KHOA KỸ THUẬT VÀ CÔNG NGHỆ

**BỘ MÔN CÔNG NGHỆ THÔNG TIN**

****

**PHÁT TRIỂN ỨNG DỤNG WEB VỚI MÃ NGUỒN MỞ**

**HỌC KỲ I, NĂM HỌC 2024-2025**

*Giảng viên hướng dẫn:*

ThS. Nguyễn Ngọc Đan Thanh

*Sinh viên thực hiện:*

Võ Trọng Nghĩa – 110121273

Cao Khải Minh – 110121145

Giang Quốc Huy – 117521002

Kim Hữu Ngân – 110121141

Lớp: DA21TTC

***Trà Vinh, tháng 10 năm 2024***

**NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN**

*Trà Vinh, ngày ….. tháng …… năm ……*

**Giáo viên hướng dẫn**

*(Ký tên và ghi rõ họ tên)*

*Trà Vinh, ngày ….. tháng …… năm ……*

**Giáo viên hướng dẫn**

*(Ký tên và ghi rõ họ tên)*

**NHẬN XÉT CỦA THÀNH VIÊN HỘI ĐỒNG**

*Trà Vinh, ngày ….. tháng …… năm ……*

**Thành viên hội đồng**

*(Ký tên và ghi rõ họ tên)*

**LỜI CẢM ƠN**

Đầu tiên tôi xin cảm ơn cô Nguyễn Ngọc Đan Thanh đã tận tâm, nhiệt tình hướng dẫn tôi thực hiện đề tài “**Xây dựng Website quản lý sinh viên.”**

Tiếp theo tôi xin cảm ơn tất cả những ý kiến để tôi có thể nâng tầm Website của bản thân.

**MỤC LỤC**

[CHƯƠNG 1: TỔNG QUAN 7](#_Toc180862207)

[1.1 Lý do chọn đề tài : 7](#_Toc180862208)

[1.2 Đối tượng và phạm vi nghiên cứu: 7](#_Toc180862209)

[1.2.1 Đối tượng nghiên cứu: 7](#_Toc180862210)

[1.2.2 Phạm vi nghiên cứu: 7](#_Toc180862211)

[1.3 Mục tiêu nghiên cứu: 7](#_Toc180862212)

[1.4 Nội dung nghiên cứu: 7](#_Toc180862213)

[1.5 Phương pháp nghiên cứu: 7](#_Toc180862214)

[CHƯƠNG 2: NGHIÊN CỨU LÝ THUYẾT 8](#_Toc180862215)

[2.1 Tổng quan về Visual Studio Code 8](#_Toc180862218)

[2.1.1 Sự khác nhau giữa Visual Studio Code và Visual Studio 8](#_Toc180862219)

[2.1.2 Sử dụng Visual Studio Code 8](#_Toc180862220)

[2.2 Tổng quan về PHP 9](#_Toc180862221)

[2.2.1 Ứng dụng ngôn ngữ PHP trong lập trình 10](#_Toc180862222)

[2.2.2 Ưu nhược điểm của ngôn ngữ lập trình PHP 10](#_Toc180862223)

[2.3 Tổng quan về XAMPP 11](#_Toc180862224)

[2.3.1 Các thành phần chính của Xampp 12](#_Toc180862225)

[2.4 Các bước tấn công và khắc phục 14](#_Toc180862226)

[CHƯƠNG 3: HIỆN THỰC HÓA NGHIÊN CỨU 22](#_Toc180862227)

[3.1. Các bước thực hiện Rewrite URL 22](#_Toc180862228)

[3.2. Các bước đăng ký Google API và lấy ID Google API 23](#_Toc180862229)

[CHƯƠNG 4: KẾT QUẢ NGHIÊN CỨU 31](#_Toc180862230)

[4.1 Giao diện đăng nhập, đăng ký. 31](#_Toc180862231)

[4.2 Giao diện quản lý thông tin sinh viên, thông tin lớp 32](#_Toc180862232)

[4.3 Giao diện thêm thông tin sinh viên, lớp 33](#_Toc180862233)

[4.4 Sửa thông tin sinh viên, lớp 34](#_Toc180862234)

[4.5 Tích hợp Google API( Google Maps) vào Website 35](#_Toc180862235)

[CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 37](#_Toc180862236)

[5.1 Kết luận 37](#_Toc180862237)

[5.2 Hướng phát triển 37](#_Toc180862238)

[DANH MỤC TÀI LIỆU THAM KHẢO 38](#_Toc180862239)

**DANH MỤC HÌNH ẢNH**

[Hình 2. 1. Tấn công website với SQL injection 15](#_Toc180862240)

[Hình 2. 2. Hình thức tấn công công website - Brute force 16](#_Toc180862241)

[Hình 2. 3. Tấn công website - DDoS 17](#_Toc180862242)

[Hình 2. 4. Tấn công website XSS 18](#_Toc180862243)

[Hình 2. 5. Lỗi chèn phiên 19](#_Toc180862244)

[Hình 3. 1.RewriteRule 23](#_Toc180862245)

[Hình 3. 2. Chọn để dự án cho Google API 24](#_Toc180862246)

[Hình 3. 3. Tạo dự án 24](#_Toc180862247)

[Hình 3. 4. Điền thông tin cho dự án 25](#_Toc180862248)

[Hình 3. 5. Vào Library 25](#_Toc180862249)

[Hình 3. 6. Tìm kiếm Maps JavaScript API và Places API 26](#_Toc180862250)

[Hình 3. 7. Chọn Maps JavaScript API và bật lên 26](#_Toc180862251)

[Hình 3. 8. Chọn Places API và bật lên 27](#_Toc180862252)

[Hình 3. 9. Trở lại trang chính chọn Credentials 27](#_Toc180862253)

[Hình 3. 10. Chọn API key 28](#_Toc180862254)

[Hình 3. 11. Chọn đúng điền thông tin 28](#_Toc180862255)

[Hình 3. 12. Chọn và làm theo cú pháp 29](#_Toc180862256)

[Hình 3. 13. Chỉnh sửa 30](#_Toc180862257)

[Hình 3. 14. Kết quả thực hiện 30](#_Toc180862258)

[Hình 4. 1. Giao diện đăng nhập 31](#_Toc180862259)

[Hình 4. 2. Giao diện đăng ký 32](#_Toc180862260)

[Hình 4. 3. Quản lý thông tin sinh viên 32](#_Toc180862261)

[Hình 4. 4. Quản lý thông tin sinh viên 33](#_Toc180862262)

[Hình 4. 5. Thêm thông tin sinh viên 33](#_Toc180862263)

[Hình 4. 6. Thêm thông tin lớp 34](#_Toc180862264)

[Hình 4. 7. Sửa thông tin sinh viên 34](#_Toc180862265)

[Hình 4. 8. Sửa thông tin lớp 35](#_Toc180862266)

[Hình 4. 9. Nhấn vào đường link ở cột địa chỉ để truy cập Google Maps 35](#_Toc180862267)

[Hình 4. 10. Kết quả 36](#_Toc180862268)

**MỞ ĐẦU**

Trong thời đại cách mạng khoa học kỹ thuật như hiện nay việc chuyển đổi số là nhu cầu cấp thiết để có thể phát triển bền vững. Bắt kịp xu thế Trường Đại học Trà Vinh đang cố hệ thống hóa nhiều thứ : quản lý, điểm, . . . và nhiều thứ khác.

