**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC SƯ PHẠM KĨ THUẬT TPHCM**

**KHOA ĐÀO TẠO CHẤT LƯỢNG CAO**

o0o



**ĐỒ ÁN CUỐI KÌ**

**MẬT MÃ HỌC**

**Đề tài: Xây dựng Website, cấp chứng chỉ SSL, mã hóa Cơ sở dữ liệu**

**GVHD: THS Trần Đắc Tốt**

**SVTH**

**- Nguyễn Hoàng Khánh Long- 20110518**

**Lớp: 2011CLCNW**

**Học Kỳ: II**

**Niên Khóa: 2022-2023**

**TPHCM, Ngày 10 tháng 05 năm 2023**

**Mục Lục**

**[I) Giới thiệu 1](#_30j0zll)**

**[1. Mục tiêu và phạm vi của đồ án 1](#_1fob9te)**

**[2. Lý do lựa chọn đề tài 1](#_3znysh7)**

**[II) CỞ SỞ LÝ THUYẾT 2](#_2et92p0)**

**[1) Cở bản về Website và quy trình xây dựng Website 2](#_tyjcwt)**

**[2) Định nghĩa và tầm quan trọng của chứng chỉ SSL 2](#_3dy6vkm)**

**[3) Các phương pháp mã hóa và lợi ích của việc mã hóa CSDL 3](#_1t3h5sf)**

**[III) THIẾT KẾ VÀ TRIỂN KHAI WEBSITE 3](#_4d34og8)**

**[1) Lựa chọn công nghệ xây dựng Website 3](#_2s8eyo1)**

**[2) Thiết kế giao diện người dùng 3](#_17dp8vu)**

**[3) Tạo và cấp chứng chỉ SSL cho Website 6](#_3rdcrjn)**

**[IV) Mã hóa Cơ sở dữ liệu 7](#_35nkun2)**

**[1. Bảo mật Cơ sở dữ liệu và các rủi ro liên quan 7](#_1ksv4uv)**

**[2. Áp dụng phương pháp mã hóa cơ sở dữ liệu 8](#_44sinio)**

**[V) Tổng kết 10](#_1y810tw)**

**[1) Tóm tắt 10](#_4i7ojhp)**

**[2) Đánh giá 10](#_2xcytpi)**

**[3) Đề xuất và cải tiến 11](#_1ci93xb)**

**[VI) Tài liệu tham khảo 12](#_3as4poj)**

1. **Giới thiệu**
2. **Mục tiêu và phạm vi của đồ án**
3. **Mục tiêu**

* Xây dựng một website có tính bảo mật cao: Mục tiêu chính là xây dựng một website có khả năng bảo vệ thông tin người dùng, đảm bảo tính toàn vẹn và bảo mật của dữ liệu truyền và lưu trữ trên website.
* Cấp chứng chỉ SSL: Mục tiêu là triển khai chứng chỉ SSL (Secure Socket Layer) cho website, giúp tạo ra một kênh truyền thông an toàn giữa máy chủ và người dùng, đảm bảo rằng dữ liệu được truyền tải một cách bảo mật và không bị giả mạo.
* Mã hóa CSDL: Mục tiêu là áp dụng các phương pháp mã hóa để bảo vệ dữ liệu trong Cơ sở dữ liệu (CSDL) của website, đảm bảo rằng dữ liệu không thể truy cập hoặc đọc được một cách trái phép.

1. **Phạm vi**

* Xây dựng website: xây dựng website bán sách bao gồm 2 trang dành cho Admin, User. Ngôn ngữ chính là Java. Thiết kế giao diện, triển khai chứng chỉ SSL, mã hóa Cơ sở dữ liệu
* Cấp chứng chỉ SSL: Tập trung vào việc triển khai chứng chỉ SSL cho website, bao gồm quy trình cấp phát chứng chỉ, cấu hình và cài đặt trên máy chủ web.
* Mã hóa CSDL: Phạm vi cũng bao gồm áp dụng các phương pháp mã hóa dữ liệu đã học trong CSDL(RSA,AES,SHA-256), nhằm đảm bảo tính bảo mật của dữ liệu trong quá trình lưu trữ và truy xuất.

1. **Lý do lựa chọn đề tài**

* Tính cấp thiết và quan trọng của bảo mật: Trong thời đại số hóa ngày càng phát triển, việc bảo vệ thông tin và dữ liệu trở nên cực kỳ quan trọng. Bảo mật website, cấp chứng chỉ SSL và mã hóa CSDL là những biện pháp cơ bản để đảm bảo tính bảo mật và quyền riêng tư của người dùng.
* Xây dựng niềm tin và tạo uy tín cho người dùng: Một trang web được bảo mật tốt sẽ tạo sự tin tưởng và uy tín đối với người dùng. Việc triển khai chứng chỉ SSL và mã hóa CSDL giúp người dùng cảm thấy an tâm khi cung cấp thông tin cá nhân và giao dịch trực tuyến trên trang web.
* Nâng cao hiệu suất và độ tin cậy của hệ thống: Mã hóa CSDL và sử dụng chứng chỉ SSL giúp ngăn chặn các cuộc tấn công từ bên ngoài và truy cập trái phép vào hệ thống.Cho dù CSDL bị đánh cắp thì cũng bị mã hóa . Điều này đồng nghĩa với việc nâng cao hiệu suất hoạt động của hệ thống và đảm bảo độ tin cậy của dữ liệu trong CSDL.
* Học hỏi và phát triển kỹ năng: Đề tài này đòi hỏi sự hiểu biết về bảo mật, mã hóa và triển khai website. Nghiên cứu và thực hiện đề tài sẽ giúp nâng cao kiến thức và kỹ năng về xây dựng web và mật mã, mở ra cơ hội phát triển trong ngành công nghệ thông tin.

1. **CỞ SỞ LÝ THUYẾT**
2. **Cở bản về Website và quy trình xây dựng Website**

- Định nghĩa Website: Một website là một tập hợp các trang web liên kết với nhau, được truy cập thông qua mạng internet. Nó cung cấp thông tin, dịch vụ, và tương tác với người dùng.

- Quy trình xây dựng website: Quy trình xây dựng website bao gồm các bước như thu thập yêu cầu, thiết kế giao diện, triển khai và duy trì.Xây dựng cơ sở dữ liệu (SQL). Các công nghệ và ngôn ngữ như HTML, CSS, Java được sử dụng trong Website này.

1. **Định nghĩa và tầm quan trọng của chứng chỉ SSL**

- Định nghĩa: SSL (Secure Socket Layer) là một giao thức bảo mật dùng để tạo một kênh truyền thông an toàn giữa máy chủ và người dùng trên internet. Nó sử dụng mã hóa để đảm bảo tính toàn vẹn và bảo mật của dữ liệu truyền tải.

- Tầm quan trọng: Chứng chỉ SSL đóng vai trò quan trọng trong việc bảo vệ thông tin cá nhân và tạo niềm tin tưởng cho người dùng. Nó giúp ngăn chặn các cuộc tấn công giữa người trung gian, đảm bảo rằng dữ liệu không bị thay đổi hoặc đánh cắp trong quá trình truyền tải.

