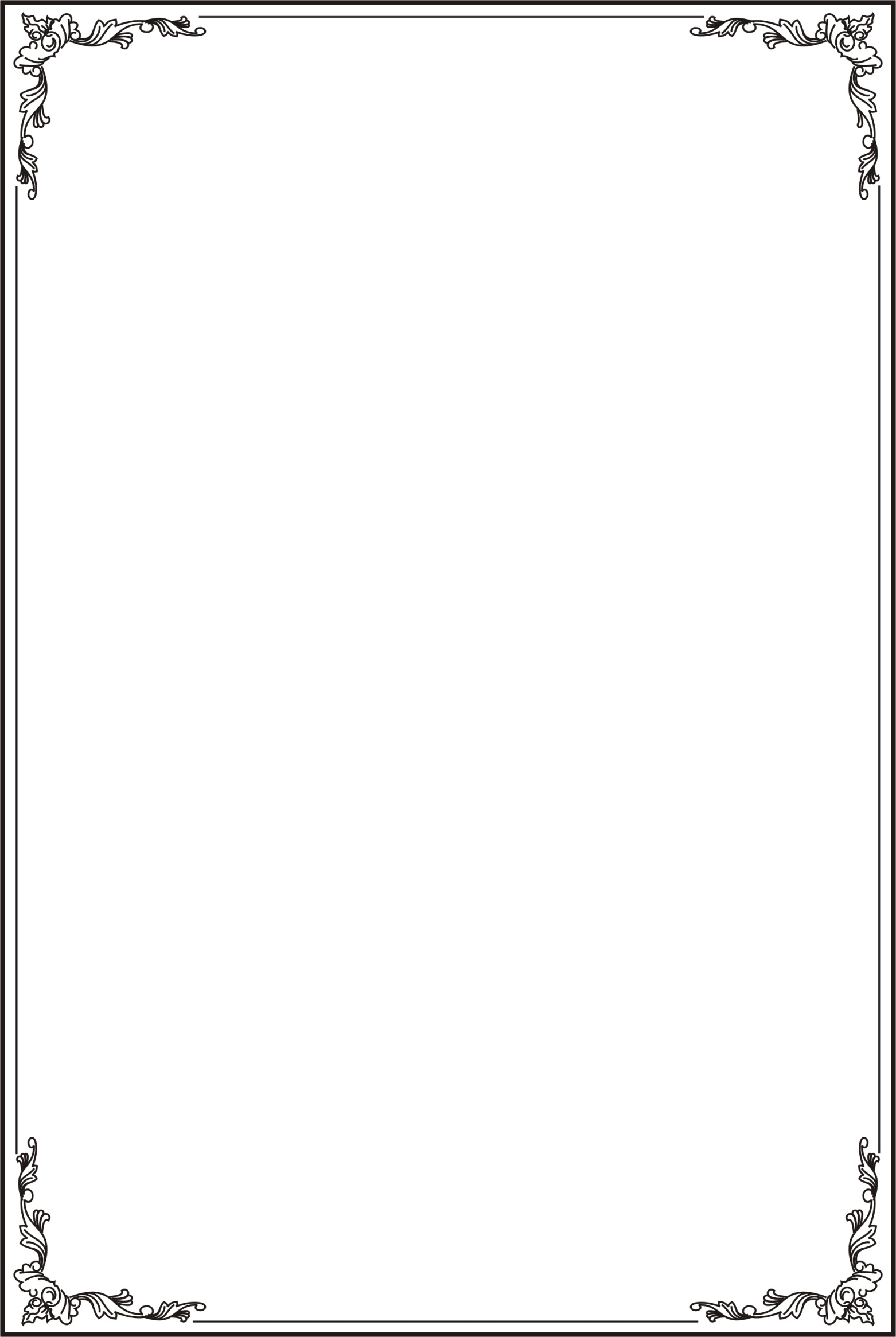
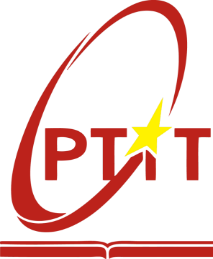
****BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

~~~~~~\*~~~~~~

**BÁO CÁO CHUYÊN ĐỀ  
AN TOÀN PHẦN MỀM**

***Đề tài:***

**XÂY DỰNG HỆ THỐNG THANH TOÁN TRỰC TUYẾN KẾT HỢP MD5 VÀ AES**

**GVHD: TS. Huỳnh Trọng Thưa**

**Thực hiện: Nguyễn Kim Hiệp N14DCAT063**

**Nguyễn Quang Tuấn Lộc N14DCAT097**

**Lớp: D14CQAT01-N**

**Khóa: 2014 – 2019**

**Hệ: Đại học chính quy**

**TPHCM, 11-2018**

**MỤC LỤC**

[Bảng chia nhiệm vụ 3](#_Toc531304457)

[Mục lục hình ảnh 3](#_Toc531304458)

[CHƯƠNG 1: ĐẶC TẢ CHƯƠNG TRÌNH 1](#_Toc531304459)

[**1.1** **Tổng quan về giao diện của ứng dụng** 1](#_Toc531304460)

[CHƯƠNG 2: THIẾT KẾ CHƯƠNG TRÌNH 3](#_Toc531304461)