Vì thế là một sinh viên của Trường và cũng là một sinh viên ngành công nghệ thông tin bản thân tôi thấy hiện nay việc số hóa để quản lý sinh viên là vô cùng cần thiếtnên tôi quyết định sẽ làm một trang **website quản lý sinh viên.**

Tôi mong sẽ giúp được trường của mình quản lý sinh viên một cách hiệu quả hơn.

# CHƯƠNG 1: TỔNG QUAN

## Lý do chọn đề tài :

Việc quản lý sinh viên trong trường còn quá thủ công cần phải thông qua lớp trưởng các lớp. Vì vậy tôi thấy việc số hóa quản lý sinh viên là việc vô cùng cần thiết để hỗ trợ nhà trường.

## Đối tượng và phạm vi nghiên cứu:

### Đối tượng nghiên cứu:

Nghiên cứu cách quản lý sinh viên hiệu quả.

### Phạm vi nghiên cứu:

* Nội dung: nghiên cứu cách thức quản lý sinh viên một cách tối ưu.
* Không gian: tại Trường Đại học Trà Vinh.

## Mục tiêu nghiên cứu:

Hiểu và vận dụng những gì đã học để làm ra một Website có thể thu nhập, chứa thông tin của sinh viên trong trường.

Vận dụng những lý thuyết để tạo giao diện trang web mà ai cũng có dễ dàng sử dụng.

Thiết kế và thử các chức năng của trang web.

## Nội dung nghiên cứu:

Vận dụng các kiến thức về php và html để làm ra một trang web.

Thiết kế giao diện thân thiện với người dùng.

Thêm các chức năng như: thêm, sửa, xóa, ….

## 1.5 Phương pháp nghiên cứu:

* Nghiên cứu lý thuyết: Tìm hiểu, thu thập, nghiên cứu các văn bản có liên quan đến chủ đề của đề tài.
* Nghiên cứu thực nghiệm: Thiết kế và thử nghiệm trang web.

# CHƯƠNG 2: NGHIÊN CỨU LÝ THUYẾT



## Tổng quan về Visual Studio Code

Đối với nhiều lập trình viên, trình soạn thảo code là một công cụ không thể thiếu trong quá trình xây dựng các ứng dụng web. Ưu điểm của chúng là dung lượng khá nhẹ, ít tốn RAM và được tích hợp các tính năng gần giống với IDE. Trong đó, Visual Studio Code là cái tên quen thuộc nhất với dân IT hiện nay.

Visual Studio Code (VS Code) là một trình soạn thảo mã nguồn mở gọn nhẹ nhưng có khả năng vận hành mạnh mẽ trên 3 nền tảng là Windows, Linux và macOS được phát triển bởi Microsoft. Nó hỗ trợ cho JavaScript, Node.js và TypeScript, cũng như cung cấp một hệ sinh thái mở rộng vô cùng phong phú cho nhiều ngôn ngữ lập trình khác.

Có thể nói, VS Code là sự kết hợp giữa một trình soạn thảo mã nguồn với những công cụ phát triển mạnh mẽ như Git, Debug hay Syntax Highlighter.

### Sự khác nhau giữa Visual Studio Code và Visual Studio

Do tên gọi khá tương đồng nên có nhiều người nhầm lẫn giữa Visual Studio Code và Visual Code. Trên thực tế, chúng hoàn toàn khác nhau.

VS Code là một trình soạn thảo văn bản. Visual Studio là một môi trường phát triển tích hợp.

VS Code có thể chạy trên nhiều nền tảng. Visual Studio chỉ có thể chạy trên Windows hoặc Mac (đây là 2 sản phẩm khác nhau)

Tốc độ của VS Code được đánh giá là nhanh hơn so với Visual Studio.

Kích thước tải xuống của VS Code nhỏ hơn Visual Studio.

### Sử dụng Visual Studio Code

**Hoạt động đa nền tảng**

VS Code được thiết kế để có thể chạy tốt trên macOS, Linux và Windows. Vì thế, bạn có thể thoải mái sử dụng trình soạn thảo này mà không cần lo lắng về vấn đề lựa chọn nền tảng tương thích.

**Đơn giản trong việc chỉnh sửa, xây dựng và gỡ lỗi**

Như đã nói ở trên, tốc độ là một trong những ưu thế vượt trội của VS Code. Nó có thể hỗ trợ rất nhiều các loại ngôn ngữ lập trình khác nhau như Java, Python, C++, C#, Golang hay PHP. Điều này cho phép bạn có thể ứng dụng rất nhiều tính năng thú vị như đánh dấu cú pháp, tự động thụt lề, đối sánh dấu ngoặc,… cho công việc của mình.

Hệ thống phím tắt sinh động, trực quan giúp thao tác trở nên nhanh chóng hơn, từ đó năng suất và hiệu quả lập trình cũng được tăng lên. Ngoài ra, tính năng nhắc mã IntelliSense chuyên nghiệp trên VS Code sẽ tự động phát hiện đoạn mã không đầy đủ và thông báo cho lập trình viên. Hoặc nó có thể tự động bổ sung cú pháp còn thiếu khi bạn quên không khai báo biến.

Gỡ lỗi cũng là một tính năng nổi bật của VS Code. Nó giúp bạn xem mã nguồn, kiểm tra các các biến, Call Stack và thực thi lệnh trong bảng điều khiển. Bên cạnh đó, trình soạn thảo này còn hỗ trợ Git phục vụ cho việc kiểm soát nguồn mà không đòi hỏi phải rời khỏi trình chỉnh sửa.

**Sự hỗ trợ của cộng đồng GitHub**

Visual Studio Code là một dự án mã nguồn mở nên bạn hoàn toàn có thể tham gia đóng góp và tìm kiếm sự giúp đỡ từ cộng đồng GitHub.

**Kiến trúc cực mạnh mẽ và có thể mở rộng**

VS Code được xây dựng dựa trên Electron, kết hợp các công nghệ web như Node.js và JavaScript với tốc độ và sự linh hoạt của các ứng dụng gốc. Ngoài ra, kiến trúc dịch vụ công cụ của VS Code giúp nó tích hợp được với các công nghệ hỗ trợ Visual Studio như Roslyn cho .NET, TypeScript, công cụ gỡ lỗi Visual Studio,…

Nhờ những ưu điểm nổi bật của mình, VS Code trở thành một trong những sự lựa chọn hàng đầu của rất nhiều lập trình viên, giúp đảm bảo tiến độ và đạt hiệu quả công việc cao.

https://vn.got-it.ai/blog/visual-studio-code-la-gi-loi-the-tu-viec-su-dung-visual-studio-code

## Tổng quan về PHP

PHP (viết tắt đệ quy của PHP: Hypertext Preprocessor) là tập hợp con của các ngôn ngữ script như JavaScript và [Python](https://www.python.org/doc/essays/blurb/). Sự khác biệt là ngôn ngữ PHP chủ yếu được sử dụng để giao tiếp phía server trong khi JavaScript có thể được sử dụng cho cả frontend cũng như backend và Python – chỉ dành cho phía client (backend) là một công cụ mạnh mẽ để tạo ra các trang web động và tương tác.

