**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CƠ BẢN I**

**BỘ MÔN TIN HỌC CƠ SỞ**



****

**LẬP TRÌNH WEB**

| **Giảng viên hướng dẫn** | **: Nguyễn Trọng Khánh** |
| --- | --- |
| **Họ và tên sinh viên** | **: Đỗ Mạnh Quyền** |
| **Mã sinh viên** | **: B20DCCN563** |
| **Lớp** | **: Hè 2025** |
| **Nhóm** | **: 12 (đã tách ra riêng)** |

***Hà Nội – 2025***

# Báo cáo cuối kì môn LTW

## Trình bày bài toán:

### Bối cảnh và nhu cầu:

* Người dân địa phương cần một kênh tin tức nhanh chóng, chính xác về các sự kiện, thông báo, hoạt động của khu vực.

#### Mục tiêu:

* Xây dựng website tin tức địa phương dễ sử dụng, phân quyền quản trị.
* Cho phép staff tạo bài (draft/pending), admin duyệt và public.
* Hỗ trợ phân loại (chuyên mục), tìm kiếm, bình luận nhanh.

## Frontend:

### Công nghệ:

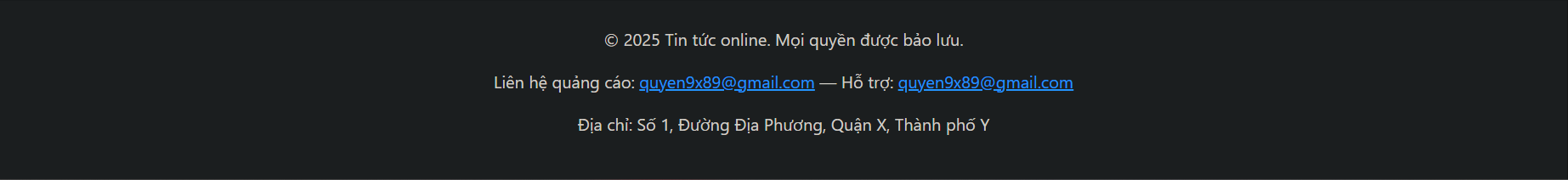
* HTML5/CSS3, Bootstrap 5: responsive, grid system.
* JavaScript (vanilla) minimal: xử lý collapse navbar, form validation.

### Cấu trúc giao diện:

* Header: logo, menu danh mục, ô tìm kiếm toàn site.



* Footer: thông tin liên hệ, quảng cáo, bản quyền.



### Trang chính:

* index.php: phân trang, card layout, chỉ show bài published
* **Carousel**/sidebar: phần mở rộng.

### Trang chi tiết:

* post\_detail.php: hiển thị đầy đủ, breadcrumbs, bình luận.

### Trang danh mục:

* category.php: show bài theo chuyên mục, tương tự index.

### Trang tìm kiếm:

* tim-kiem.php: filter time, sort, category, show kết quả tìm kiếm

## Backend:

### Công nghệ:

* PHP và MySQL
* Session-based auth

### Cấu trúc thư mục:

* …/Public: index.php, post\_detail.php, category.php, tim-kiem.php, header.php, footer.php
* …/Public/admin: login.php, logout.php, index.php, add\_post.php, edit\_post.php, delete\_post.php, publish\_post.php, add\_category.php, edit\_category.php, delete\_category.php, add\_user.php, edit\_user.php, delete\_user.php

### Authentication(xác thực) & Authorization(phân quyền):

* Bảng user (role: admin, staff)
* Staff tạo bài lưu status = pending, chỉ admin phê duyệt
* Admin CRUD tất cả, staff chỉ SRUD bài của mình

### Module chính:

* **Posts**: quản lý bài viết với:
* Upload ảnh, gắn author\_id, workflow status (draft → pending → published).
* **Categories**: CRUD chuyên mục để phân loại tin.
* **Users**: admin thêm staff, phân quyền.
* **Comments**: user gửi bình luận, hiển thị ngay mà không duyệt.

### Bảo mật:

* Prepared statements, XSS prevention (htmlspecialchars).
* CSRF token (nâng cao).  
    
  Prepared Statements (Câu lệnh chuẩn bị sẵn): Là một kỹ thuật để tránh SQL Injection – loại tấn công phổ biến nhất nhằm chèn mã SQL vào biểu mẫu hoặc URL.  
  $stmt = $pdo->prepare("SELECT \* FROM posts WHERE id = ?");  
  $stmt->execute([$id]);  
    
  XSS prevention (htmlspecialchars): XSS (Cross-site scripting) xảy ra khi người dùng nhập nội dung chứa mã HTML/JavaScript nguy hiểm(ví dụ: <script>alert('x')</script>) và hệ thống hiển thị lại nội dung đó mà không xử lý.   
  echo htmlspecialchars($post['title']);  
    
  CSRF Token (nâng cao): là tấn công lợi dụng trình duyệt người dùng đã đăng nhập để thực hiện hành động trái phép.  
  // Khi render form

$\_SESSION['csrf\_token'] = bin2hex(random\_bytes(32));

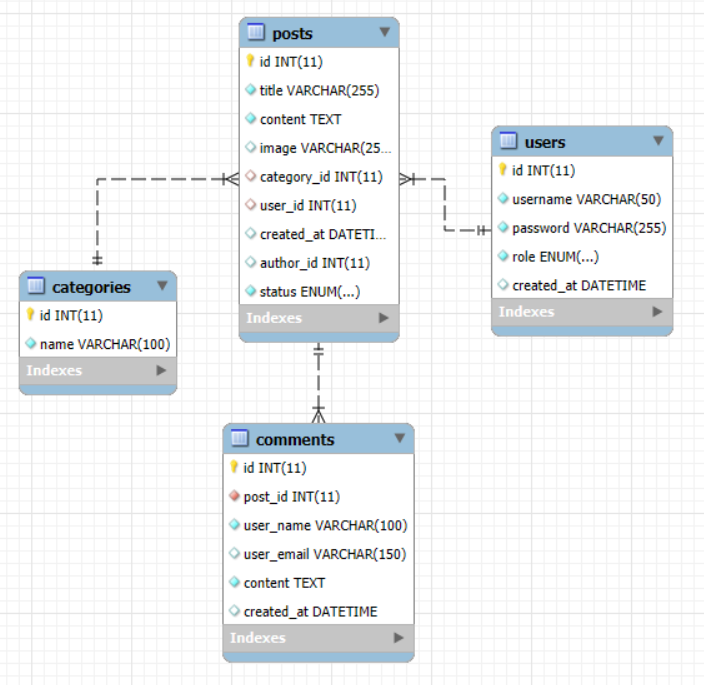
echo '<input type="hidden" name="csrf\_token" value="'.$\_SESSION['csrf\_token'].'">';

