Shape, square

Description automatically generated

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HỒ CHÍ MINH**

**KHOA CÔNG NGHỆ THÔNG TIN**

**🕯✡🕮🕮✡🕯**

|  |  |
| --- | --- |
|  | |
|  |  |

A picture containing text

Description automatically generatedLogo

Description automatically generated

**BÁO CÁO ĐỒ ÁN CUỐI KỲ**

**BẢO MẬT WEB**

**BẢO MẬT HỆ THỐNG WEBSITE KINH DOANH QUÀ LƯU NIỆM**

**GVHD: Ths. Lê Thị Minh Châu**

**Nhóm sinh viên thực hiện :**

Chu Trần Minh Đức 20110266

Lê Anh Kiệt 20110664

Huỳnh Công Quyền 20110258

Lương Xuân Thắng 20110724

**Tp. Hồ Chí Minh, tháng 5 năm 2023**

**Nhận xét của giảng viên**

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

Tháng 5 năm 2023

**Giáo viên chấm điểm**

# LỜI CẢM ƠN

Lời nói đầu tiên, nhóm thực hiện xin được gửi đến cô **Lê Thị Minh Châu** – giảng viên bộ môn lời cảm ơn chân thành và sâu sắc nhất.

Nhóm thực hiện xin cảm ơn sự quan tâm và giúp đỡ tận tình của cô trong suốt quá trình giảng dạy. Cảm ơn cô đã luôn giải đáp những thắc mắc cũng như đưa ra những nhận xét, góp ý giúp nhóm thực hiện cải thiện chất lượng công việc của nhóm.

Vì khả năng còn hạn chế nên trong quá trình thực hiện báo cáo không tránh khỏi sai sót, kính mong nhận được những ý kiến đóng góp từ cô để nhóm có thể cải thiện hơn sau này.

Nhóm thực hiện xin chân thành cảm ơn.

**MỤC LỤC**

# PHÂN CHIA CÔNG VIỆC

|  |  |  |  |
| --- | --- | --- | --- |
| Họ và tên | MSSV | Phân công | Mức độ hoàn thành |
| Chu Trần Minh Đức | 20110266 |  |  |
| Lê Anh Kiệt | 20110664 |  |  |
| Huỳnh Công Quyền | 20110258 |  |  |
| Lương Xuân Thắng | 20110724 |  |  |

# Phần 1: Giới thiệu project

## 1. Giới thiệu

### 1.1. Mục đích

MeowMeow shop là một hệ thống webside dùng để bán các loại mặt hàng lưu niệm cho phép khách hàng có thể thỏa thích lựa chọn và mua sắm online. MeowMeow shop sẽ cập nhật nhiều loại mặt hàng hot nhất, được ưa chuộng nhất và cập nhật nhiều thông tin mới về các mặt hàng sản phẩm để khách hàng nắm bắt đầy đủ nhất. MeowMeow shop cho phép khách hàng tạo tài khoản để thanh toán sản phẩm. Đối với khách hàng đã thanh toán xong MeowMeow shop sẽ cập nhật trạng thái đơn hàng cho khách hàng và liên hệ cho khách hàng.

### 1.2. Đối tượng của đề tài

* Khách hàng.
* Quản lý.
* Nhân viên.

### 1.3.Chức năng

#### 1.2.1. Khách hàng

* Đăng ký tài khoản: Người dùng tiến hành đăng ký tài khoản, thông tin cần cung cấp để đăng ký bao gồm: tên đăng nhập, mật khẩu, tên người dùng, gmail, số điện thoại, Địa chỉ, giới tính, ngày tháng năm sinh.
* Đăng nhập tài khoản: Người dùng nhập tên tài khoản và mật khẩu để đăng nhập vào tài khoản.
* Tìm kiếm sản phẩm: Người dùng có thể tìm kiếm các loại sản phẩm dựa vào tên sản phẩm.
* Cập nhập giỏ hàng: Người dùng có thể thêm, xóa, sửa các sản phẩm trong giỏ hàng.
* Mua hàng: Người dùng có thể chọn các sản phẩm trong giỏ hàng và hoàn thành
* Thay đổi thông tin tài khoản: Người dùng có thể thay đổi thông tin tài khoản cá nhân.
* Xem danh sách đơn hàng: người dùng có thể xem các đơn hàng đã đặt trên hệ thống website.
* Xem chi tiết sản phẩm: người dùng có thể xem thông tin chi tiết của sản phẩm.

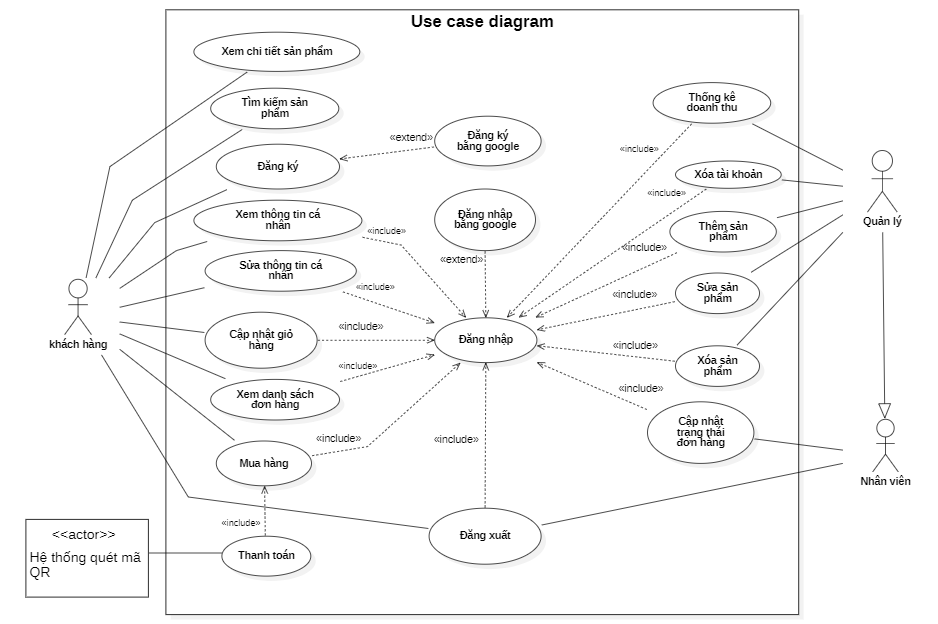
#### 1.2.2. Nhân viên

* Cập nhật trạng thái đơn hàng: Nhân viên có thể tiếp nhận đơn hàng, sửa đổi trạng thái đơn hàng, chuẩn bị hàng để gửi.

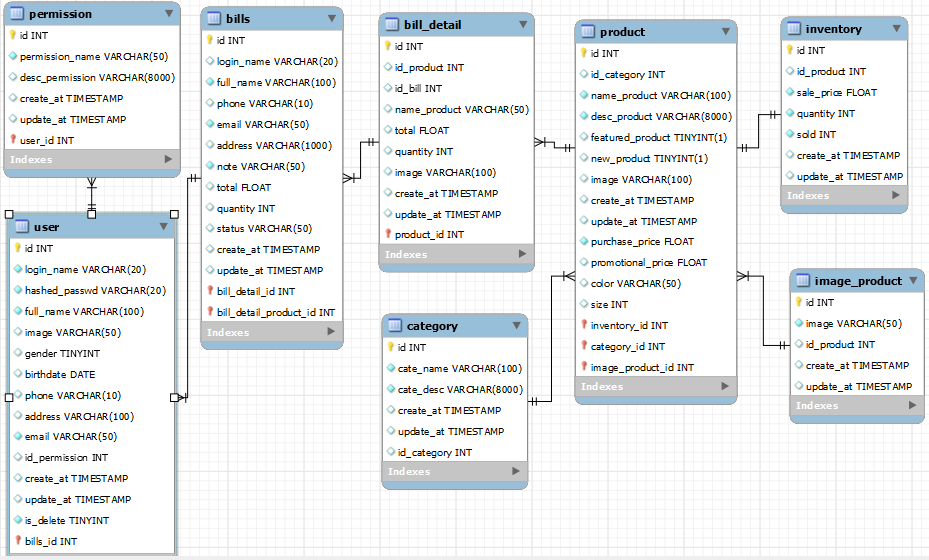
#### 1.2.3. Quản lý

* Quản lý tài khoản: Quản lý có thể xem, xóa các thông tin liên quan đến tài khoản.
* Quản lý sản phẩm: Quản lý có thể xem, thêm, xóa, sửa sản các thông tin liên quan đến sản phẩm.
* Thống kê doanh thu: Quản lý có thể thống kê doanh thu theo ngày, tháng, năm.