1. **Các phương pháp mã hóa và lợi ích của việc mã hóa CSDL**

- Phương pháp mã hóa CSDL: Có nhiều phương pháp mã hóa CSDL như mã hóa đối xứng (Symmetric Encryption), mã hóa không đối xứng (Asymmetric Encryption), và hàm băm (Hashing). Mỗi phương pháp có ưu điểm và nhược điểm riêng, và nhóm chứng em sử dụng mã AES, RC4,SHA-256.

- Lợi ích của mã hóa CSDL: Mã hóa CSDL giúp bảo vệ dữ liệu quan trọng trong Cơ sở dữ liệu khỏi việc truy cập trái phép. Nó đảm bảo tính bảo mật và quyền riêng tư của thông tin nhạy cảm như thông tin cá nhân, tài khoản tài khoản người dùng hay dữ liệu hệ thống.

1. **THIẾT KẾ VÀ TRIỂN KHAI WEBSITE**
2. **Lựa chọn công nghệ xây dựng Website**

- Nền tảng Web:

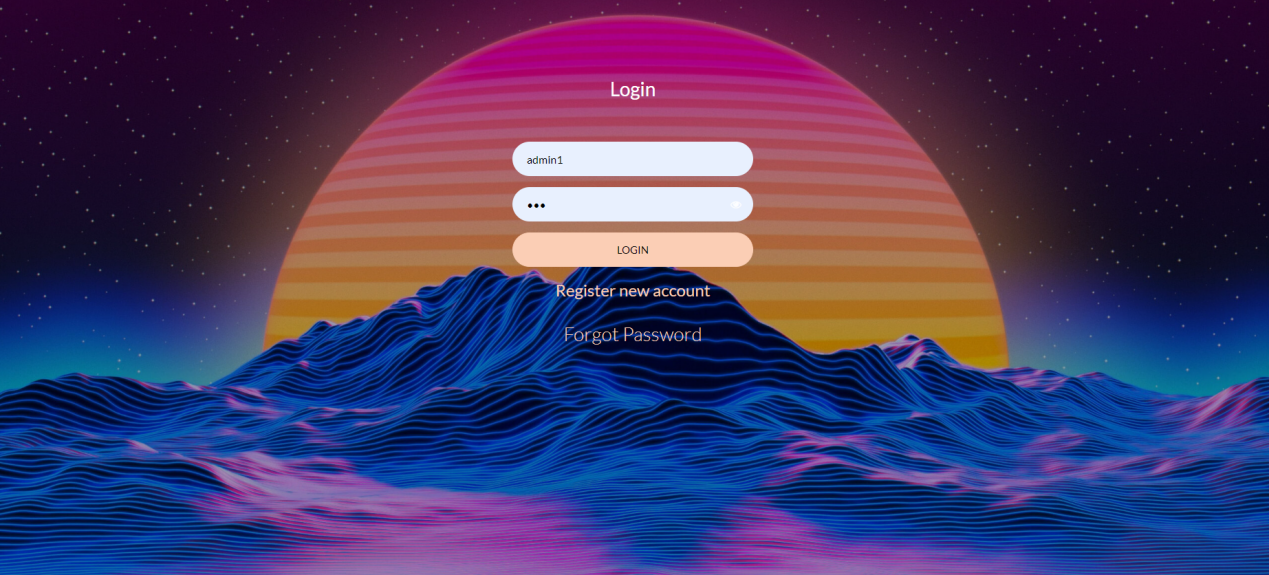
+ Xây dựng web bằng ngôn ngữ chính là Java

+ Xây dựng giao diện: HTML, CSS, JavaScript

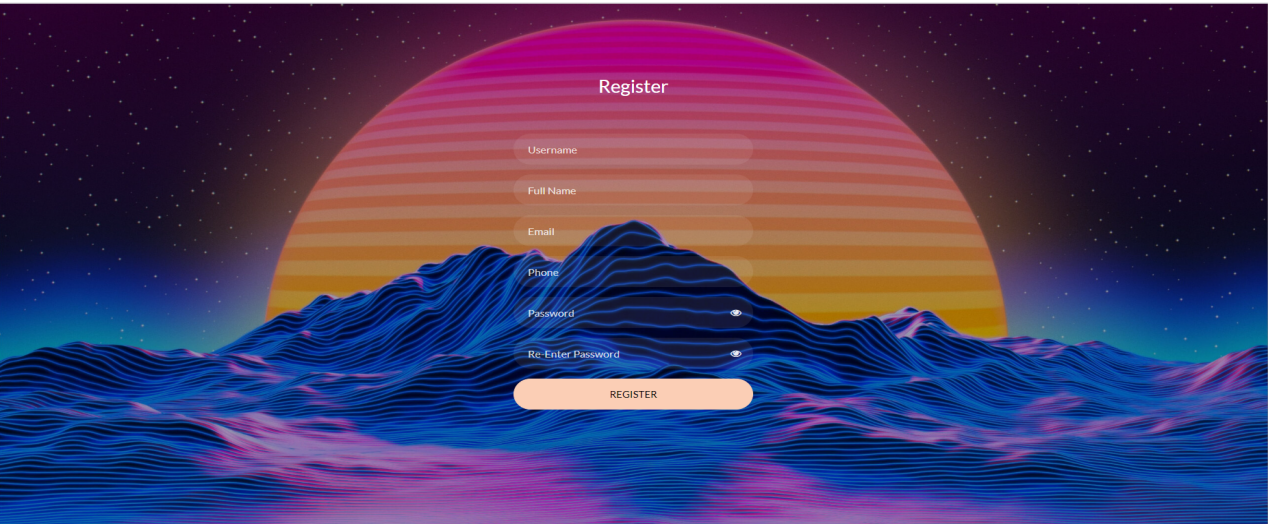
+ Ứng dụng: Eclipse

+ Cơ sở dữ liệu: Microsoft SQL Server Management Studio (SQL)