Khi các lập trình viên PHP viết chương trình, chuỗi lệnh sẽ được xử lý trên server sau đó sinh ra mã HTML trên client. Dựa vào đó, các ứng dụng trên website sẽ hoạt động một cách dễ dàng.

[Ngôn ngữ PHP](https://topdev.vn/blog/category/lap-trinh/php/) thường được dùng trong việc xây dựng và phát triển website bởi nó có thể kết nối dễ dàng với các website khác có sử dụng [HTML](https://topdev.vn/blog/html-la-gi-cac-the-html-co-ban-va-ung-dung/). PHP cũng là ngôn ngữ lập trình có mã nguồn mở, tương thích với nhiều nền tảng khác nhau như MacOS, Linux, Windows,… PHP được nhiều người dùng đánh giá là dễ đọc nên đa số các lập trình viên sẽ lựa chọn học PHP trước khi bắt đầu vào nghề.

### Ứng dụng ngôn ngữ PHP trong lập trình

Một số ứng dụng phổ biến của PHP trong ngành IT:

Thiết lập chương trình cho hệ thống máy chủ: Đây là một ứng dụng chủ yếu nhất của PHP. Các PHP Developer sẽ phải thực hiện các thao tác như phân tích ngôn ngữ lập trình PHP, xây dựng máy chủ web và trình duyệt web.

Tạo các dòng tập lệnh: Các lập trình viên sẽ tạo ra một dòng tập lệnh để vận hành chương trình PHP mà không cần đến máy chủ. Kiểu lập trình này được sử dụng trên các hệ điều hành phổ biến như Linux hay Windows.

Xây dựng các ứng dụng làm việc: Bạn có thể ứng dụng những điểm mạnh vốn có của PHP để xây dựng ứng dụng phần mềm. Các lập trình viên thường dùng PHP – GTK làm nền tảng xây dựng phần mềm vì đây là nhánh mở rộng của ngôn ngữ lập trình này và không có sẵn trong các bản phân phối chính thức hiện nay.

Hỗ trợ cho mọi loại cơ sở dữ liệu khác nhau: Khi một website có hỗ trợ cơ sở dữ liệu tốt sẽ giúp ích cho việc vận hành, sao lưu và đặc biệt là backup dữ liệu đề phòng trường hợp xảy ra an ninh mạng.

### Ưu nhược điểm của ngôn ngữ lập trình PHP

**Ưu điểm**

PHP được sử dụng phổ biến bởi nhiều lợi ích mà nó mang lại. Dưới đây là một số ưu điểm cơ bản của ngôn ngữ PHP:

Mã nguồn mở và miễn phí: PHP sử dụng miễn phí nên giúp tiết kiệm đáng kể ngân sách dự án. Việc cài đặt và sử dụng ngôn ngữ này cũng rất dễ dàng, bạn chỉ cần học chăm chỉ trong 3 – 6 tháng là đã có thể sử dụng thuần thục.

Tính linh hoạt: PHP là một ngôn ngữ đa nền tảng, có thể hoạt động trên bất kỳ hệ điều hành nào (Windows, Linux, macOS,…). Hơn nữa, PHP còn có thể kết hợp với nhiều ngôn ngữ lập trình khác để xây dựng các tính năng công nghệ một cách hiệu quả nhất.

Hệ thống thư viện phong phú, tính cộng đồng cao: Do sự phổ biến của ngôn ngữ PHP nên việc tìm các thư viện code hay hàm liên quan đến PHP sẽ cực kỳ đơn giản. Chưa kể, bạn sẽ nhận được sự trợ giúp từ các diễn đàn, đội nhóm chuyên sâu của PHP giúp việc học tập hay làm việc trở nên dễ dàng.

Cơ sở dữ liệu đa dạng: PHP cho phép kết nối với hầu hết các cơ sở dữ liệu khác như [mySQL](https://topdev.vn/blog/gioi-thieu-ve-mysql/), SQLite, PostgreSQL, MS-SQL,…

**Nhược điểm**

Mặc dù sở hữu nhiều lợi ích nhưng ngôn ngữ PHP vẫn có một số hạn chế nhất định, trong đó vấn đề bảo mật được nhiều người quan tâm nhất. Bởi bản chất của PHP có mã nguồn mở nên các lỗ hổng của mã nguồn sẽ bị công khai ngay sau khi chúng được tìm thấy. Và các lỗ hổng này có thể bị khai thác cho các mục đích xấu trước khi chúng ta kịp sửa chữa.

Bên cạnh đó, ngôn ngữ lập trình PHP chỉ hoạt động được trên các website và giao diện không được gọn gàng, đẹp mắt. Độ bảo mật và hiệu suất của ngôn ngữ này cũng chưa tốt.

## Tổng quan về XAMPP

Phần mềm Xampp là một trong những phần mềm được nhiều lập trình viên sử dụng để [thiết lập website](https://monamedia.co/dich-vu/thiet-ke-website/) theo ngôn ngữ PHP. XAMPP có công dụng thiết lập web server có cài đặt sẵn các công cụ như PHP, Apache, MySQL… Xampp sở hữu thiết kế giao diện thân thiện với người dùng, cho phép các lập trình viên có thể đóng mở hoặc reboot các tính năng của server mọi lúc. Ngoài ra, Xampp cũng được xây dựng theo source code mở.

Đánh giá một cách tổng thể, Xampp được đánh giá là một trong những phần mềm trọng yếu trong việc xây dựng website dành cho các lập trình viên PHP. Xampp cài đặt các thành tố trọng yếu, hỗ trợ lẫn nhau bao gồm:

Apache

PHP (thiết lập nền tảng để các tập tin script \*.php hoạt động);

MySql (hệ quản trị dữ liệu)

Perl

### Các thành phần chính của Xampp

Cho những người chưa thật sự để ý đến thuật ngữ Xampp, chúng là chữ viết tắt của X, Apache, MySQL, PHP và Perl. Chữ X là viết tắt cho cross platform, ám chỉ phần mềm này có thể tương thích với nhiều hệ điều hành như Windows, Mac, Linux, Solaris…

**Apache**

Apache là một website software sử dụng source code mở hoàn toàn miễn phí, được sử dụng bởi 46% trên tổng số các website trên toàn cầu. Phần mềm web này được thiết lập và cập nhật bởi Apache Software Foundation.

Ra đời hơn 20 năm về trước, Apache được nhiều chuyên gia công nhận là một trong những web server uy tín, đáng sử dụng cho các website. Song song với NGINX (một phần mềm web phổ biến khác), Apache giúp website sở hữu một server hoàn thiện hơn, có thể tải nhiều nội dung lên cho website của mình nổi bật hơn mà không gặp phải bất kỳ trở ngại nào.

**MySQL**

MySQL là một hệ thống quản lý cơ sở dữ liệu liên kết có ưu điểm nhanh chóng, dễ dùng cho các lập trình viên. MySQL được ứng dụng khá nhiều cho các website thương mại điện tử hiện nay.

Hệ thống được phát triển bởi công ty Thụy Điển này hiện được nhiều lập trình viên hàng đầu trên thế giới ưa chuộng bởi những ưu điểm sau.

MySQL là một opensource, hoàn toàn miễn phí.