## 2. Lược đồ usecase

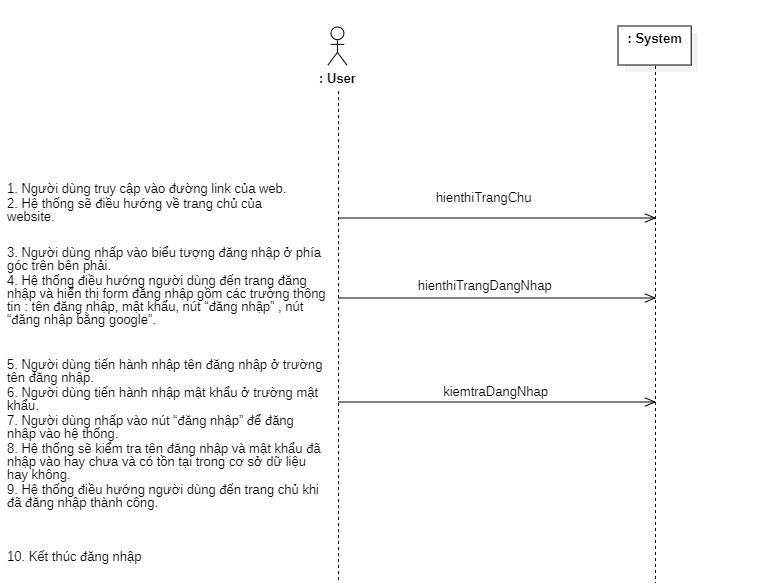


## 3. Lược đồ quan hệ ERD

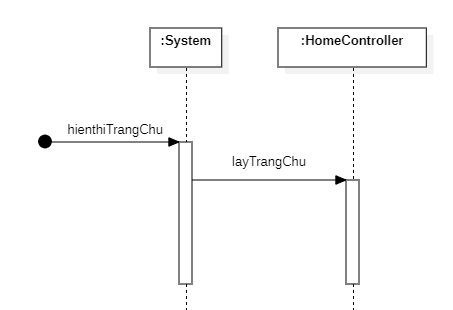


## 5. Lược đồ trình tự (Sequence Diagram – SD)

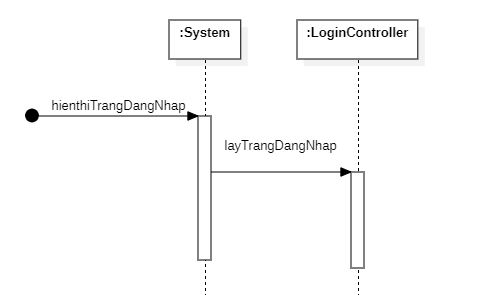
### 5.1. SSD đăng nhập



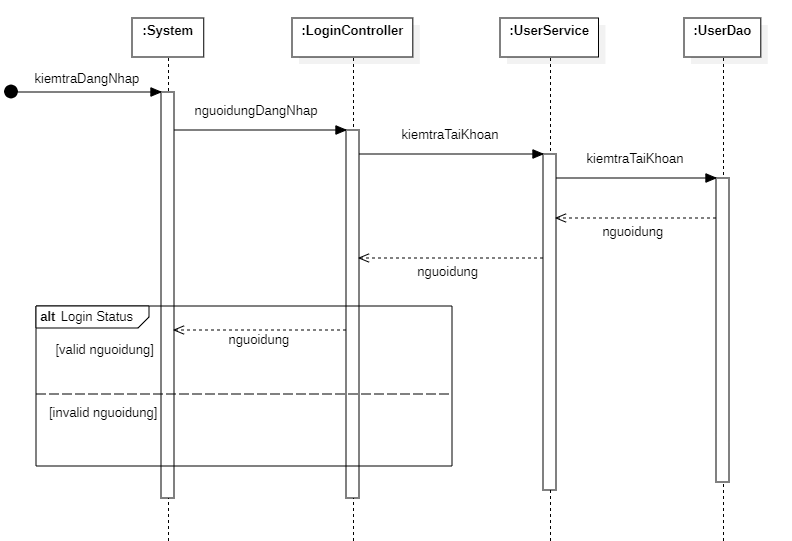
#### 5.1.1. SD hienthiTrangChu



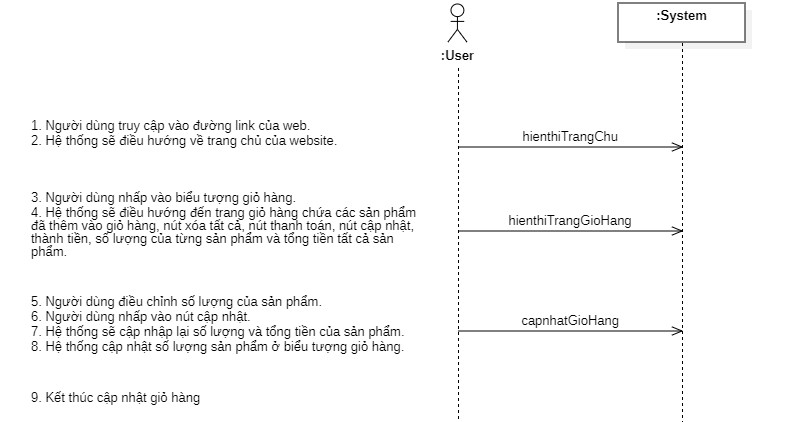
#### 5.1.2. SD hienthiTrangDangNhap



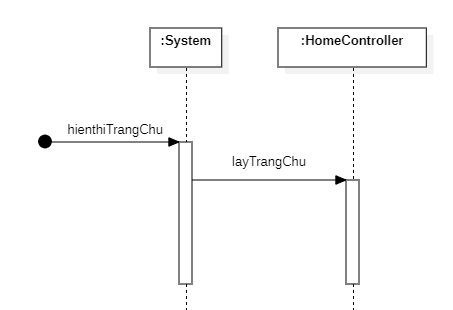
