

**ĐẠI HỌC QUỐC GIA TP-HCM**

**TRƯỜNG ĐẠI HỌC BÁCH KHOA TP-HCM**

**KHOA KHOA HỌC & KĨ THUẬT MÁY TÍNH**

****

**Môn: Lập trình Web**

**ĐỀ TÀI:**

**WEBSITE CHIA SẺ CÁC BÀI VIẾT HAY**

**Giảng viên hướng dẫn: Nguyễn Hữu Hiếu**

**Lớp: L02**

**Nhóm:**

1. Bùi Thị Trúc Ly 1511920
2. Dương Thanh Nam 1512058
3. Tạ Văn Thông 1513307
4. Nguyễn Vũ 1514106

Năm học 2018 - 2019

Mục lục

[I. GIỚI THIỆU ĐỀ TÀI 3](#_Toc532381451)

[II. CHI TIẾT THIẾT KẾ 3](#_Toc532381452)

[**1. Thiết kế cơ sở dữ liệu 3**](#_Toc532381453)

[a. ERD 3](#_Toc532381454)

[b. Class diagram 4](#_Toc532381455)

[c. Thiết kế cụ thể 4](#_Toc532381456)

[**2. Cấu trúc mã nguồn 8**](#_Toc532381457)

[**3. Môi trường 8**](#_Toc532381458)

[**4. Chức năng theo đối tượng sử dụng 11**](#_Toc532381459)

[**5. Chống SQL Injection 12**](#_Toc532381460)

[a. Định nghĩa 12](#_Toc532381461)

[b. Hậu quả của SQL Injecton 12](#_Toc532381462)

[c. Hướng giải quyết 12](#_Toc532381463)

[III. CÁC TÍNH NĂNG 13](#_Toc532381464)

[**1. Khách 13**](#_Toc532381465)

[**2. Người dùng 17**](#_Toc532381466)

[**3. Quản trị viên 20**](#_Toc532381467)

[IV. PHÂN CÔNG CÔNG VIỆC 22](#_Toc532381468)

[V. THAM KHẢO 22](#_Toc532381469)

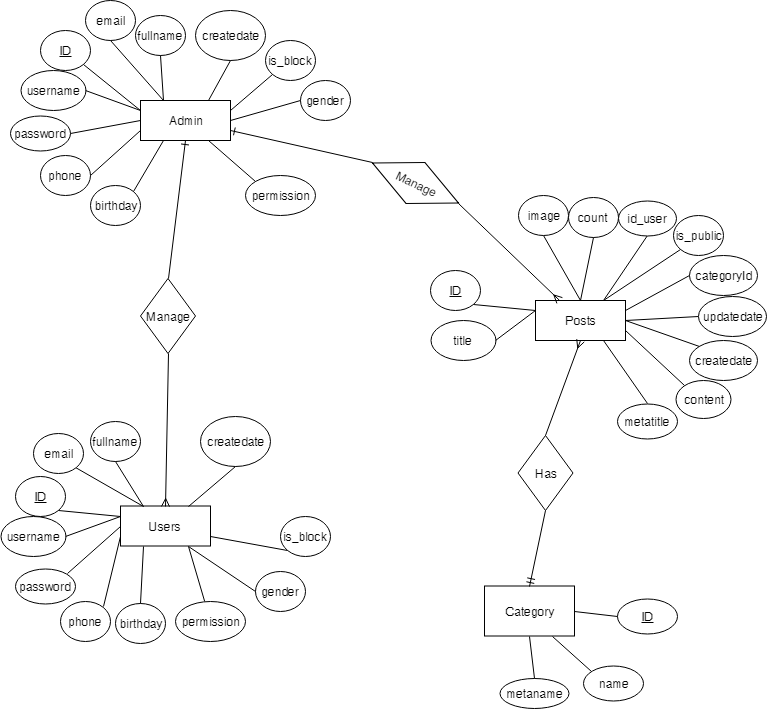
# GIỚI THIỆU ĐỀ TÀI

Thời đại công nghệ phát triển, việc chia sẻ những bài viết hay trải nghiệm thú vị cá nhân đối với người khác là một nhu cầu thiết yếu. Với yêu cầu phát triển một website chia sẻ các bài viết, nhóm đã lên kế hoạch thực hiện một website để mọi người cùng chia sẻ các bài viết hay, trải nghiệm về du lịch. Ở bài tập lớn này, nhóm thực hiện phần back-end và chỉnh sửa phần front-end của website. Bài báo cáo sẽ trình bày các phần chính về back-end của website và quá trình thực hiện của nhóm.

# CHI TIẾT THIẾT KẾ

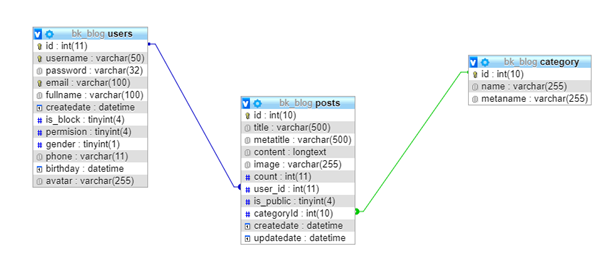
## Thiết kế cơ sở dữ liệu

### ERD



*Hình 1: ERD*

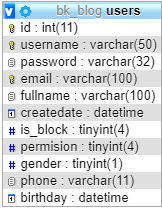
1. **Class diagram**



*Hình 2: Class diagram*

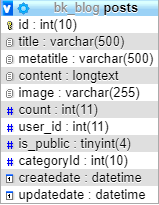
1. **Thiết kế cụ thể**

* Users



Trong đó,

* Id: mã người dùng
* Username: tên đăng nhập
* Password: mật khẩu
* Email: email người dùng
* Fullname: tên đầy đủ của người dùng
* Createdate: ngày người dùng đăng kí vào hệ thống
* Is\_block: tình trạng tài khoản có bị block hay chưa (0:chưa, 1: có)
* Permission: quyền truy cập (1:admin, 2: user thường)
* Gender: giới tính (1: nam, 0: nữ)
* Phone: số điện thoại
* Birthday: ngày sinh
* Posts