Hiệu suất hoạt động của MySQL rất mạnh mẽ, kể cả khi khối lượng dữ liệu khổng lồ. Có thể kiểm tra toàn vẹn dữ liệu với [SQL Trigger](https://freelancervietnam.vn/sql-trigger-la-gi-su-khac-biet-va-cach-thuc-xu-dung/).

Cái tên nói lên tất cả, hệ thống này sử dụng ngôn ngữ dữ liệu SQL để cấu trúc hóa website của bạn.

MySQL tương thích với hầu hết các hệ điều hành (Windows, Mac, Linux…) cùng các ngôn ngữ lập trình như PHP, C++, Java…

MySQL rất tương thích với PHP, ngôn ngữ lập trình phổ biến của nhiều lập trình viên.

MySQL có hệ thống thông tin khổng lồ, chứa đến 50 triệu hàng dữ liệu trong 1 board. Dữ liệu tối thiểu của board này là 4GB, còn tối đa là 8TB (tùy theo độ mạnh của hệ điều hành)

MySQL cho phép điều chỉnh tùy ý để các lập trình viên có thể thao tác thay đổi cho website của mình.

**PHP**

PHP (viết tắt của Hypertext Pre-processor, tiền thân là Personal Home Page) là một ngôn ngữ lập trình kịch bản, được ứng dụng trong các loại website (tĩnh và động) và [ứng dụng website](https://monamedia.co/lap-trinh-phan-mem-web-app/). Các script được viết bằng ngôn ngữ lập trình PHP sẽ được các server có cài đặt PHP hiểu được và “tiêu hóa” chúng. Cụ thể, các script này sẽ được lưu dưới dạng tệp đuôi “.php”, sau đó các server sẽ diễn giải chúng và đưa lên website tùy theo template web mà lập trình viên lựa chọn.

Ngôn ngữ lập trình PHP có thể được nhúng trong HTML, được ứng dụng trong quản lý các loại nội dung website (nhất là nội dung động) cũng như quản lý các dữ liệu thống kê liên quan đến website như số phiên, thời gian phiên… PHP được sử dụng nhiều trong các loại Database phổ biến như MySQL, PostgreSQL, Oracle, Sybase, Informix, và Microsoft SQL Server.

PHP thực thi rất tuyệt vời, đặc biệt khi được biên dịch như là một Apache Module trên Unix side. MySQL Server, khi được khởi động, thực thi các truy vấn phức tạp với các tập hợp kết quả khổng lồ trong thời gian Record-setting.

Các chuyên gia code từng đánh giá rằng PHP là một ngôn ngữ lập trình tuyệt vời, có khả năng phiên dịch không khác gì một Apache Module trên Unixside. Đồng thời, chúng còn cho phép hoạt động theo các giao thức nổi tiếng như POP3, IMAP, và LDAP. Ngoài ra, ngôn ngữ lập trình cải tiến từ PHP, PHP4, còn tương hỗ với một [ngôn ngữ lập trình](https://monamedia.co/top-10-ngon-ngu-lap-trinh-phan-mem-tot-nhat-hien-nay/) khác là Java cùng các cấu trúc đối tượng phân phối như COM và COBRA nhằm vào mục đích thiết lập website cùng ứng dụng website. Đặc biệt hơn nữa, PHP có cú pháp nhập lệnh tương tự với ngôn ngữ lập trình C.

**Perl**

PERL có tên đầy đủ là Practical Extraction and Report Language, là một trong những ngôn ngữ lập trình hiện đại hoạt động song song với PHP trong Xampp có khả năng lọc bỏ những dữ liệu thừa và cung cấp những dữ liệu quan trọng trong việc thiết lập website. Tuy không nổi bằng PHP, Perl cũng có những ưu điểm nhất định khiến nhiều lập trình viên trên toàn thế giới cảm thấy ấn tượng và ứng dụng cho website của mình.

Tự động quản lý và phân tích dữ liệu website.

Có thể hoạt động tốt với các chuỗi cú pháp, ký tự.

Cộng đồng sử dụng Perl khá lớn, góp công vào việc xây dựng kho mã lệnh CPAN khổng lồ cho các lập trình viên.

Tương tự như PHP, Perl có cú pháp giống ngôn ngữ lập trình C.

Độ linh hoạt của Perl cao, cho phép lập trình viên có thể tùy biến chúng để giải quyết các vấn đề liên quan đến website và ứng dụng.

## Các bước tấn công và khắc phục

**Các hình thức tấn công website phổ biến và cách khắc phục**

An ninh mạng cho website luôn là vấn đề được các doanh nghiệp ưu tiên hàng đầu bởi website là nơi lưu trữ các thông tin quan trọng của doanh nghiệp và dữ liệu của khách hàng. Khi website bị tấn công hoặc xâm nhập sẽ kéo theo những rủi ro gây thiệt hại nặng nề cho doanh nghiệp.

**Tấn công bằng phần mềm độc hại (Malware attack)**

Tấn công malware là hình thức phổ biến nhất. [Malware](https://cystack.net/vi/blog/muon-hinh-van-trang-cac-loai-malware)bao gồm spyware (phần mềm gián điệp), [ransomware](https://cystack.net/blog/ransomware-la-gi/) (mã độc tống tiền), virus và worm (phần mềm độc hại có khả năng lây lan nhanh). Thông thường, tin tặc sẽ tấn công người dùng thông qua các lỗ hổng bảo mật, cũng có thể là dụ dỗ người dùng click vào một đường link hoặc email (phishing) để phần mềm độc hại tự động cài đặt vào máy tính. Một khi được cài đặt thành công, malware sẽ gây ra:

* Ngăn cản người dùng truy cập vào một file hoặc folder quan trọng (ransomware)
* Cài đặt thêm những phần mềm độc hại khác
* Lén lút theo dõi người dùng và đánh cắp dữ liệu (spyware)
* Làm hư hại phần mềm, phần cứng, làm gián đoạn hệ thống.

**Tấn công website với SQL injection**

SQL injection là một hình thức tấn công cho phép các tin tặc sử dụng các lỗ hổng tại kênh đầu vào của trang web với mục đích đánh cắp dữ liệu quan trọng tại nơi lưu trữ những thông tin có giá trị hay các cơ sở dữ liệu của trang web.

A hand holding a sign

Description automatically generated

Hình 2. 1. Tấn công website với SQL injection

Ngôn ngữ truy vấn mang tính cấu trúc SQL là loại ngôn ngữ phổ biến để tạo, sửa hoặc lấy dữ liệu trên hệ quản trị cơ sở dữ liệu của ứng dụng.

Chính vì vậy, các cơ sở dữ liệu có trong SQL sẽ không thể tránh khỏi nguy cơ bị tấn công và các chương trình chống virus cũng không đảm bảo chặn được 100% các cuộc tấn công SQL injection.

Cách tốt nhất để ngăn chặn được hình thức tấn công này là bạn phải thường xuyên cập nhật, kiểm tra và vá các lỗ hổng bảo mật của tất cả các ứng dụng, dịch vụ, máy chủ hoặc sử dụng source code.

**Tấn công Brute force**

Việc các tin tặc sử dụng phần mềm để các ký tự khác nhau được sắp xếp lại thành một mật khẩu đúng được gọi là hình thức tấn công website Brute force. Nhiều quản trị viên của website thường chủ quan trong việc đặt username và mật khẩu, không thường xuyên thay đổi mật khẩu hay không bảo mật cho đường dẫn đăng nhập.

