**TRƯỜNG ĐẠI HỌC THỦ DẦU MỘT VIỆN KỸ THUẬT – CÔNG NGHỆ**



**TIỂU LUẬN MÔN HỌC**

**AN TOÀN VÀ BẢO MẬT THÔNG TIN**

**Xây dựng giải pháp bảo mật cho website dụng cụ thể thao ATH**

**GVHD: ThS. Lê Từ Minh Trí**

**SVTH:** Nguyễn Hữu Thành **MSSV**: 2124802010803 Nguyễn Hoàng Duy **MSSV**: 2124802010251 Phạm Hồng Huy **MSSV**: 2124802010427  
Võ Quốc Thái **MSSV:** 2124802010801

**TRƯỜNG ĐẠI HỌC THỦ DẦU MỘT VIỆN KỸ THUẬT – CÔNG NGHỆ**



**TIỂU LUẬN MÔN HỌC**

**AN TOÀN VÀ BẢO MẬT THÔNG TIN**

**Xây dựng giải pháp bảo mật cho website dụng cụ thể thao ATH**

**GVHD: ThS. Lê Từ Minh Trí**

**SVTH:** Nguyễn Hữu Thành **MSSV**: 2124802010803 Nguyễn Hoàng Duy **MSSV**: 2124802010251 Phạm Hồng Huy **MSSV**: 2124802010427  
Võ Quốc Thái **MSSV:** 2124802010801

**BẢNG PHÂN CÔNG CỦA NHÓM**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên thành viên** | **Nội dung công việc** | **Kết quả** |
| 1 | Phạm Hồng Huy | Viết báo cáo | 100% |
| Thực hiện Bảo Mật | 100% |
| 2 | Nguyễn Hữu Thành | Viết báo cáo | 100% |
| Thực hiện khai thác | 100% |
| 3 | Võ Quốc Thái | Viết báo cáo | 100% |
| Thực hiện khai thác | 100% |
| 4 | Nguyễn Hoàng Duy | Viết báo cáo | 100% |
| Thực hiện khai thác | 100% |

**LỜI CẢM ƠN**

Em xin chân thành gửi lời cảm ơn đến thầy Lê Từ Minh Trí!

Mặc dù đã cố gắng hoàn thành đề tài tốt nhất nhưng do thời gian và kiến thức còn có hạn nên nhóm em không thể tránh khỏi những thiếu sót nhất định, rất mong nhận được sự cảm thông, chia sẻ và tận tình đóng góp chỉ bảo của quý thầy cô cũng như các bạn.

Bình Dương, ngày 28 tháng 04 năm 2024 Sinh viên

Nguyễn Hoàng Duy

Nguyễn Hữu Thành

Phạm Hồng Huy

Võ Quốc Thái

**LỜI CAM ĐOAN**

Em xin cam đoan:

Những nội dung trong báo cáo này là do em thực hiện dưới sự hướng dẫn trực tiếp của Thầy Lê Từ Minh Trí.

Mọi tham khảo dùng trong báo cáo đều được trích dẫn rõ ràng tên tác giả, tên công trình, thời gian, địa điểm công bố.

Mọi sao chép không hợp lệ, vi phạm quy chế đào tạo, hay gian lận, em xin chịu hoàn toàn trách nhiệm.

Bình Dương, ngày ... tháng ... năm 20...

Sinh viên

Nguyễn Hoàng Duy

Nguyễn Hữu Thành

Phạm Hồng Huy

Võ Quốc Thái

**NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN**

*Bình Dương, ngày …… tháng …… năm 20...*

**GIÁO VIÊN HƯỚNG DẪN**

*ThS.Lê Từ Minh Trí*

**TÓM TẮT**

Bảo mật thông tin luôn luôn là vấn đề được đặt lên hàng đầu nhất là với thời đại 4.0 hiện nay. Các trang mạng cũng như các hệ điều hành luôn là miếng mồi ngon cho các hacker xâm nhập để đánh cắp thông tin của khách hàng. Chúng sử dụng các lỗ hổng trên hệ diều hành để xâm nhập bất hợp pháp vào máy tính của bạn và cài vào đó một số phần mềm hoặc chiếm luôn quyền điều hành của máy tính bạn nhằm phá hoại hoặc đánh cắp các thông tin bảo mật trong máy tinh cá nhân.