#### 5.1.3. SD kiemtraDangNhap



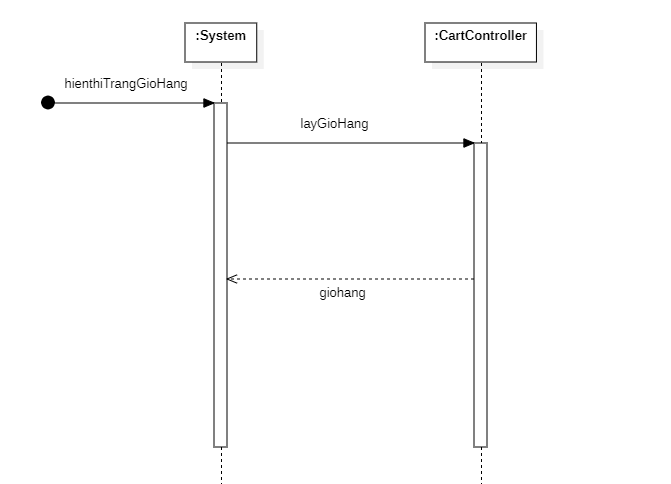
### 5.2. SSD cập nhật giỏ hàng



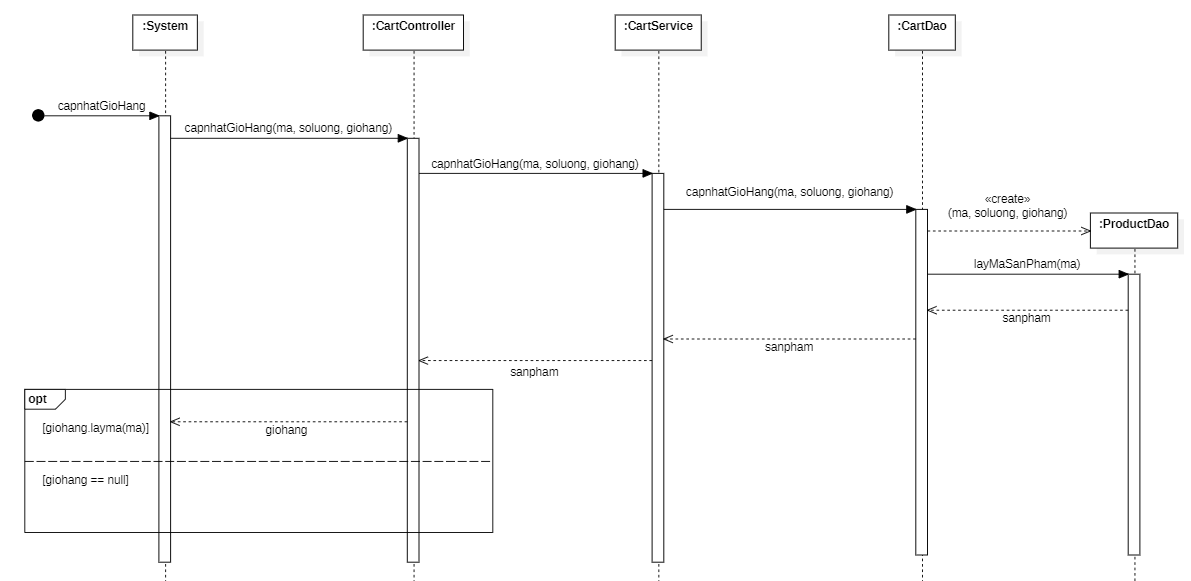
#### 5.2.1. SD hienthiTrangChu



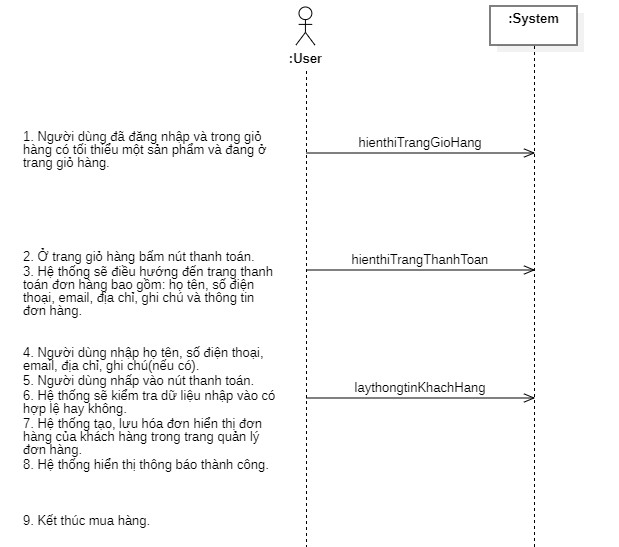
#### 5.2.2. SD hienthiTrangGioHang



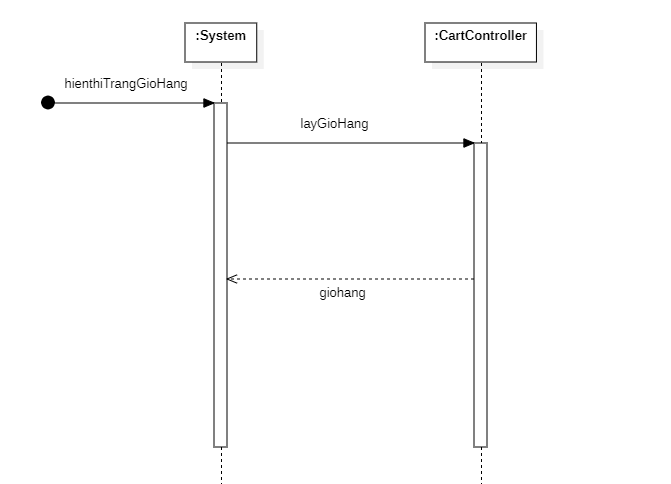
#### 5.2.3. SD capnhatGioHang



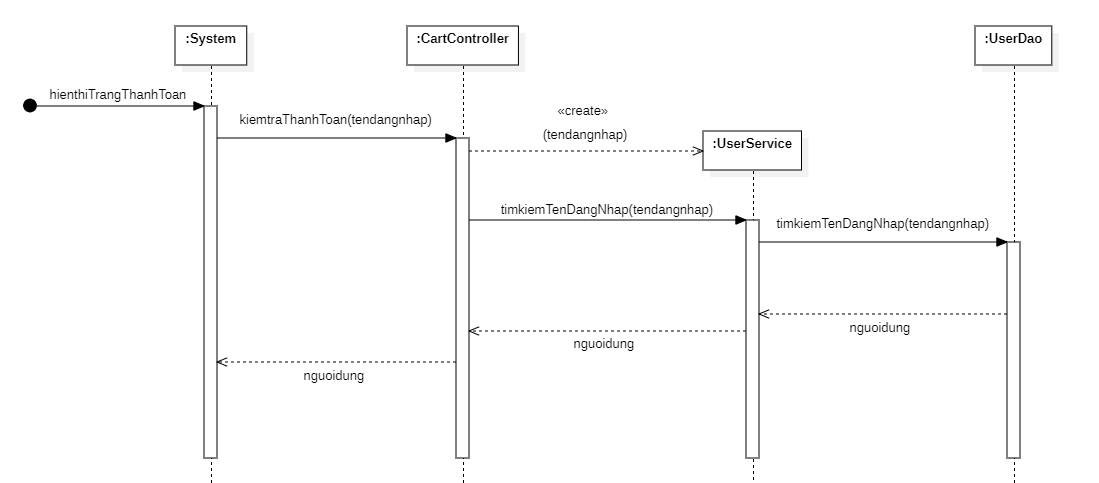
### 5.3. SSD mua hàng



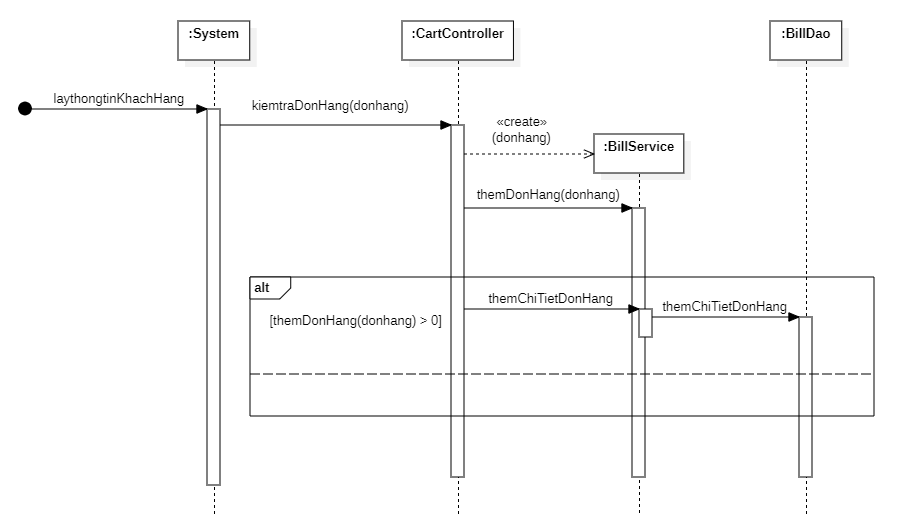
