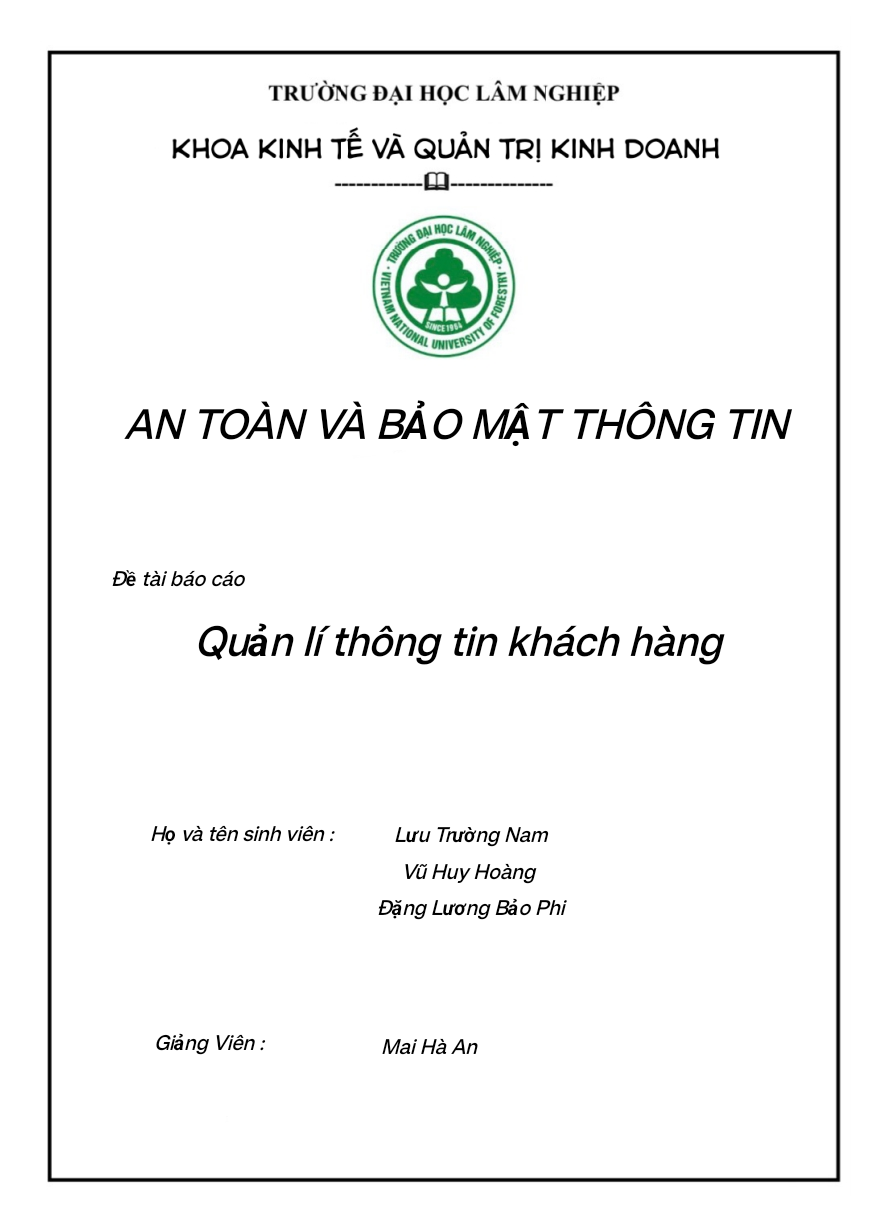
****

# 

# Chương I. KHÁI NIỆM, MỤC TIÊU

## 1. Khái niệm bảo mật thông tin

- Bảo mật thông tin (Information Security) không đơn thuần là bảo vệ thông tin của cá nhân người dùng mà còn là sự duy trì tính bảo mật, tính toàn vẹn toàn diện và tính sẵn sàng cho toàn bộ thông tin liên quan tới tài sản, dữ liệu, thông tin riêng của tổ chức, cá nhân. Tập hợp các quy trình và công cụ bảo mật để bảo vệ trên diện rộng thông tin nhạy cảm của doanh nghiệp, tránh để thông tin đó bị lạm dụng, truy nhập trái phép, gián đoạn hoặc phá hủy.