// Khi xử lý POST

if ($\_POST['csrf\_token'] !== $\_SESSION['csrf\_token']) {

die("CSRF token mismatch!");

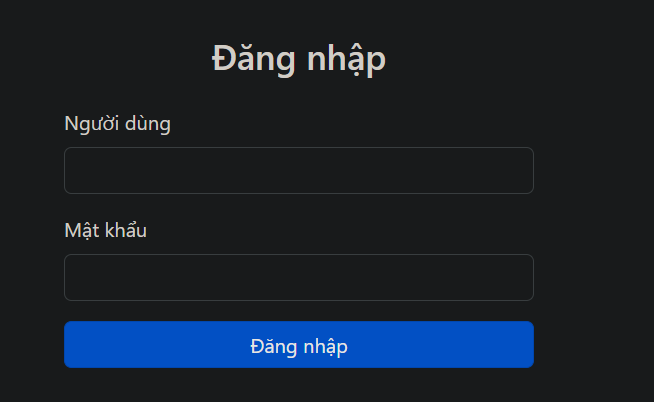
}



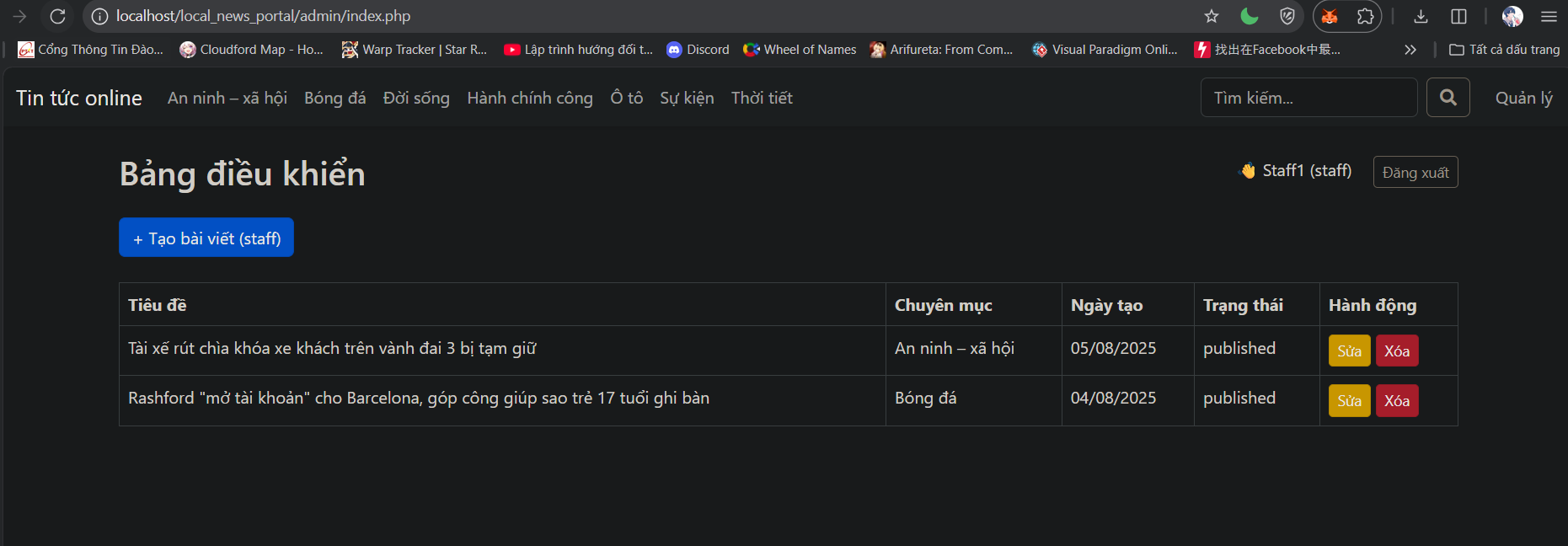
## Kết quả:

1. Demo:
2. Quản lý:

* Đăng nhập: có 2 role là staff và admin, đều đăng nhập qua giao diện login:

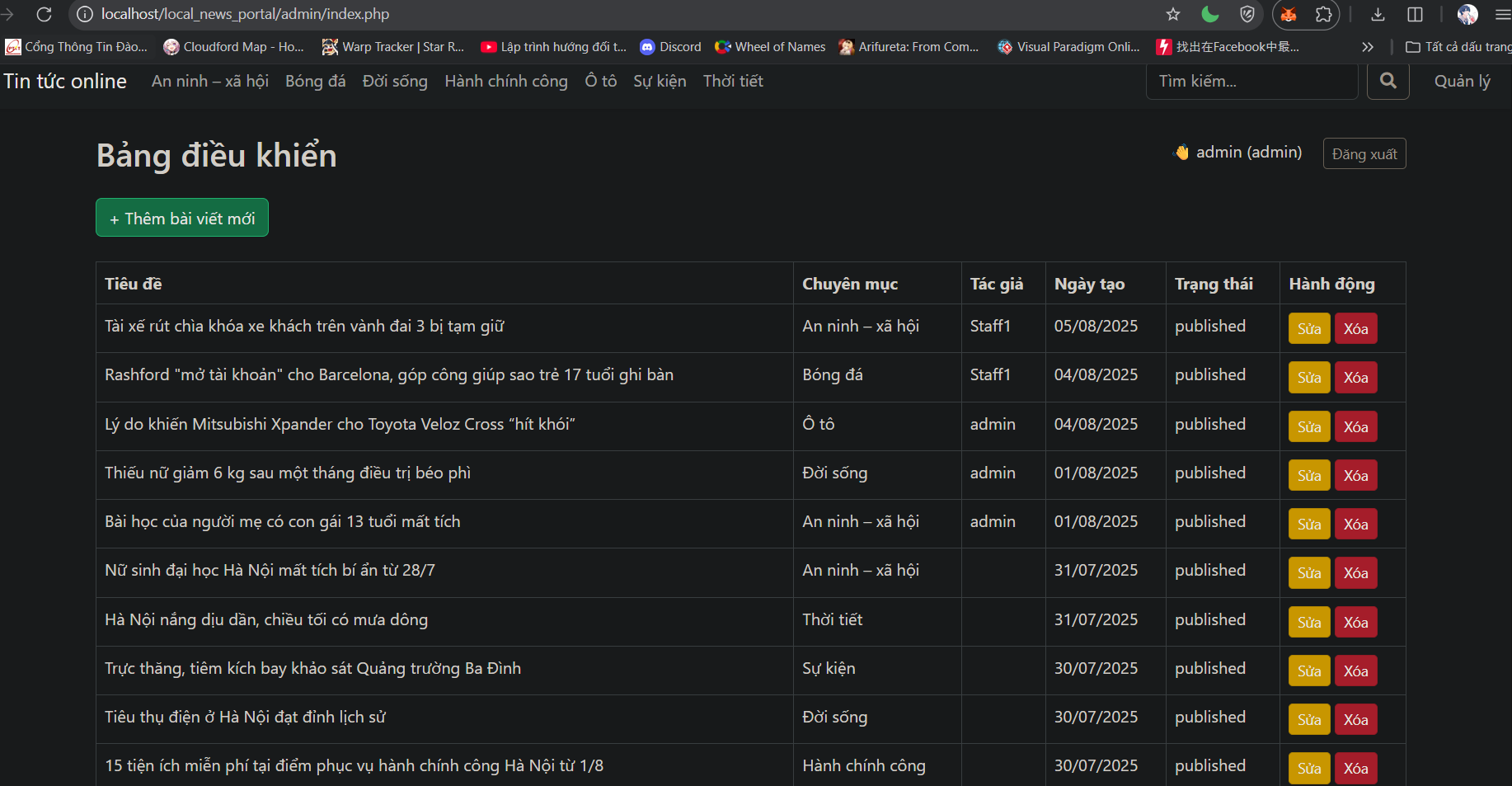
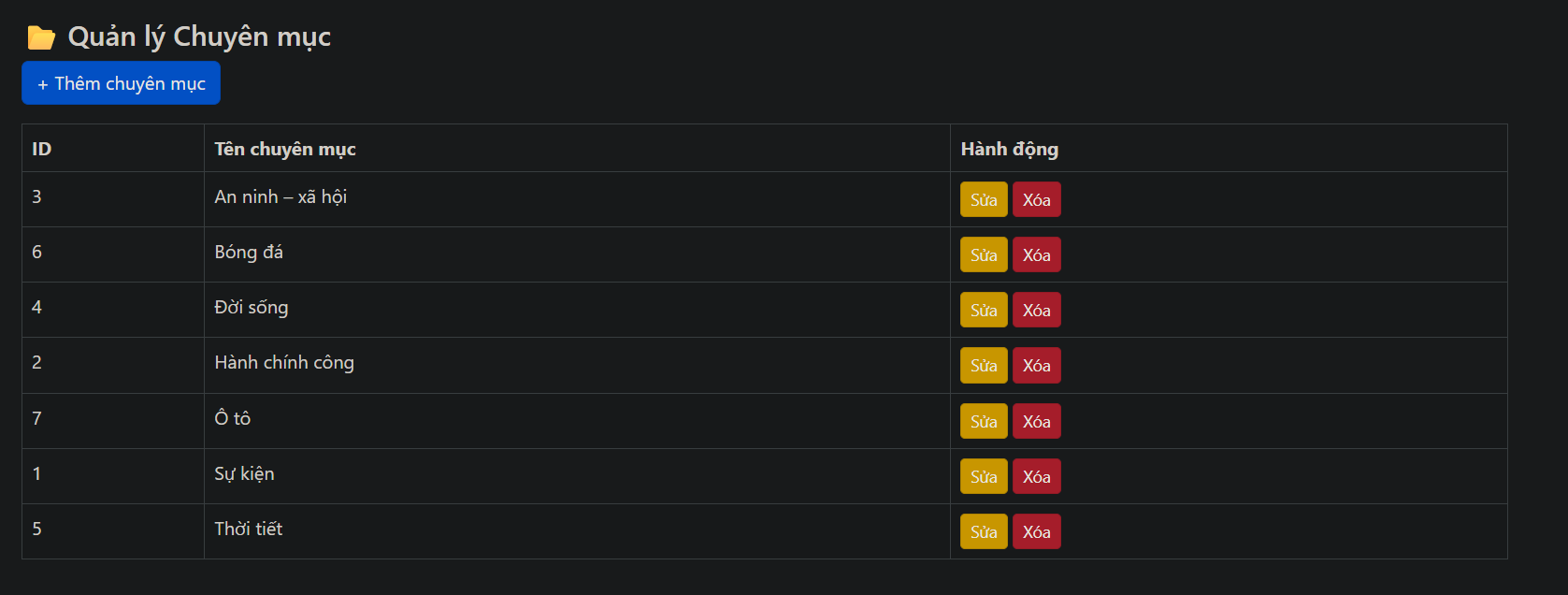
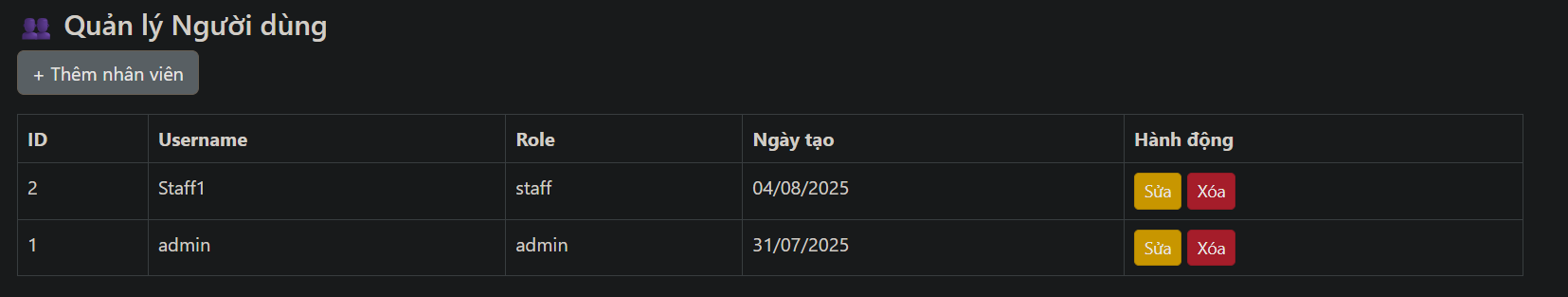