Đề tài "Xây dựng giải pháp bảo mật cho website dụng cụ thể thao ATH bằng mã khoá mật khẩu" nhằm nghiên cứu và đề xuất các giải pháp bảo mật sử dụng mã khoá mật khẩu để bảo vệ website ATH, một trang web cung cấp dụng cụ thể thao

Các giải pháp bảo mật có thể được áp dụng bao gồm sử dụng thuật toán mã hóa mạnh như bcrypt, Argon2, hoặc PBKDF2 để mã hóa mật khẩu người dùng, đảm bảo rằng mật khẩu không thể bị đoán hay phục hồi ngược. Ngoài ra, việc thiết lập chính sách mật khẩu mạnh yêu cầu người dùng sử dụng mật khẩu có độ dài tối thiểu, chứa các loại ký tự phức tạp như chữ hoa, chữ thường, số và ký tự đặc biệt.

Để ngăn chặn các cuộc tấn công, cần áp dụng các biện pháp phòng ngừa như hạn chế số lần đăng nhập sai, sử dụng mã xác thực hai yếu tố (2FA) để tăng cường bảo mật và thực hiện kiểm tra đầu vào cẩn thận để ngăn chặn các cuộc tấn công SQL injection và cross-site scripting (XSS).

Cũng rất quan trọng là bảo vệ dữ liệu trên mạng bằng cách sử dụng giao thức HTTPS để mã hóa thông tin giao tiếp giữa máy khách và máy chủ, đảm bảo rằng dữ liệu không thể bị đánh cắp hoặc xem trộm trong quá trình truyền tải.

Cuối cùng, việc đào tạo và nâng cao nhận thức an ninh cho nhóm phát triển và người quản lý là rất quan trọng để hiểu rõ về các mối đe dọa an ninh và áp dụng các biện pháp bảo mật thích hợp.

**MỤC LỤC**

[**CHƯƠNG 1. GIỚI THIỆU CHUNG 2**](#_Toc166872234)

[**1.1. Lý do thực hiện đề tài 3**](#_Toc166872235)

[**1.2. Tổng quan về vấn đề nghiên cứu 3**](#_Toc166872236)

[**CHƯƠNG 2. CƠ SỞ LÝ THUYẾT 4**](#_Toc166872237)

[**2.1. Khái niệm về bảo mật 4**](#_Toc166872238)

[**2.2. Vấn đề an toàn thông tin của Việt Nam hiện nay 6**](#_Toc166872239)

[**2.3. Giới Thiệu Về Visual Studio 7**](#_Toc166872240)

[**CHƯƠNG 3: KẾT QUẢ THỰC NGHIỆM 8**](#_Toc166872241)

[**3.1 Mã Hóa Mật Khẩu Bằng bcrypt 8**](#_Toc166872242)

[3.1.1 Khái Niệm bcrypt 8](#_Toc166872243)

[3.1.2 Giao Diện Đăng Nhập Dùng Bcrypt 8](#_Toc166872244)

[**3.2 reCAPTCHA Trong WebSite 10**](#_Toc166872245)

[3.1.1 Khái Niệm reCAPTCHA 10](#_Toc166872246)

[3.2.2 Giao Diện Đăng Nhập Dùng reCAPTCHA 12](#_Toc166872247)

[**3.3 Two-Factor Authentication - 2FA Trong WebSite** 12](#_Toc166872248)

[3.3.1 Khái Niệm Two-Factor Authentication - 2FA 12](#_Toc166872249)

[3.3.2 Giao Diện Xác Thực 2 Lớp 13](#_Toc166872250)

[**3.4 Bảo Mật Chống Brute Force Attack** 15](#_Toc166872251)

[3.4.1 Khái niệm Bảo Mật Chống Brute Force Attack 15](#_Toc166872252)

[3.4.2 Giao Diện Bảo Mật Chống Brute Force Attack 15](#_Toc166872253)

[**CHƯƠNG 4: KẾT LUẬN 17**](#_Toc166872254)

[**4.1. Kết quả đạt được 17**](#_Toc166872255)

[**4.2. Hướng phát triển 17**](#_Toc166872256)

[**TÀI LIỆU THAM KHẢO 19**](#_Toc166872257)

[**Sách, bài giảng 19**](#_Toc166872258)

**Mục Lục Hình**

[Hình 3.1 Hình Ảnh Đăng Ký 9](#_Toc166910592)

[Hình 3.2 Hình Ảnh Mã Hóa Mật Khẩu bcrypt 10](#_Toc166910593)

[Hình 3.3 Hình Bảo Mật Đăng Nhập reCAPTCHA 12](#_Toc166910594)

[Hình 3.4 Hình Bảo Mật Đăng Nhập reCAPTCHA Thành Công 12](#_Toc166910595)

[Hình 3.5 Hình Bảo Mật Đăng Nhập OTP 13](#_Toc166910596)

[Hình 3.6 Hình OTP Gửi Về Mail 14](#_Toc166910597)

[Hình 3.7 Hình Ảnh Đăng Nhập Bị Khóa 15](#_Toc166910598)