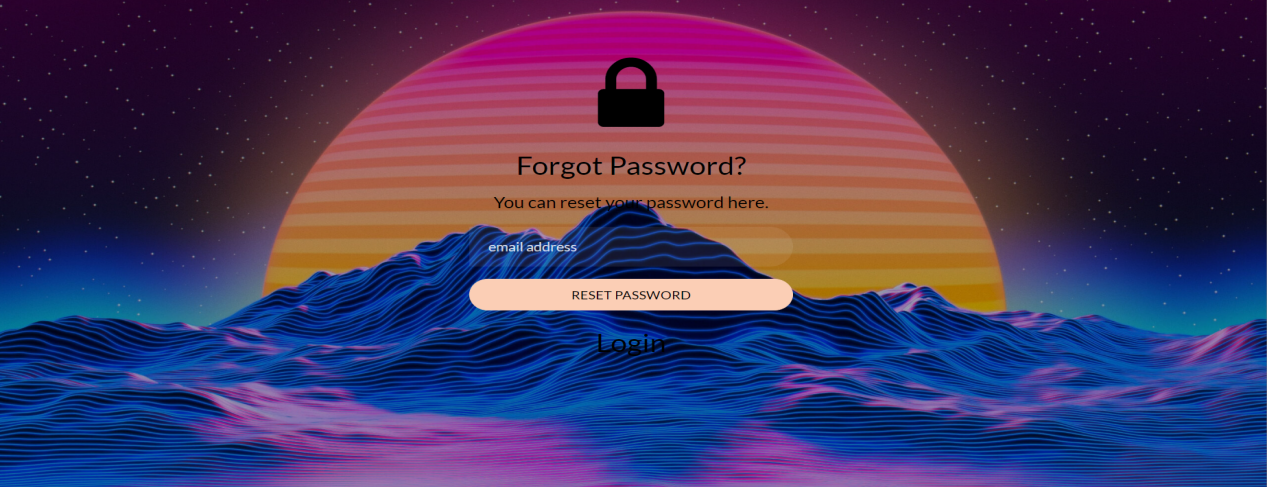
1. **Thiết kế giao diện người dùng**



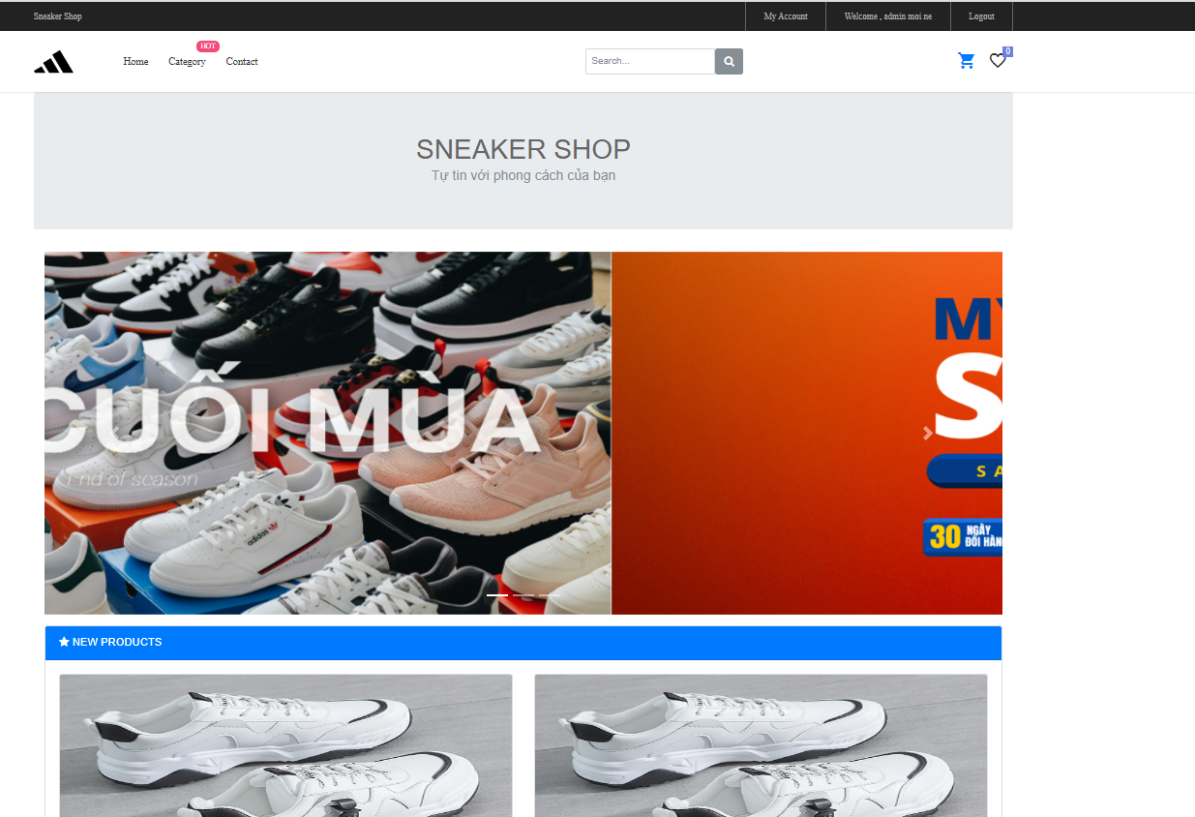
Giao diện đăng nhập



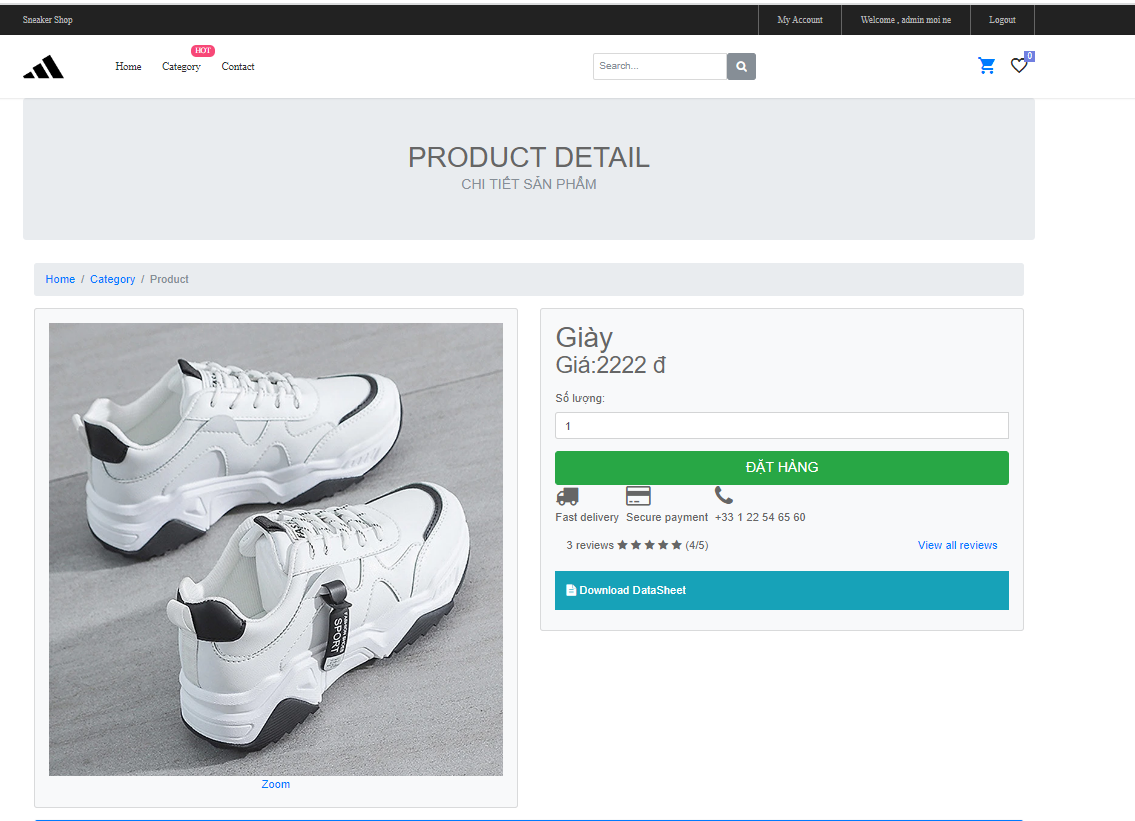
Giao diện Đăng ký tài khoản user mới



