

BÀI TẬP THỰC HÀNH 07

Chuẩn bị:

- Sử dụng kết quả của BTTH06, thực hiện tiếp các yêu cầu của BTTH07.
- Tạo tập tin **model\nguoidung.php**, khai báo lớp NGUOIDUNG với các phương thức sau:
 - Kiểm tra người dùng hợp lệ
 - Lấy thông tin một người dùng
 - Và các phương thức khác (cho yêu cầu phần II & III)

```
<?php
class NGUOIDUNG{
    // khai báo các thuộc tính (SV tự viết)

    public function kiemtranguoidunghople($email,$matkhau){
        $db = DATABASE::connect();
        try{
            $sql = "SELECT * FROM nguoidung WHERE email=:email AND
matkhau=:matkhau AND trangthai=1";
            $cmd = $db->prepare($sql);
            $cmd->bindValue(":email", $email);
            $cmd->bindValue(":matkhau", md5($matkhau));
            $cmd->execute();
            $valid = ($cmd->rowCount() == 1);
            $cmd->closeCursor();
            return $valid;
        }
        catch(PDOException $e){
            $error_message=$e->getMessage();
            echo "<p>Lỗi truy vấn: $error_message</p>";
            exit();
        }
    }

    // lấy thông tin người dùng có $email
    public function laythongtinnguoidung($email){
        $db = DATABASE::connect();
        try{
            $sql = "SELECT * FROM nguoidung WHERE email=:email";
            $cmd = $db->prepare($sql);
            $cmd->bindValue(":email", $email);
            $cmd->execute();
            $ketqua = $cmd->fetch();
            $cmd->closeCursor();
            return $ketqua;
        }
        catch(PDOException $e){
            $error_message=$e->getMessage();
            echo "<p>Lỗi truy vấn: $error_message</p>";
            exit();
        }
    }

    // lấy tất cả ng dùng
    public function laydanhsachnguoidung(){
        $db = DATABASE::connect();
```

```

        try{
            $sql = "SELECT * FROM nguoidung";
            $cmd = $db->prepare($sql);
            $cmd->execute();
            $ketqua = $cmd->fetchAll();
            return $ketqua;
        }
        catch(PDOException $e){
            $error_message=$e->getMessage();
            echo "<p>Lỗi truy vấn: $error_message</p>";
            exit();
        }
    }

    // Thêm ng dùng mới, trả về khóa của dòng mới thêm
    // (SV nên truyền tham số là 1 đối tượng kiểu người dùng, không nên truyền
    nhiều tham số rời rạc như thế này)
    public function themnguoidung($email,$matkhou,$sodt,$hoten,$loai){
        $db = DATABASE::connect();
        try{
            $sql = "INSERT INTO nguoidung(email,matkhou,sodienthoai,hoten,loai)
VALUES(:email,:matkhou,:sodt,:hoten,:loai)";
            $cmd = $db->prepare($sql);
            $cmd->bindValue(':email',$email);
            $cmd->bindValue(':matkhou',md5($matkhou));
            $cmd->bindValue(':sodt',$sodt);
            $cmd->bindValue(':hoten',$hoten);
            $cmd->bindValue(':loai',$loai);
            $cmd->execute();
            $id = $db->lastInsertId();
            return $id;
        }
        catch(PDOException $e){
            $error_message=$e->getMessage();
            echo "<p>Lỗi truy vấn: $error_message</p>";
            exit();
        }
    }

    // Cập nhật thông tin ng dùng: họ tên, số dt, email, ảnh đại diện
    // (SV nên truyền tham số là 1 đối tượng kiểu người dùng, không nên truyền
    nhiều tham số rời rạc như thế này)
    public function capnhatnguoidung($id,$email,$sodt,$hoten,$hinhanh){
        $db = DATABASE::connect();
        try{
            $sql = "UPDATE nguoidung set hoten=:hoten, email=:email,
sodienthoai=:sodt, hinhanh=:hinhanh where id=:id";
            $cmd = $db->prepare($sql);
            $cmd->bindValue(':id',$id);
            $cmd->bindValue(':email',$email);
            $cmd->bindValue(':sodt',$sodt);
            $cmd->bindValue(':hoten',$hoten);
            $cmd->bindValue(':hinhanh',$hinhanh);
            $ketqua = $cmd->execute();
            return $ketqua;
        }
        catch(PDOException $e){
            $error_message=$e->getMessage();
            echo "<p>Lỗi truy vấn: $error_message</p>";
            exit();
        }
    }

    // Đổi mật khẩu