[Hình 3.8 Hình Ảnh Tài Khoản Bị Khóa Khi Đăng Nhập Sai 7 Lần 16](#_Toc166910599)

# CHƯƠNG 1. GIỚI THIỆU CHUNG

### Lý do thực hiện đề tài

Đề tài "Xây dựng giải pháp bảo mật cho website dụng cụ thể thao ATH" đã được chọn dựa trên những lý do quan trọng. Trong thời đại số hóa hiện nay, bảo mật thông tin trở thành ưu tiên hàng đầu. Với website ATH cung cấp dụng cụ thể thao, việc bảo vệ thông tin khách hàng, giao dịch và tài khoản người dùng là vô cùng quan trọng. Sử dụng mã khoá mật khẩu là một phương pháp bảo mật phổ biến và có thể áp dụng rộng rãi. Nó đơn giản trong triển khai và tiện lợi cho người dùng cuối, đồng thời đảm bảo một cấu trúc bảo mật cơ bản. Việc nghiên cứu và xây dựng giải pháp bảo mật sử dụng mã khoá mật khẩu cho website ATH đáp ứng nhu cầu bảo mật và có thể áp dụng cho nhiều dự án tương tự. Đồng thời, việc tuân thủ các quy định pháp lý về bảo mật thông tin cá nhân và đáp ứng yêu cầu của khách hàng là một yếu tố không thể bỏ qua. Tóm lại, đề tài này được chọn dựa trên sự quan trọng của bảo mật thông tin, tính phổ biến và khả thi của mã khoá mật khẩu, khả năng áp dụng rộng và yêu cầu từ thị trường và quy định pháp lý.

### Tổng quan về vấn đề nghiên cứu

Trong thời đại của sự phát triển không ngừng của công nghệ thông tin, việc bảo mật thông tin trở thành một trong những ưu tiên hàng đầu.Đề tài tập trung vào việc nghiên cứu và đề xuất giải pháp bảo mật sử dụng mã khoá mật khẩu để bảo vệ thông tin và tài khoản người dùng trên website ATH. Các biện pháp bảo mật có thể bao gồm sử dụng thuật toán mã hóa mạnh, thiết lập chính sách mật khẩu mạnh, áp dụng mã xác thực hai yếu tố, kiểm tra đầu vào cẩn thận và sử dụng giao thức HTTPS. Công việc cũng nhấn mạnh việc đào tạo nhóm phát triển và người quản lý về an ninh thông tin. Mục tiêu là đảm bảo an toàn và bảo mật cho thông tin cá nhân và tài khoản người dùng trên website ATH.

## CHƯƠNG 2. CƠ SỞ LÝ THUYẾT

### Khái niệm về bảo mật

#### Khái niệm an toàn thông tin

An toàn thông tin là khả năng bảo vệ thông tin quan trọng và hệ thống thông tin khỏi các mối đe dọa, cuộc tấn công và sự xâm nhập không mong muốn. Đây là quá trình áp dụng các biện pháp và công nghệ để đảm bảo tính bảo mật, sẵn sàng và toàn vẹn của thông tin, dữ liệu và hệ thống mạng. Trong một thế giới ngày nay, nơi mà thông tin di chuyển nhanh chóng qua mạng internet và các phương tiện điện tử khác, an toàn thông tin trở thành một vấn đề quan trọng không chỉ đối với các tổ chức và doanh nghiệp mà còn với mỗi người dùng cá nhân.

Trong bối cảnh của Cuộc cách mạng Công nghiệp 4.0, Việt Nam không tránh khỏi những thách thức liên quan đến an ninh thông tin mạng. Sự phổ biến của Công nghệ Thông tin và Truyền thông (CNTT) đã đưa ra nhiều cơ hội mới nhưng cũng mở ra hàng loạt vấn đề về an toàn thông tin mạng, cả ở quy mô toàn cầu và ở Việt Nam cụ thể.

Các chuyên gia đồng lòng nhận định rằng tình hình an toàn thông tin mạng đang phức tạp hóa. Các tổ chức, cơ quan và doanh nghiệp ở Việt Nam đang phải đối mặt với một loạt các cuộc tấn công mạng ngày càng phổ biến, đặc biệt là các cuộc tấn công có quy mô lớn và mức độ phức tạp cao. Những cuộc tấn công này thường mang tính chất tinh vi, khó lường, khó dự đoán.