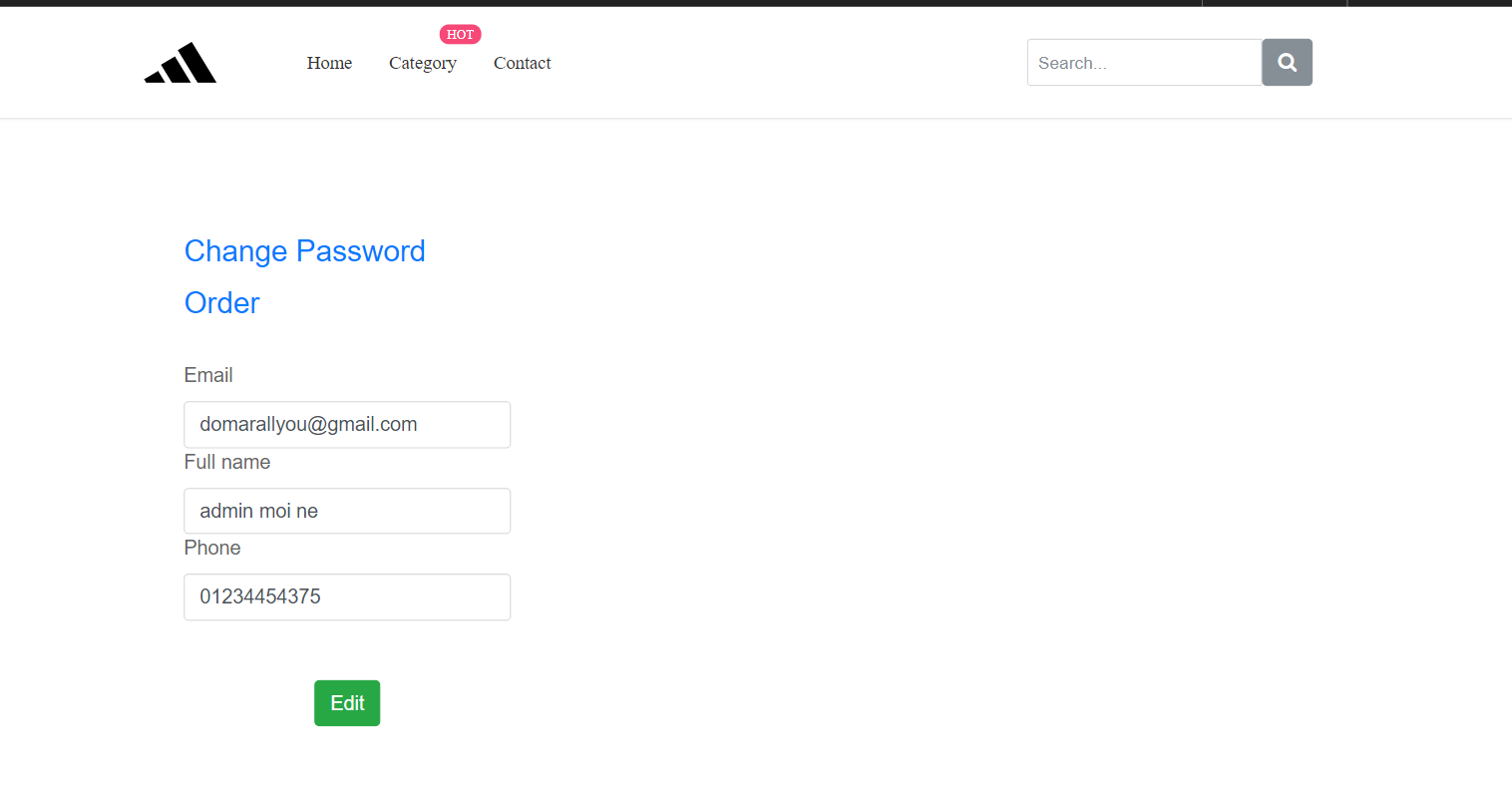
Giao diện phục vụ cho người dùng muốn lấy lại mật khẩu



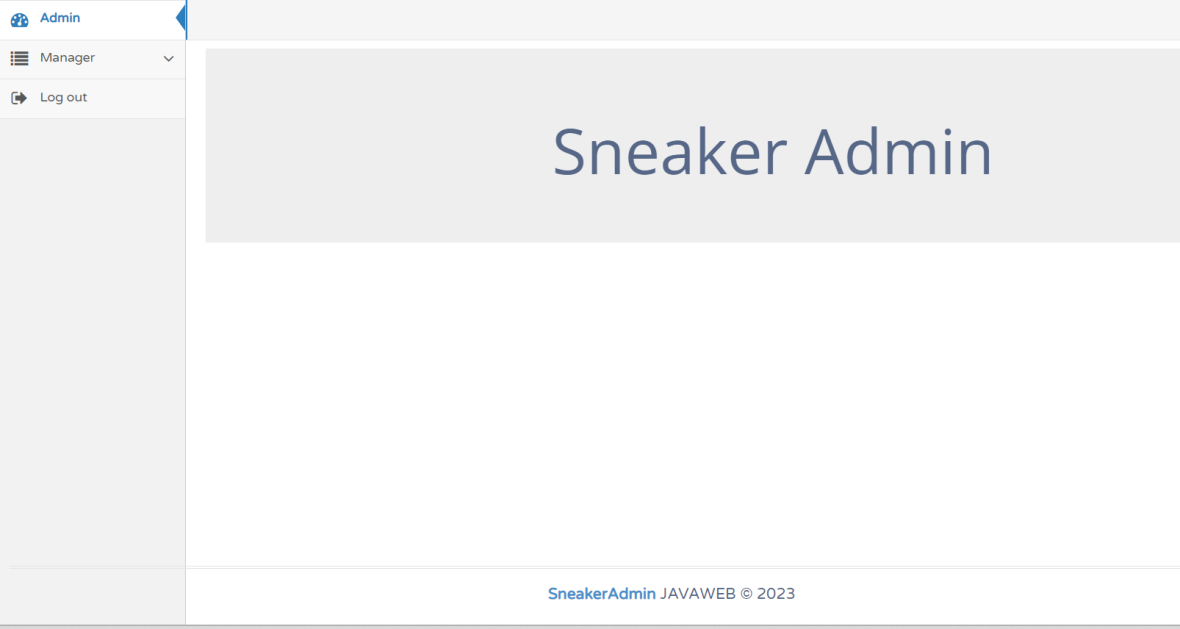
Giao diện sau khi đăng nhập đối với tài khoản có quyền user