- Bốn yếu tố không thể tách rời trong việc bảo mật thông tin là:

+ Tính bảo mật: Đảm bảo thông tin đó được bảo mật chặt chẽ, những người muốn tiếp cận thông tin phải được phân quyền truy cập;

+ Tính toàn vẹn: Bảo vệ sự hoàn chỉnh toàn diện cho hệ thống thông tin;

+ Tính chính xác: Thông tin đưa ra phải chính xác, đầy đủ, không được sai lệch hay không được vi phạm bản quyền nội dung;

+ Tính sẵn sàng: Việc bảo mật thông tin luôn phải sẵn sàng, có thể thực hiện bất cứ đâu, bất cứ khi nào.

- Bảo mật thông tin khách hàng là một tập hợp những phương thức nhằm giữ an toàn những dữ liệu khách hàng khỏi bị truy cập hoặc bị thay đổi trái phép ngay cả khi nó đã được lưu trữ và được truyền từ máy này sang một thiết bị khác. Do đó việc bảo mật thông tin khách hàng luôn được các doanh nghiệp ưu tiên hàng đầu.

## 2. Tại sao phải bảo mật thông tin khách hàng?

## + Bảo mật thông tin khách hàng là trách nhiệm của các tổ chức tín dụng, các chi nhánh ngân hàng và các cơ quan, tổ chức này không được tự ý tiết lộ thông tin khách hàng ra bên ngoài hay thực hiện bất kì hành vi bất chính nào như việc trục lợi, sử dụng trái phép, mua bán, trao đổi, tặng cho, sửa chữa, thay đổi hoặc công khai hóa thông tin đó.

## - Bảo mật thông tin khách hàng mang lại rất nhiều lợi cho mối quan hệ giữa khách hàng và doanh nghiệp. Bởi việc xây dựng hệ thống data khách hàng sẽ tạo điều kiện thuận lợi để cá nhân hóa trải nghiệm mức độ hài lòng của khách hàng cũng như đáp ứng mọi nhu cầu của người dùng. Không những thế giá trị của việc bảo mật thông tin khách hàng là cốt lõi đánh giá sự tin tưởng với doanh nghiệp. Điều này sẽ giúp doanh nghiệp tăng trưởng doanh thu và xây dựng thương hiệu bền vững sau này.

## + Trước tình hình phát triển mạnh của công nghệ số thì xu hướng người tiêu dùng thường thao tác trên các trang web mua sắm online, dẫn đến nhiều hành vi khai thác và xâm phạm bí mật thông tin khách hàng trong các doanh nghiệp xảy ra phổ biến. Cho nên việc đảm bảo những dữ liệu khách hàng là điều rất cần thiết.

## - Việc làm thất thoát thông tin khách hàng là điều cực kỳ đáng lo ngại. Nó không chỉ gây tổn thất cho khách hàng mà còn mất đi sự uy tín cho doanh nghiệp trong việc bảo mật thông tin khách hàng. Mất sự uy tín vốn có của doanh nghiệp Trong thời đại Internet tin tức luôn được cập nhật liên tục. Nếu công ty của không có khả năng bảo mật thông tin khách hàng hiệu quả làm thất thoát dữ liệu khách hàng thì chắc chắn những công khai tiêu cực sẽ có thể làm hỏng danh tiếng doanh nghiệp của bạn vĩnh viễn. Chính vì vậy chỉ một sai lầm nhỏ cũng khiến khách hàng quay lưng với bạn.

## 3. Mục tiêu đề tài

- Mục tiêu của việc bảo mật thông tin là ngăn chặn những truy cập và hành vi trái phép liên quan tới tài sản, dữ liệu và thông tin riêng của tổ chức/cá nhân. Một số mục tiêu cụ thể có thể là phòng ngừa hiện tượng đánh cắp dữ liệu và ngăn chặn tin tặc đánh cắp danh tính

- Bảo mật thông tin quan trọng vì nó giúp bảo vệ tài nguyên hệ thống và bảo đảm tính riêng tư. Nó giúp bảo đảm mọi thông tin quan trọng không bị rò rỉ hay đánh cắp. Nếu không được bảo mật tốt, các mối quan hệ kinh doanh quan trọng có thể bị tổn hại.

