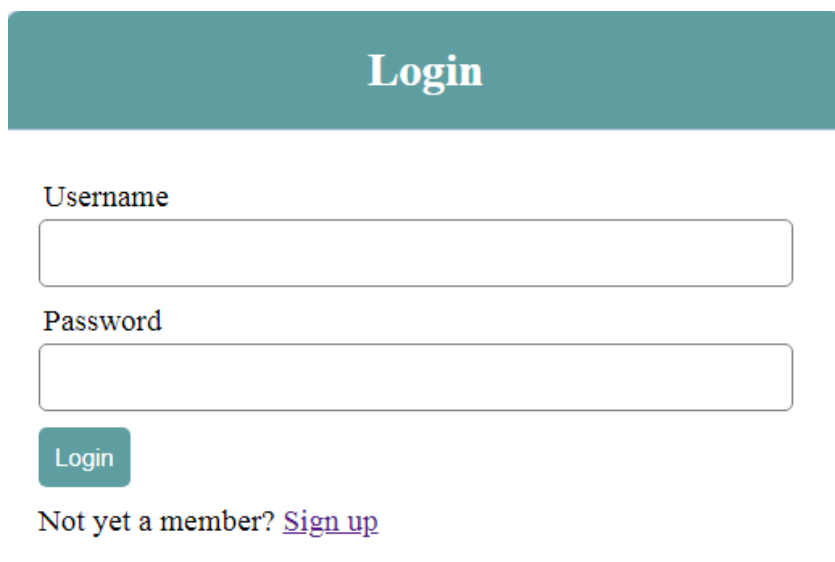
Confirm password

Register

Already a member? [Sign in](#)

Description

Above page indicates the registration page so that the users details can be stored in the database



The Login form features a teal header with the title 'Login' in white. Below the header, there are two input fields: 'Username' and 'Password'. Each field is a simple white rectangle with a thin grey border. At the bottom left of the form is a teal 'Login' button. To the right of the button, the text 'Not yet a member?' is followed by a purple underlined link 'Sign up'.

Login

Username

Password

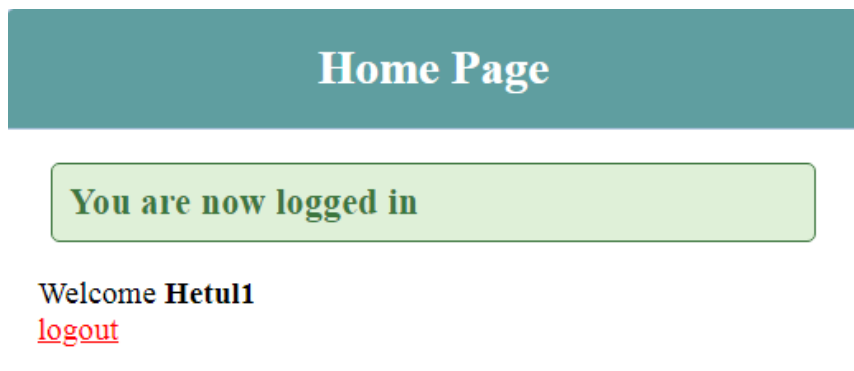
Login

Not yet a member? [Sign up](#)

Description

The above page indicates the login page in which the user can enter the credentials and get to the

required webpage



Description

The above page indicates that the user has successfully logged in