Trong đó,

* Id: mã bài đăng
* Title: tiêu đề bài viết
* Metatitle: tên rút gọn
* Content: nội dung bài viết
* Image: hình ảnh trong bài viết
* Count: số lượt xem bài viết
* User\_id: mã người dùng đăng bài viết
* Is\_public: tình trạng bài viết có được public hay không
* CategoryId: mã thể loại bài viết
* Createdate: ngày tạo bài viết
* Updatedate: ngày chỉnh sửa bài viết
* Category



Trong đó,

* Id: mã thể loại bài viết
* Name: tên thể loại
* Metaname: tên rút gọn

1. **Mã nguồn SQL:**

*-- phpMyAdmin SQL Dump*

*-- version 4.8.2*

*-- https://www.phpmyadmin.net/*

*-- Phiên bản máy phục vụ: 10.1.34-MariaDB*

*-- Phiên bản PHP: 7.2.7*

**CREATE** **TABLE** `category` (

`id` **int**(10) **NOT** **NULL**,

`name` **varchar**(255) **DEFAULT** **NULL**,

`metaname` **varchar**(255) **DEFAULT** **NULL**

) **ENGINE**=**MyISAM** **DEFAULT** **CHARSET**=**utf8**;

**CREATE** **TABLE** `posts` (

`id` **int**(10) **NOT** **NULL**,

`title` **varchar**(500) **CHARACTER** **SET** **utf8** **COLLATE** utf8\_vietnamese\_ci **DEFAULT** **NULL**,

`metatitle` **varchar**(500) **DEFAULT** **NULL**,

`content` **longtext** **CHARACTER** **SET** **utf8** **COLLATE** utf8\_vietnamese\_ci,

`image` **varchar**(255) **DEFAULT** **NULL**,

`count` **int**(11) **DEFAULT** **NULL**,

`user\_id` **int**(11) **DEFAULT** **NULL**,

`is\_public` **tinyint**(4) **DEFAULT** '0',

`categoryId` **int**(10) **DEFAULT** **NULL**,

`createdate` **datetime** **DEFAULT** **NULL**,

`updatedate` **datetime** **DEFAULT** **NULL**

) **ENGINE**=**MyISAM** **DEFAULT** **CHARSET**=**utf8**;

**CREATE** **TABLE** `users` (

`id` **int**(11) **NOT** **NULL**,

`username` **varchar**(50) **NOT** **NULL**,

`password` **varchar**(32) **NOT** **NULL**,

`email` **varchar**(100) **NOT** **NULL**,

`fullname` **varchar**(100) **NOT** **NULL**,

`createdate` **datetime** **NOT** **NULL**,

`is\_block` **tinyint**(4) **NOT** **NULL** **DEFAULT** '0',

`permision` **tinyint**(4) **NOT** **NULL** **DEFAULT** '0',

`gender` **tinyint**(1) **DEFAULT** **NULL**,

`phone` **varchar**(11) **DEFAULT** **NULL**,

`birthday` **datetime** **DEFAULT** **NULL**,

`avatar` **varchar**(255) **DEFAULT** **NULL**

) **ENGINE**=**MyISAM** **DEFAULT** **CHARSET**=**utf8**;

**ALTER** **TABLE** `category`

**ADD** **PRIMARY** **KEY** (`id`);

**ALTER** **TABLE** `posts`

**ADD** **PRIMARY** **KEY** (`id`),

**ADD** **KEY** `categoryId` (`categoryId`),

**ADD** **KEY** `user\_id` (`user\_id`);

**ALTER** **TABLE** `users`

**ADD** **PRIMARY** **KEY** (`id`),

**ADD** **UNIQUE** **KEY** `username` (`username`),

**ADD** **UNIQUE** **KEY** `email` (`email`);

*-- AUTO\_INCREMENT cho bảng `category`*

--

**ALTER** **TABLE** `category`

**MODIFY** `id` **int**(10) **NOT** **NULL** **AUTO\_INCREMENT**, **AUTO\_INCREMENT**=5;

--

*-- AUTO\_INCREMENT cho bảng `posts`*

--

**ALTER** **TABLE** `posts`

**MODIFY** `id` **int**(10) **NOT** **NULL** **AUTO\_INCREMENT**, **AUTO\_INCREMENT**=32;

--

*-- AUTO\_INCREMENT cho bảng `users`*

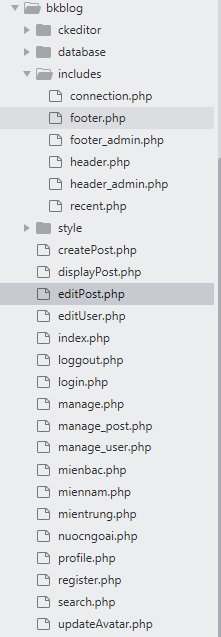
--

**ALTER** **TABLE** `users`

**MODIFY** `id` **int**(11) **NOT** **NULL** **AUTO\_INCREMENT**, **AUTO\_INCREMENT**=13;

**COMMIT**;

## Cấu trúc mã nguồn



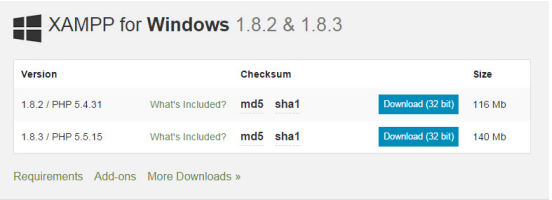
*Hình 3: Cấu trúc mã nguồn*

## Môi trường

* Ngôn ngữ: PHP, HTML, JAVASCRIPT
* Cơ sở dữ liệu: MySQL
* Ứng dụng XAMPP tích hợp sẵn Apache, PHP, MySQL, tomcat,...