#### 5.3.1. SD hienthiTrangGioHang



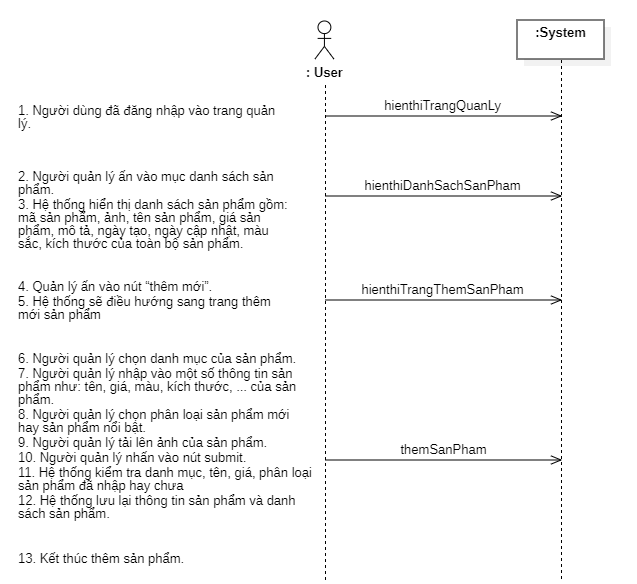
#### 5.3.2. SD hienthiTrangThanhToan



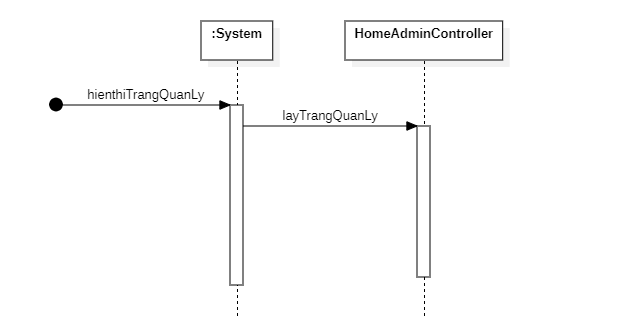
#### 5.3.3. SD laythongtinKhachHang



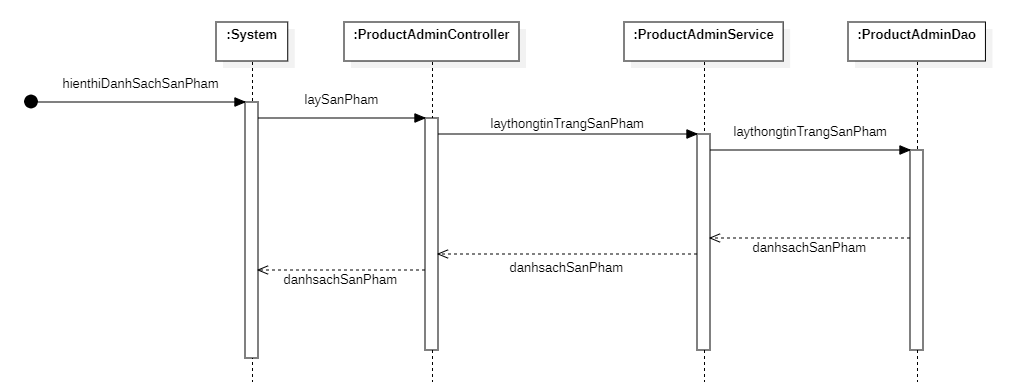
### 5.4. SSD thêm sản phẩm



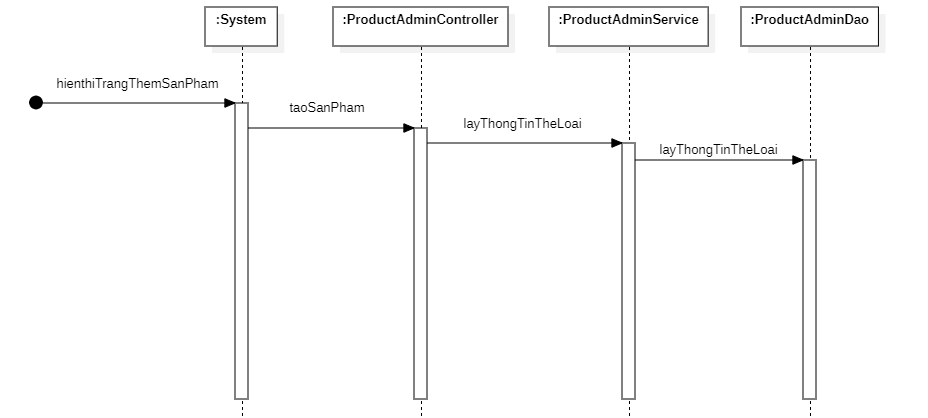
#### 5.4.1. SD hienthiTrangQuanLy



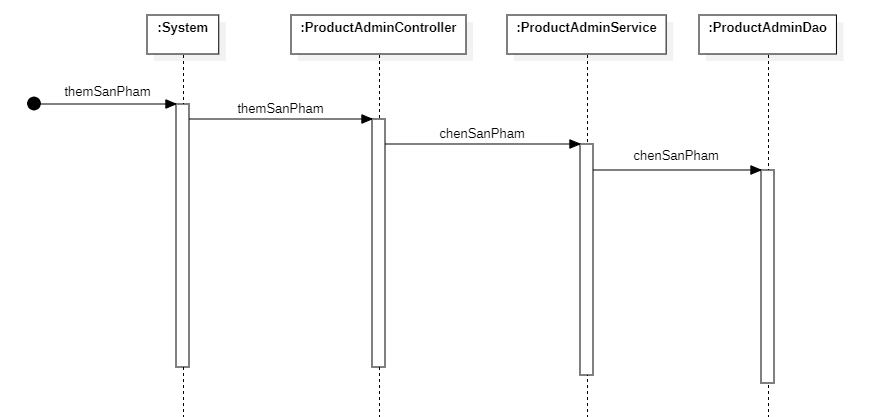
#### 5.4.2. SD hienthiDanhSachSanPham



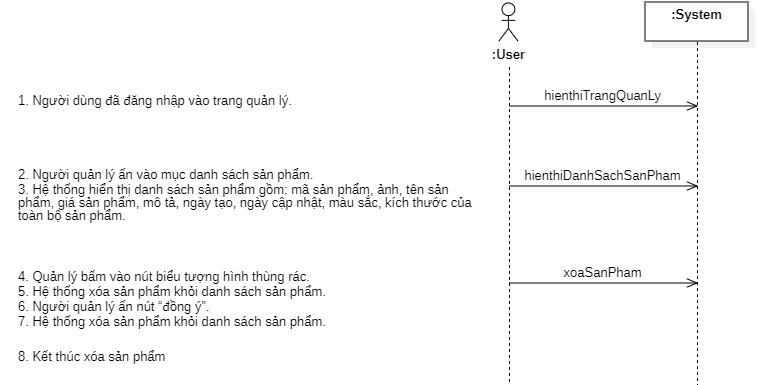