[Mô hình của ứng dụng 3](#_Toc531304462)

[**2.1** **Giải thuật** 4](#_Toc531304463)

[ Kiểm tra mật khẩu: 4](#_Toc531304464)

[ Xuất mật khẩu: 4](#_Toc531304465)

[ Đăng nhập: 4](#_Toc531304466)

[ Hàm thêm vào giỏ hàng: 4](#_Toc531304467)

[ Hàm thanh toán: 4](#_Toc531304468)

[CHƯƠNG 3: XÂY DỰNG CHƯƠNG TRÌNH 5](#_Toc531304469)

[**3.1** **Chuẩn bị** 5](#_Toc531304470)

[**3.2** **Code** 5](#_Toc531304471)

[ Hàm login dươc mã hóa trước khi gửi đi tại client : 5](#_Toc531304472)

[ Hàm tạo Token : 5](#_Toc531304473)

[ Hàm mã hóa giỏ hàng và thanh toán AES 6](#_Toc531304474)

[ Tạo Intercepter để check token còn hạn sử dụng ko 7](#_Toc531304475)

[ Gắn Token vào đầu header sử dụng 7](#_Toc531304476)

[CHƯƠNG 4: KẾT QUẢ 9](#_Toc531304477)

[**4.1 Kết quả đạt được.** 9](#_Toc531304478)

# Bảng chia nhiệm vụ

|  |  |
| --- | --- |
| **Nguyễn Kim Hiệp** | **Nguyễn Quang Tuấn Lộc** |
| Tạo Token dùng SHA-1 | Xây dựng Frontend người dùng |
| Xây dựng các API | Encrypted AES |
| Xây dựng giải pháp MD5 cho Login | Xây dựng Database |

# Mục lục hình ảnh

[Hình 1: Giao diện đăng nhập 1](#_Toc531304657)

[Hình 2: Giao diện mua hàng 1](#_Toc531304658)

[Hình 3: Giao diện đơn hàng 2](#_Toc531304659)

[Hình 4: Giao diện thanh toán trực tuyến 2](#_Toc531304660)

[Hình 6: Sơ đồ mã hóa Password 3](#_Toc531304661)

[Hình 7: Sơ đồ mã hóa Token 3](#_Toc531304662)

[Hình 8 : Hàm MD5 password tại client 5](#_Toc531304663)

[Hình 9 : Hàm mã hóa MD5 khi tạo User 5](#_Toc531304664)