Điều này vô tình đã giúp các tin tặc có thể dễ dàng tìm được thông tin đăng nhập. Chúng sẽ sử dụng các thông tin tìm được để truy cập vào website và tiến hành thực hiện những hành vi trái phép tại đó.

[](https://bizflyportal.mediacdn.vn/bizflyportal/techblog/tan16306405462331.jpg)

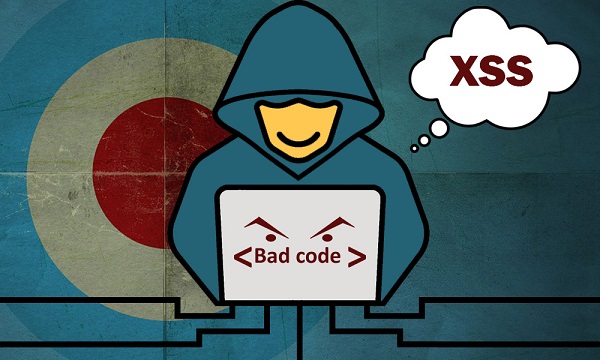
Hình 2. 2. Hình thức tấn công công website - Brute force

Để có thể đối phó với loại tấn công này, bạn cần:

* Tăng cường độ mạnh cho mật khẩu bằng cách đặt mật khẩu có tối thiểu 8 ký tự, bao gồm chữ hoa, chữ thường, ký tự đặc biệt và không nên tuân theo một ý nghĩa hay trật tự nào cả.
* Sử dụng các cơ chế chứng thực Digest Authentication hoặc Basic.
* Hạn chế đăng nhập sai tài khoản hoặc khoá tài khoản do đăng nhập sai.
* Xác định dấu hiệu của hình thức tấn công này bằng cách sử dụng module Mod\_Dosevasive.

Tấn công DDoS website

Nếu bạn nhận thấy website của mình đang phải nhận một lượng traffic lớn hoặc không thể truy cập được vào website thì khả năng cao trang web đã trở thành đối tượng bị [tấn công DDoS](https://bizfly.vn/techblog/ddos-la-gi.html). Đây là hình thức tấn công được các tin tặc sử dụng để đánh sập máy chủ bằng số lượng request khổng lồ.

[](https://bizflyportal.mediacdn.vn/bizflyportal/images/tan16303320291005.jpeg)

Hình 2. 3. Tấn công website - DDoS

Điều này khiến cho khách hàng không thể truy cập được vào website và không thể thực hiện bất kỳ tương tác, mua hàng hay tìm kiếm những thông tin cần thiết. Nó được xem là loại hình tấn công nghiêm trọng gây ra những hậu quả nặng nề cho doanh nghiệp, ảnh hưởng tiêu cực đến website.

Vì vậy, để đảm bảo an toàn cho website bạn nên:

* Nâng cao ý thức bảo mật website cho các quản trị viên.
* Kiểm tra mã nguồn website định kỳ và cấu hình security cho trang web.
* Hạn chế cài đặt các plugin lạ.
* Backup dữ liệu định kỳ theo ngày, theo tuần hoặc theo tháng.

**Tấn công website XSS**

XSS là một hình thức tấn công mạng mà trong đó, các phần nội dung của website đáng tin cậy sẽ bị các tin tặc chèn mã độc hại vào đó. Hầu hết các đoạn mã độc hại được viết bằng Client-Site Script như JScript, JavaScript, DHTML thậm chí là cả các thẻ HTML.

[](https://bizflyportal.mediacdn.vn/bizflyportal/images/tan16303317374859.jpeg)

Hình 2. 4. Tấn công website XSS

Với hình thức tấn công này, các tin tặc sẽ không tấn công trực tiếp vào nạn nhân mà sẽ khai thác các lỗ hổng trong trang web - nơi mà các nạn nhân truy cập. Tuy nhiên, XSS chỉ gây tổn hại với các trang web tại phía client và những người duyệt trang đó sẽ vô tình trở thành nạn nhân trực tiếp.

Để có thể tránh được loại tấn công này, bạn nên:

* Từ chối nhận các dữ liệu sai và cho phép các dữ liệu hợp lệ.
* Kiểm tra và lọc các dữ liệu đầu vào một cách thường xuyên.
* Lọc các dữ liệu tấn công XSS bằng cách sử dụng Mod\_Security.

**Lỗi chèn phiên**

Lỗi chèn phiên hay phương thức chiếm phiên thường xảy ra khi một tài khoản truy cập bất kỳ tiến hành thực hiện quá trình chứng thực tài khoản, mật khẩu đối với các server. Server sẽ dựa trên những thông tin này để tạo ra một giá trị session ID duy nhất cho phép người dùng có thể duy trì kết nối.

Nếu giá trị session ID này bị tin tặc đoán được thì khả năng người dùng hợp lệ khác bị chúng chiếm phiên là rất lớn. Bạn có thể đối phó với loại hình tấn công này bằng cách:

[](https://bizflyportal.mediacdn.vn/bizflyportal/techblog/loi16306406839064.jpeg)

Hình 2. 5. Lỗi chèn phiên

* Tránh trường hợp bị nghe lén dữ liệu bằng cách sử dụng SSL trong quá trình chứng thực.
* Thuật toán mã hoá mạnh và sử dụng các cơ chế ngẫu nhiên để tạo ra giá trị session ID.
* Để khiến cho quá trình tấn công web gặp khó khăn thì session ID phải đủ lớn.
* Thời gian tồn tại của session ID phải được giới hạn.

**Lỗi chứng thực yếu**

Khi một trang web cho phép một tài khoản bất kỳ không có đủ điều kiện truy cập vào các nội dung nhạy cảm thì lỗi chứng thực yếu sẽ xuất hiện. Tình trạng này có thể dễ dàng gặp được tại các trang quản trị website.

<https://bizfly.vn/techblog/tan-cong-website.html>

**Tấn công giả mạo (Phishing attack)**

Phishing là hình thức giả mạo thành một đơn vị/cá nhân uy tín để chiếm lòng tin của người dùng, thông thường qua email. Mục đích của tấn công Phishing thường là đánh cắp dữ liệu nhạy cảm như thông tin thẻ tín dụng, mật khẩu, đôi khi phishing là một hình thức để lừa người dùng cài đặt malware vào thiết bị (khi đó, phishing là một công đoạn trong cuộc tấn công malware).

**Tấn công trung gian (Man-in-the-middle attack)**

Tấn công trung gian (MitM), hay **tấn công nghe lén**, xảy ra khi kẻ tấn công xâm nhập vào một giao dịch/sự giao tiếp giữa 2 đối tượng. Khi đã chen vào giữa thành công, chúng có thể đánh cắp dữ liệu của giao dịch đó.

Loại hình này xảy ra khi:

* Nạn nhân truy cập vào một mạng Wifi công cộng không an toàn, kẻ tấn công có thể “chen vào giữa” thiết bị của nạn nhân và mạng Wifi đó. Vô tình, những thông tin nạn nhân gửi đi sẽ rơi vào tay kẻ tấn công.
* Khi phần mềm độc hại được cài đặt thành công vào thiết bị, một kẻ tấn công có thể dễ dàng xem và điều chỉnh dữ liệu của nạn nhân.