Một số vấn đề chính gây ra sự lo ngại trong lĩnh vực an toàn thông tin mạng tại Việt Nam bao gồm:

* Mật khẩu yếu: Sự lơ là trong việc tạo mật khẩu mạnh và quản lý mật khẩu an toàn có thể tạo ra lỗ hổng lớn trong hệ thống bảo mật.
* Nhận thức về vấn đề an toàn thông tin kém: Nhiều tổ chức và cá nhân vẫn chưa nhận ra tầm quan trọng của việc bảo vệ thông tin cá nhân và doanh nghiệp.
* Kỹ năng kém: Sự thiếu hụt về kỹ năng và kiến thức trong lĩnh vực an toàn thông tin là một thách thức lớn.
* Chi phí cập nhật kỹ năng: Chi phí để cập nhật và duy trì kiến thức và kỹ năng an toàn thông tin cũng là một nguyên nhân gây khó khăn.

Trong bối cảnh này, việc nâng cao nhận thức và chuẩn bị cho các biện pháp bảo mật là cần thiết để đối phó với những thách thức về an toàn thông tin mạng tại Việt Nam

#### Khái niệm về lỗ hổng bảo mật

Lỗ hổng bảo mật là một khái niệm rất thường thấy trong lĩnh vực an ninh mạng. Đây là khái niệm để chỉ một điểm yếu (kỹ thuật hoặc phi kỹ thuật) của một phần mềm, phần cứng, giao thức, hay một hệ thống thông tin. Nhắc đến lỗ hổng bảo mật là nhắc đến lỗi kỹ thuật ở phần mềm, phần cứng.

Bảo mật máy tính là kỹ thuật để giúp máy tính hoạt động bình thường trước các cuộc tấn công. Hầu hết mọi người hiện nay đều thừa nhận tầm quan trọng của việc bảo mật máy tính, tuy nhiên việc lập trình kém là nguyên nhân của phần lớn các cuộc tấn công mạng. Những lỗ hổng này được chia làm 3 loại: Lỗ hổng do tương tác không an toàn giữa các thành phần, lỗ hổng do quản lý tài nguyên và lỗ hổng do phòng thủ kém.

Lỗ hổng do tương tác không an toàn giữa các thành phần gồm có:

* SQL injection: Khi dữ liệu nhập vào từ người dùng không được xác thực có thể dẫn đến việc chèn các truy vấn độc hại vào cơ sở dữ liệu, thực hiện các hoạt động không mong muốn như truy cập, sửa đổi hoặc xóa dữ liệu.
* OS command injection: do các lệnh của hệ điều hành không được kiểm tra và xử lý đầu vào từ người dùng. Ví dụ như thực hiện lệnh ping từ ứng dụng đến địa chỉ 192.168.1.0 với đầu vào là “ping 192.168.1.0; dir” thì lệnh “dir” sẽ được thực thi để liệt kê các file và thư mục trên máy chủ.
* Cross-Site Scripting (XSS): Khi ứng dụng web cho phép các đoạn mã JavaScript được chèn vào các trang web từ người dùng thì có thể dẫn đến thực thi mã độc.
* Lỗ hổng không kiểm tra tệp upload
* Giả mạo yêu cầu trên trang web (Cross-Site Request Forgery - CSRF) để thực hiện các hoạt động trái phép trên tài khoản của người dùng như: thay đổi thông tin cá nhân, thực hiện giao dịch trái phép.
* Chuyển hương đến trang web không đáng tin cậy (Open Redirect)

Lỗ hổng do quản lý tài nguyên kém như: Lỗi tràn bộ nhớ đệm, giới hạn không đúng đường dẫn hoặc thư mục hạn chế, tải xuống phần mềm mà không kiểm tra trước, sử dụng chức năng gây hại cho dữ liệu máy tính, không kiểm tra định dạng chuỗi, lỗi tràn số nguyên.

Lỗ hổng do phòng thủ kém như: thiếu tính năng xác thực cho phần mềm, thiếu mã hóa dữ liệu, thực thi 1 số quyền không cần thiết, phân quyền sai, sử dụng thuật toán bị lỗi hoặc dễ gây ra lỗi, sử dụng các phương thức mã hóa 1 chiều.