* Staff: Sau khi đăng nhập bằng người dùng staff, staff có thể vào trang quản lý

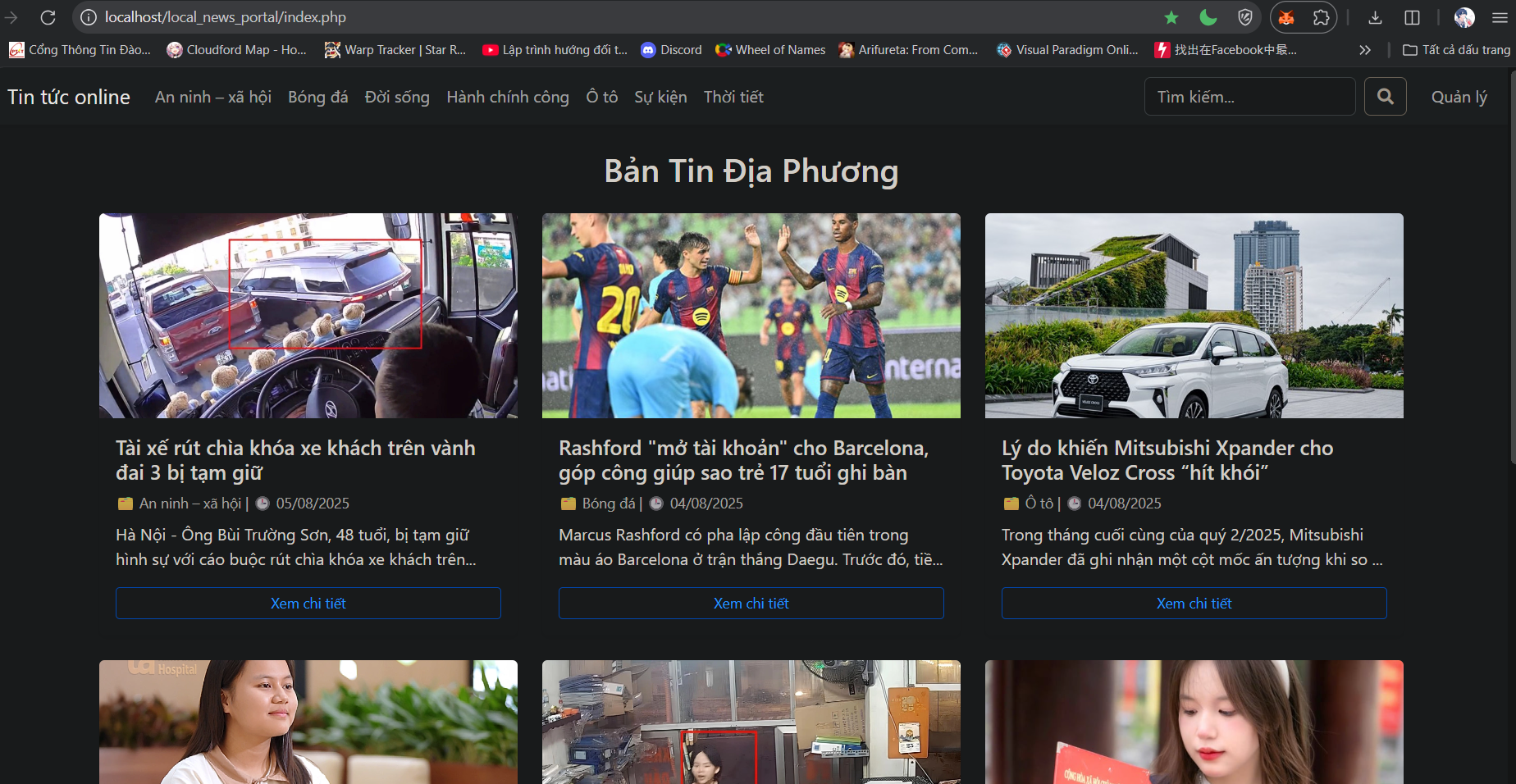
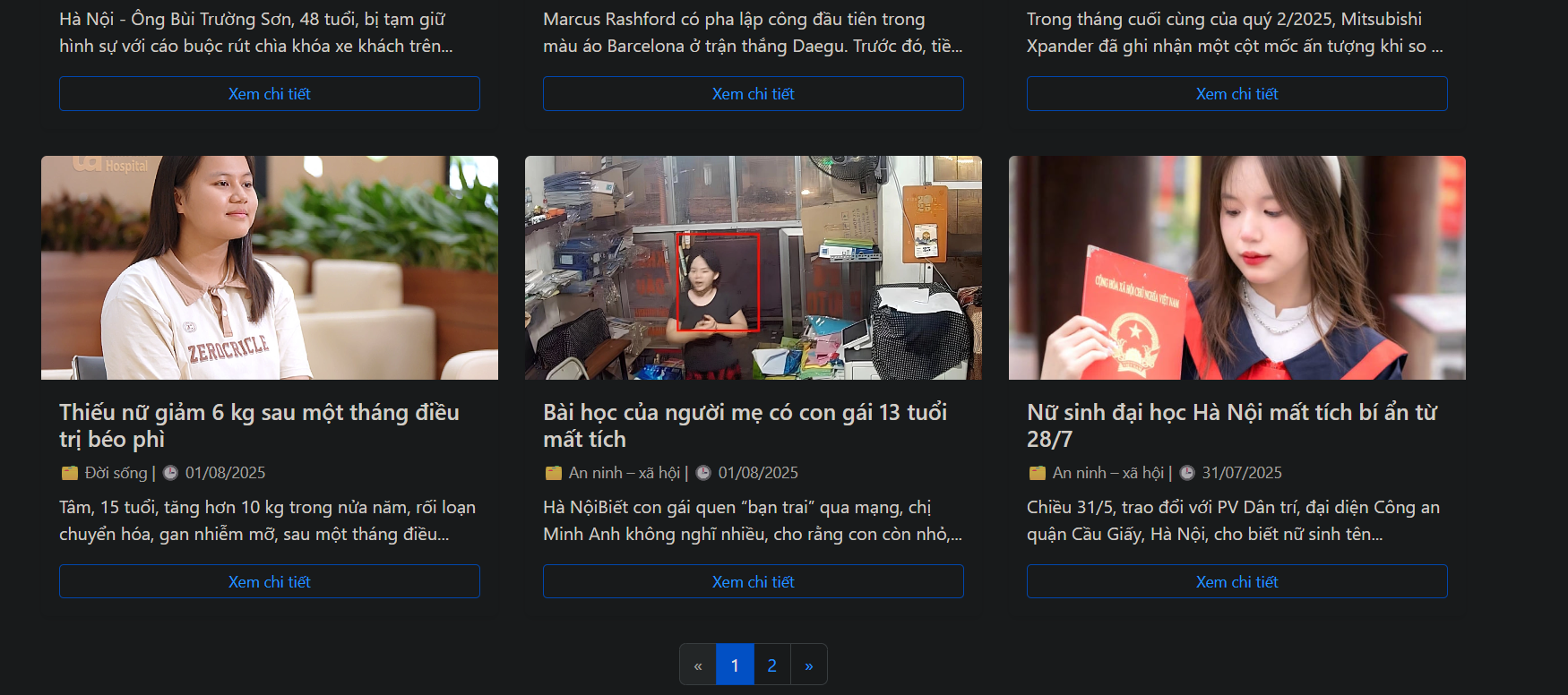


