

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN



HCMUTE

BÁO CÁO CUỐI KỲ

BẢO MẬT WEB

Đề Tài
XÁC ĐỊNH VÀ KHẮC PHỤC
CÁC VẤN ĐỀ BẢO MẬT WEBSITE HỘI THẢO

SINH VIÊN THỰC HIỆN:

Trần Huỳnh Phiêu
Nguyễn Minh Thông

15110276
15110323

GIÁO VIÊN HƯỚNG DẪN:

ThS. Lê Thị Minh Châu

HỌC KỲ II
NĂM HỌC 2017 – 2018
Tp. Hồ Chí Minh – 6/2018

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN



HCMUTE

BÁO CÁO CUỐI KỲ

BẢO MẬT WEB

Đề Tài
XÁC ĐỊNH VÀ KHẮC PHỤC
CÁC VẤN ĐỀ BẢO MẬT WEBSITE HỘI THẢO

SINH VIÊN THỰC HIỆN: Trần Huỳnh Phiêu 15110276
Nguyễn Minh Thông 15110323

GIÁO VIÊN HƯỚNG DẪN: ThS. Lê Thị Minh Châu

HỌC KỲ II
NĂM HỌC 2017 – 2018
Tp. Hồ Chí Minh – 6/2018

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

LỜI CẢM ƠN

Lời đầu tiên, Nhóm thực hiện đề tài xin gửi lời cảm ơn, lời chúc sức khỏe đến tập thể giảng viên khoa Công nghệ thông tin trường ĐH Sư phạm Kỹ thuật Tp.Hồ Chí Minh đã tạo ra môi trường học tập thuận lợi cho sinh viên trong khoa có thể hoàn thành tốt các đề tài được đưa ra.

Chúng tôi xin bài tỏ lòng biết ơn đến Thạc sĩ Lê Thị Minh Châu đã trực tiếp giảng dạy môn học Bảo mật Web và hướng dẫn tận tình để chúng tôi có một kết quả tốt nhất khi hoàn thành đề tài.

Chúng tôi xin cảm ơn đến tập thể sinh viên lớp Bảo mật web – buổi học vào sáng thứ 6 các tuần trong học kỳ II năm học 2017 – 2018 đã cùng nhau chia sẻ tài liệu, các giải thuật, ý tưởng phát triển các nội dung trong website để nhóm chúng tôi cũng như các nhóm bạn cùng nhau học tập phát triển và đạt được kết quả thuận lợi nhất trong đề các đề tài đã được giảng viên giao cho.

Quá trình tìm kím các vấn đề bảo mật và khắc phục trên Website Hội thảo đã nhận được sự hỗ trợ tận tình của quý thầy cô, bạn bè. Tiếp theo đây phần mềm vẫn sẽ được tiếp tục xây dựng hoàn thiện hơn để những kiến thức đã học được có thể áp dụng vào thực tế ứng dụng, rất mong nhận được sự quan tâm tiếp tục của quý thầy cô hướng dẫn và các thế hệ sinh viên ĐH Sư phạm Kỹ thuật Tp. Hồ Chí Minh.

Trân trọng cảm ơn!