### Vấn đề an toàn thông tin của Việt Nam hiện nay

Ở Việt Nam, an ninh mạng và an toàn thông tin đang trở thành một trong những ưu tiên hàng đầu của các tổ chức, doanh nghiệp. Một trong những thách thức lớn nhất mà Việt Nam đang phải đối mặt là sự gia tăng về các cuộc tấn công mạng và việc đánh cắp thông tin. Các tổ chức tội phạm mạng hay hacker không ngừng tìm lỗ hổng trong hệ thống mạng để xâm nhập và lấy cắp thông tin quan trọng của các tổ chức, doanh nghiệp và cá nhân. Điều này đặt ra một thách thức lớn đối với các cơ quan chức năng và doanh nghiệp tại Việt Nam, khi họ phải đảm bảo rằng hệ thống mạng của mình được bảo vệ chặt chẽ để ngăn chặn các cuộc tấn công này. Tuy nhiên, cũng có những nỗ lực đáng kể đang được thực hiện để cải thiện an toàn thông tin ở Việt Nam. Một phần không thể thiếu trong việc nâng cao an toàn thông tin là việc tăng cường nhận thức và kiến thức về an ninh mạng trong cộng đồng. Chương trình giáo dục và tuyên truyền được tổ chức để nâng cao nhận thức của người dân về các nguy cơ mạng và cách phòng tránh chúng. Điều này đóng vai trò quan trọng trong việc xây dựng một cộng đồng mạng có ý thức và có khả năng tự bảo vệ trước các mối đe dọa mạng. Bên cạnh đó, việc phát triển và thúc đẩy việc sử dụng các công nghệ bảo mật tiên tiến cũng đang được chú trọng. Các doanh nghiệp và tổ chức tại Việt Nam đang đầu tư mạnh mẽ vào các giải pháp bảo mật mạng như máy chủ ảo, mã hóa dữ liệu, và hệ thống phát hiện xâm nhập để bảo vệ thông tin quan trọng của họ khỏi các cuộc tấn công mạng. An toàn thông tin đang trở thành một trong những ưu tiên hàng đầu của Việt Nam trong bối cảnh bùng nổ của công nghệ thông tin và internet. Dù đang đối mặt với nhiều thách thức, nhưng nhờ vào sự tập trung và nỗ lực từ nhiều phía, Việt Nam đang dần đi đến việc cải thiện hệ thống bảo mật mạng và nâng cao nhận thức của cộng đồng về an ninh mạng.

### Giới Thiệu Về Visual Studio

Visual Studio là một môi trường phát triển tích hợp (Integrated Development Environment - IDE) được phát triển bởi Microsoft. Nó cung cấp một loạt các công cụ và tài nguyên hỗ trợ cho việc phát triển phần mềm, từ việc viết mã, biên dịch, gỡ lỗi, xây dựng, kiểm thử và triển khai ứng dụng.

Visual Studio hỗ trợ nhiều ngôn ngữ lập trình như C, C++, C#, Java, Python, JavaScript và nhiều ngôn ngữ khác. IDE này cung cấp các tính năng như cú pháp kiểm tra, gợi ý mã, gỡ lỗi tương tác, quản lý phiên bản và đa nền tảng, giúp nhà phát triển tăng hiệu suất và sự chính xác trong quá trình phát triển phần mềm.

Visual Studio cũng cung cấp các công cụ phát triển ứng dụng di động, web và desktop. Nó hỗ trợ việc xây dựng ứng dụng Windows, ứng dụng di động trên nền tảng iOS và Android, ứng dụng web bằng ASP.NET và Node.js, ứng dụng đám mây và nhiều hơn nữa. Visual Studio có tích hợp các trình biên dịch, trình gỡ lỗi và trình quản lý dự án, giúp nhà phát triển tạo ra các ứng dụng đa dạng và chất lượng cao.

Ngoài ra, Visual Studio có thể mở rộng thông qua các tiện ích và phần mở rộng của bên thứ ba, cho phép nhà phát triển tùy chỉnh và mở rộng chức năng của IDE dựa trên nhu cầu cụ thể.

# CHƯƠNG 3: KẾT QUẢ THỰC NGHIỆM

## 3.1 Mã Hóa Mật Khẩu Bằng bcrypt

### 3.1.1 Khái Niệm bcrypt

bcrypt là một thuật toán mã hóa mật khẩu được rộng rãi sử dụng để bảo vệ thông tin đăng nhập của người dùng. Nó cung cấp một cách an toàn để lưu trữ mật khẩu trong cơ sở dữ liệu mà không tiết lộ thông tin gốc. Thuật toán này sử dụng một hàm băm mạnh kết hợp với salt (muối) và yếu tố làm việc để tạo ra một chuỗi mã hóa mật khẩu.

Salt là một giá trị ngẫu nhiên được kết hợp với mật khẩu ban đầu trước khi tiến hành quá trình mã hóa. Điều này đảm bảo rằng các mật khẩu giống nhau sẽ có chuỗi mã hóa khác nhau, ngăn chặn việc sử dụng bảng băm để tìm ra mật khẩu gốc.

Work factor là một tham số quan trọng trong bcrypt, quyết định độ phức tạp của quá trình băm. Khi work factor càng cao, quá trình băm mật khẩu tốn nhiều thời gian hơn và khó khăn hơn để tấn công bằng cách thử từng mật khẩu. Điều này giúp bảo vệ mật khẩu khỏi các cuộc tấn công brute-force và từ điển.