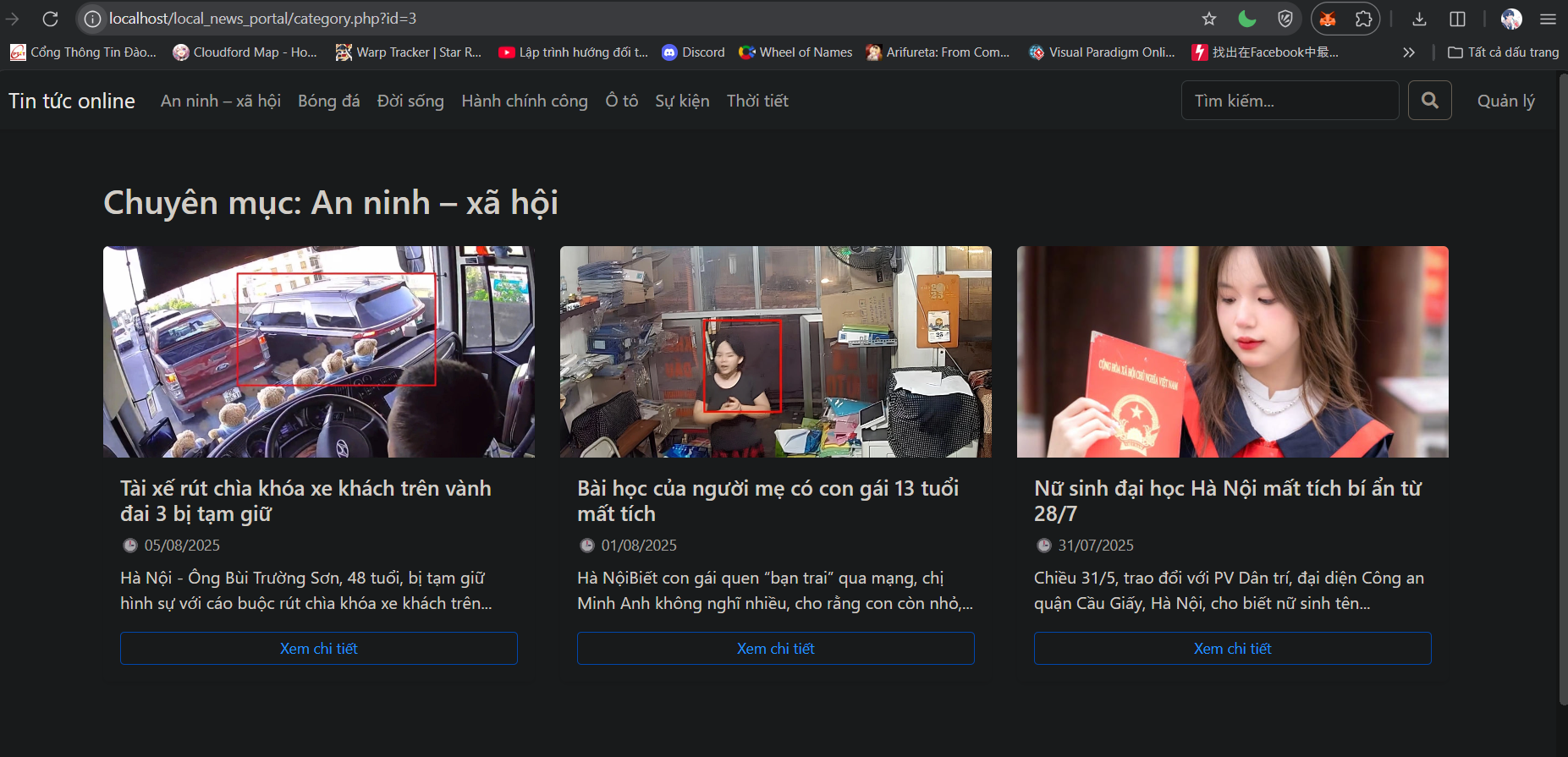
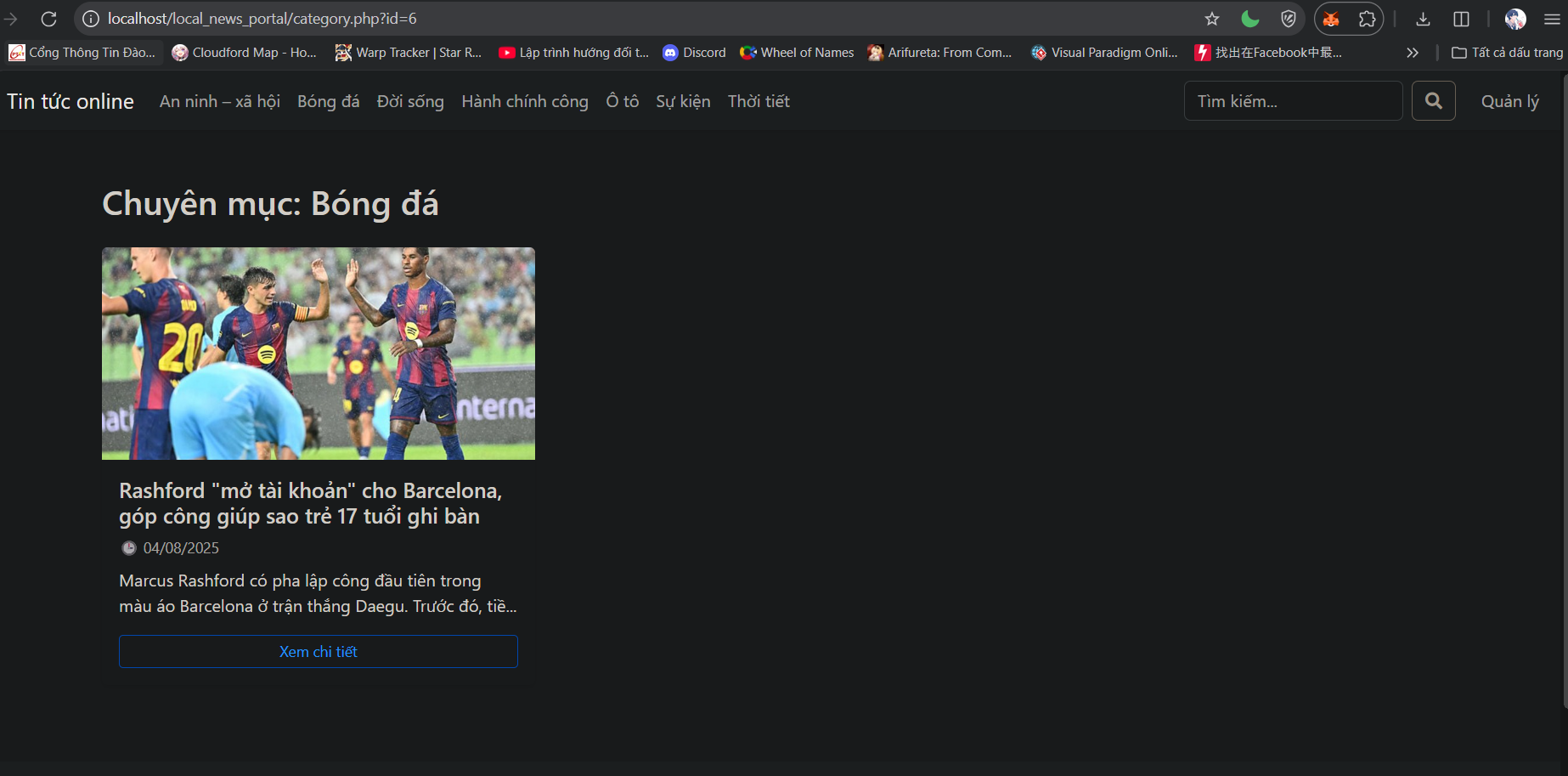
Staff có thể tạo bài viết với tư cách staff, sửa và xóa bài viết