MỤC LỤC

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN	3
LỜI CẢM ƠN.....	4
MỤC LỤC	5
BÁO CÁO ĐỒ ÁN MÔN BẢO MẬT WEB	7
1. MỤC ĐÍCH – YÊU CẦU.....	7
2. TRÌNH BÀY BÀI TẬP LỚN	7
2.1. Mô tả phân công công việc.....	7
2.2. Thiết kế giao diện	7
2.2.1. Trang chủ	8
2.2.2. Trang phân loại nội dung “Công nghệ”	10
2.2.3. Trang phân loại nội dung “Giáo dục”	10
2.2.4. Trang phân loại nội dung “Giải trí”	11
2.2.5. Trang phân loại nội dung “Cuộc sống”	11
2.2.6. Trang phân loại nội dung “Thế giới”	12
2.2.7. Trang liên hệ	12
2.2.8. Cửa sổ đăng nhập.....	13
2.2.9. Cửa sổ đăng ký	13
2.2.10. Trang quản lý bài viết của Writer.....	14
2.2.11. Trang thêm bài viết của Writer.....	14
2.2.12. Trang quản lý bài viết chờ phê duyệt của Reviewer	15
2.2.13. Logo trang web.....	15
2.2.14. Trang quản lý bài viết của Administrator	16
2.2.15. Trang quản lý phê duyệt bài viết của Administrator	16
2.2.16. Trang quản lý tài khoản của Administrator	16
2.2.17. Trang thêm tài khoản dành cho Administrator	17
2.2.18. Trang phê duyệt bài viết.....	17
2.2.19. Trang thông tin cá nhân của các tài khoản	18
2.3. Đặc tả phần mềm	18
2.3.1. Usecase chức năng phần mềm	18
2.3.2. Đặc tả Usecase	20
2.3.3. Xác định và mô tả Actor	21
2.4. Thiết kế code	21
2.4.1. Bảng mô tả các lớp trong chương trình	21
2.5. Thiết kế cơ sở dữ liệu	22
2.5.1. Mô hình Diagram.....	22

2.5.2. Mô hình ERD.....	22
2.5.3. Mô tả các bảng trong cơ sở dữ liệu.....	23
2.5.4. Mô tả các trường trong các bảng	23
2.6. Chạy Demo	25
3. BẢO MẬT WEBSITE	25
3.1. Sử dụng các công cụ quét lỗ hổng bảo mật	25
3.2. Vấn đề bảo mật về chặn gói tin qua mạng thông thường	26
3.3. Về Access Control Flaws	27
3.3.1. Admin đã đăng nhập có quyền xem và xóa tài khoản bất kỳ	27
3.4. Về Authentication Flaws	28
3.4.1. Truy suất đến các trang quản lý thông qua URL	28
3.5. Về Buffer Overflows	29
3.5.1. Vượt số lượng ký tự quy định của các trường trong database.....	29
3.5.2. Giới hạn độ dài các textbox hoặc textarea không tác dụng với những kẻ tấn công	30
3.6. Về Code Quality	30
3.7. Về Concurrency	31
3.8. Về Cross site Scripting	31
3.8.1. Stored XSS.....	31
3.8.2. Đọc dữ liệu có sẵn mã độc tấn công XSS	32
3.9. Về Injection Flaws.....	34

BÁO CÁO ĐỒ ÁN MÔN BẢO MẬT WEB

1. MỤC ĐÍCH – YÊU CẦU

Mẫu này được sử dụng cho trình bày bài tập lớn, sinh viên bắt buộc thực hiện nghiêm ngặt theo mẫu này cả về nội dung lẫn hình thức.

Các qui định về nội dung trong mẫu này nhằm đảm bảo sinh viên hiểu rõ bài tập lớn đang thực hiện ở hai khía cạnh: làm cái gì (what to do) và làm thế nào (how to do). Ngoài ra, mẫu này cũng giúp giảng viên đảm bảo:

- SV hiểu được những gì các thành viên khác hoặc chính mình làm.
- Đối với những phần sinh viên không tự làm mà tham khảo ở nguồn khác, sinh viên cần phải hiểu rõ cơ chế hoạt động, chứ không copy thụ động.