Bcrypt sử dụng một hàm băm mạnh như Blowfish để thực hiện quá trình mã hóa mật khẩu. Kết quả là một chuỗi mã hóa dài và không thể đọc ngược, đảm bảo tính bảo mật cao.

Khi người dùng đăng ký hoặc thay đổi mật khẩu, mật khẩu sẽ được mã hóa bằng bcrypt và lưu trữ trong cơ sở dữ liệu. Khi người dùng đăng nhập, mật khẩu nhập vào sẽ được mã hóa bằng bcrypt và so sánh với mật khẩu đã lưu trữ. Nếu hai chuỗi mã hóa trùng khớp, người dùng được phép truy cập vào hệ thống.

Tuy bcrypt là một thuật toán mã hóa mật khẩu mạnh, nhưng để đảm bảo tính an toàn tối đa, cần áp dụng các biện pháp bảo mật khác như đảm bảo mật khẩu đủ mạnh, áp dụng mã xác thực hai yếu tố và kiểm tra đầu vào cẩn thận.

3.1.2 Giao Diện Đăng Nhập Dùng Bcrypt

**A screenshot of a computer

Description automatically generated**

Hình 3. 1.Hình Ảnh Đăng Ký

A screenshot of a computer

Description automatically generated

Hình 3. 2 Hình Ảnh Mã Hóa Mật Khẩu bcrypt

**3.2**  **reCAPTCHA Trong WebSite**

3.1.1 Khái Niệm reCAPTCHA

reCAPTCHA là một dịch vụ được cung cấp bởi Google nhằm giúp phân biệt giữa người dùng thật và người dùng tự động (bot) trên các trang web. Nó được sử dụng để bảo vệ các hình thức gửi thông tin, đăng ký, đăng nhập và các hoạt động tương tự khỏi các cuộc tấn công tự động hoặc spam.

reCAPTCHA yêu cầu người dùng thực hiện một nhiệm vụ đơn giản như xác nhận hình ảnh, giải captcha hoặc thực hiện một số thao tác để chứng minh rằng họ là người thật. Nhiệm vụ này thường dựa trên khả năng nhận diện hình ảnh, đánh giá hoặc chọn các phần tử tương tự nhau trong hình ảnh.

reCAPTCHA sử dụng một loạt các kỹ thuật phân tích và học máy để xác định xem người dùng có phải là người thật hay không. Nó dựa trên dữ liệu từ hàng triệu người dùng trên toàn thế giới để xây dựng mô hình phân loại và cải thiện khả năng nhận diện. Các thông tin về hành vi của người dùng, như cách di chuột, thời gian hoạt động và các tương tác trước đó, cũng được sử dụng để phân biệt giữa người dùng thật và bot.

reCAPTCHA có hai phiên bản chính: reCAPTCHA v2 và reCAPTCHA v3. Trong reCAPTCHA v2, người dùng thường được yêu cầu xác nhận hình ảnh hoặc giải captcha. Trong khi đó, reCAPTCHA v3 hoạt động ẩn danh, tự động xác định xem người dùng có đáng tin cậy hay không dựa trên hành vi của họ trên trang web.

reCAPTCHA giúp ngăn chặn cuộc tấn công từ bot và bảo vệ thông tin cá nhân, ngăn chặn spam và hạn chế các hoạt động gian lận trên các trang web. Nó đã trở thành một công cụ phổ biến và quan trọng trong việc xác thực người dùng và đảm bảo an toàn cho các hoạt động trực tuyến.

3.2.2 Giao Diện Đăng Nhập Dùng reCAPTCHA

A screenshot of a computer

Description automatically generated

Hình 3. 3 Hình Bảo Mật Đăng Nhập reCAPTCHA

A screenshot of a computer

Description automatically generated

Hình 3. 4 Hình Bảo Mật Đăng Nhập reCAPTCHA Thành Công

**3.3 Two-Factor Authentication - 2FA Trong WebSite**

3.3.1 Khái Niệm Two-Factor Authentication - 2FA

Xác thực hai yếu tố (Two-Factor Authentication - 2FA) là một phương thức bảo mật quan trọng trong việc xác thực người dùng. Bằng cách yêu cầu người dùng cung cấp hai yếu tố độc lập để chứng minh danh tính, 2FA tạo ra một lớp bảo mật bổ sung. Quá trình này bao gồm hai yếu tố chính: yếu tố đầu tiên là mật khẩu, được xem là kiến thức chỉ có người dùng biết, và yếu tố thứ hai là mã OTP (One-Time Password) được tạo ra một cách ngẫu nhiên và có thời hạn giới hạn.