**Tấn công từ chối dịch vụ (DoS và DDoS)**

DoS (Denial of Service) là hình thức tấn công mà tin tặc “đánh sập tạm thời” một hệ thống, máy chủ, hoặc mạng nội bộ. Để thực hiện được điều này, chúng thường tạo ra một lượng traffic/request khổng lồ ở cùng một thời điểm, khiến cho hệ thống bị quá tải, từ đó người dùng không thể truy cập vào dịch vụ trong khoảng thời gian mà cuộc tấn công DoS diễn ra.

Một hình thức biến thể của DoS là DDoS (Distributed Denial of Service): tin tặc sử dụng một mạng lưới các máy tính (botnet) để tấn công nạn nhân. Điều nguy hiểm là chính các máy tính thuộc mạng lưới botnet cũng không biết bản thân đang bị lợi dụng để làm công cụ tấn công.

**Khai thác lỗ hổng Zero-day (Zero day attack)**

Lỗ hổng Zero-day (0-day vulnerabilities) là các lỗ hổng bảo mật chưa được công bố, các nhà cung cấp phần mềm chưa biết tới, và dĩ nhiên, chưa có bản vá chính thức. Chính vì thế, việc khai thác những lỗ hổng “mới ra lò” này vô cùng nguy hiểm và khó lường, có thể gây hậu quả nặng nề lên người dùng và cho chính nhà phát hành sản phẩm.

**Giải pháp chống tấn công mạng**

**Đối với cá nhân**

* Bảo vệ mật khẩu cá nhân bằng cách: đặt mật khẩu phức tạp, bật tính năng bảo mật 2 lớp – xác nhận qua điện thoại,… Chi tiết tại: [3 kiểu Tấn công Password cơ bản & cách phòng chống](https://cystack.net/blog/3-hinh-thuc-tan-cong-password-co-ban)
* Hạn chế truy cập vào các điểm wifi công cộng
* Không sử dụng phần mềm bẻ khóa (crack)
* Luôn cập nhật phần mềm, hệ điều hành lên phiên bản mới nhất.
* Cẩn trọng khi duyệt email, kiểm tra kỹ tên người gửi để phòng tránh lừa đảo.
* Tuyệt đối không tải các file hoặc nhấp vào đường link không rõ nguồn gốc.
* Hạn chế sử dụng các thiết bị ngoại vi (USB, ổ cứng) dùng chung.
* Sử dụng một phần mềm diệt Virus uy tín.

**Đối với tổ chức, doanh nghiệp**

* [Xây dựng một chính sách bảo mật](https://cystack.net/blog/xay-dung-chinh-sach-bao-mat-cho-doanh-nghiep) với các điều khoản rõ ràng, minh bạch
* Lựa chọn các phần mềm, đối tác một cách kỹ càng. Ưu tiên những bên có cam kết bảo mật và cam kết cập nhật bảo mật thường xuyên.
* Tuyệt đối không sử dụng các phần mềm crack
* Luôn cập nhật phần mềm, firmware lên phiên bản mới nhất.
* Sử dụng các dịch vụ đám mây uy tín cho mục đích lưu trữ.
* Đánh giá bảo mật & Xây dựng một chiến lược an ninh mạng tổng thể cho doanh nghiệp, bao gồm các thành phần: [bảo mật website,](https://cystack.net/blog/bao-mat-website) bảo mật hệ thống máy chủ, mạng nội bộ, hệ thống quan hệ khách hàng (CRM), [bảo mật IoT](https://cystack.net/blog/bao-mat-thiet-bi-iot), bảo mật hệ thống CNTT – vận hành…
* Tổ chức các buổi đào tạo, [training kiến thức sử dụng internet an toàn cho nhân viên](https://cystack.net/blog/lam-sao-de-nang-cao-y-thuc-bao-mat-cua-nhan-vien/).

CHƯƠNG 3: HIỆN THỰC HÓA NGHIÊN CỨU

1. Các bước thực hiện Rewrite URL

**Các bước Rewrite URL trong web server**

Việc **Rewrite URL** giúp tối ưu hóa đường dẫn (SEO-friendly) và làm cho URL dễ nhớ, bảo mật hơn. Dưới đây là các bước thực hiện URL rewriting trên hai nền tảng phổ biến: **Apache** và **Nginx**.

**Bước 1: Kích hoạt mod mod\_rewrite có sẵn trong Apache:**

– Bẳng cách cấu hình trong file httpd.conf.

– Ngoài ra, môi trường Shared hosting mặc định đã hỗ trợ.

**Bước 2: Tạo 1 file .htaccess thư mục gốc của web của bạn có nội dung như sau:**

Đầu tiên bật Rewrite Engine:

RewriteEngine on

Tiếp đến là viết cú pháp RewriteRule:

Để hiểu thêm chi tiết về RewriteRule “ đây là đường dẫn phụ có thể thay thế ” “còn đây là đường dẫn chính đến thư mục”

A screenshot of a computer program

Description automatically generated

Hình 3. 1.RewriteRule

1. Các bước đăng ký Google API và lấy ID Google API

**Bước 1:** Trước tiên truy cập vào đường link: <https://console.cloud.google.com/apis/dashboard?project=quick-country-438806-q5>

Tạo dự án chọn **Select a project** để tao dự án

A screenshot of a project

Description automatically generated

Hình 3. 2. Chọn để dự án cho Google API

**Bước 2:** rồi chọn **NEW PROJECT** để tạo mới project.

A screenshot of a browser

Description automatically generated

Hình 3. 3. Tạo dự án

**Bước 3:** Điền tên project theo ý muốn của bạn và chọn **CREATE**.

A screenshot of a web page

Description automatically generated

Hình 3. 4. Điền thông tin cho dự án

**Bước 4:** Tạo project xong chúng ta vào **Library**.

A screenshot of a search engine

Description automatically generated

Hình 3. 5. Vào Library

**Bước 5:** Trong Library các bạn tìm kiếm **Maps JavaScript API** và **Places API** rồi chọn **Enable** để kích hoạt.

A screenshot of a computer

Description automatically generated

Hình 3. 6. Tìm kiếm Maps JavaScript API và Places API

Chọn **Enable** kích hoạt **Maps JavaScript API**, chờ một chút cho quá trình kích hoạt được diễn ra.

A screenshot of a browser

Description automatically generated

Hình 3. 7. Chọn Maps JavaScript API và bật lên

Tương tự như trên, chúng ta kích hoạt **Places API**.

A screenshot of a computer

Description automatically generated

Hình 3. 8. Chọn Places API và bật lên

Bước 6: Sau khi kích hoạt xong chúng ta quay trở lại trang chính chọn **Credentials**.

A screenshot of a computer

Description automatically generated

Hình 3. 9. Trở lại trang chính chọn Credentials

Tiếp theo chọn **CREATE CREDENTIALS -> API key**.

A screenshot of a computer

Description automatically generated

Hình 3. 10. Chọn API key

Và điền những thông tin và chọn theo hình sau đó nhấn SAVE.