#### 5.4.3. SD hienthiTrangThemSanPham



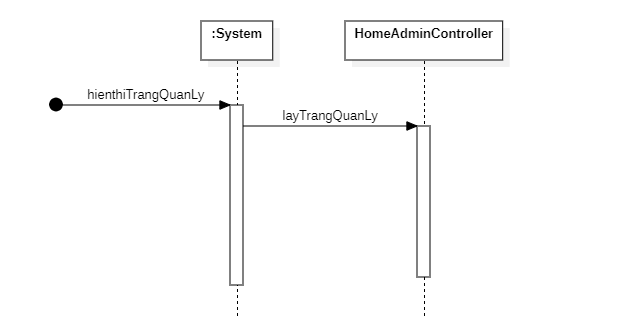
#### 5.4.4. SD themSanPham



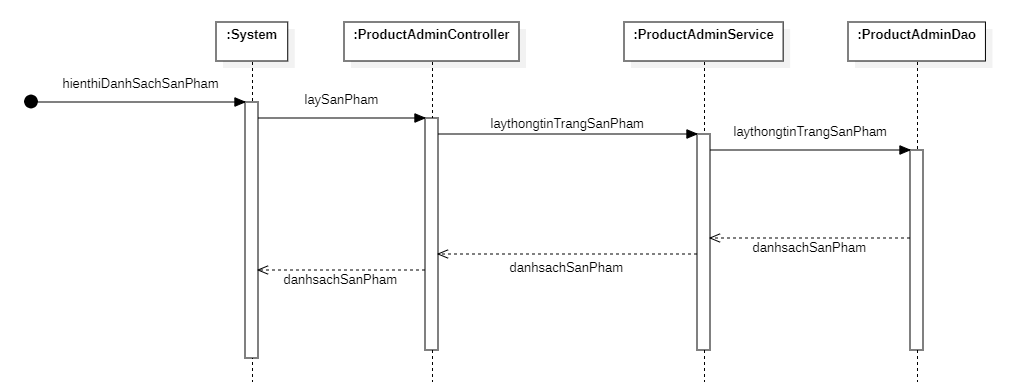
### 5.5. SSD xóa sản phẩm



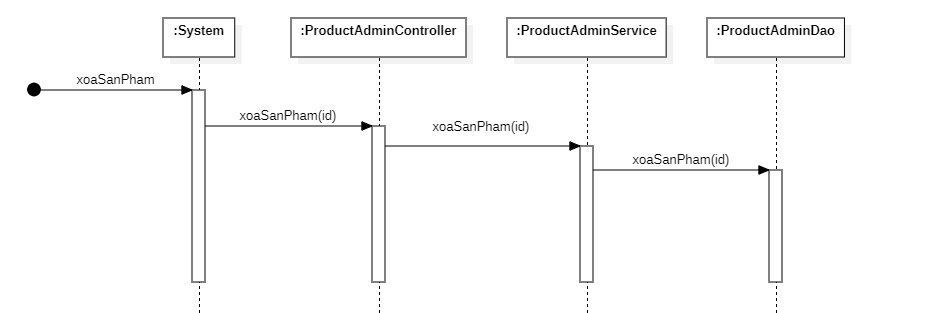
#### 5.5.1. SD hienthiTrangQuanLy



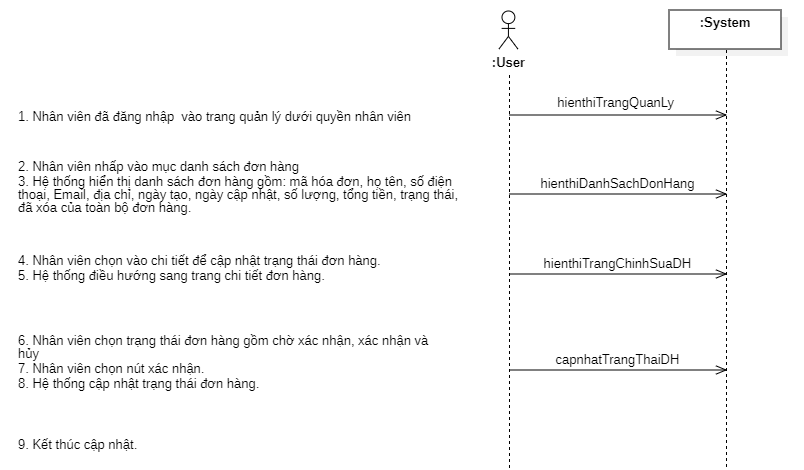
#### 5.5.2. SD hienthiDanhSachSanPham



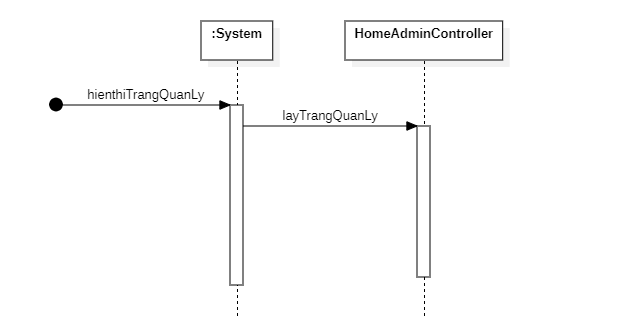
#### 5.5.3. SD xoaSanPham



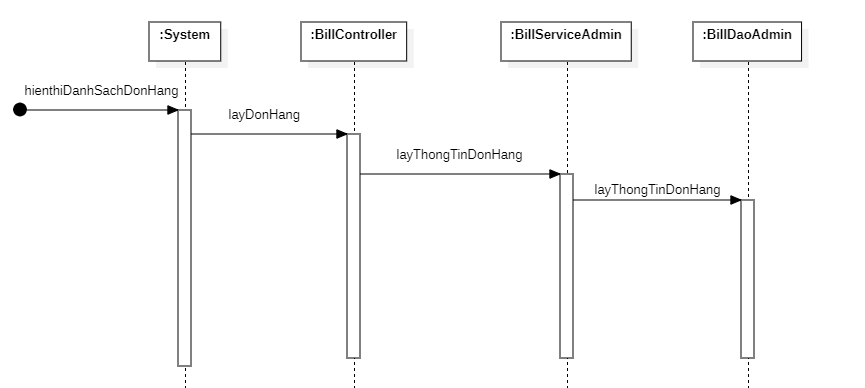
### 5.6. SSD cập nhật trạng thái đơn hàng