[Hình 10 : Tạo Token trên Server 5](#_Toc531304665)

[Hình 10 : Lưu Token trên Client để sử dung 6](#_Toc531304666)

[Hình 11 : Mã hóa AES thanh toán 6](file:///C:\Users\ghost\Downloads\Báo%20cáo%20ATPM.docx#_Toc531304667)

[Hình 12 : Mã hóa AES cho giỏ hàng 7](#_Toc531304668)

[Hình 13 : Check Token 7](#_Toc531304669)

[Hình 14 : Gắn Token 7](#_Toc531304670)

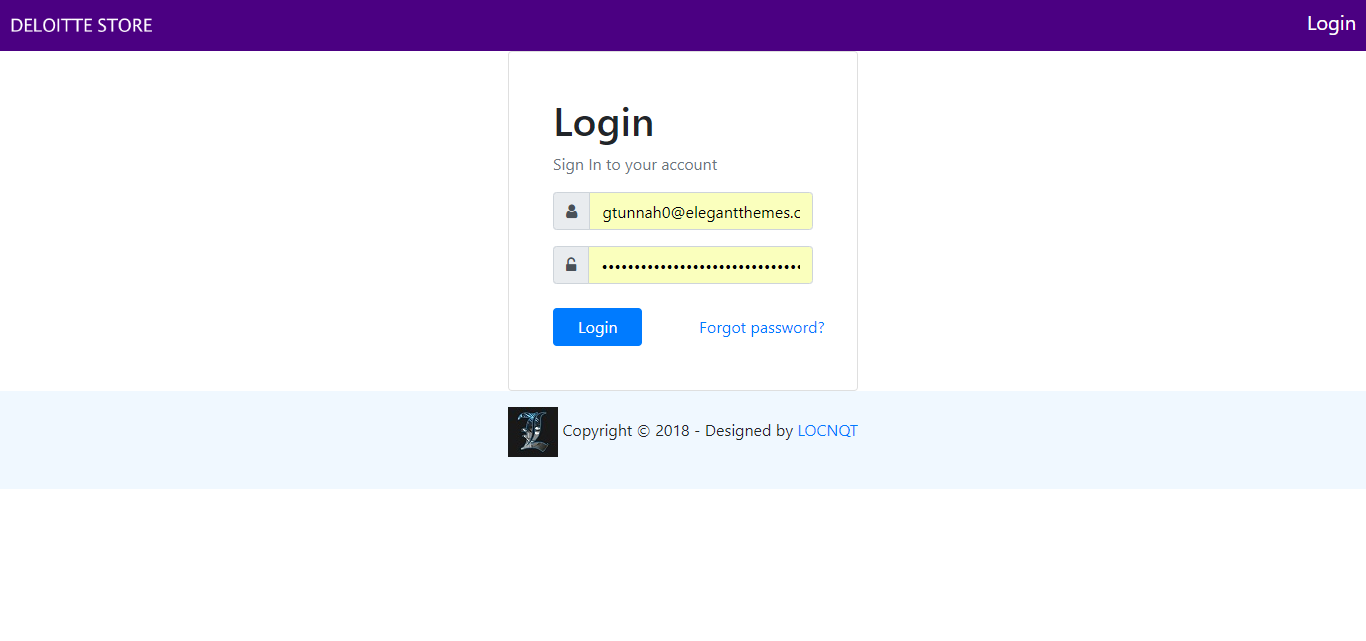
[Hình 15 : Dùng Guard chắn người dùng vào trang cần login 8](#_Toc531304671)

[Hình 16: Thanh toán thành công 9](#_Toc531304672)

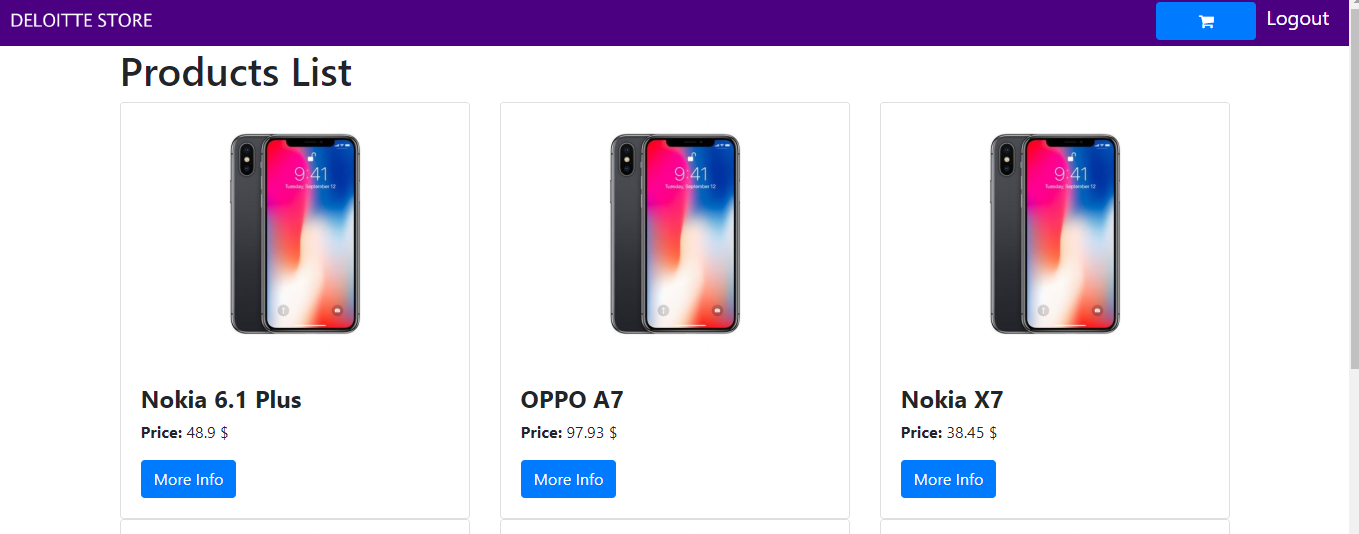
[Hình 20 : Mã thẻ bị mã hóa 10](#_Toc531304673)

# CHƯƠNG 1: ĐẶC TẢ CHƯƠNG TRÌNH

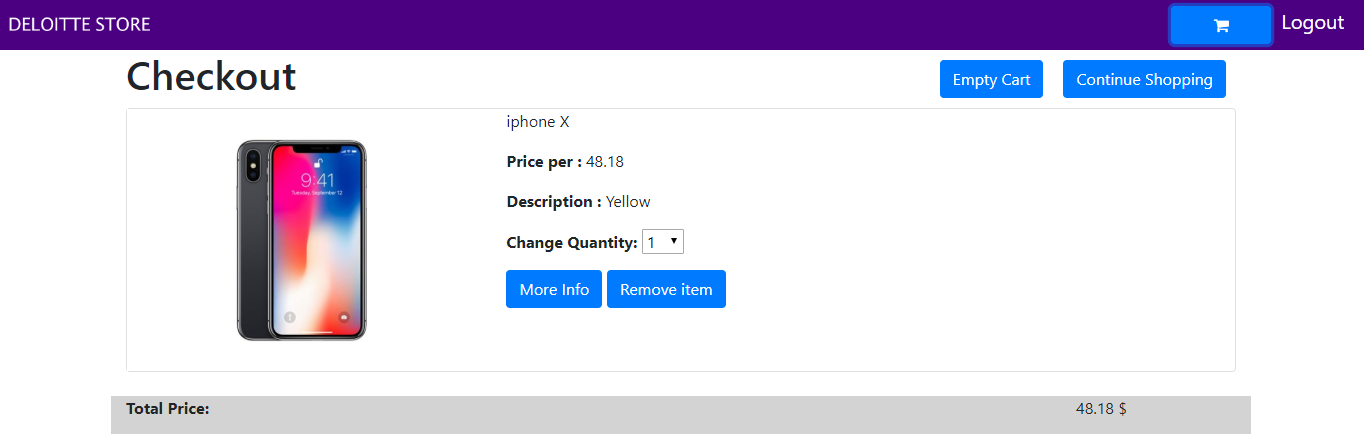
## **Tổng quan về giao diện của ứng dụng**



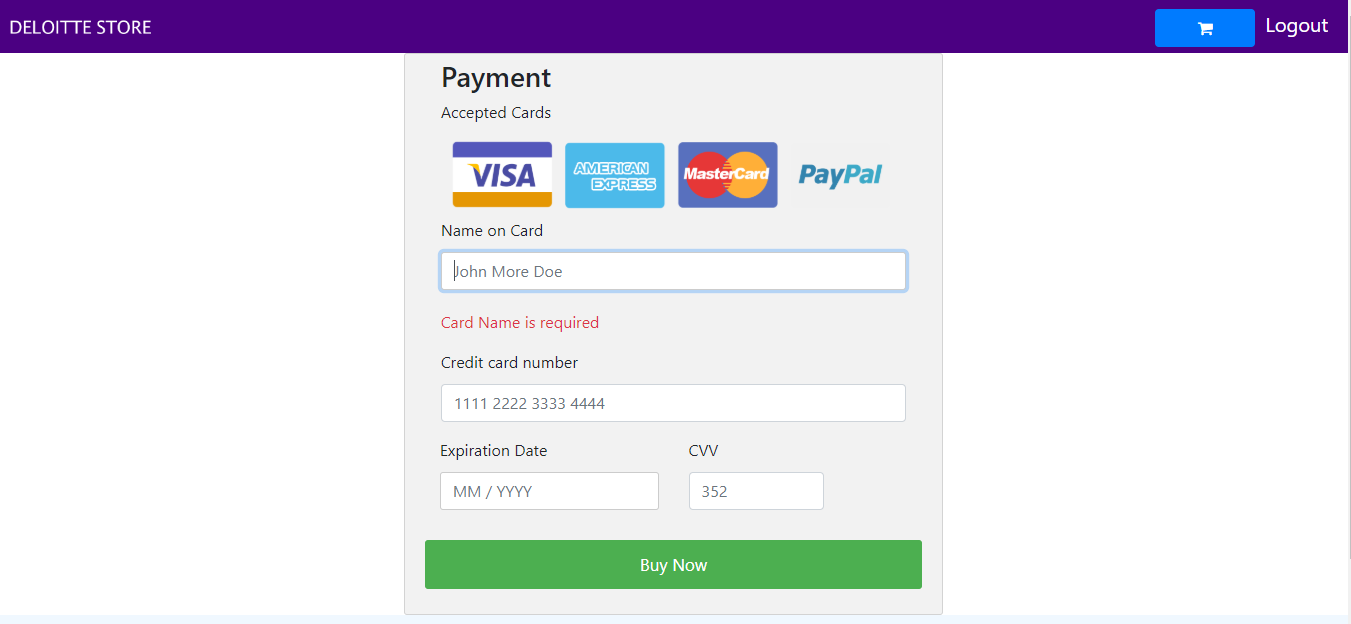