```

```

public function doimatkhou($email,$matkhau){
    $db = DATABASE::connect();
    try{
        $sql = "UPDATE nguoidung set matkhau=:matkhau where email=:email";
        $cmd = $db->prepare($sql);
        $cmd->bindValue(':email',$email);
        $cmd->bindValue(':matkhau',md5($matkhau));
        $ketqua = $cmd->execute();
        return $ketqua;
    }
    catch(PDOException $e){
        $error_message=$e->getMessage();
        echo "<p>Lỗi truy vấn: $error_message</p>";
        exit();
    }
}

// Đổi quyền (loại người dùng: 1 quản trị, 2 nhân viên. Không cần nâng cấp
quyền đối với loại người dùng 3 khách hàng)
public function doiloainguoidung($email,$loai){
    $db = DATABASE::connect();
    try{
        $sql = "UPDATE nguoidung set loai=:loai where email=:email";
        $cmd = $db->prepare($sql);
        $cmd->bindValue(':email',$email);
        $cmd->bindValue(':loai',$loai);
        $ketqua = $cmd->execute();
        return $ketqua;
    }
    catch(PDOException $e){
        $error_message=$e->getMessage();
        echo "<p>Lỗi truy vấn: $error_message</p>";
        exit();
    }
}

// Đổi trạng thái (0 khóa, 1 kích hoạt)
public function doitrangthai($id,$trangthai){
    $db = DATABASE::connect();
    try{
        $sql = "UPDATE nguoidung set trangthai=:trangthai where id=:id";
        $cmd = $db->prepare($sql);
        $cmd->bindValue(':id',$id);
        $cmd->bindValue(':trangthai',$trangthai);
        $ketqua = $cmd->execute();
        return $ketqua;
    }
    catch(PDOException $e){
        $error_message=$e->getMessage();
        echo "<p>Lỗi truy vấn: $error_message</p>";
        exit();
    }
}
}
?>

```

- Tập tin **admin/index.php**: thực hiện kiểm tra người dùng

```
<?php
session_start(); // bắt đầu session (đặt ở đầu trang)
header("location:ktnguoidung"); // thực hiện kiểm tra người dùng
?>
```

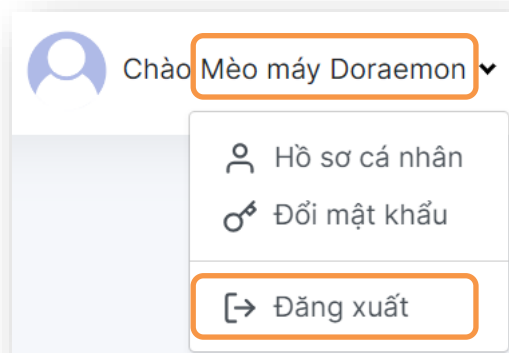
- Các tập tin **admin/qldanhmuc/index.php**, **admin/qlmathang/index.php** (và các trang index.php khác trong admin): bổ sung vào đầu trang lệnh kiểm soát người dùng đã đăng nhập mới được phép truy cập, chưa thì chuyển hướng ra ngoài.

```
if(!isset($_SESSION["nguoidung"]))
    header("location:../index.php");
```

- Tập tin **admin/inc/top.php**: bổ sung một số thông tin vào menu người dùng

```
<li class="nav-item dropdown">
  <a class="nav-icon dropdown-toggle d-inline-block d-sm-none" href="#" data-bs-toggle="dropdown">
    <i class="align-middle" data-feather="settings"></i>
  </a>

  <a class="nav-link dropdown-toggle d-none d-sm-inline-block" href="#" data-bs-toggle="dropdown">
    
    <span class="text-dark">
      Chào
      <?php if(isset($_SESSION["nguoidung"])) echo $_SESSION["nguoidung"]["hoten"]; else echo "bạn"; ?>
    </span>
  </a>
  <div class="dropdown-menu dropdown-menu-end">
    <a class="dropdown-item" href="#"><i class="align-middle me-1" data-feather="user"></i>
      Hồ sơ cá nhân</a>
    <a class="dropdown-item" href="#"><i class="align-middle me-1" data-feather="key"></i>
      Đổi mật khẩu</a>
    <div class="dropdown-divider"></div>
    <a class="dropdown-item" href="../../ktnguoidung/index.php?action=dangxuat">
      <i class="align-middle me-1" data-feather="log-out"></i> Đăng xuất
    </a>
  </div>
</li>
```