A screenshot of a computer

Description automatically generated

Hình 3. 11. Chọn đúng điền thông tin

A screenshot of a computer

Description automatically generated

Hình 3. 12. Chọn và làm theo cú pháp

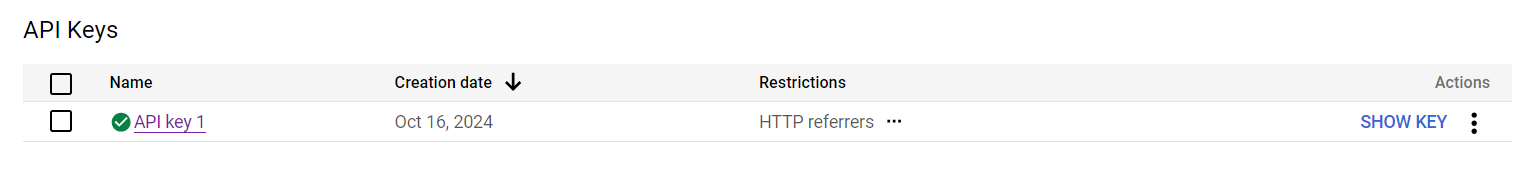
**Bước 7:** Nếu nhưng nó hiện thông báo lỗi thì nhấn vào -> … chọn Edit API Key. Và điền những thông tin như bước 6.

A screenshot of a computer

Description automatically generated

Hình 3. 13. Chỉnh sửa

Và đây là kết quả sao khi làm xong các bước trên.

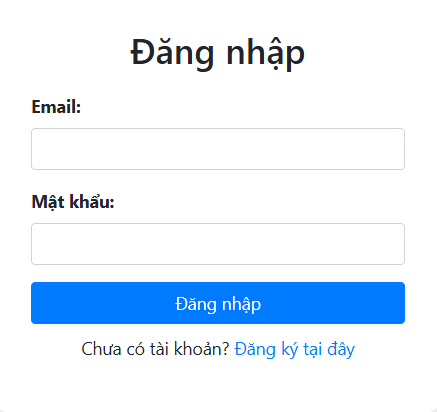


Hình 3. 14. Kết quả thực hiện

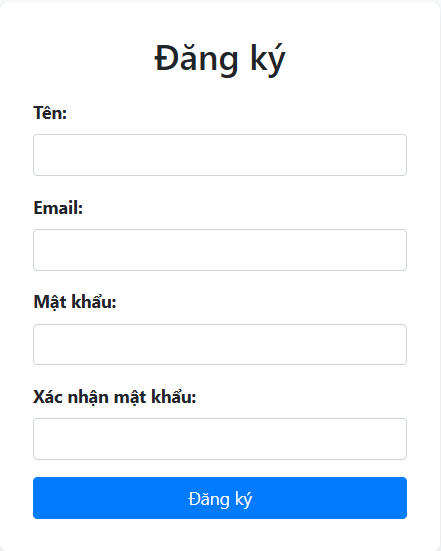
Tiếp theo nhấn vào API Key 1 và coppy ID của Google API.