Hình 1: Giao diện đăng nhập



Hình 2: Giao diện mua hàng



Hình 3: Giao diện đơn hàng



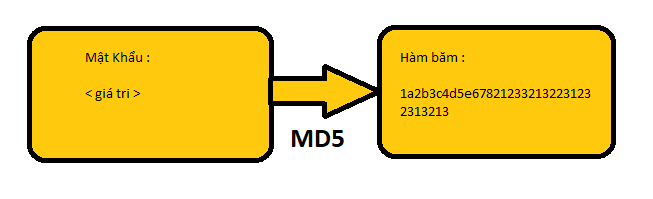
Hình 4: Giao diện thanh toán trực tuyến

# CHƯƠNG 2: THIẾT KẾ CHƯƠNG TRÌNH

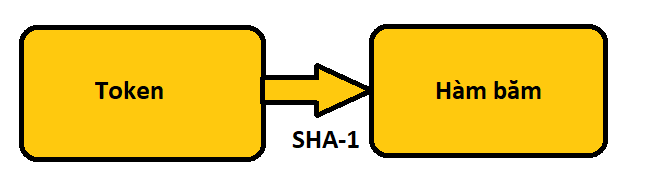
# Mô hình của ứng dụng



Hình 5: Mô hình Web API



Hình 6: Sơ đồ mã hóa Password



Hình 7: Sơ đồ mã hóa Token

1. **Giải thuật**

* Kiểm tra mật khẩu:

Trước khi mật khẩu được gửi lên Server sẽ được giải mã qua mã hóa MD5

* Xuất mật khẩu:

Khi một tài khoản mới được tạo mật khẩu cũng được mã hóa MD5 và lưu vào DataBase

* Đăng nhập:

Mật khẩu khi đăng nhập thành công sẽ được trả về Token để giữ trong suốt thời gian duyệt Web. Thời gian của 1 Token là 30 phút.