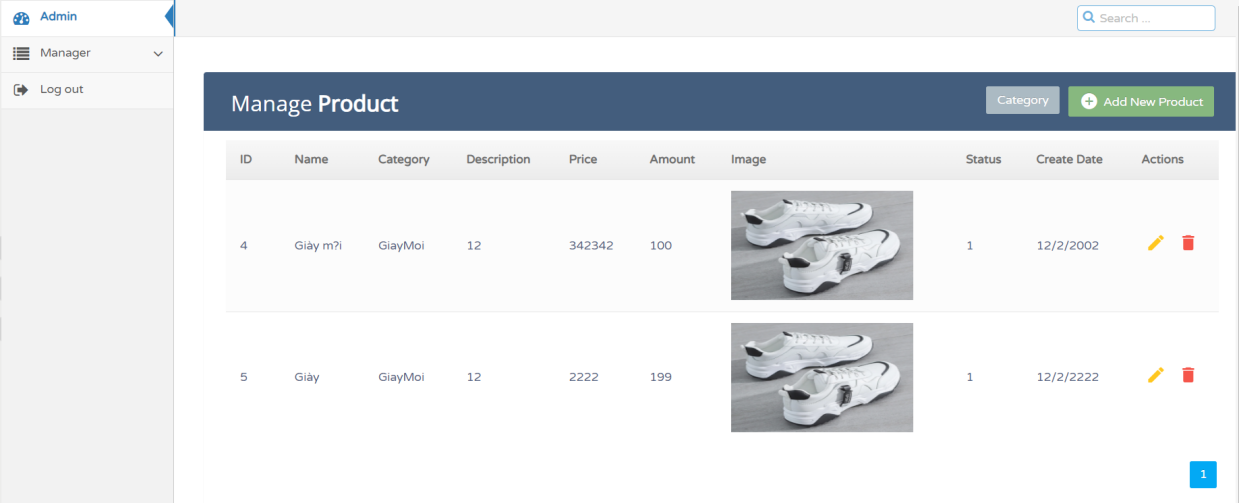
Giao diện thông tin của một sản phẩm được bày bán



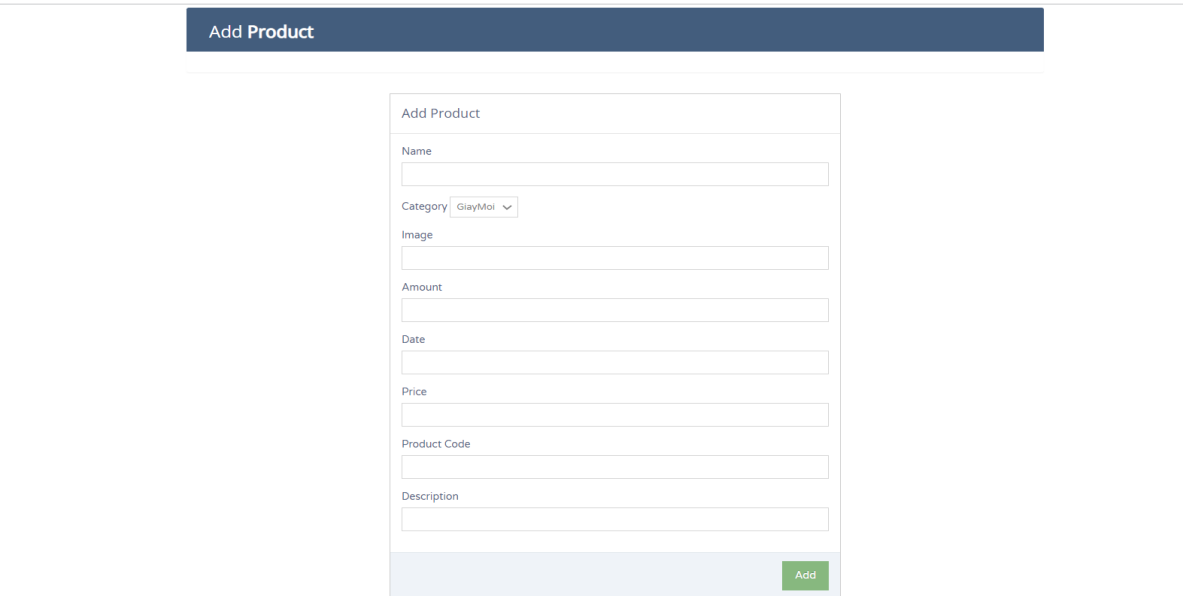
Xem lại thông tin cá nhân của người dùng



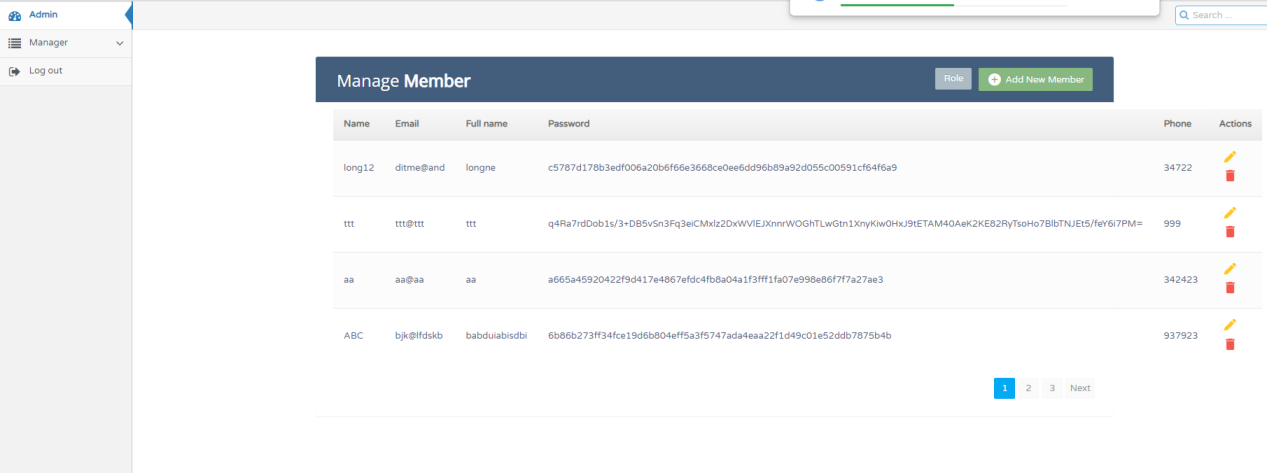
Giao diện Sau khi Login đối với tài khoản admin