2. TRÌNH BÀY BÀI TẬP LỚN

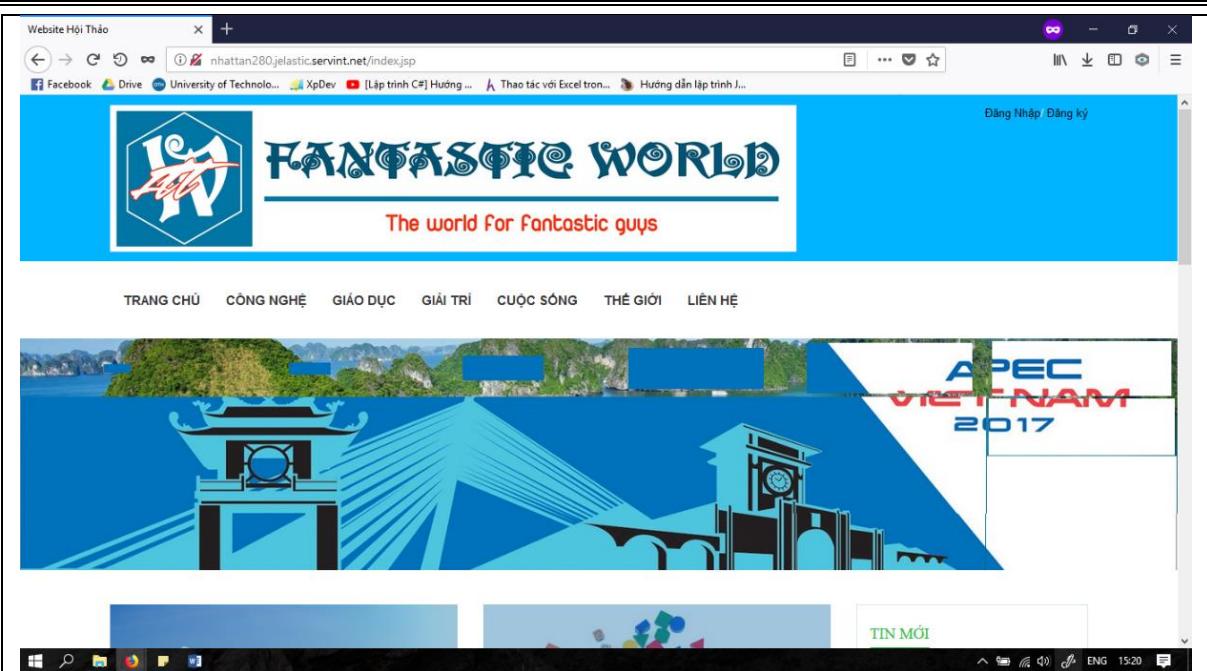
2.1. Mô tả phân công công việc

2.2. Thiết kế giao diện

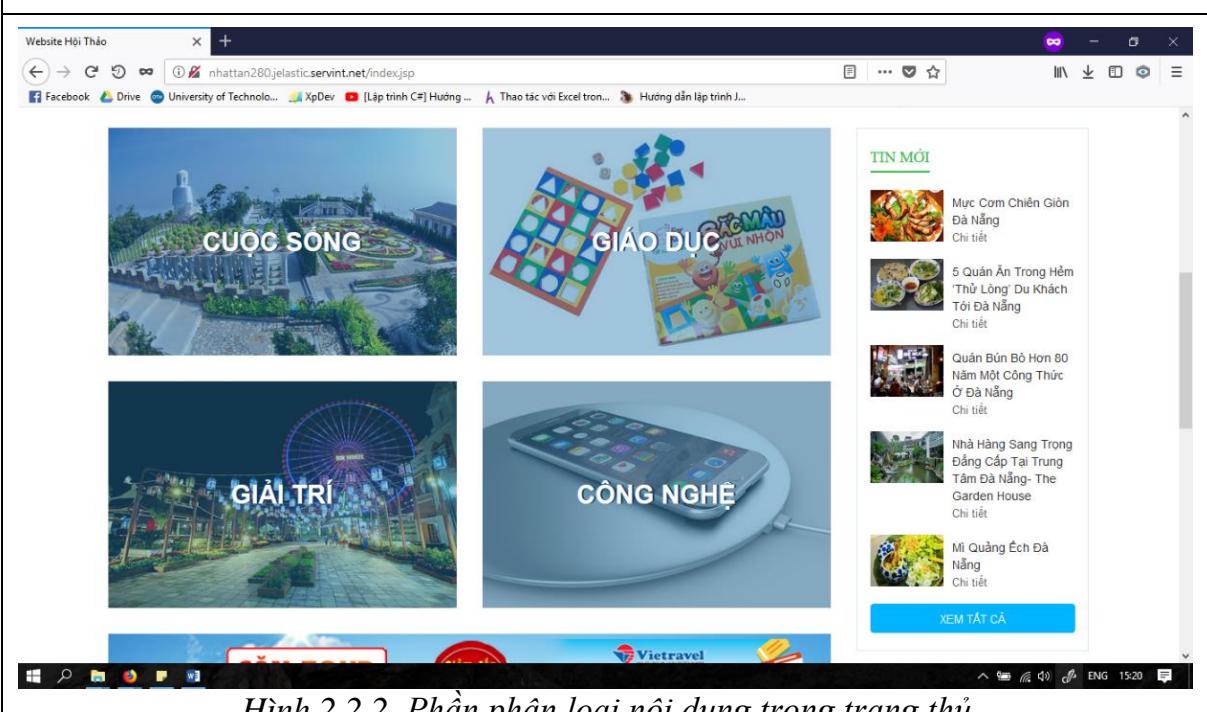
STT	Giao diện	Mục đích
1	MH1: Trang chủ	Hiển thị tổng quan về các nội dung của trang web Sở hữu đường dẫn đến các nội dung và các trang khác trong websitr
2	MH2: Trang phân loại nội dung “Công nghệ”	Tổng hợp nội dung các bài đăng liên quan đến lĩnh vực công nghệ
3	MH3: Trang phân loại nội dung “Giáo dục”	Tổng hợp nội dung các bài đăng liên quan đến lĩnh vực giáo dục
4	MH4: Trang phân loại nội dung “Giải trí”	Tổng hợp nội dung các bài đăng liên quan đến lĩnh vực giải trí
5	MH5: Trang phân loại nội dung “Cuộc sống”	Tổng hợp nội dung các bài đăng liên quan đến lĩnh vực cuộc sống
6	MH6: Trang phân loại nội dung “Thế giới”	Tổng hợp nội dung các bài đăng liên quan đến lĩnh vực Thế giới
7	MH7: Trang liên hệ	Chứa thông tin liên hệ đến đơn vị chủ quản website
8	MH8: Cửa sổ đăng nhập	Thực hiện giải quyết đăng nhập cho các chức năng của trang web.
9	MH9: Cửa sổ đăng ký	Thực hiện giải quyết đăng ký tài khoản “Writer” mới.
10	MH10: Trang quản lý bài viết của Writer	Cho phép Writer của trang web có thể quản lý các bài viết ứng với tài khoản đăng nhập của mình.