Token sẽ được mã hóa qua SHA-1.

* Hàm thêm vào giỏ hàng:

Khi người dùng chọn lệnh Add to Cart thì sẽ gửi 1 lệnh Post tới Database, database sẽ lưu xuống cơ sở dữ liệu, và 1 bản sẽ lưu trên Storge của trình duyệt.

* Hàm thanh toán:

Người dùng chọn thương thức thanh toán thì toàn bộ thông tin người dùng sẽ được mã hóa AES, sau đó gửi lên Server. Server sẽ giải mã và kiểm tra thông tin. Sau đó sẽ gửi 1 mã xác nhận OTP cho người dùng. Người dùng sẽ nhập mã OTP để xác nhận hoàn tất. Mọi thông tin sẽ được lưu dưới database

# CHƯƠNG 3: XÂY DỰNG CHƯƠNG TRÌNH

1. **Chuẩn bị**

Công cụ : Visual Studio 2017 (ASP.NET Core 2.1), Visual Studio Code

Ngôn ngữ : C#, Angular

1. **Code**

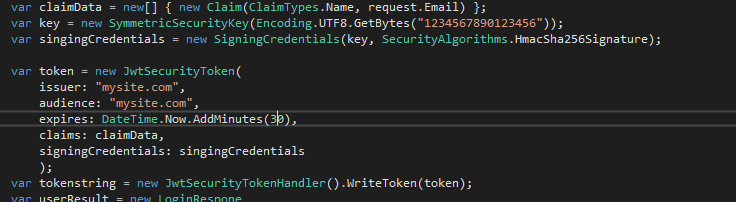
* Hàm login dươc mã hóa trước khi gửi đi tại client :



Hình 8 : Hàm MD5 password tại client



Hình 9 : Hàm mã hóa MD5 khi tạo User

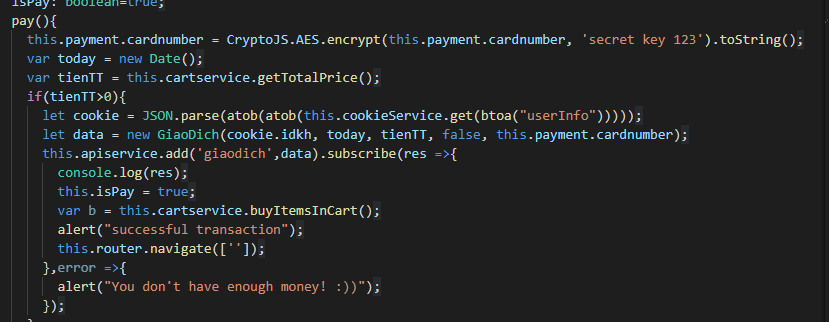