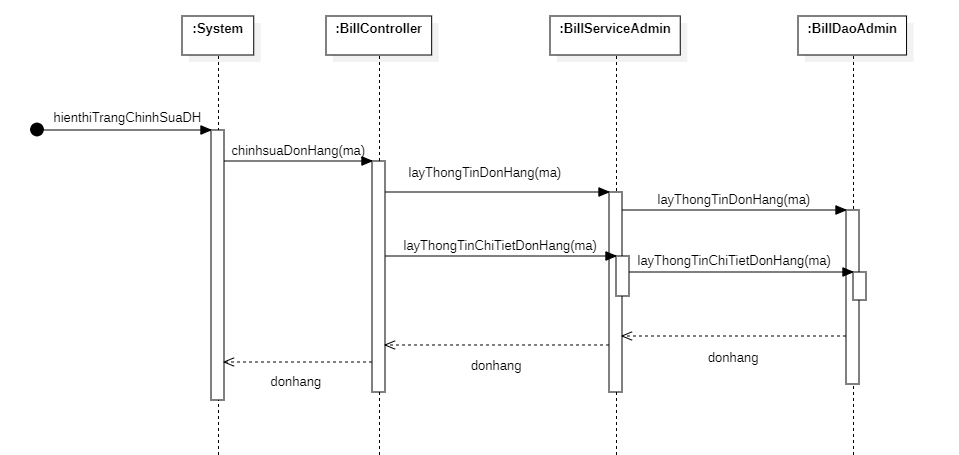
#### 5.6.1. SD hienthiTrangQuanLy



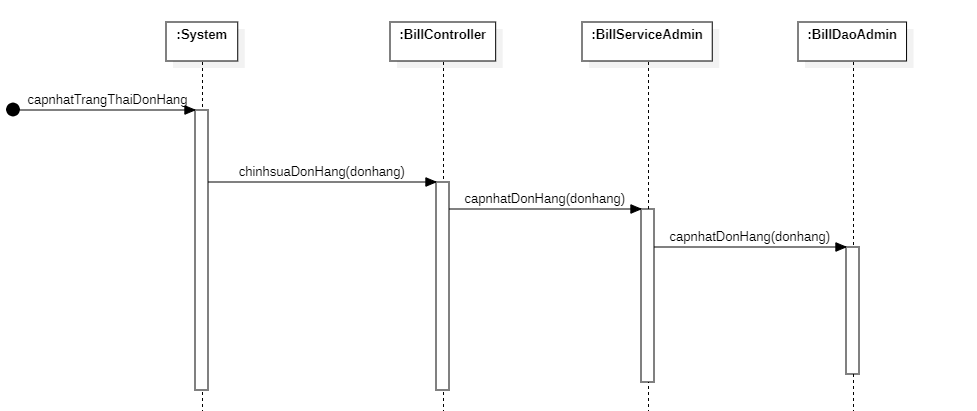
#### 5.6.2. SD hienthiDanhSachDonHang



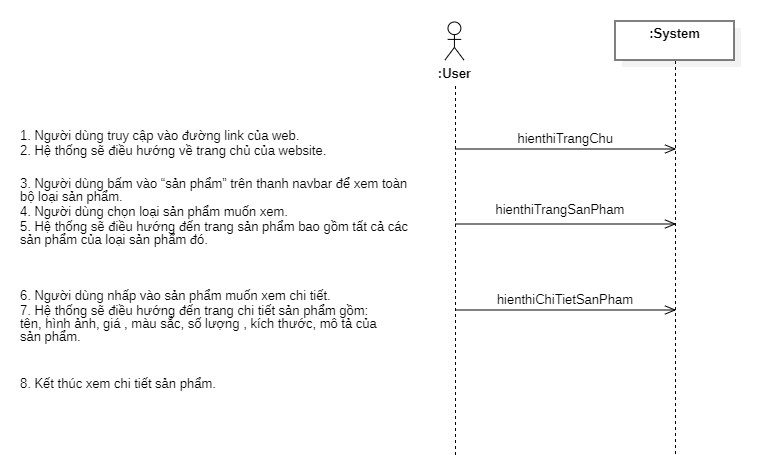
#### 5.6.3. SD hienthiTrangChinhSuaDH



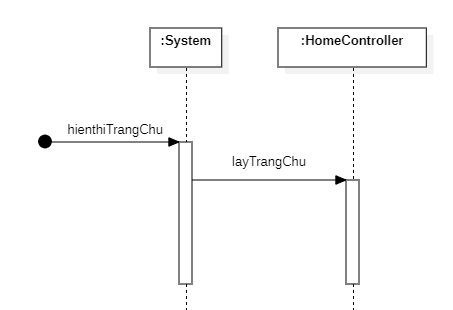
#### 5.6.4. SD capnhatTrangThaiDonHang



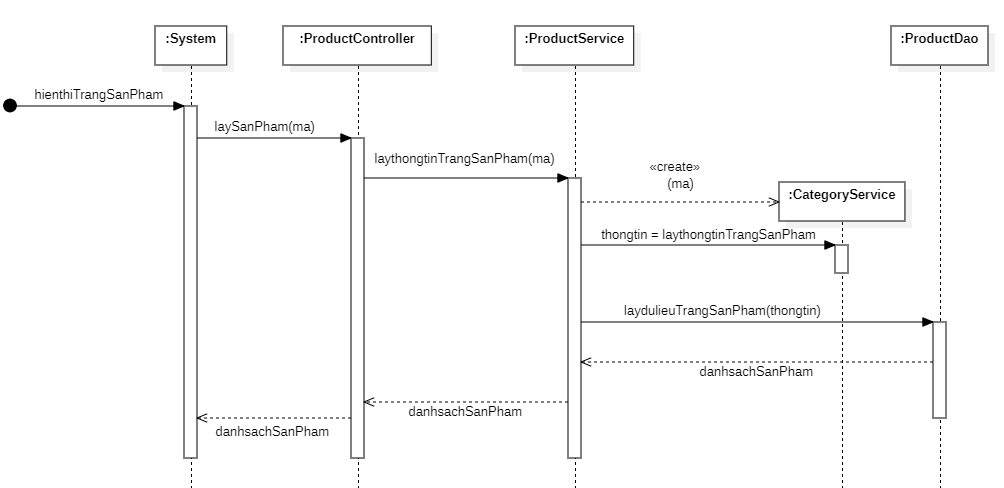
### 5.7. SSD xem chi tiết sản phẩm



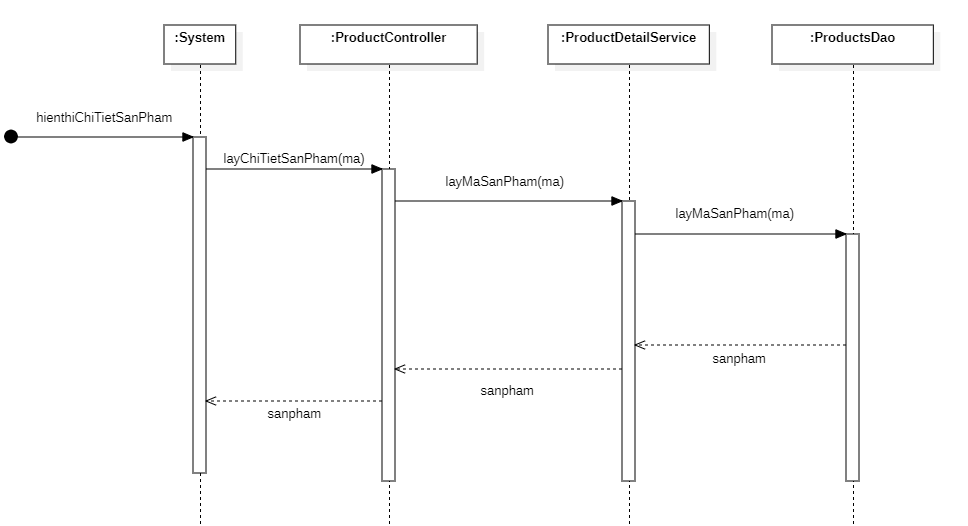
#### 5.7.1. SD hienthiTrangChu



#### 5.7.2. SD hienthiTrangSanPham



#### 5.7.3. SD hienthiChiTietSanPham



## 6. Hướng dẫn cài đặt và chạy

### 6.1. Sơ lược về project

- Link project: <https://github.com/CTminhduc/SouvenirShop_BMW.git>

- Ngôn ngữ lập trình: Java

- Framework: Spring MVC

- Cơ sở dữ liệu: MySQL

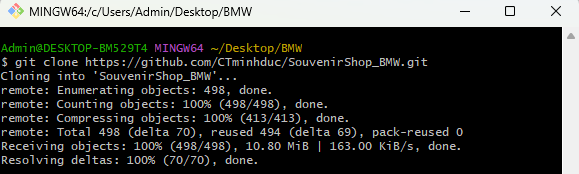
- Version control: GitHub

- IDE: Spring tool suite 4.0 for Eclipse

### 6.2. Hướng dẫn cài đặt

**Bước 1:** Tải project từ github về bằng câu lệnh:

git clone <https://github.com/CTminhduc/SouvenirShop_BMW.git>



**Bước 2:** Import project vào IDE

Mở 1 IDE bất kỳ hỗ trợ java ( Nên dùng STS cho eclipse ). Chọn file -> Open Project From file System -> Directory -> Chọn project -> Finish

# Phần 2: Bảo mật website

## Kiểm tra thủ công (manual)

### Insecure Direct Object Reference ( IDOR )

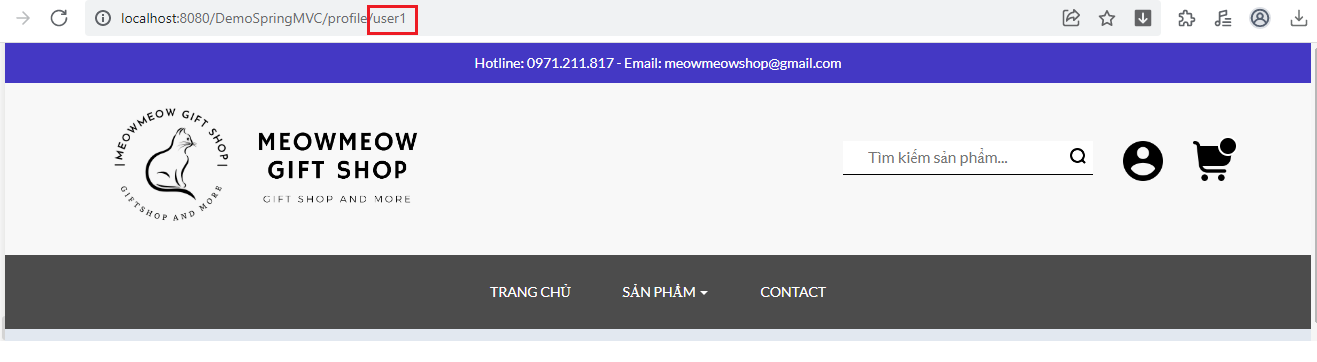
#### Khái niệm

IDOR là cụm từ viết tắt của Insecure Direct Object Reference (Tham chiếu đối tượng trực tiếp không an toàn). Lỗ hổng này nằm trong TOP 10 lỗ hổng nguy hiểm mà OWASP đã đưa ra IDOR. Lỗ hổng này xảy ra khi chương trình cho phép người dùng truy cập tài nguyên (dữ liệu, file, thư mục, database..) một cách trực tiếp thông qua dữ liệu do người dùng cung cấp nhưng kém an toàn.