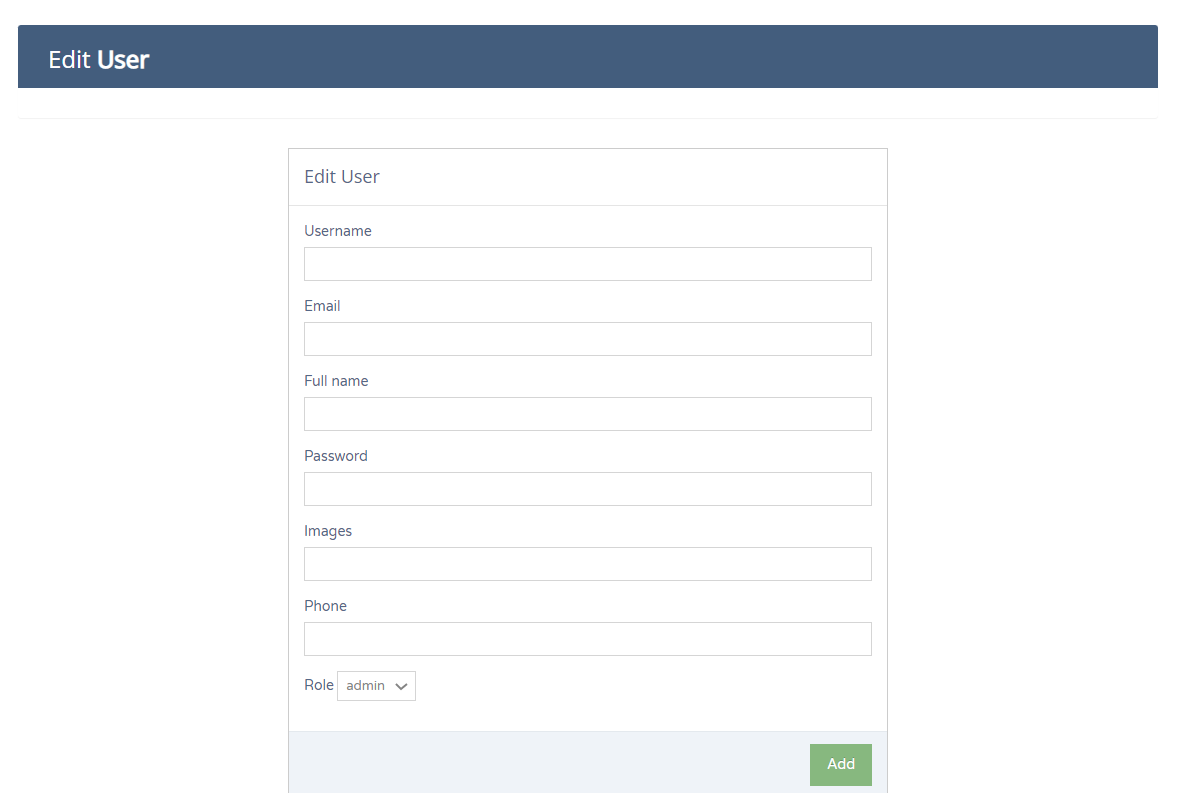
Giao diện đối với việc quản lý các sản phẩm của admin



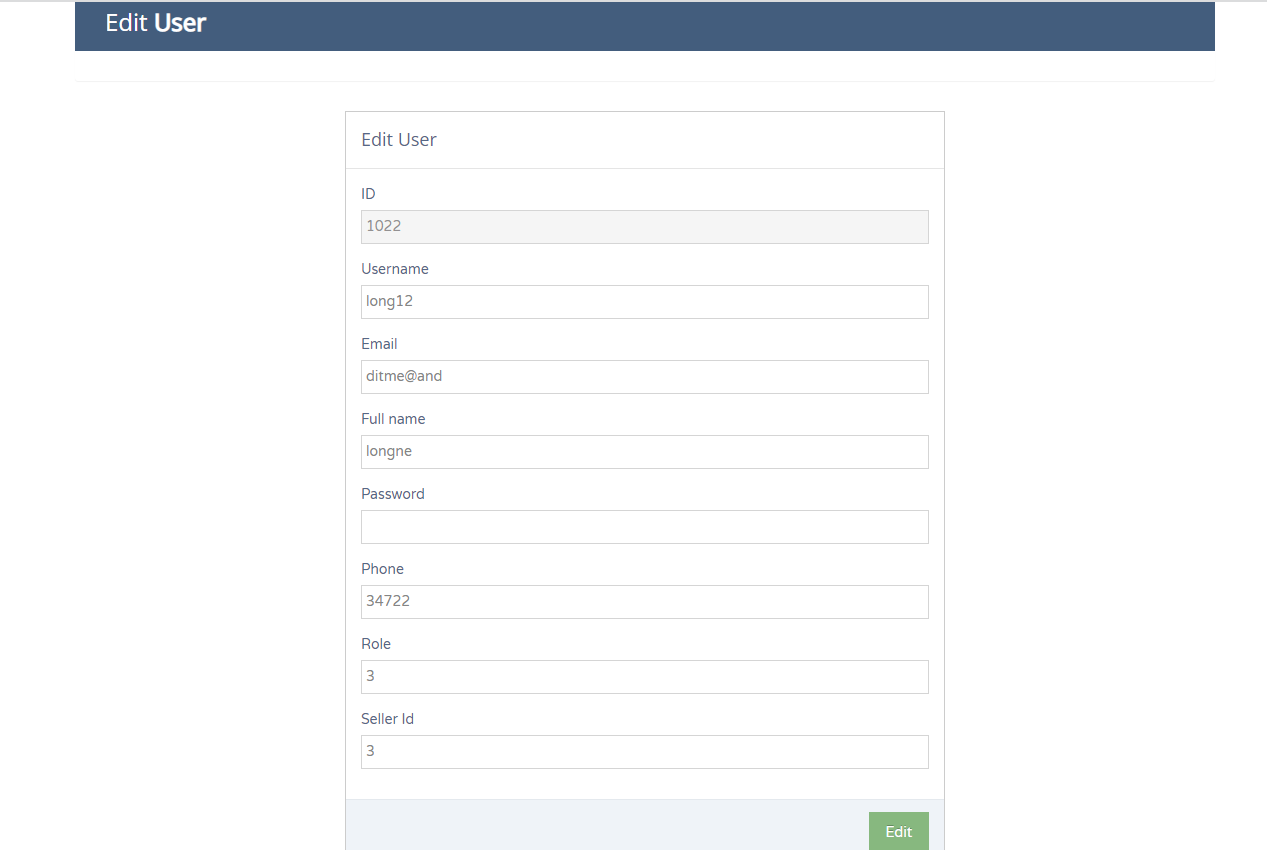
Giao diện khi admin muốn thêm một sản phẩm mới