1. **Hướng dẫn cài đặt Xampp**

Để tải Xampp, đầu tiên bạn truy cập vào địa chỉ https://www.apachefriends.org/download.html và chọn phiên bản XAMPP phù hợp với hệ điều hành của máy tính bạn đang sử dụng.

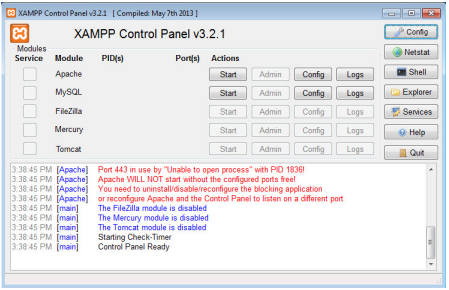


*Hình 4: Tải Xampp*

Sau khi tải file cài đặt về xong hãy chạy nó, sau đó chọn **Next**. Ở phần chọn đường dẫn, bạn hãy chọn đường dẫn cần lưu cài đặt của XAMPP. Lưu ý rằng đường dẫn này bạn phải nhớ vì khi cài đặt web lên localhost, bạn phải truy cập vào thư mục này. Bạn nên để mặc định là C:\xampp. Tiếp tục ấn **Next**. Sau khi cài xong, ấn nút **Finish** để kết thúc cài đặt và mở bảng điều khiển của XAMPP. Tuy nhiên, hãy khởi động lại máy sau khi cài đặt xong để tránh tình trạng không khởi động được localhost.

1. **Khởi động localhost**

Bây giờ bạn hãy vào thư mục C:\xampp và mở file xampp-panel.exe lên để bật bảng điều khiển của XAMPP.



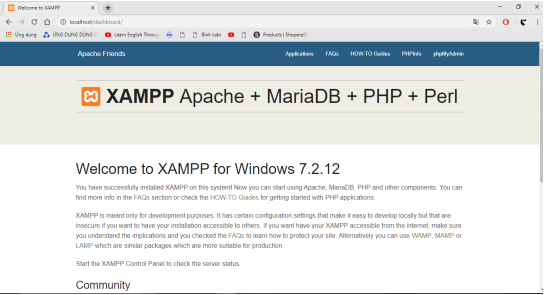
*Hình 5: Giao diện hoạt động của Xampp*

Bạn để ý sẽ thấy hai ứng dụng Apache và MySQL có nút **Start**, đó là dấu hiệu bảo 2 ứng dụng này chưa được khởi động, hãy ấn vào nút **Start** của từng ứng dụng để khởi động Webserver Apache và MySQL Server lên thì mới chạy được localhost. Nếu cả hai ứng dụng chuyển sang màu xanh như hình dưới là đã khởi động thành công.



*Hình 6: Giao diện Xampp khi đã khởi động*

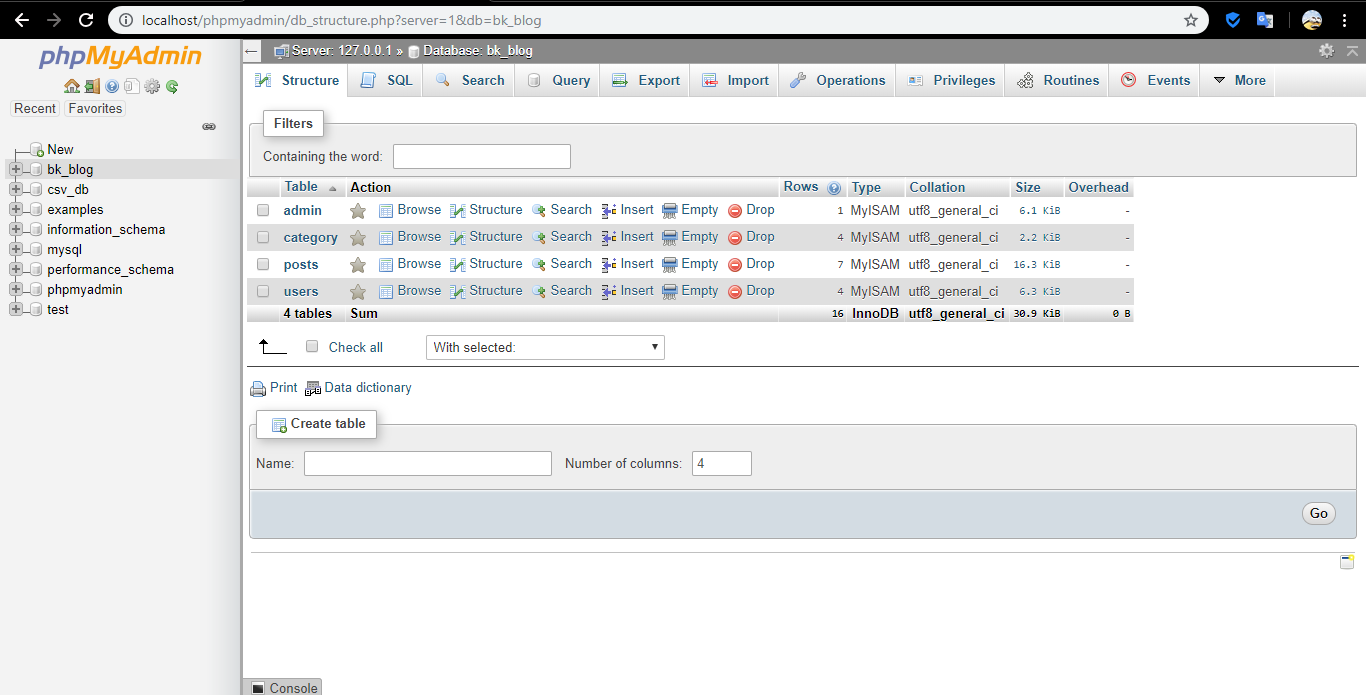
Sau khi khởi động xong, bạn hãy truy cập vào website với địa chỉ là http://localhost sẽ thấy nó hiển thị ra trang giới thiệu XAMPP như hình dưới.