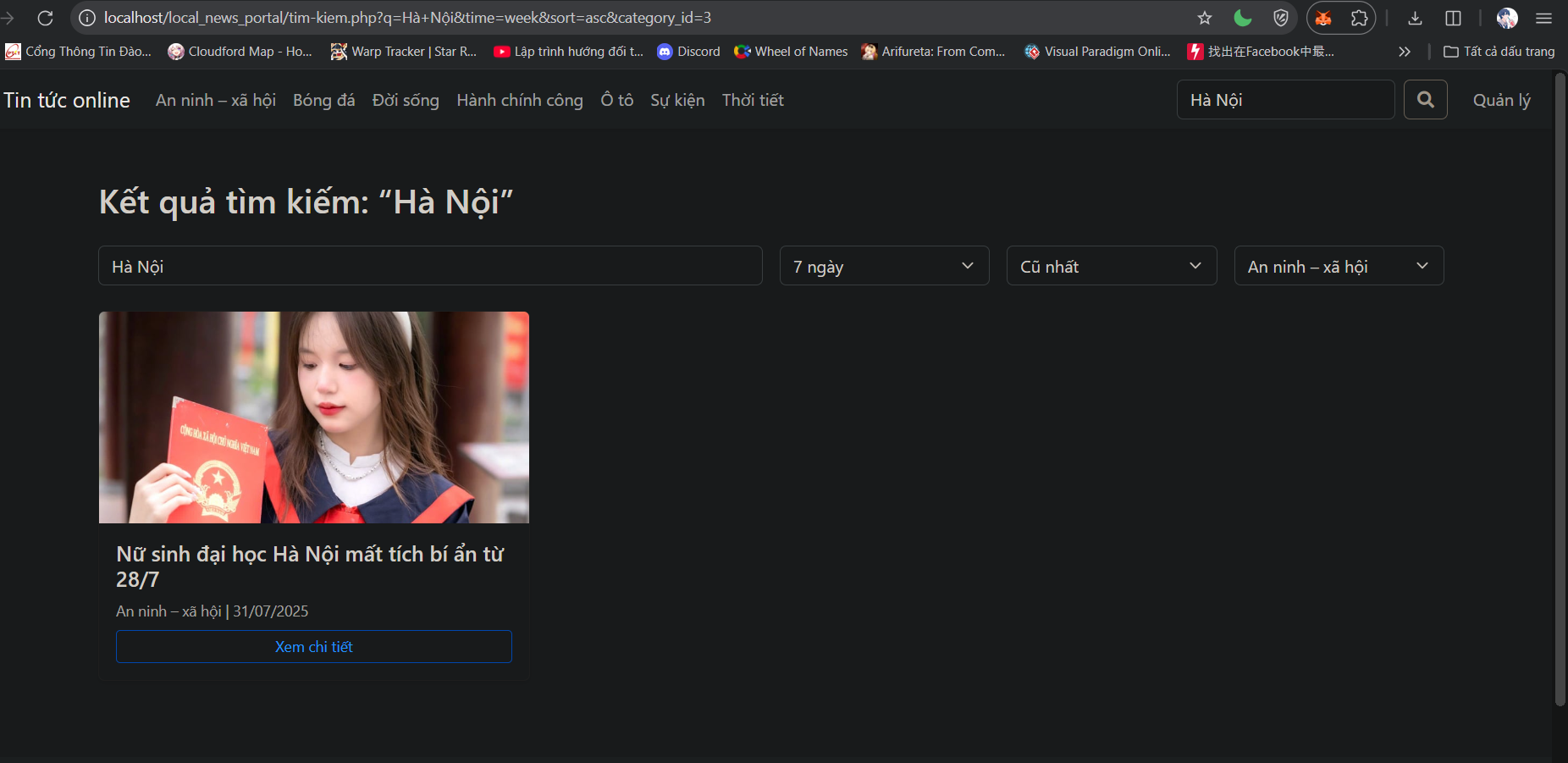
* Admin: Sau khi đăng nhập người dùng admin, admin có thể vào trang quản lý