Nguyên nhân sâu xa của lỗ hổng IDOR nằm ở cơ chế phân quyền và kiểm soát truy cập người dùng trên website. Việc website không phân quyền đúng cũng như kiểm soát chặt chẽ việc truy cập tài nguyên của user trên hệ thống dẫn đến việc truy cập trái phép từ kẻ tấn công.

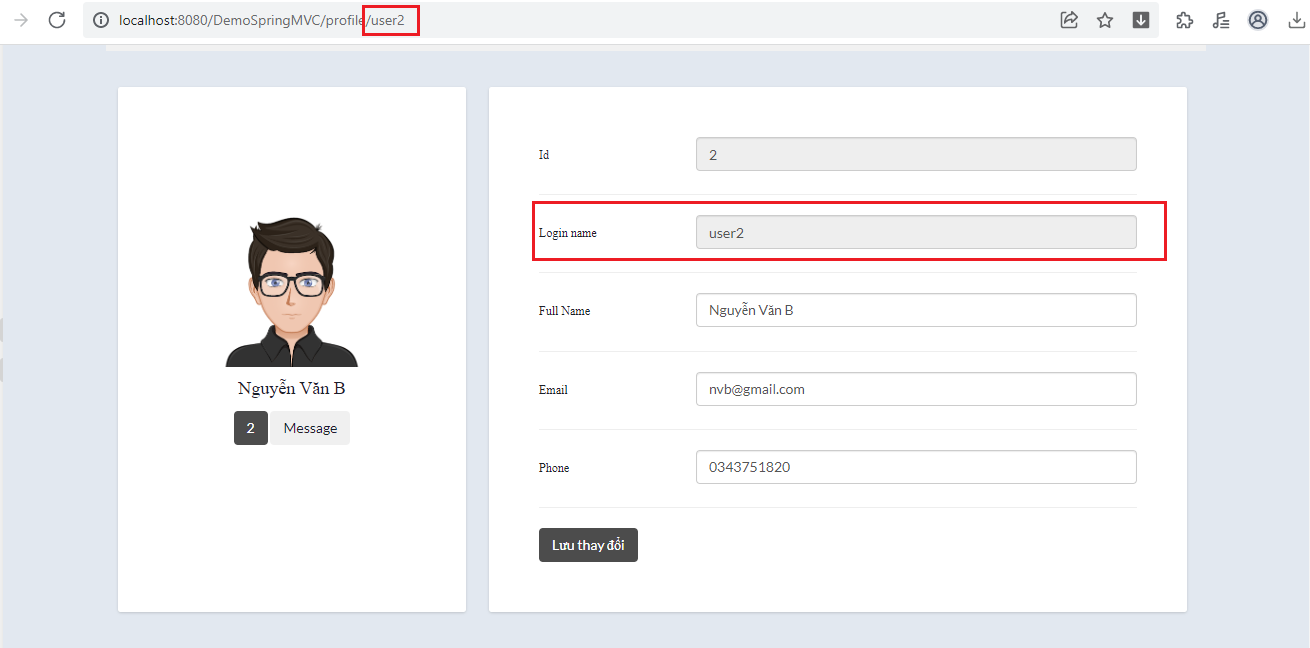
IDOR không chỉ cho phép truy cập thông tin trái phép của người dùng khác mà còn có thể cho phép kẻ tấn công thực hiện thay đổi hoặc xóa dữ liệu của người dùng khác. Vì vậy lỗ hổng này có mức độ nguy hiểm rất cao, gây hậu quả nghiêm trọng tới người dùng. Đặc biệt là các hệ thống có dữ liệu quan trọng của người dùng như: mạng xã hội, tài chính - ngân hàng, y tế..

#### Tấn công project

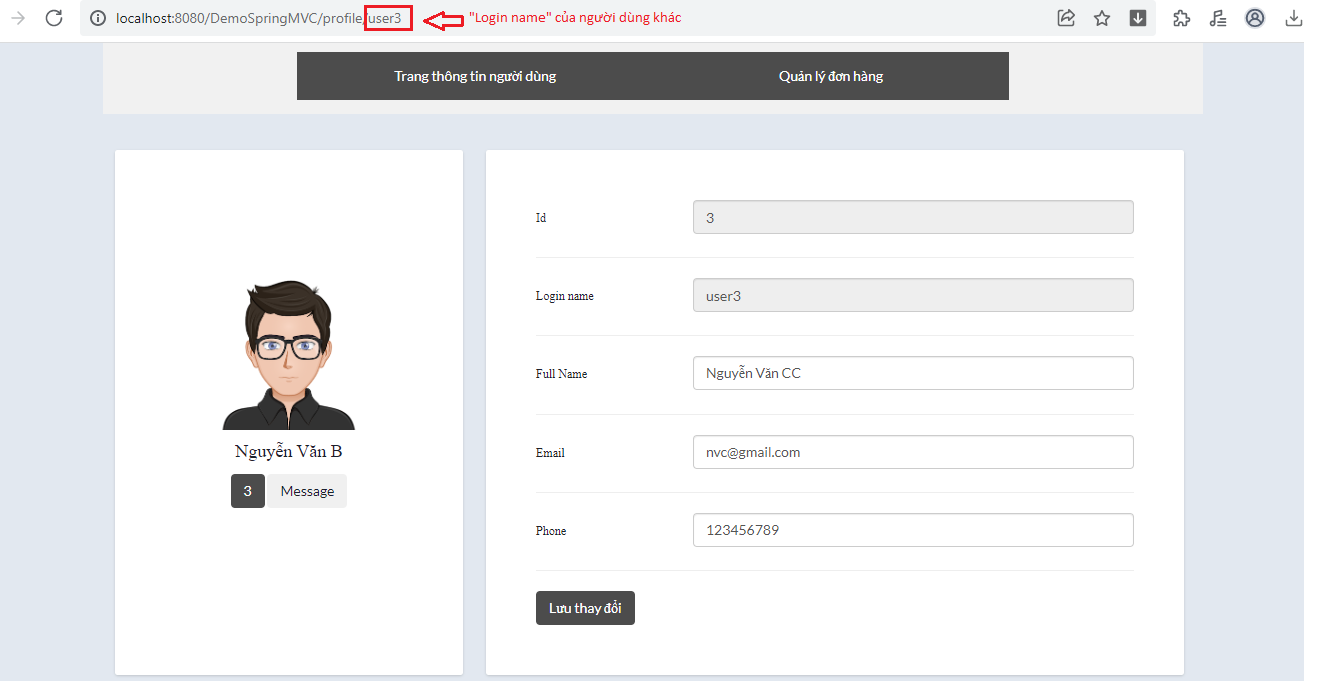
Trong project, tại trang xem thông tin cá nhân, để ý trên url người dùng sẽ thấy có thể tìm kiếm thông tin cá nhân theo “Login name” bằng cách thay đổi trực tiếp giá trị “user1” trên thanh url

Tuy nhiên vấn đề xảy ra khi người dùng thay đổi giá trị “user1” không phải của mình.

Lấy ví dụ tài khoản của người dùng với Login name: user2.



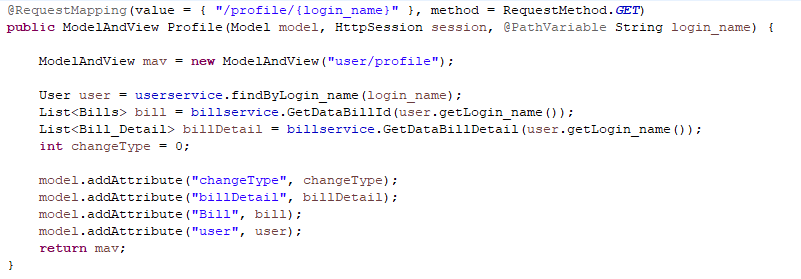
Người dùng với Login name: “user2”. Khi thay đổi giá trị “user2” trên url có thể truy cập và xem thông tin cá nhân của người dùng với Login name: “user3”



Như vậy, các thông tin cá nhân có thể bị đọc bởi người dùng khác.