*Hình 7: Khởi động localhost*

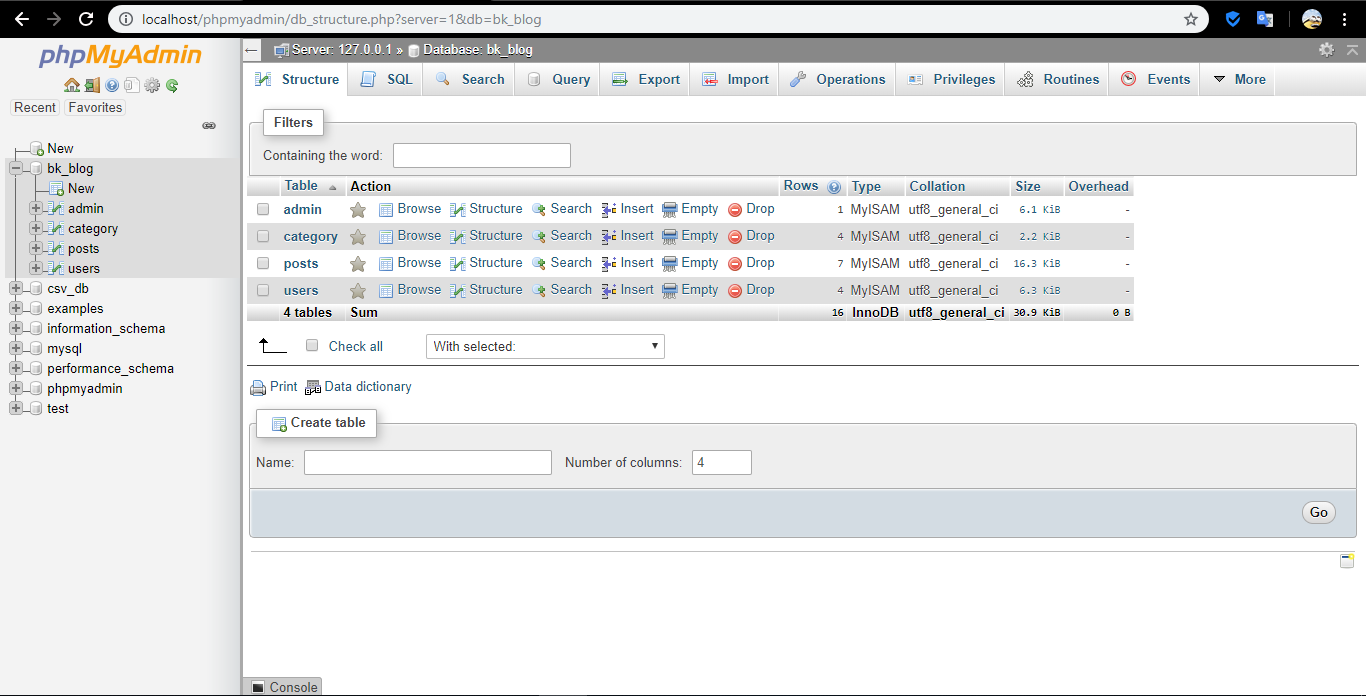
1. **Thao tác với localhost**

Bây giờ, gõ git clone https://vu97@bitbucket.org/TrucLy13/bkblog.git Sau đó copy nó vào thư mục C:\xampp\htdocs. Tiếp theo chúng ta sẽ tạo database bằng cách truy cập vào đường dẫn http://localhost/phpmyadmin. Sau đó nhấn chọn Import



*Hình 8: Import bk\_blog.sql vào phpmyadmin*

Thực hiện import file bk\_blog.sql trong thư mục Kết quả như hình bên dưới.



*Hình 9: Cơ sở dữ liệu sau khi đã import*

## Chức năng theo đối tượng sử dụng

1. **Khách (Guest)**

* Đăng ký thành viên.
* Xem bài viết.
* Tìm kiếm bài viết.

1. **Người dùng thường (User)**

* Có đầy đủ chức năng của khách.
* Đăng nhập với tài khoản đã được đăng ký.
* Tạo bài viết.
* Chỉnh sửa bài viết.
* Cập nhật thông tin cá nhân
* Thay đổi mật khẩu
* Khi user bị Admin block thì không thể tạo hay chỉnh sửa bài viết.

1. **Người quản trị (Admin)**

* Có đầy đủ chức năng của User.
* Quản lý bài viết: Admin có thể xem danh sách tất cả các bài viết và xóa bài viết.
* Quản lý user: Admin xem thông tin các user và có thể block user.

## Chống SQL Injection

1. **Định nghĩa**

SQL Injection là một kỹ thuật lợi dụng những lỗ hổng về câu truy vấn lấy dữ liệu của những website không an toàn trên web, đây là một kỹ thuật tấn công rất phổ biến và sự thành công của nó cũng tương đối cao.