Giao diện thông tin về các tài khoản của hệ thống

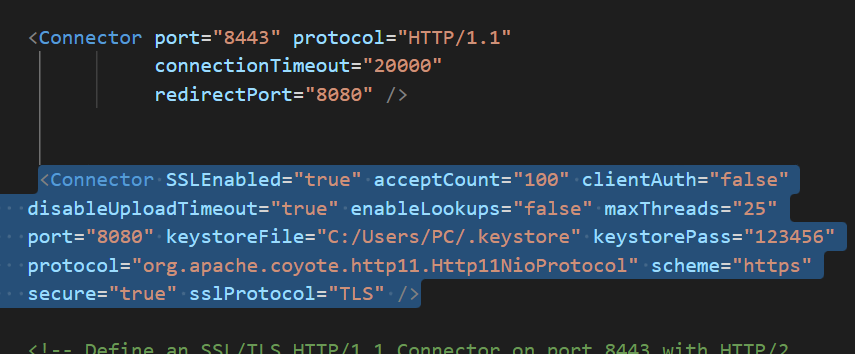


Giao diện khi admin muốn tạo một tài khoản mới

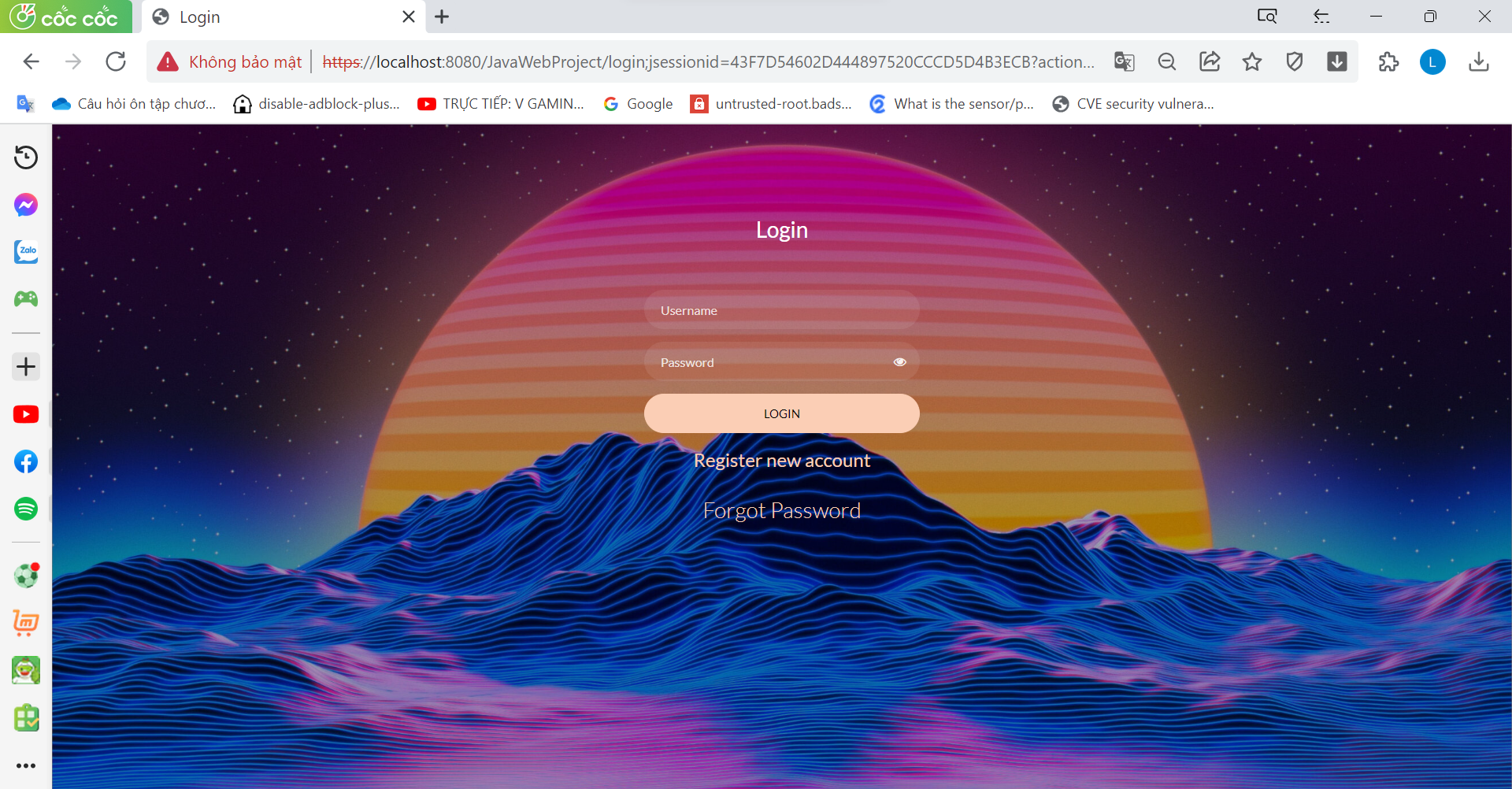


Giao diện khi admin muốn chỉnh sửa thông tin của một tài khoản có sẵn.

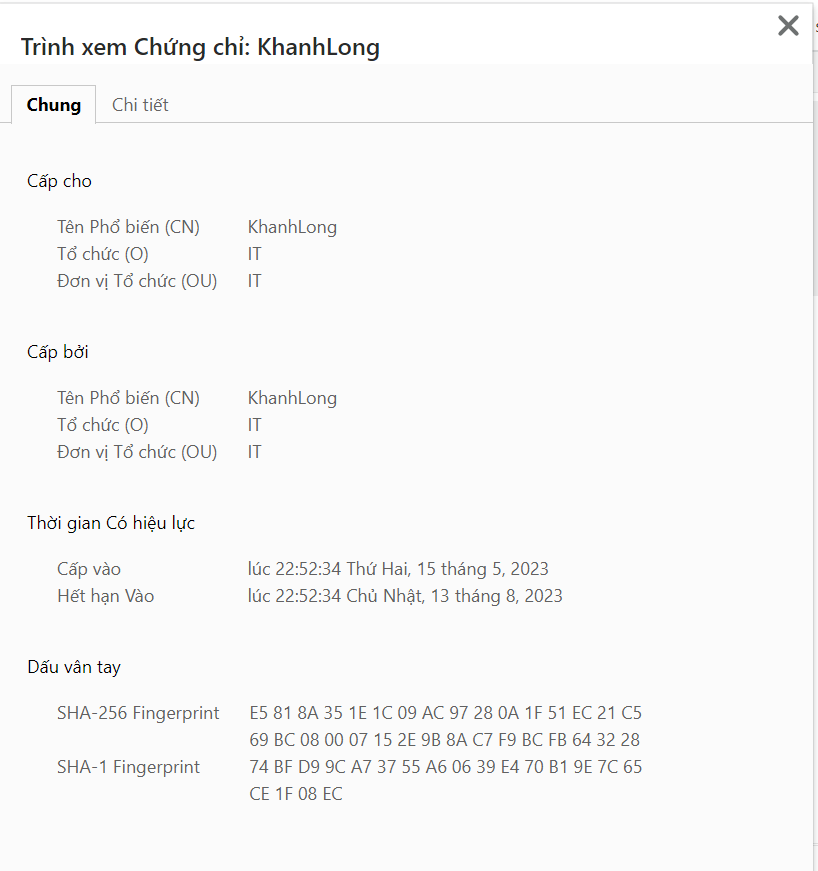
1. **Tạo và cấp chứng chỉ SSL cho Website**



File server.xml



Địa chỉ https



Chứng chỉ SSL

1. **Mã hóa Cơ sở dữ liệu**
2. **Bảo mật Cơ sở dữ liệu và các rủi ro liên quan**

- Bảo mật CSDL: Bảo mật CSDL đảm bảo tính toàn vẹn, sự riêng tư và sẵn sàng của dữ liệu trong cơ sở dữ liệu. Điều này bao gồm ngăn chặn truy cập trái phép, sửa đổi trái phép và tiết lộ thông tin quan trọng.