**. Bài toán của tôi**

## Tạo ra 1 trang web khi người dùng đăng nhập với đăng ký vào thì sẽ lưu trữ thông tin ( tài khoản và mật khẩu ) và sử dụng mã hóa thông tin đa bảng để mã hóa mật khẩu để bảo mật thông tin của khách hàng không bị đánh cắt và được bảo mật an toàn và tôi đã sử dụng phpmyadmin để lưu trữ thông tin và mã hóa mật khẩu

1. **Trên thế giới đã làm gì**

Trên thế giới, họ sẽ sử dụng một số phương pháp và công nghệ thông thường được sử dụng để giải quyết vấn đề bảo mật thông tin người dùng trên trang web:

* Sử dụng giao thức HTTPS: Để đảm bảo việc truyền thông tin an toàn giữa máy khách và máy chủ, giao thức HTTPS (HTTP Secure) được sử dụng. Nó sử dụng SSL (Secure Sockets Layer) hoặc TLS (Transport Layer Security) để mã hóa dữ liệu và đảm bảo tính toàn vẹn của nó.
* Mã hóa mật khẩu: Thay vì lưu trữ mật khẩu người dùng dưới dạng văn bản thuần túy, các hệ thống thường sử dụng phương pháp mã hóa mật khẩu. Một trong những thuật toán mã hóa phổ biến được sử dụng là bcrypt, vì nó cung cấp một cách an toàn và chống lại các cuộc tấn công dò mật khẩu.
* Quản lý phiên làm việc: Để đảm bảo tính bảo mật và xác thực của người dùng sau khi đăng nhập, các hệ thống thường sử dụng phiên làm việc. Mỗi phiên làm việc được liên kết với một mã phiên duy nhất, được lưu trữ và kiểm tra để xác nhận quyền truy cập của người dùng.
* Thực thi chính sách bảo mật: Để đảm bảo an toàn cho thông tin người dùng, các hệ thống thường thiết lập và thực thi các chính sách bảo mật. Điều này có thể bao gồm việc đặt quyền truy cập vào dữ liệu, kiểm tra tính hợp lệ của đầu vào và giám sát hoạt động của người dùng để phát hiện các hành vi đáng ngờ.
* Kiểm tra bảo mật thường xuyên: Việc kiểm tra bảo mật định kỳ và kiểm tra thâm nhập được thực hiện để tìm lỗ hổng bảo mật và khắc phục chúng. Những kiểm tra này có thể được thực hiện bởi nhóm bảo mật nội bộ hoặc bởi bên thứ ba chuyên về kiểm thử thâm nhập.

**+ Còn những vấn đề gì khó khăn chưa giải quyết được hoặc giải quyết chưa tốt ?**

- Chưa nắm vững kiến thức về ngôn ngữ C# nên code bảo mật vẫn còn nhiều lỗ hổng

- Kiến thức tràn lan trên mạng khó để lọc ra và sử dụng chúng

- Mặc dù em đã tìm hiểu và học hỏi trên mạng những vẫn có một số kiến thức em không hiểu rõ

**Chương II.** **Các bước làm đề tài**

**Bước 1 Tạo form đăng nhập**

+ Sử dụng toolbox để tạo ra form đăng nhập hệ thống có button, laber, Picturebox, textbox.

+ Tạo giao diện form đăng nhập với các control như hai TextBox “Tài khoản” và “Mật khẩu” để người dùng nhập vào tài khoản và mật khẩu của họ

+ Ở chỗ picturebox ta thêm hình ảnh tự chọn để phù hợp form đăng nhập

**Bước 2 Viết code cho phần form đăng nhập**

+ Tạo database csdl để lưu chữ dữ liệu tài khoản và mật khẩu của khách hàng(Dùng ngôn ngữ C# )

+ Ta kết nối cơ sở dữ liệu với C# bằng quyền chứng thực của Windows trong C# bằng cách sử dụng thuộc tính Integrated Security = SSPI hoặc Integrated Security = True trong chuỗi kết nối.

+ Kết nối CSDL với quyền chứng thực của SQL Server trong C# bằng cách thay Integrated Security=True bằng hai thông số User Id và PWD trong chuỗi kết nối. Lưu trữ chuỗi kết nối trong tập tin App.config.