1. **Hậu quả của SQL Injecton**

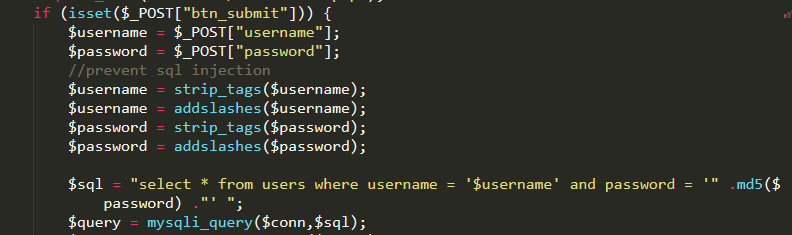
* Hậu quả lớn nhất mà SQL Injection gây ra là: Làm lộ dữ liệu trong database. Tuỳ vào tầm quan trọng của dữ liệu mà hậu quả dao động ở mức nhẹ cho đến vô cùng nghiêm trọng.
* Lộ dữ liệu khách hàng có thể ảnh hưởng rất nghiêm trọng đến công ty. Hình ảnh công ty có thể bị ảnh hưởng, khách hàng chuyển qua sử dụng dịch vụ khác, dẫn đến phá sản v…v...
* Lỗ hỗng này cũng ảnh hưởng lớn đến khách hàng. Do họ thường dùng chung một mật khẩu cho nhiều tài khoản, chỉ cần lộ mật khẩu một tài khoản thì các tài khoản khác cũng lộ theo.
* Đây cũng là lý do mình nhắc nhở phải mã hoá mật khẩu, nếu database có bị tấn công thì người dùng cũng không bị mất mật khẩu. (Đây là lý do vietnamwork bị ăn chửi vì không mã hoá mật khẩu).

1. **Hướng giải quyết**

Để bảo vệ bản thân trước SQL Injection, ta có thể thực hiện các biện pháp sau.

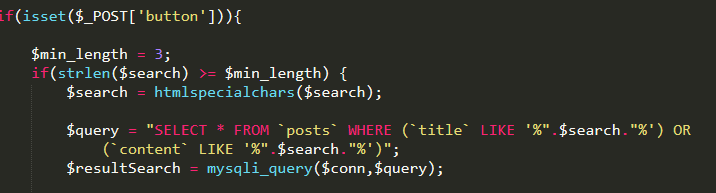
* Lọc dữ liệu từ người dùng: Cách phòng chống này tương tự như XSS. Ta sử dụng filter để lọc các kí tự đặc biệt (; ” ‘) hoặc các từ khoá (SELECT, UNION) do người dùng nhập vào. Nên sử dụng thư viện/function được cung cấp bởi framework. Viết lại từ đầu vừa tốn thời gian vừa dễ sơ sót.
* Không cộng chuỗi để tạo SQL: Sử dụng parameter thay vì cộng chuỗi. Nếu dữ liệu truyền vào không hợp pháp, SQL Engine sẽ tự động báo lỗi, ta không cần dùng code để check.
* Không hiển thị exception, message lỗi: Hacker dựa vào message lỗi để tìm ra cấu trúc database. Khi có lỗi, ta chỉ hiện thông báo lỗi chứ đừng hiển thị đầy đủ thông tin về lỗi, tránh hacker lợi dụng.
* Phân quyền rõ ràng trong DB: Nếu chỉ truy cập dữ liệu từ một số bảng, hãy tạo một account trong DB, gán quyền truy cập cho account đó chứ đừng dùng account root hay sa. Lúc này, dù hacker có inject được sql cũng không thể đọc dữ liệu từ các bảng chính, sửa hay xoá dữ liệu.
* Backup dữ liệu thường xuyên: Các cụ có câu “cẩn tắc vô áy náy”. Dữ liệu phải thường xuyên được backup để nếu có bị hacker xoá thì ta vẫn có thể khôi phục được.

Cụ thể trong assignment này chúng em giải quyết bằng cách dùng các hàm strip\_tags(), addslashes() để lọc dữ liệu đầu vào do user nhập.



*Hình 10: Hàm strip\_tags(), addslashes()*

hoặc hàm htmlspecialchars():