Yêu cầu:

PHẦN I: Viết chức năng xác thực người dùng, người dùng đăng nhập thành công mới có thể truy cập được vào các tài nguyên trong thư mục admin.

Xin chào!

Vui lòng đăng nhập để tiếp tục

Email

Mật khẩu

Đăng nhập

Chưa có tài khoản? [Đăng ký](#)

Hướng dẫn:

- Trong thư mục **admin**, tạo thư mục **ktnguoidung** cùng các tập tin *index.php*, *main.php*, *login.php*.
- Tập tin **ktnguoidung/login.php**: tạo form như mẫu.

```
<!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="preconnect" href="https://">
  <title>Đăng nhập - ABC Shop</title>
  <link href="../inc/css/app.css" rel="stylesheet">
  <script src="../inc/js/app.js"></script>
  <link href="https://" rel="stylesheet">
</head>
<body>
<main class="d-flex w-100">
<div class="container d-flex flex-column">
<div class="row vh-100">
<div class="col-sm-10 col-md-8 col-lg-6 col-xl-5 mx-auto d-table h-100">
<div class="d-table-cell align-middle">
<div class="text-center mt-4">
  <h1 class="h2">Xin chào!</h1>
  <p class="lead">Vui lòng đăng nhập để tiếp tục</p>
</div>
<div class="card">
  <div class="card-body">
```

```

        <div class="m-sm-3">
            <form action="index.php" method="post">
                <div class="mb-3">
                    <label class="form-label">Email</label>
                    <input class="form-control form-control-lg"
type="email"
                        name="txtemail" placeholder="Nhập email" />
                </div>
                <div class="mb-3">
                    <label class="form-label">Mật khẩu</label>
                    <input class="form-control form-control-lg"
type="password"
                        name="txtmatkhau" placeholder="Nhập mật khẩu" />
                </div>
                <div class="d-grid gap-2 my-3">
                    <input type="hidden" name="action" value="xldangnhap">
                    <input type="submit" class="btn btn-lg btn-primary"
value="Đăng nhập">
                </div>
            </form>
        </div>
    </div>
<div class="text-center mb-3">
    Chưa có tài khoản? <a href="#">Đăng ký</a>
</div>
</div>
</div>
</div>
</div>
</div>
</main>
</body>
</html>

```

- Tập tin **ktnguoidung/index.php**:

```

<?php
require("../model/database.php");
require("../model/nguoidung.php");

// Biến $isLogin cho biết người dùng đăng nhập chưa
$isLogin = isset($_SESSION["nguoidung"]);
// Kiểm tra hành động $action: yêu cầu đăng nhập nếu chưa xác thực
if(isset($_REQUEST["action"])){
    $action = $_REQUEST["action"];
}
elseif($isLogin == FALSE){
    $action = "dangnhap";
}
else{
    $action="macdinh";
}
$nd = new NGUOIDUNG();
switch($action){
    case "macdinh":
        include("main.php");
        break;
    case "dangnhap":
        include("login.php");
        break;
    case "xldangnhap":
        $email = $_POST["txtemail"];
        $matkhau = $_POST["txtmatkhau"];
        if($nd->kiemtranguoidunghople($email,$matkhau)==TRUE){

```

```

        $_SESSION["nguoidung"] = $nd->laythongtinnguoidung($email);
        include("main.php");
    }
    else{
        include("login.php");
    }
    break;
case "dangxuat":
    unset($_SESSION["nguoidung"]);
    include("login.php");
    break;
default:
    break;
}
?>

```

- Tập tin **ktnguoidung/main.php**:

```

<?php include("../inc/top.php"); ?>
<div>

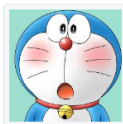
<h4>Trang quản trị</h4>
<p>SV hãy cập nhật nội dung tùy thích...</p>

</div>
<?php include("../inc/bottom.php"); ?>

```

PHẦN II: Quản lý thông tin cá nhân (mỗi tài khoản được phép quản lý thông tin của chính mình).