+ Ta sử dụng Server Explorer sau đó add connection DESKTOP-DS1KSSQ\SQLEXPRESS

+ Sau đó chọn database name Login là cơ sở dữ liệu sql đã lưu trước đó. Ta lấy đoạn data source trong conection string sau đó dán vào SqlConnection conn = new SqlConnection(“@”)

**Bước 3 Sử lí sự kiện trong button đăng nhập**

+Khi giao diện form đăng nhập và database đã được chuẩn bị cũng như kết nối tới SQL Server thành công, bạn có thể bắt đầu xử lý sự kiện cho từng control trong giao diện vừa tạo

+Cho Button “Đăng nhập” để kiểm tra xem thông tin được nhập bởi người dùng có trùng khớp với dữ liệu trong database hay không.

+Ta gán String tk= TxtTaiKhoan.text

String mk= TxtMatKhau.text

String sql = "select \*from NguoiDung where Taikhoan='" + tk + "'and MatKhau ='" + mk+ "'"

+MessageBox.show nếu đăng nhập thành công và đúng trong sql nó sẽ hiển thị đăng nhập thành công . Nếu đăng nhập không có tài khoản hoặc sai mật khẩu sẽ hiện tài khoản hoặc mật khẩu không chính sác và đăng nhập thất bại.

**Bước 4 Khi đăng nhập thành công**

+Tạo form home là đăng nhập thành công hệ thống ta cũng sử dụng toolbox (button, pictureBox và laber)

+Sau đó ta sử lý button đăng xuất If (MessageBox.show (“Bạn có muốn đăng xuất không”) ta sẽ cho 2 lựa chọn “có” hoặc “không”).

**Sử dụng C# là phương án phù hợp nhất đối với nhóm của bọn em, phương án đòi hỏi phải có chút kinh nghiệm và dễ hiểu dễ học trên mọi nền tảng trực tuyến có nhiều nội dung tham khảo để có thể hoàn thành được**

**+ Đề xuất sẽ cải thiện bài toán đó**

Để cải thiện bài toán toán một cách tốt hơn cần :

1. Thiết kế cơ sở dữ liệu: Tạo một bảng trong cơ sở dữ liệu để lưu trữ thông tin tài khoản của người dùng. Bảng này có thể bao gồm các trường như ID, tên đăng nhập, mật khẩu, và dung lượng lưu trữ đã sử dụng.
2. Mã hóa mật khẩu: Khi người dùng đăng ký hoặc thay đổi mật khẩu, sử dụng một thuật toán mã hóa mạnh như bcrypt để mã hóa mật khẩu trước khi lưu vào cơ sở dữ liệu. Mã hóa mật khẩu giúp bảo vệ thông tin người dùng khỏi việc đánh cắp trong trường hợp cơ sở dữ liệu bị tấn công.
3. Lưu trữ thông tin người dùng trong cơ sở dữ liệu:

* Để bảo mật dữ liệu người dùng, hãy sử dụng các kỹ thuật như chuỗi kết nối an toàn (SSL/TLS) khi thiết lập kết nối với cơ sở dữ liệu.
* Hãy đảm bảo rằng cơ sở dữ liệu của bạn được bảo vệ khỏi các cuộc tấn công như SQL injection bằng cách sử dụng câu lệnh truy vấn tham số hóa hoặc ORM (Object-Relational Mapping).

1. Quản lý dung lượng lưu trữ:
   * Thêm một cột trong bảng "users" để lưu trữ dung lượng đã sử dụng của mỗi người dùng.
   * Khi người dùng tải lên tập tin, hãy kiểm tra dung lượng đã sử dụng và giới hạn dung lượng tải lên theo giới hạn được quy định (ví dụ: 3GB).
   * Cập nhật dung lượng đã sử dụng sau mỗi lần tải lên thành công.
2. Xác thực và phân quyền người dùng:
   * Sử dụng phương pháp xác thực bảo mật như JWT (JSON Web Tokens) để quản lý phiên đăng nhập của người dùng.
   * Xác thực người dùng trước khi cho phép tải lên tập tin hoặc truy cập vào các tính năng quan trọng trên trang web.
   * Thiết lập các quyền và vai trò cho người dùng, đảm bảo rằng chỉ những người dùng được phân quyền mới có thể tải lên và truy cập vào các tài nguyên quan trọng.
3. Bảo mật giao tiếp và tải lên tập tin:
   * Sử dụng giao thức HTTPS để mã hóa thông tin truyền qua mạng giữa trình duyệt và máy chủ, đảm bảo rằng dữ liệu không bị đánh cắp hoặc thay đổi trong quá trình truyền.
   * Kiểm tra và xác minh tập tin tải lên để đảm bảo rằng chỉ các tập
   * Kiểm tra và xác minh tập tin tải lên để đảm bảo rằng chỉ các tập tin hợp lệ được chấp nhận. Bạn có thể sử dụng các kiểu tập tin định sẵn hoặc kiểm tra phần mở rộng tệp tin để đảm bảo tính toàn vẹn của dữ liệu.