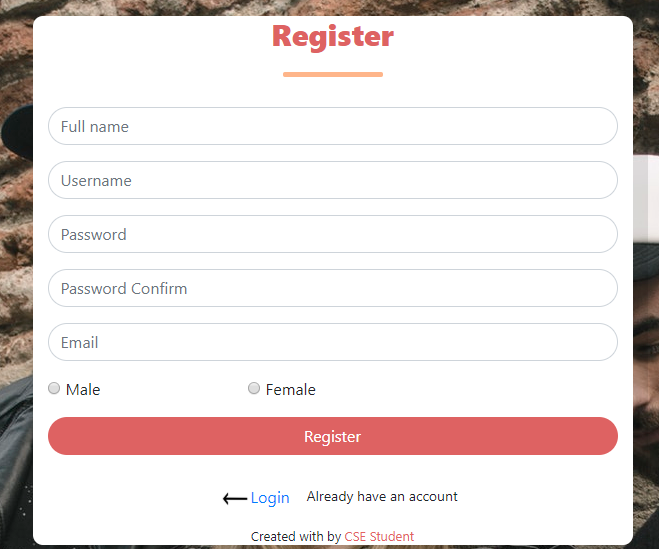


*Hình 11: Hàm htmlspecialchars()*

# CÁC TÍNH NĂNG

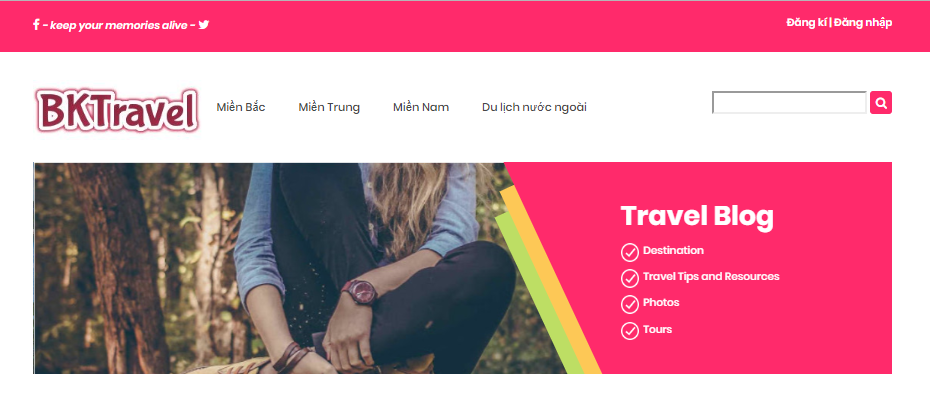
## Khách

1. Đăng ký thành viên

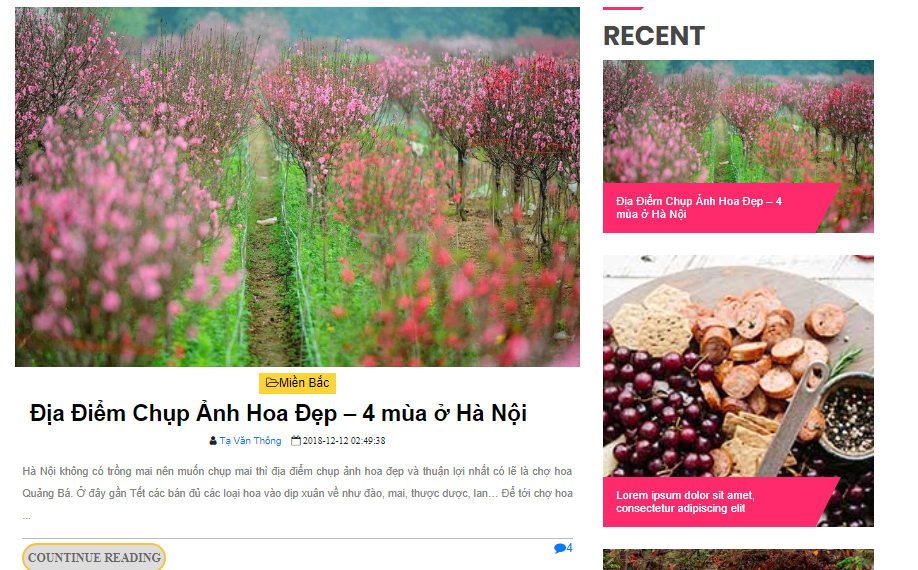


*Hình 12: Giao diện đăng kí*

1. Trang chủ

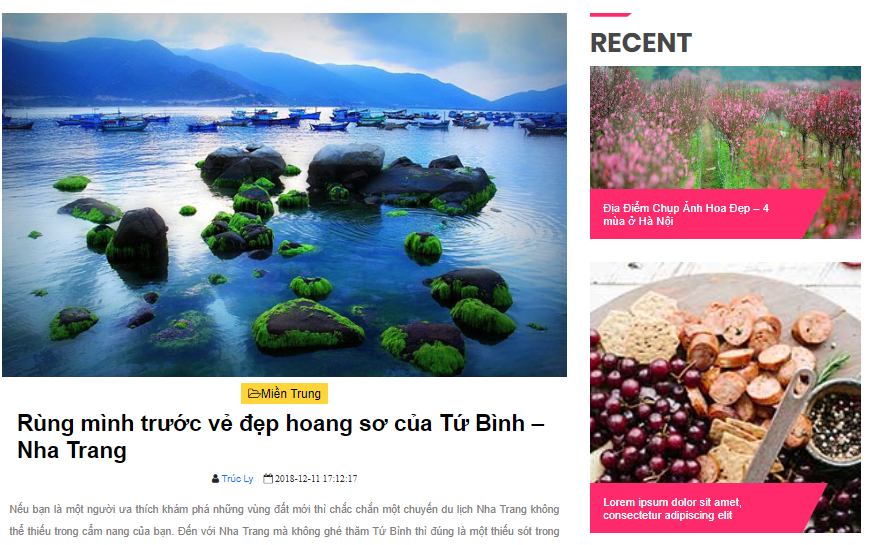


*Hình 13: Giao diện trang chủ*

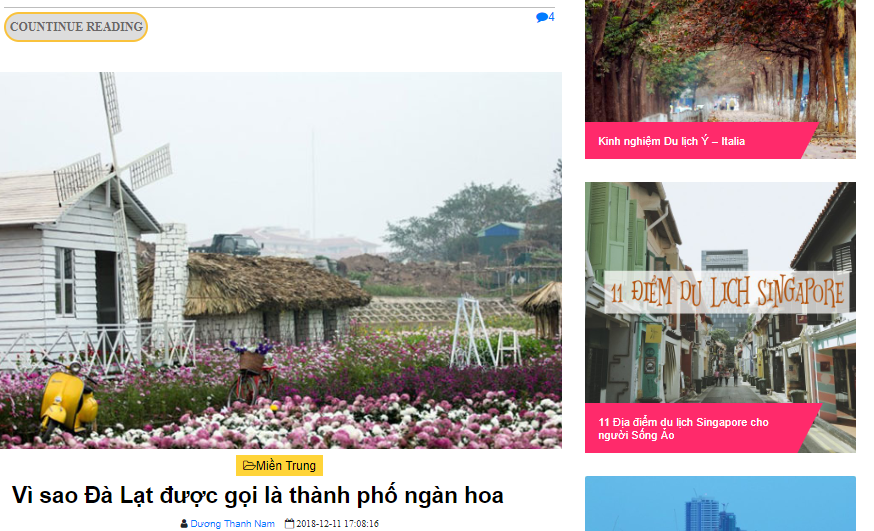


*Hình 14: Giao diện các bài viết*

1. Danh sách bài viết theo vùng



*Hình 15: Giao diện danh sách các bài viết theo vùng*



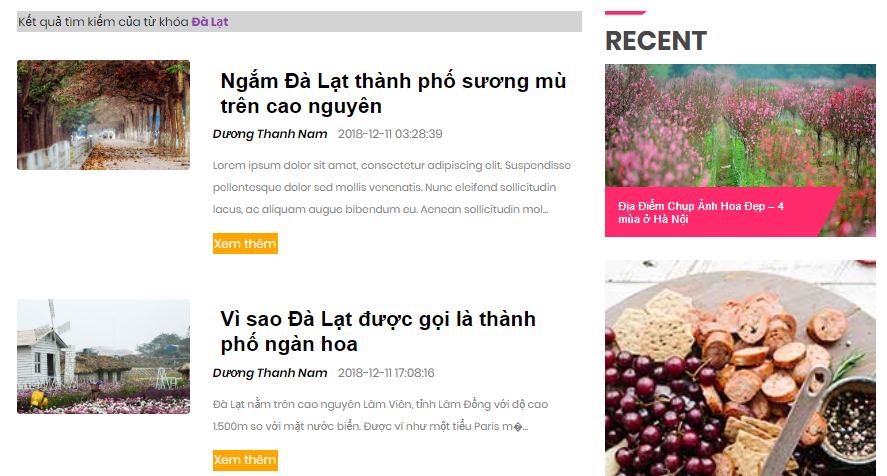
*Hình 16: Giao diện danh sách các bài viết theo vùng*