Khi người dùng muốn đăng nhập vào tài khoản, họ cần cung cấp cả mật khẩu và mã OTP để xác thực danh tính. Mật khẩu đảm bảo rằng chỉ người dùng biết thông tin này, trong khi mã OTP đảm bảo rằng người dùng có trong tay hoặc trên thiết bị của mình. Mã OTP có thể được nhận thông qua tin nhắn văn bản, ứng dụng di động, email hoặc các thiết bị vật lý như USB token hoặc thẻ thông minh.

Qua việc yêu cầu cả hai yếu tố, 2FA tăng cường đáng kể độ an toàn của quá trình xác thực. Người tấn công sẽ gặp khó khăn hơn trong việc xâm nhập vào tài khoản người dùng, vì họ cần phải có cả mật khẩu và mã OTP. Nếu một yếu tố bị lộ, yếu tố còn lại vẫn đảm bảo an toàn cho tài khoản người dùng.

2FA đã trở thành một biện pháp bảo mật phổ biến và được sử dụng rộng rãi trong nhiều dịch vụ trực tuyến và ứng dụng di động. Nó cung cấp một tầng bảo vệ bổ sung, giúp ngăn chặn các cuộc tấn công xâm nhập trực tuyến và bảo vệ thông tin cá nhân của người dùng một cách hiệu quả.

3.3.2 Giao Diện Xác Thực 2 Lớp

A screenshot of a computer

Description automatically generated

Hình 3. 5 Hình Bảo Mật Đăng Nhập OTP



Hình 3. 6 Hình OTP Gửi Về Mail

**3.4 Bảo Mật Chống Brute Force Attack**

3.4.1 Khái niệm Bảo Mật Chống Brute Force Attack

Bảo mật chống brute force attack với khóa đăng nhập sau 7 lần (Lockout Policy)

Khái niệm bảo mật chống brute force attack với khóa đăng nhập sau 7 lần (lockout policy) là một phương pháp được áp dụng để ngăn chặn các cuộc tấn công brute force attack trong hệ thống bảo mật. Theo khái niệm này, hệ thống sẽ tạm thời khóa tài khoản sau khi người dùng nhập sai mật khẩu đăng nhập một số lần vượt quá ngưỡng cho phép, thường là 7 lần.

Ý tưởng của việc áp dụng khóa đăng nhập sau 7 lần thử sai là giới hạn số lần thử mật khẩu sai mà một người dùng có thể thực hiện trước khi bị hệ thống khóa tài khoản. Khi một người dùng nhập sai mật khẩu quá nhiều lần, hệ thống sẽ xem như có nguy cơ tấn công brute force attack và sẽ áp dụng biện pháp bảo vệ bằng cách khóa tài khoản một khoảng thời gian nhất định trước khi cho phép người dùng thử lại.

Việc áp dụng khóa đăng nhập sau 7 lần thử sai giúp làm khó cho kẻ tấn công, bởi vì họ sẽ phải đợi một khoảng thời gian trước khi có thể tiếp tục thử mật khẩu. Điều này làm tăng thời gian và công sức cần thiết để thực hiện brute force attack, giúp bảo vệ hệ thống và tài khoản người dùng khỏi việc bị xâm nhập.

3.4.2 Giao Diện Bảo Mật Chống Brute Force Attack

A screenshot of a computer

Description automatically generated

Hình 3. 7 Hình Ảnh Đăng Nhập Bị Khóa

A screenshot of a computer

Description automatically generated

Hình 3. 8 Hình Ảnh Tài Khoản Bị Khóa Khi Đăng Nhập Sai 7 Lần

# CHƯƠNG 4: KẾT LUẬN

### Kết quả đạt được

Giải pháp bảo mật sử dụng mã khoá mật khẩu đã được nghiên cứu và đề xuất. Các biện pháp bảo mật như mã hóa mật khẩu, chính sách mật khẩu mạnh và mã xác thực hai yếu tố đã được triển khai để đảm bảo tính bảo mật cao cho thông tin và tài khoản người dùng trên website ATH.

Cải thiện đáng kể độ an toàn của website ATH. Việc sử dụng thuật toán mã hóa mạnh và áp dụng các biện pháp bảo mật như hạn chế số lần đăng nhập sai và kiểm tra đầu vào cẩn thận đã giúp ngăn chặn các cuộc tấn công phổ biến như SQL injection và cross-site scripting.

Tăng cường lòng tin cậy từ người dùng. Với việc triển khai các biện pháp bảo mật hiệu quả và đảm bảo an toàn thông tin cá nhân, website ATH đã tạo ra một môi trường an toàn và đáng tin cậy cho người dùng, làm tăng khả năng thu hút và giữ chân khách hàng.