#### Nguyên nhân

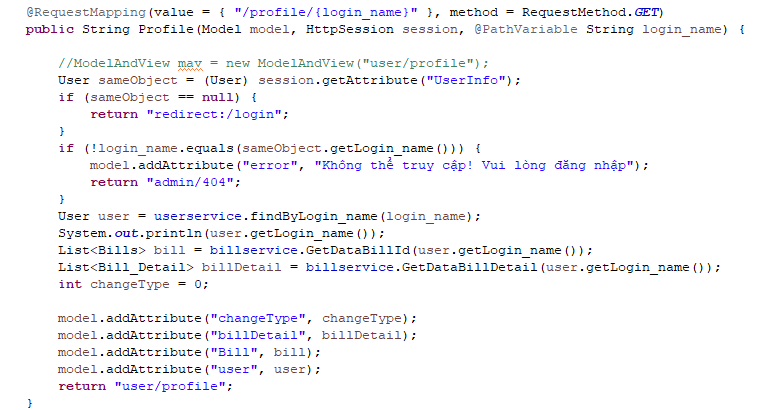
Nguyên nhân đến từ phía server đã không tiến hành kiểm tra trước khi người dùng tiến hành đăng nhập vào trang web.



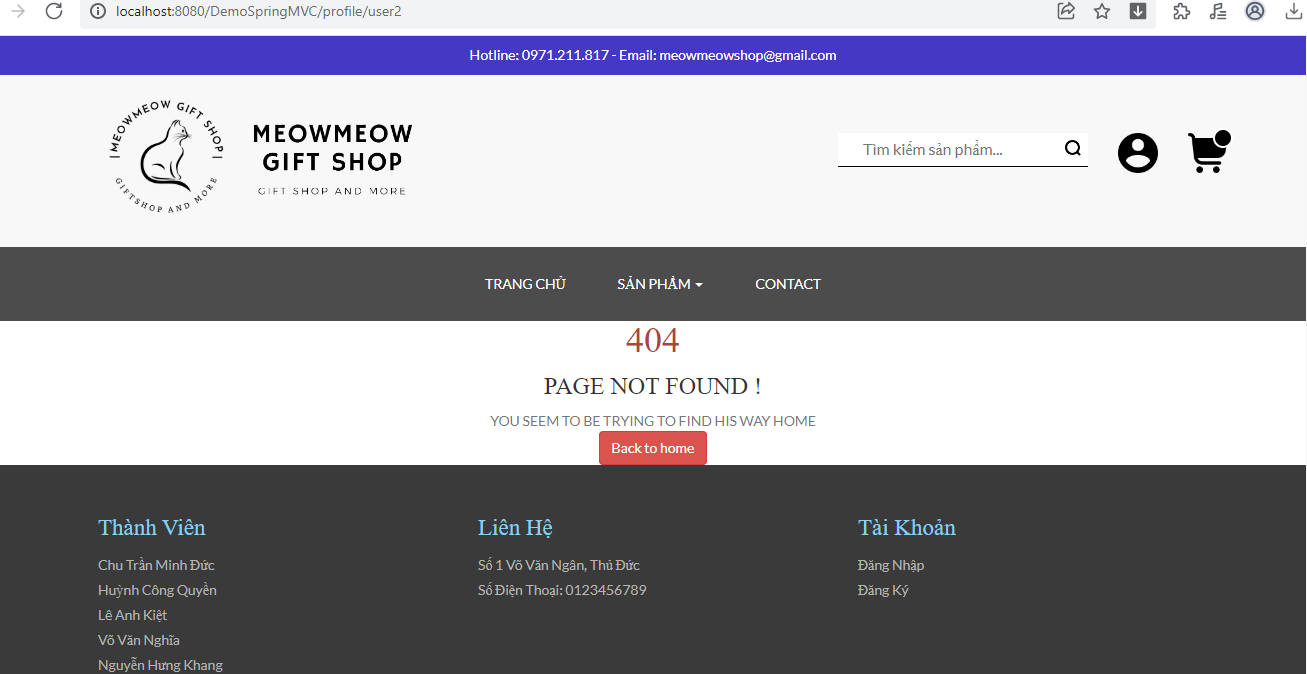
Việc giá trị Login name được lấy trực tiếp từ đường dẫn mà không qua bất kỳ kiểm tra nào đã khiến cho thông tin hóa cá nhân có thể dễ dàng bị truy cập bởi người dùng trái phép.

#### Khắc phục

Nên để khắc phục, ta sẽ tiến hành viết thêm code kiểm tra:



Khi người dùng cố ý thay đổi “Login name” để truy cập vào thông tin cá nhân của người khác, website sẽ dẫn đến màn hình lỗi:



IDOR là một lỗ hổng nguy hiểm có thể đe dọa quyền riêng tư của người dùng và tính toàn vẹn của ứng dụng của bạn. Việc tuân thủ các cơ chế phân quyền chặt chẽ và kiểm tra ứng dụng kĩ sẽ giúp các bạn hạn chế được nguy cơ về lỗ hổng bảo mật IDOR.

## Quét bằng OWAS ZAP

### Các lỗi OWASP ZAP quét được



### Vulnerable Library

#### Khái niệm

Vulnerabe library là các thành phần thư viện chứa các lỗi bảo mật có thể bị tấn công bởi hacker. Ngày nay, các trang web đều sử dụng rất nhiều các gói thư viện được xây dựng sẵn từ các bên thứ 3. Nếu lập trình viên không chú ý kỹ khi sử dụng các thư viện này. Rất có thể các thư viện chứa các lỗ hổng bảo mật chưa được phát hiện hoặc được phát hiện và được vá ở các phiên bản tiếp theo. Nhưng trang web vẫn sử dụng các gói thư viện cũ và dẫn đến các lỗi không đáng có.

#### Lỗ hổng trong project

ZAP đã quét được 1 số thư viện chứa lỗ hổng bảo mật trong trang web như:



Lỗi thư viện boostrap-3.1.1.min.js

* Phiên bản hiện tại là 3.1.1, phiên bản này có thể bị tấn công XSS thông qua các:

+ Plugin: tooltip, collapse, scrollspy.

+ Attribute: data-target, data-viewport, data-template, data-content, data-title.

* Link tham khảo: <https://security.snyk.io/package/npm/bootstrap/3.1.1>

Lỗi thư viện jquery.min.js

* Phiên bản này chứa các lỗ hổng có thể bị tấn công qua:

+ Cross-Site Scripting (XSS): kẻ tấn công chèn mã độc hoặc mã độc dạng script vào trang web, khiến người dùng khác thực thi mã độc đó trong trình duyệt của họ.

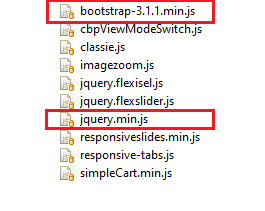
+ Denial-of-Service (DoS): Một lỗ hổng bảo mật trong jQuery có thể bị khai thác để gửi các yêu cầu không hợp lệ hoặc yêu cầu quá tải tới máy chủ, gây ra sự cố với dịch vụ hoặc hệ thống không thể sử dụng được.

+ Remote Code Execution (RCE): Nếu ứng dụng web chấp nhận và thực thi các lệnh trên máy chủ từ đầu vào không an toàn, kẻ tấn công có thể khai thác lỗ hổng này để thực thi mã nguy hiểm hoặc điều khiển máy chủ từ xa.

+ Prototype Polution: kẻ tấn công có thể sửa đổi Object.prototype

#### Khắc phục

Trang web sử dụng các thư viện cũ, lỗi thời, chứa các lỗ hổng đã được thông báo và sửa lỗi ở các phiên bản tiếp theo. Vì vậy, việc cập nhật phiên bản thư viện là cần thiết đối với 2 thư viện này.



Link tải phiên bản boostrap mới nhất: <https://getbootstrap.com/docs/5.3/getting-started/download/>

Link tải phiên bản jquery mới nhất: <https://code.jquery.com/jquery-3.7.0.min.js>