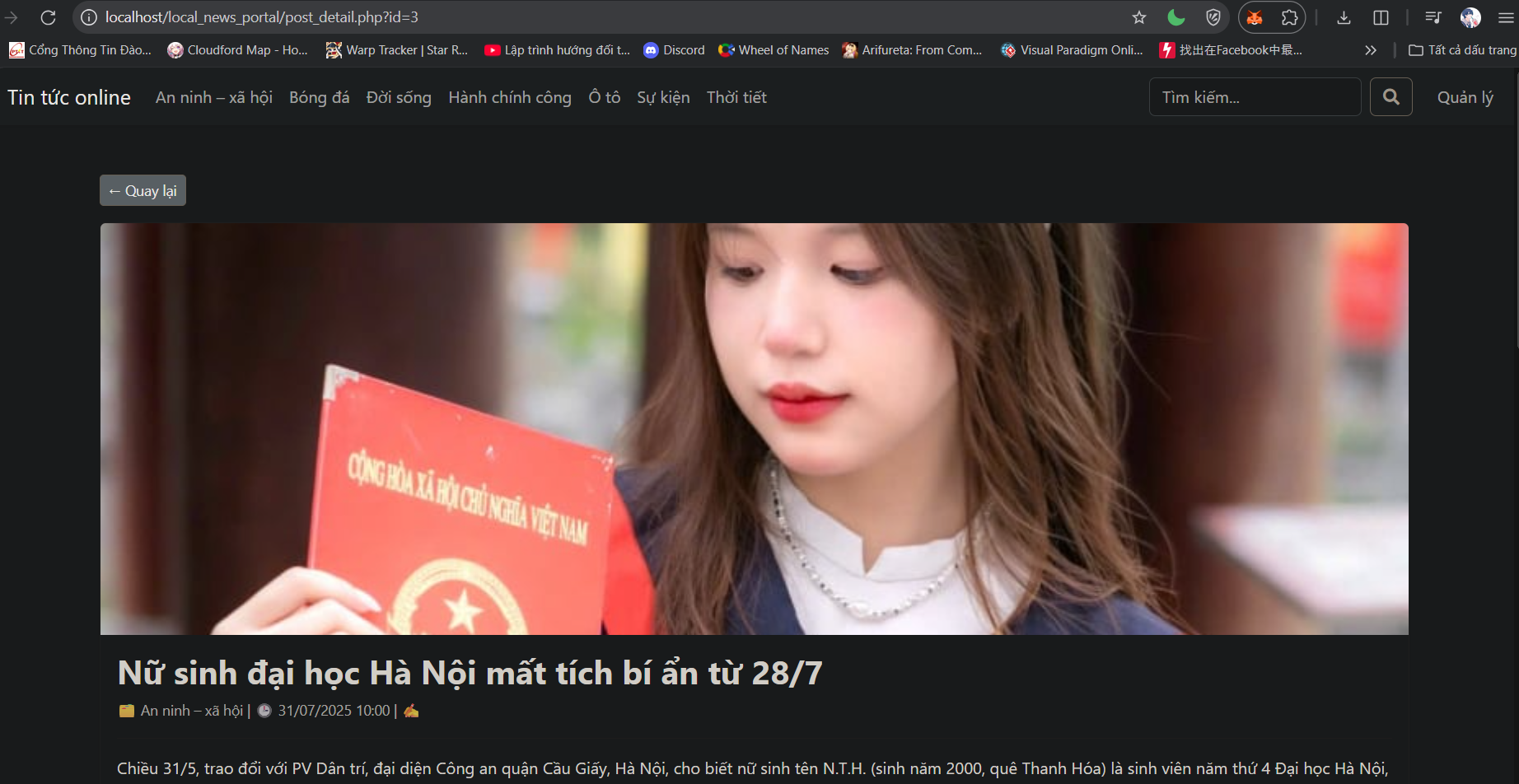
  
  
  
Admin có đầy đủ các chức năng thêm, sửa, xóa bài viết; thêm sửa xóa chuyên mục và người dùng  
Ngoài ra khi staff hay admin thêm bài viết sẽ phải duyệt bài viết trước khi đăng lên trang tin tức và admin không thể xóa admin

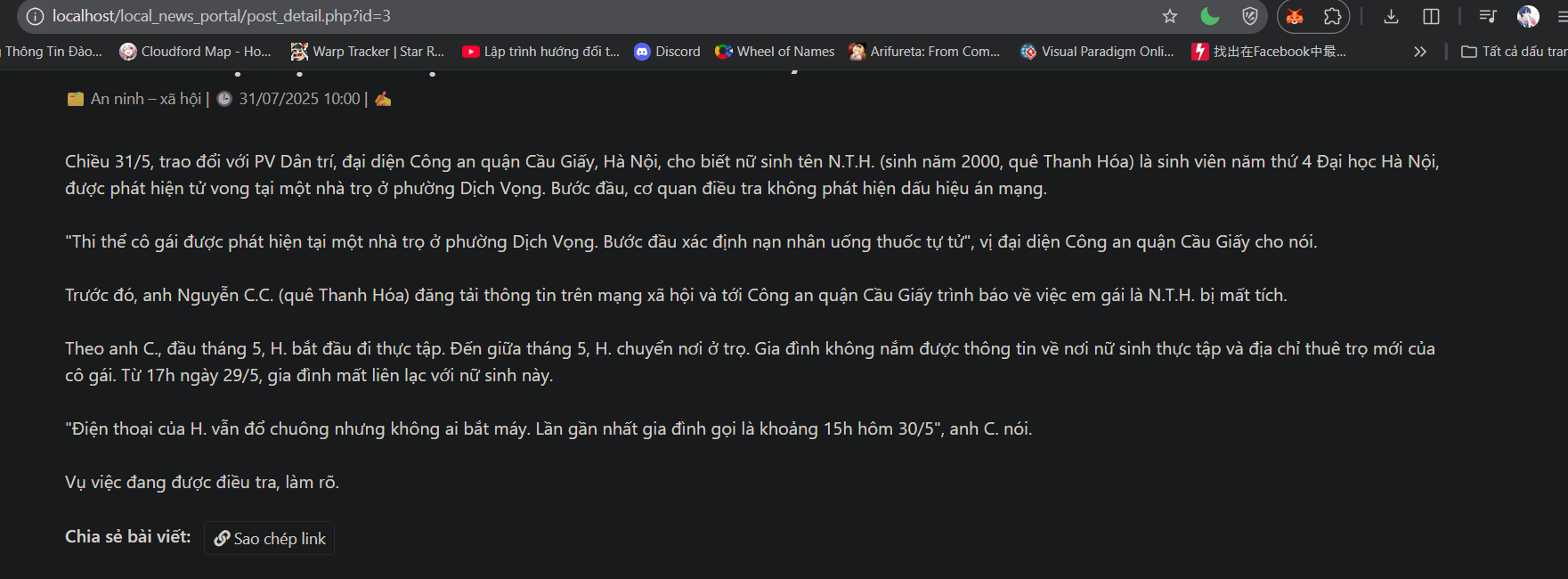
* Trang tin tức:

  
  
Giới hạn của 1 trang là 6 bài viết, bất cứ người dùng nào cũng có thể truy cập vào trang tin tức hay chi tiết của tin tức đó mà không phải đăng nhập

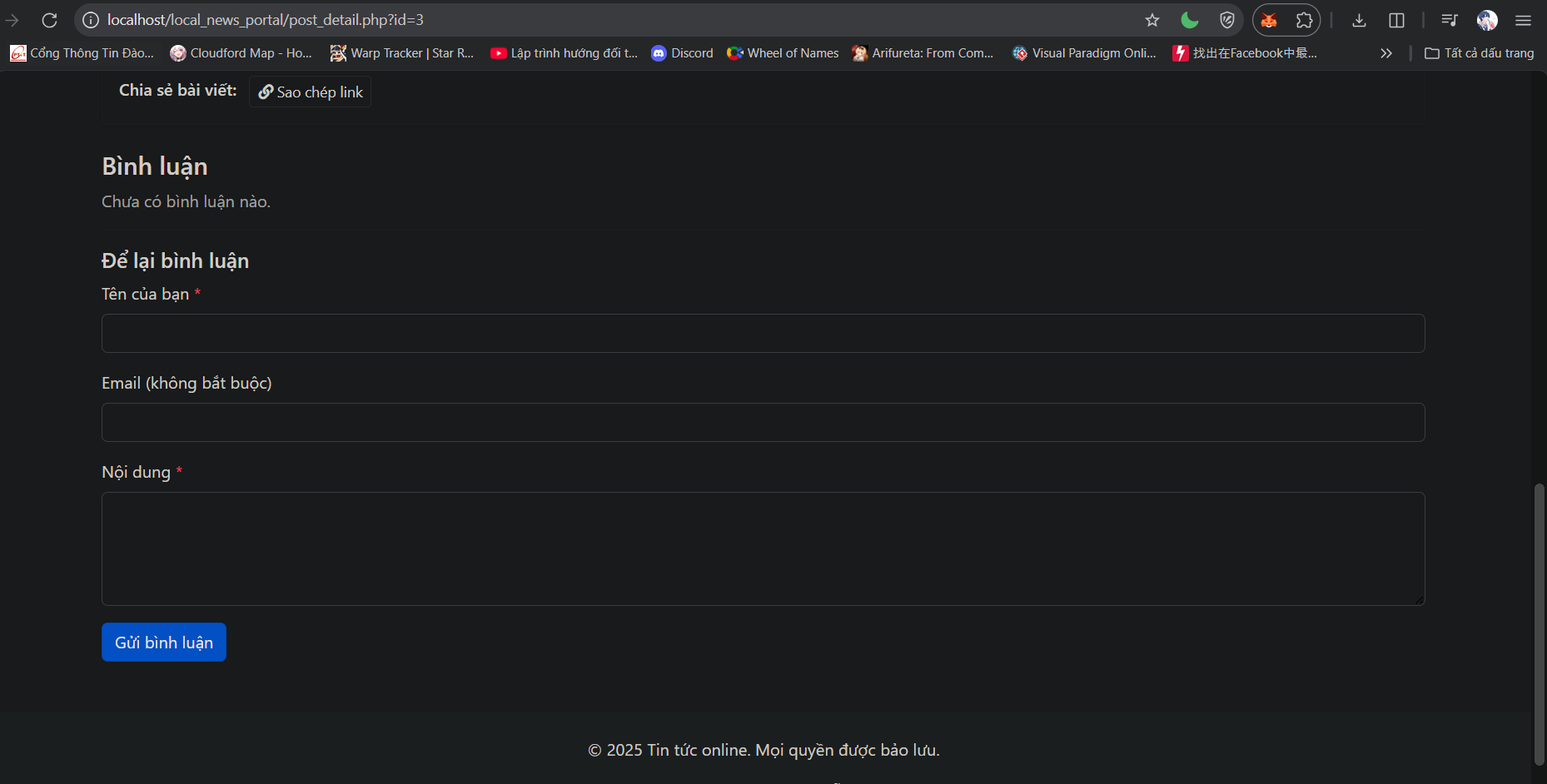
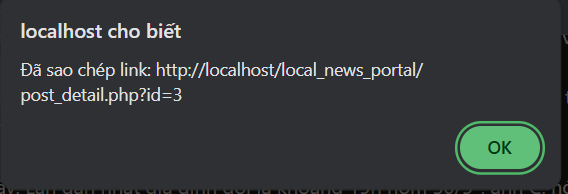
Trang chuyên mục: là trang chỉ dành riêng cho chuyên mục đó, tương tự trang chính  
  


Trang tìm kiếm: người dùng có thể tìm kiếm từ khóa, lọc trong khoảng thời gian, sắp xếp và chuyên mục  
  
  
Trang chi tiết tin tức:

Gồm 1 nút quay lại ở đầu và thông tin bài viếviết  




Dưới thông tin bài viết có nút share và phần bình luận  
Bình luận hiện tại không cần phải đăng nhập

  
Khi bấm vô nút share, bảng thông báo sẽ hiện ra và thông báo đã copy link  


1. Hạn chế và hướng phát triển:

* Hạn chế: thiếu API cho mobie, chưa CSRF token, caching
* Hướng phát triển: nâng cấp MVC