Tuân thủ quy định pháp lý về bảo mật thông tin cá nhân. Việc xây dựng giải pháp bảo mật cho website ATH giúp đáp ứng các yêu cầu quy định pháp lý về bảo vệ thông tin cá nhân, đảm bảo rằng dữ liệu khách hàng được bảo vệ và xử lý theo quy định của pháp luật.

### Hướng phát triển

* + - Nâng cao mức độ bảo mật: Tiếp tục nghiên cứu và triển khai các biện pháp bảo mật tiên tiến hơn để đảm bảo tính bảo mật cao hơn cho website ATH. Điều này có thể bao gồm sử dụng các thuật toán mã hóa mạnh hơn, triển khai các biện pháp bảo vệ chống lại các cuộc tấn công mới và nâng cấp các chính sách mật khẩu.
    - Tích hợp công nghệ mới: Khám phá và tích hợp các công nghệ mới để tăng cường bảo mật. Ví dụ, xem xét việc sử dụng các phương pháp xác thực mạnh hơn như công nghệ sinh trắc học hoặc xác thực đa yếu tố để bảo vệ tài khoản người dùng.
    - Phân tích và giám sát bảo mật: Xây dựng hệ thống phân tích và giám sát bảo mật để phát hiện và ngăn chặn các hoạt động đáng ngờ trên website ATH. Sử dụng công nghệ như học máy và phân tích hành vi để xác định các hành vi bất thường và cảnh báo kịp thời.
    - Kiểm tra thâm nhập và kiểm tra bảo mật: Thực hiện các kiểm tra thâm nhập và kiểm tra bảo mật định kỳ để xác định các lỗ hổng và điểm yếu trong hệ thống. Điều này giúp đảm bảo rằng website ATH vẫn duy trì một mức độ bảo mật cao và luôn sẵn sàng đối phó với các mối đe dọa mới.
    - Đào tạo và nâng cao nhận thức về an ninh: Tiếp tục đào tạo nhóm phát triển và người quản lý về an ninh thông tin để nâng cao nhận thức và kiến thức về các mối đe dọa an ninh mới nhất và các biện pháp bảo mật tiên tiến.
    - Đáp ứng yêu cầu người dùng: Liên tục lắng nghe phản hồi từ người dùng và cải thiện giải pháp bảo mật dựa trên những yêu cầu và mong muốn của họ. Điều này giúp tăng cường sự hài lòng và tin tưởng từ phía người dùng.

# TÀI LIỆU THAM KHẢO

### Sách, bài giảng

[1]. Lê Từ Minh Trí. *Bài giảng An toàn và bảo mật thông tin*. Đại học Thủ Dầu Một, 2024.

[2]. Jason Andress, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress, 2014.

[3]. Thái Thanh Tùng, Giáo trình Mật mã học và Hệ thống Thông tin an toàn. NXB Thông tin và Truyền thông, 2011.

[4]. Stallings, William, and Lawrie Brown. Computer security: principles and practice.

Pearson, 2015.

**Website**

[5]. Vulnerabilities-By-Types. [www.cvedetails.com/vulnerabilities-by-types.php](http://www.cvedetails.com/vulnerabilities-by-types.php) [Ngày truy cập:24/04/2024]

[6]. Huỳnh Hiếu, Tích hợp google reCAPCHA vào PHP, HuynhHieu Catch Passion.

Nguồn: <https://huynhhieu.com/tich-hop-google-recaptcha-vao-php/>

[Ngày truy cập:13/05/2024]

[7]. JULY, ASP.NET core 3.1- Hash and Verify Passwords with BCrypt, jasonwatmore, năm 2020.

Nguồn: <https://jasonwatmore.com/post/2020/07/16/aspnet-core-3-hash-and-verify-passwords-with-bcrypt> [Ngày truy cập: 13/05/2024]

[8]. Kiên Nguyễn, Two-Factor Authentication (2FA) hoạt động như thế nào?, Trang TOPDev Việc Làm IT Hàng Đầu.

Nguồn: <https://topdev.vn/blog/two-factor-authentication-2fa-hoat-dong-nhu-the-nao/>  
[Ngày truy cập: 14/05/2024]

[9]. Tìm hiểu tấn công Brute Force Attack và cách phòng chống, securitybox.vn.  
Nguồn: <https://securitybox.vn/6958/tim-hieu-tan-cong-brute-force-attack-va-cach-phong-chong/> [Ngày truy cập: 14/05/2024]

[10]. Dzenana Kajtaz, Send and Receive Emails in C#, mailtrap, On January 25, 2024.  
Nguồn: <https://mailtrap.io/blog/csharp-send-email/> [Ngày truy cập: 14/05/2024]