1. Xem chi tiết bài viết



*Hình 17: Giao diện chi tiết bài viết*

1. Tìm kiếm bài viết



*Hình 18: Giao diện danh sách bài viết tìm kiếm*

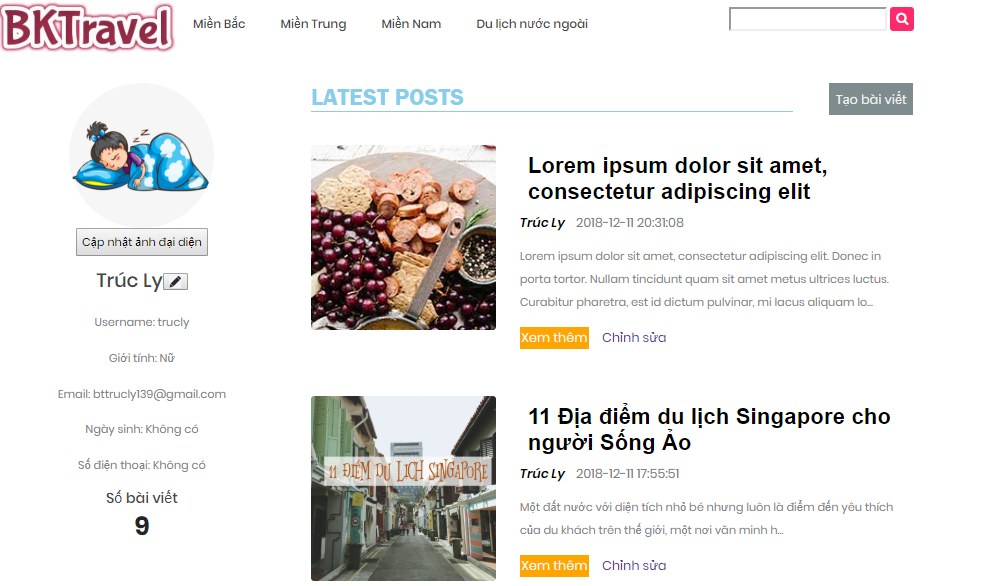
## Người dùng

1. Đăng nhập với tài khoản đã đăng ký



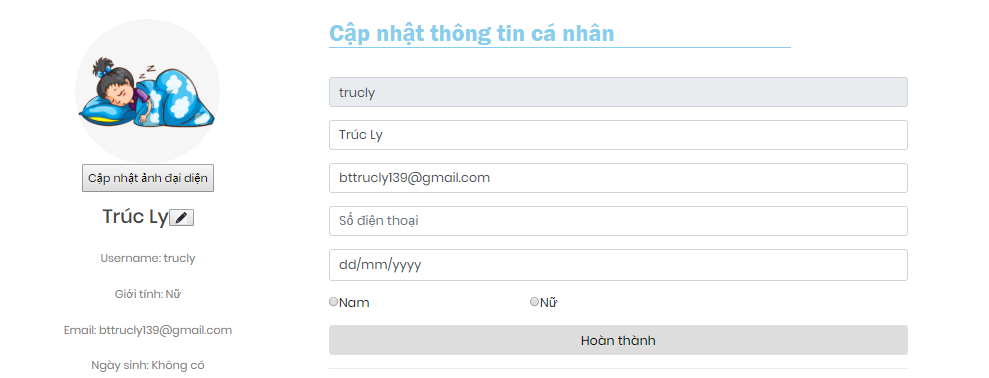
*Hình 19: Giao diện màn hình đăng nhập*

1. Trang cá nhân



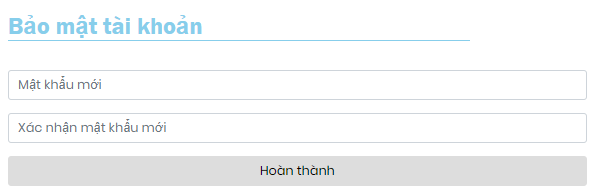
*Hình 20: Giao diện trang cá nhân*

1. Cập nhật thông tin cá nhân



*Hình 21: Giao diện cập nhật thông tin cá nhân*

1. Đổi mật khẩu



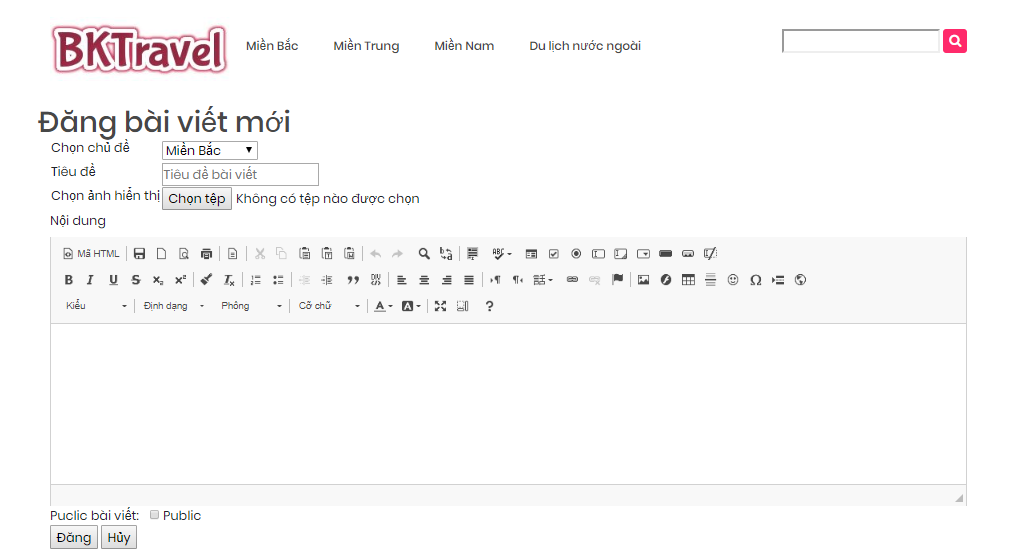
*Hình 22: Giao diện đổi mật khẩu*

1. Thay đổi ảnh đại diện



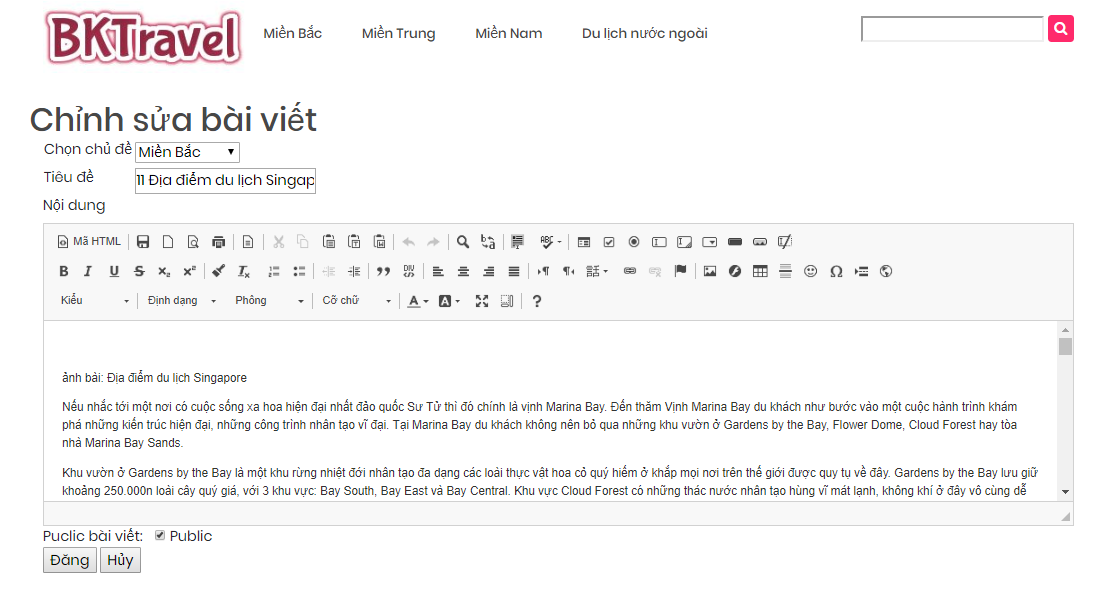
*Hình 23: Giao diện thay đổi ảnh đại diện*

1. Tạo bài viết



*Hình 24: Giao diện tạo bài viết*

1. Chỉnh sửa bài viết



Hình 25: Giao diện chỉnh sửa bài viết

## Quản trị viên

1. Màn hình chính



*Hình 26: Giao diện màn hình chính quản trị viên*

1. Quản lý bài viết



*Hình 27: Giao diện quản lí bài viết*