HỒ SƠ NGƯỜI DÙNG



Email

Số điện thoại

Họ tên

Đổi hình đại diện

- Tập tin **admin/inc/top.php**: bổ sung vào menu người dùng liên kết mở các form Cập nhật hồ sơ cá nhân, Đổi mật khẩu.

```

<a class="dropdown-item" href="../ktnguoidung/index.php?action=hoso">
    <i class="align-middle me-1" data-feather="user"></i> Hồ sơ cá nhân
</a>
<a class="dropdown-item" href="../ktnguoidung/index.php?action=matkhau">
    <i class="align-middle me-1" data-feather="key"></i> Đổi mật khẩu
</a>

```

1. Cập nhật hồ sơ cá nhân

- Tập tin `admin/ktnguoidung/index.php`:

```
case "hoso":  
    include("profile.php");  
    break;
```

- Tập tin `admin/ktnguoidung/profile.php`:

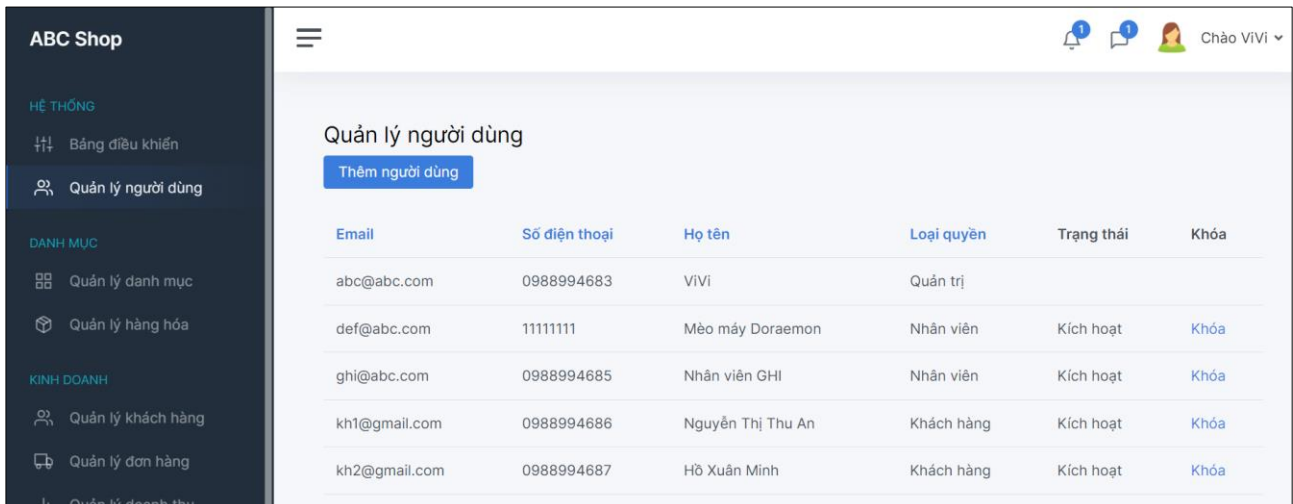
```
<div class="row" >  
    <div class="col-12 col-md-10 m-auto">  
        <div class="card p-5">  
            <div class="card-header">  
                <h4 class="text-info text-center">HỒ SƠ NGƯỜI DÙNG</h4>  
            </div>  
            <div class="card-body">  
                <form method="post" enctype="multipart/form-data" action="../ktnguoidung/index.php">  
                    <input type="hidden" name="txtid" value="<?php echo $_SESSION["nguoidung"]["id"]; ?>" >  
                    <input type="hidden" name="txthinhanh" value="<?php echo $_SESSION["nguoidung"]["hinhanh"]; ?>" >  
                    <input type="hidden" name="action" value="xlhoso" >  
                    <div class="text-center">  
                        "  
                            alt="<?php echo $_SESSION["nguoidung"]["hoten"]; ?>" width="100px">  
                    </div>  
                    <div class="my-3">  
                        <label class="form-label">Email</label>  
                        <input class="form-control" type="email" name="txtemail" placeholder="Email"  
                            value="<?php echo $_SESSION["nguoidung"]["email"]; ?>" required>  
                    </div>  
                    <div class="my-3">  
                        <label class="form-label">Số điện thoại</label>  
                        <input class="form-control" type="number" name="txtdienthoai" placeholder="Số điện thoại"  
                            value="<?php echo $_SESSION["nguoidung"]["sodienthoai"]; ?>" required>  
                    </div>  
                    <div class="my-3">  
                        <label class="form-label">Họ tên</label>  
                        <input class="form-control" type="text" name="txthoten" placeholder="Họ tên"  
                            value="<?php echo $_SESSION["nguoidung"]["hoten"]; ?>" required>  
                    </div>  
                    <div class="my-3">  
                        <label class="form-label">Đổi hình đại diện</label>  
                        <input class="form-control" type="file" name="fanh">  
                    </div>  
                    <div class="my-3 text-center">  
                        <input class="btn btn-primary" type="submit" value="Cập nhật">  
                        <input class="btn btn-warning" type="reset" value="Không">  
                    </div>  
                </form>  
            </div>  
        </div>  
    </div>  
</div>
```