* Hàm tạo Token :

Hình 10 : Tạo Token trên Server



Hình 10 : Lưu Token trên Client để sử dung

* Hàm mã hóa giỏ hàng và thanh toán AES

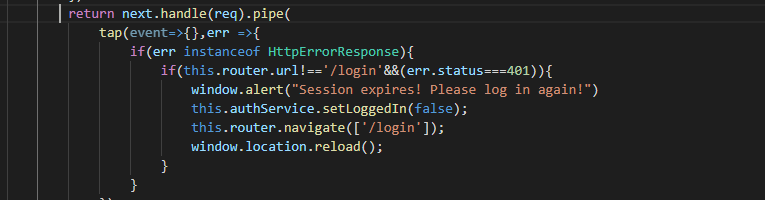




Hình 11 : Mã hóa AES thanh toán

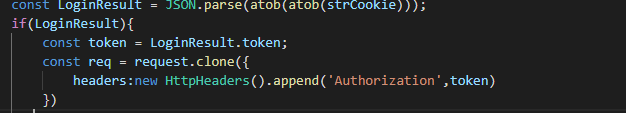
Hình 12 : Mã hóa AES cho giỏ hàng

* Tạo Intercepter để check token còn hạn sử dụng ko

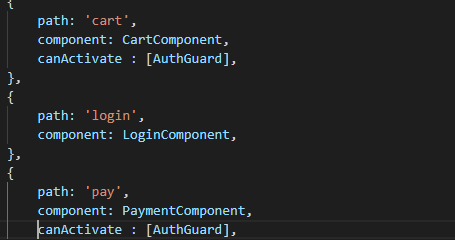


Hình 13 : Check Token

* Gắn Token vào đầu header sử dụng



Hình 14 : Gắn Token



Hình 15 : Dùng Guard chắn người dùng vào trang cần login

# CHƯƠNG 4: KẾT QUẢ

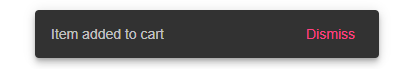
## **4.1 Kết quả đạt được.**



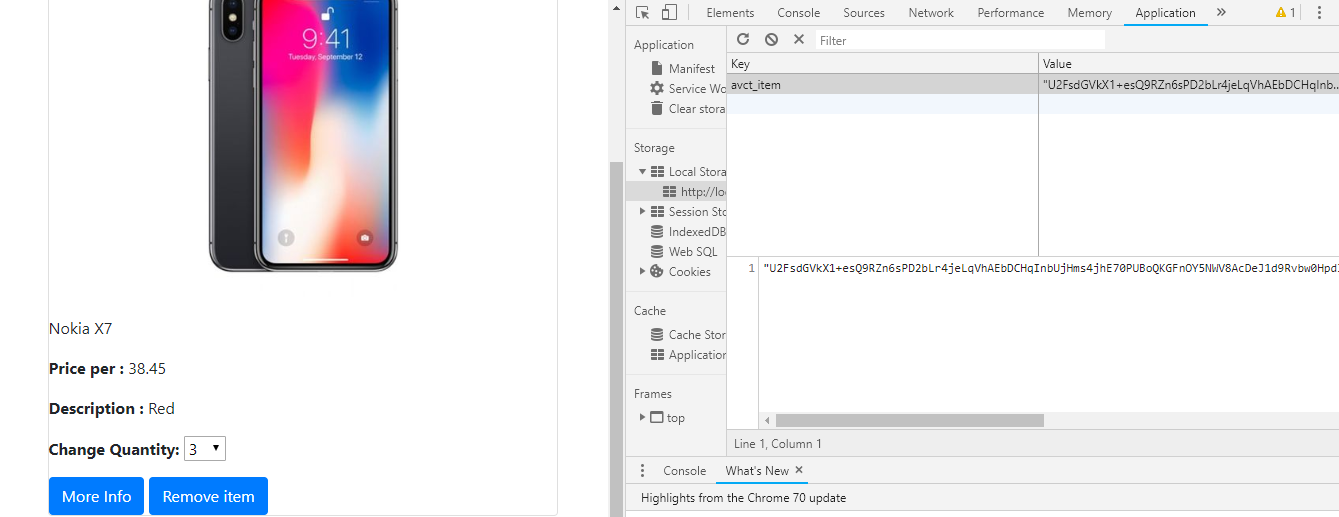
Hình 16: Thanh toán thành công



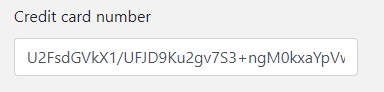
Hình 17: Đăng nhập thành công



Hình 18: Thêm vào giỏ hàng thành công



Hình 19: Thông tin giỏ hàng bị mã hóa



Hình 20 : Mã thẻ bị mã hóa