1. Quản lý user



*Hình 28: Giao diện quản lí người dùng*

# PHÂN CÔNG CÔNG VIỆC

|  |  |  |  |
| --- | --- | --- | --- |
| MSSV | Thành viên | Nhiệm vụ | Vai trò |
| 1511920 | Bùi Thị Trúc Ly | * Hiện thực các chức năng: Đăng nhập, Đăng ký, Tạo bài viết, Hiển thị danh sách bài viết, Hiển thị chi tiết bài viết * Thiết kế database * Chỉnh sửa bài viết * Hoàn thiện báo cáo và debug tổng thể | Nhóm trưởng |
| 1512058 | Dương Thanh Nam | * Hiển thị trang cá nhân, trang kết quả tìm kiếm | Thành viên |
| 1513307 | Tạ Văn Thông | * Hiện thực các chức năng quản trị (admin), Cập nhật thông tin thành viên | Thành viên |
| 1514106 | Nguyễn Vũ | * Hiển thị các bài viết ở trang chủ * Viết báo cáo. | Thành viên |

# THAM KHẢO

<https://www.w3schools.com/>

<https://getbootstrap.com/>

<https://fontawesome.com/>

Dữ liệu bài viết của trang web tham khảo từ <http://toidi.net/>

https://viblo.asia/p/sql-injection-va-cach-phong-chong-OeVKB410lkW