- Tập tin `admin/ktnguoidung/index.php`:

```
case "xlhoso":  
    $mand = $_POST["txtid"];  
    $email = $_POST["txtemail"];  
    $sodt = $_POST["txtdienthoai"];  
    $hoten = $_POST["txthoten"];  
    $hinhanh = $_POST["txthinhanh"];  
  
    if($_FILES["fanh"]["name"] != null){  
        $hinhanh = basename($_FILES["fanh"]["name"]);  
        $duongdan = "../images/users/" . $hinhanh;  
        move_uploaded_file($_FILES["fanh"]["tmp_name"], $duongdan);  
    }  
  
    $nd->capnhatnguoidung($mand,$email,$sodt,$hoten,$hinhanh);  
  
    $_SESSION["nguoidung"] = $nd->laythongtinnguoidung($email);  
    include("main.php");  
    break;
```

2. Đổi mật khẩu (SV tự viết).

PHẦN III: Quản lý người dùng (tài khoản là *Quản trị viên* mới được phép dùng chức năng này).



The screenshot shows the 'ABC Shop' admin dashboard. The sidebar on the left contains a menu with categories like 'HỆ THỐNG', 'DANH MỤC', and 'KINH DOANH'. The main content area is titled 'Quản lý người dùng' and features a 'Thêm người dùng' button and a table of users.

Email	Số điện thoại	Họ tên	Loại quyền	Trạng thái	Khóa
abc@abc.com	0988994683	ViVi	Quản trị		
def@abc.com	11111111	Mèo máy Doraemon	Nhân viên	Kích hoạt	Khóa
ghi@abc.com	0988994685	Nhân viên GHI	Nhân viên	Kích hoạt	Khóa
kh1@gmail.com	0988994686	Nguyễn Thị Thu An	Khách hàng	Kích hoạt	Khóa
kh2@gmail.com	0988994687	Hồ Xuân Minh	Khách hàng	Kích hoạt	Khóa

- Tập tin **admin/inc/top.php**: bổ sung chức năng Quản lý người dùng vào menu

```
<?php if(isset($_SESSION["nguoidung"]) && $_SESSION["nguoidung"]["loai"]==1){ ?>
<li class="sidebar-item <?php if(strpos($_SERVER['REQUEST_URI'], "qlnguoidung") != false) echo "active"; ?>">
  <a class="sidebar-link" href=".."qlnguoidung/index.php">
    <i class="align-middle" data-feather="users"></i> <span class="align-middle">Quản lý người dùng</span>
  </a>
</li>
<?php } ?>
```

- Trong thư mục **admin**, tạo thư mục **qlnguoidung** cùng các tập tin *index.php*, *main.php*, ...

1. Xem danh sách người dùng (SV tự viết).
2. Thêm người dùng mới (SV tự viết).
3. Khóa tài khoản: chỉ được khóa tài khoản là Nhân viên (SV tự viết).
4. Nâng cấp quyền (SV tự viết).