* Hạn chế kích thước tập tin tải lên để tránh việc tải lên các tệp tin quá lớn có thể gây quá tải hệ thống hoặc tạo nguy cơ bị tấn công.
* Lưu trữ tập tin tải lên trong thư mục không thực thi trên máy chủ để đảm bảo rằng chúng không thể được thực thi dưới bất kỳ hình thức nào.

1. Đảm bảo bảo mật tổng thể:

* Điều tra và triển khai các biện pháp bảo mật khác như bảo vệ chống tấn công từ chối dịch vụ (DDoS), bảo mật máy chủ, kiểm tra tự động và phát hiện xâm nhập (IDS/IPS), và các biện pháp bảo mật khác tùy thuộc vào quy mô và yêu cầu của dự án.

**+ Phương hướng triển khai nốt và nâng cấp**

Dưới đây là phương hướng triển khai nốt và nâng cấp:

1. Thiết kế giao diện người dùng:

Nghiên cứu về thiết kế giao diện: Tìm hiểu về các nguyên tắc thiết kế giao diện hợp lý và trải nghiệm người dùng.

* + Xây dựng giao diện thân thiện: Sử dụng HTML, CSS, C# và JavaScript để tạo giao diện người dùng hấp dẫn và dễ sử dụng. Tối ưu hóa trải nghiệm người dùng trên cả máy tính và thiết bị di động.

1. Giới hạn lưu lượng cho mỗi tài khoản:
   * Xác định mức giới hạn lưu lượng: Quyết định mức giới hạn lưu lượng phù hợp cho mỗi tài khoản, dựa trên yêu cầu và nguồn tài nguyên của bạn.
   * Theo dõi lưu lượng: Xây dựng chức năng theo dõi và ghi nhận lưu lượng sử dụng cho mỗi tài khoản. Cập nhật lưu lượng sau mỗi lần tải lên hoặc truy cập dữ liệu.
2. Kiểm thử:
   * Kiểm thử chức năng: Thực hiện kiểm thử toàn diện của trang form đăng nhập để đảm bảo rằng các chức năng hoạt động chính xác và không có lỗi.
   * Kiểm thử bảo mật: Thực hiện kiểm thử bảo mật để xác định các lỗ hổng bảo mật có thể tồn tại và áp dụng các biện pháp bảo mật phù hợp để khắc phục chúng.
3. Tối ưu hiệu suất:
   * Tối ưu hóa mã nguồn: Xem xét mã nguồn và cấu trúc trang web để tối ưu hóa hiệu suất, bao gồm tối ưu hóa tốc độ tải trang và tối ưu hóa cơ sở dữ liệu.
   * Sử dụng công cụ tối ưu hiệu suất: Áp dụng các công cụ tối ưu hiệu suất như caching, compression và minification để cải thiện tốc độ tải trang.
4. Bảo trì và nâng cấp:
   * Sao lưu định kỳ: Thực hiện sao lưu dữ liệu thường xuyên để đảm bảo an toàn và khả năng khôi phục.
   * Cập nhật và nâng cấp: Theo dõi các bản cập nhật phần mềm và công nghệ liên quan và thực hiện việc cập nhật và nâng cấp khi cần thiết để bảo đảm tính bảo mật và hiệu suất của trang web.

**Chương. III kết quả và kiểm tra**

+ Lưu trữ thông tin đăng nhập: Kết quả sẽ là hệ thống có khả năng lưu trữ thông tin tài khoản và mật khẩu của người dùng. Tôi có thể kiểm tra tính toàn vẹn và khả năng truy xuất dữ liệu trong cơ sở dữ liệu bằng cách thực hiện các truy vấn và kiểm tra.

+ Mã hóa mật khẩu: Kết quả sẽ là mật khẩu được mã hóa và lưu trữ an toàn trong cơ sở dữ liệu. Tôi có thể kiểm tra tính hợp lệ và độ mạnh của thuật toán mã hóa bằng cách thực hiện quá trình mã hóa và so sánh kết quả với mật khẩu ban đầu.