# CHƯƠNG 4: KẾT QUẢ NGHIÊN CỨU

## Giao diện đăng nhập, đăng ký.

****

Hình 4. 1. Giao diện đăng nhập

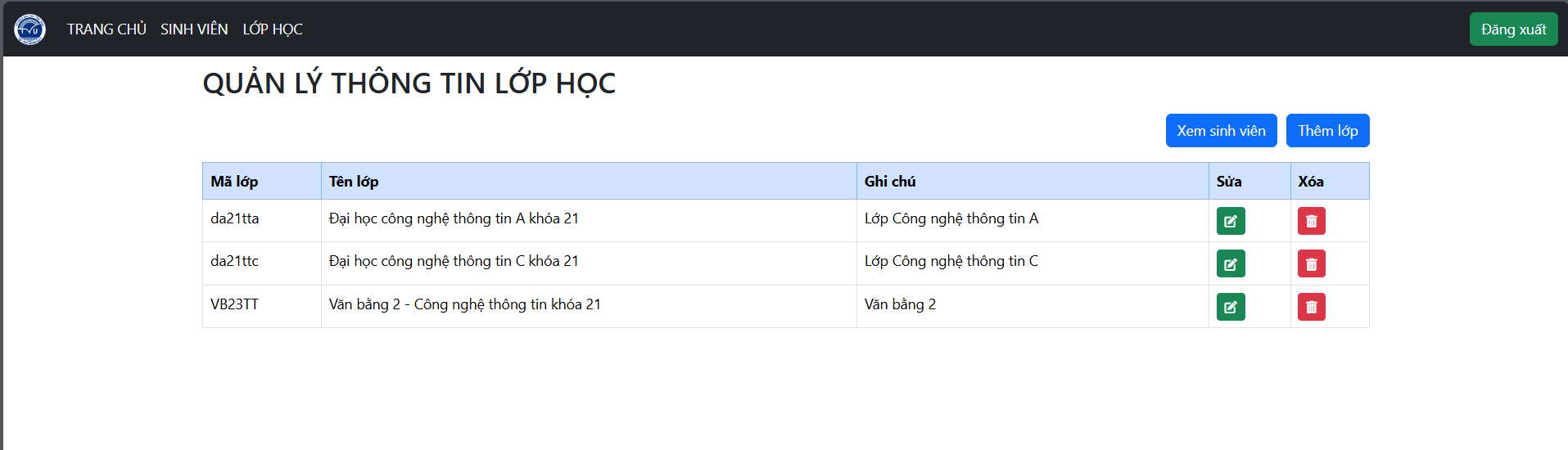


Hình 4. 2. Giao diện đăng ký

## Giao diện quản lý thông tin sinh viên, thông tin lớp

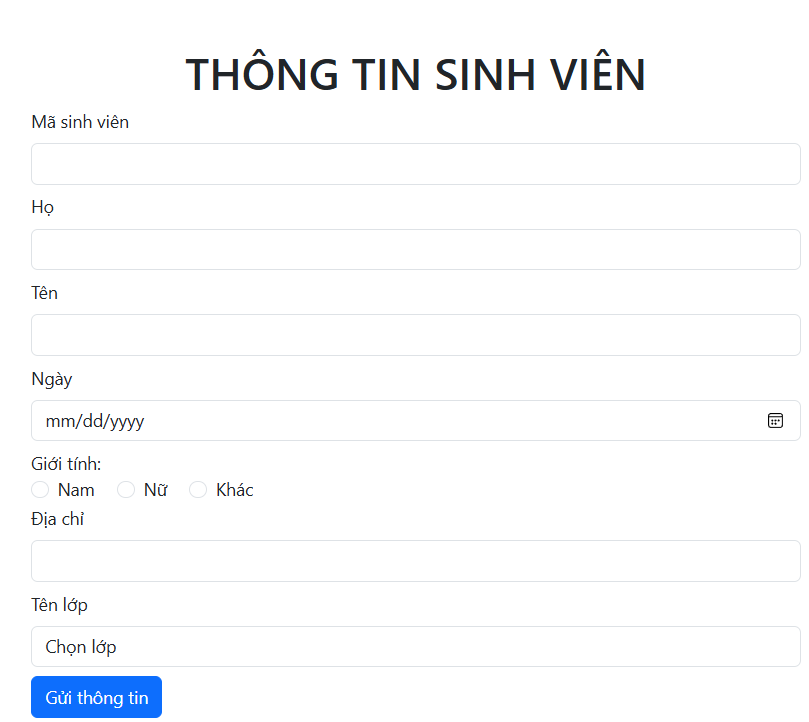


Hình 4. 3. Quản lý thông tin sinh viên



Hình 4. 4. Quản lý thông tin sinh viên

## Giao diện thêm thông tin sinh viên, lớp

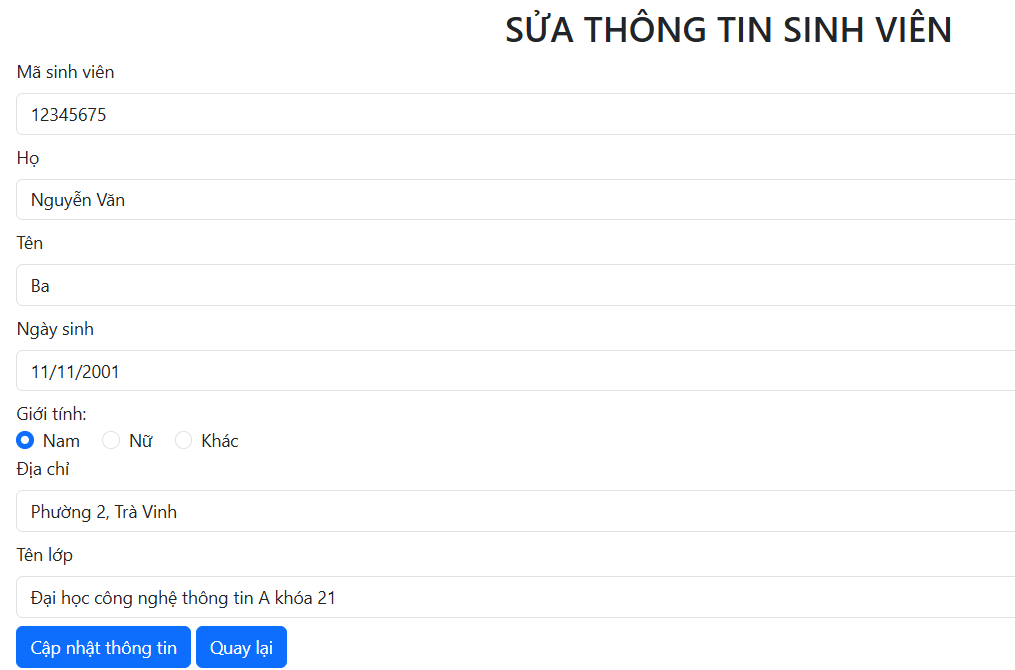


Hình 4. 5. Thêm thông tin sinh viên

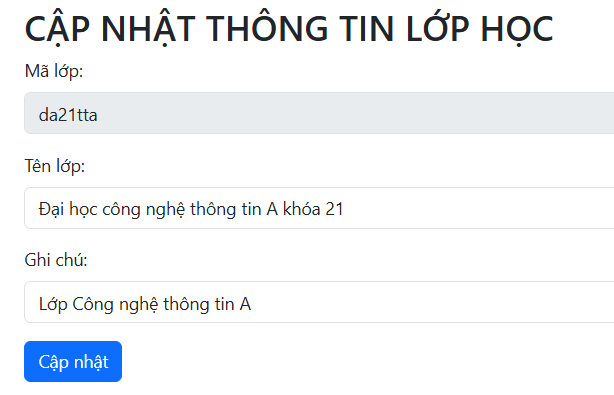


Hình 4. 6. Thêm thông tin lớp

## Sửa thông tin sinh viên, lớp



Hình 4. 7. Sửa thông tin sinh viên

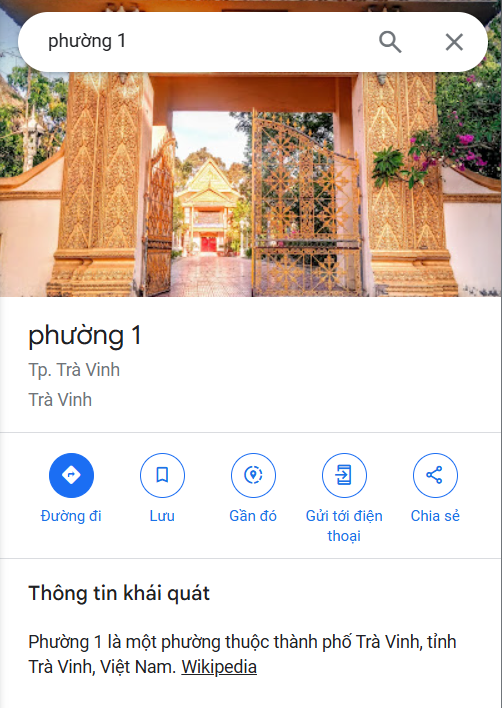


Hình 4. 8. Sửa thông tin lớp

## Tích hợp Google API( Google Maps) vào Website



Hình 4. 9. Nhấn vào đường link ở cột địa chỉ để truy cập Google Maps



Hình 4. 10. Kết quả

CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

## Kết luận

Dự án website quản lý sinh viên đã xây dựng được các chức năng cơ bản như đăng nhập, đăng ký, và quản lý thông tin sinh viên và lớp. Các chức năng quản lý (thêm, sửa, xóa) thông tin sinh viên và lớp giúp việc quản lý trở nên hiệu quả và dễ dàng hơn, hỗ trợ người dùng duy trì một hệ thống quản lý sinh viên có tổ chức. Việc tích hợp Google API và Google Maps giúp mở rộng khả năng ứng dụng của hệ thống, giúp người dùng có thể xem thông tin vị trí trực quan, dễ dàng thao tác và sử dụng. Tính năng viết lại URL giúp website trở nên thân thiện với người dùng và công cụ tìm kiếm, nâng cao trải nghiệm và tối ưu hóa hiệu suất tìm kiếm.

## Hướng phát triển

Trong tương lai, dự án có thể mở rộng và phát triển thêm các tính năng sau để tăng tính tiện ích và đáp ứng nhu cầu của người dùng:

1. Tích hợp hệ thống phân quyền người dùng: Phân chia quyền truy cập giữa các vai trò như quản trị viên, giáo viên và sinh viên, giúp quản lý hệ thống dễ dàng và an toàn hơn.

2. Bổ sung chức năng tìm kiếm và lọc nâng cao: Cung cấp các bộ lọc và công cụ tìm kiếm nâng cao giúp người dùng dễ dàng tìm kiếm thông tin sinh viên hoặc lớp theo các tiêu chí khác nhau.

3. Thống kê và báo cáo: Tạo các báo cáo về số lượng sinh viên, tình trạng học tập, hoặc các thống kê khác giúp quản lý dễ dàng đánh giá tình hình tổng quan.

DANH MỤC TÀI LIỆU THAM KHẢO

1/ https://topdev.vn/blog/ngon-ngu-lap-trinh-php-la-gi-tat-tan-tat-nhung-dieu-ban-2

2/ [can-biet-ve-php/#ung-dung-cua-ngon-ngu-php-trong-lap-trinh](https://topdev.vn/blog/ngon-ngu-lap-trinh-php-la-gi-tat-tan-tat-nhung-dieu-ban-2%20can-biet-ve-php/#ung-dung-cua-ngon-ngu-php-trong-lap-trinh)

3/ <https://monamedia.co/phan-mem-xampp-la-gi-huong-dan-cai-dat-xampp/>

4/ <https://cystack.net/vi/blog/tan-cong-mang-cyber-attack>