- Rủi ro liên quan: CSDL có thể đối mặt với các rủi ro như tấn công từ bên ngoài, nhân viên bất hảo hoặc vi phạm quyền truy cập, lỗ hổng bảo mật trong phần mềm hoặc hệ điều hành, và việc mất dữ liệu do thiên tai hoặc sự cố kỹ thuật.

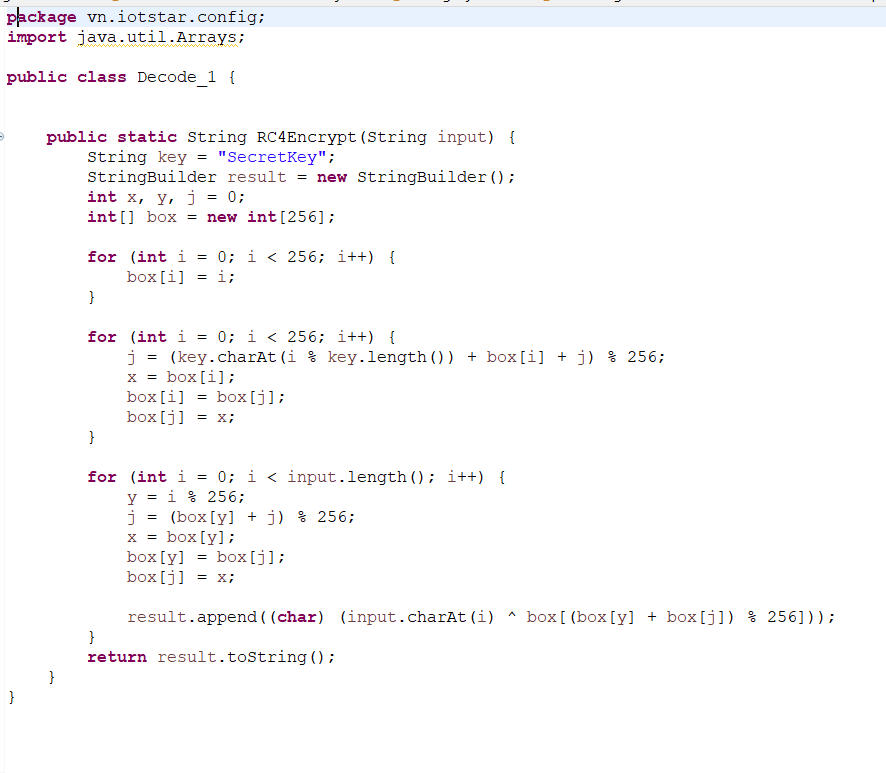
1. **Áp dụng phương pháp mã hóa cơ sở dữ liệu**

* **AES (Advanced Encryption Standard)**: là một thuật toán mã hóa đối xứng rất mạnh được sử dụng rộng rãi trong bảo mật thông tin.AES có khả năng mã hóa và giải mã dữ liệu với các khóa có độ dài 128, 192 hoặc 256 bit. AES đã được chứng minh là an toàn và hiệu quả trong nhiều ứng dụng, bao gồm bảo mật dữ liệu trong cơ sở dữ liệu.



Code mã hóa và giải mã AES

* **RC4 (Rivest Cipher 4)**: là một thuật toán mã hóa đối xứng, ban đầu được phát triển bởi Ron Rivest. RC4 có khả năng mã hóa dữ liệu dựa trên một khóa bí mật có độ dài từ 40 đến 2048 bit.



Code mã hóa RC4

* **SHA-256 (Secure Hash Algorithm 256-bit)**: là một hàm băm (hash function) thuộc gia đình các thuật toán SHA-2. SHA-256 chuyển đổi một khối dữ liệu đầu vào thành một giá trị băm dài 256 bit. SHA-256 được sử dụng rộng rãi trong việc xác thực dữ liệu và bảo mật, bao gồm việc lưu trữ mật khẩu, xác thực chữ ký điện tử và bảo vệ dữ liệu.



Code mã hask (SHA\_256)

1. **Tổng kết**
2. **Tóm tắt**

* Trong quá trình kiểm tra và đánh giá kết quả của dự án xây dựng trang web, các yếu tố quan trọng được xem xét bao gồm kiểm tra bảo mật và độ tin cậy của trang web, đánh giá hiệu suất và tốc độ truy cập, cũng như phân tích ưu điểm và nhược điểm của quá trình triển khai.

1. **Đánh giá**

* Bảo mật và độ tin cậy: Kiểm tra bảo mật trang web để đảm bảo an toàn thông tin và ngăn chặn các cuộc tấn công. Đánh giá cấp chứng chỉ SSL để đảm bảo việc mã hóa dữ liệu truyền tải và xác thực đáng tin cậy giữa máy chủ và người dùng.
* Hiệu suất và tốc độ truy cập: Đánh giá hiệu suất trang web trong việc đáp ứng yêu cầu của người dùng, bao gồm thời gian tải trang, thời gian phản hồi của máy chủ và khả năng xử lý đồng thời. Đánh giá tốc độ truy cập để đảm bảo người dùng có trải nghiệm truy cập nhanh chóng và không gặp trở ngại.

1. **Đề xuất và cải tiến**

**a) Bảo mật và độ tin cậy:**

- Nâng cao hệ thống xác thực người dùng bằng cách sử dụng các phương pháp xác thực hai yếu tố (2FA) hoặc xác thực đa yếu tố (MFA) để bảo vệ tài khoản người dùng.

- Thực hiện kiểm tra bảo mật thường xuyên để phát hiện và khắc phục lỗ hổng bảo mật mới nhất.

- Đảm bảo sử dụng chứng chỉ SSL/TLS hiện đại và cập nhật để đảm bảo mã hóa dữ liệu truyền tải và xác thực an toàn.

- Xây dựng quy trình sao lưu và phục hồi dữ liệu định kỳ để đảm bảo khả năng khôi phục dữ liệu trong trường hợp sự cố xảy ra.

**b) Hiệu suất và tốc độ truy cập:**

- Tối ưu hóa mã nguồn và cấu trúc trang web để cải thiện thời gian tải trang và thời gian phản hồi của máy chủ.

- Sử dụng các công nghệ caching như CDN (Mạng phân phối nội dung) để tăng tốc độ truy cập và giảm tải cho máy chủ.

- Đảm bảo khả năng mở rộng của hệ thống để xử lý được lượng truy cập lớn và đồng thời tăng cường khả năng xử lý dữ liệu.

**c) Quá trình triển khai:**

- Đánh giá và cải thiện quy trình triển khai bằng cách sử dụng các công cụ quản lý dự án và phân phối mã nguồn để tối ưu hóa quy trình và giảm thiểu rủi ro.

- Thực hiện kiểm thử tự động và kiểm thử bảo mật để phát hiện lỗi sớm và đảm bảo chất lượng của mã nguồn.

- Xây dựng một hệ thống giám sát liên tục để theo dõi hiệu suất và bảo mật của trang web, cung cấp thông báo sớm về các vấn đề có thể phát sinh.

1. **Tài liệu tham khảo**