11	MH11: Trang thêm bài viết của Writer	Trang nhập liệu một nội dung bài viết mới của Writer
12	MH11: Trang quản lý bài viết chờ phê duyệt của Reviewer	Trang cho phép Reviewer phê xem danh sách các bài đăng gửi đến trang web chờ phê duyệt.
13	MH13: Logo trang web	Là hình ảnh đặt thù đại diện riêng cho trang web hội thảo.
14	MH14: Trang quản lý bài viết của Adminitrator	Trang quản lý bài viết của Admin bao gồm lựa chọn dẫn sang các trang quản lý phê duyệt bài viết, quản lý tài khoản. Tại trang này admin quản lý bài viết của chính mình và.
15	MH15: Trang quản lý phê duyệt bài viết của Adminitrator	Trang quản lý phê duyệt bài viết của Admin bao gồm lựa chọn dẫn sang các trang quản lý bài viết, quản lý tài khoản. Tại trang này admin phê duyệt bài viết được các Writer gửi đến chờ xét duyệt.
16	MH16: Trang quản lý tài khoản của Adminitrator	Trang quản lý tài khoản của Admin bao gồm lựa chọn dẫn sang các trang quản lý phê duyệt bài viết, quản lý bài viết. Tại trang này admin quản lý thông tin các tài khoản đang có trong hệ thống làm việc với các thông tin cá nhân và quyền hạn trong trang web.
17	MH17: Trang thêm tài khoản dành cho Adminitrator	Thêm mới một tài khoản vào trang web. Quyền của tài khoản được lựa chọn tự do bởi admin.
18	MH18: Trang phê duyệt bài viết	Dùng cho Adminitrator và Reviewer trong việc kiểm tra các bài viết được Writer gửi đến trang web.
19	MH19: Trang thông tin cá nhân của các tài khoản	Xem lại thông tin cá nhân được lưu kèm với từng user đăng nhập vào trang web Cập nhật thông tin cá nhân của tài khoản nếu có sự sai sót, chức năng này không thể thay đổi quyền trong trang web.

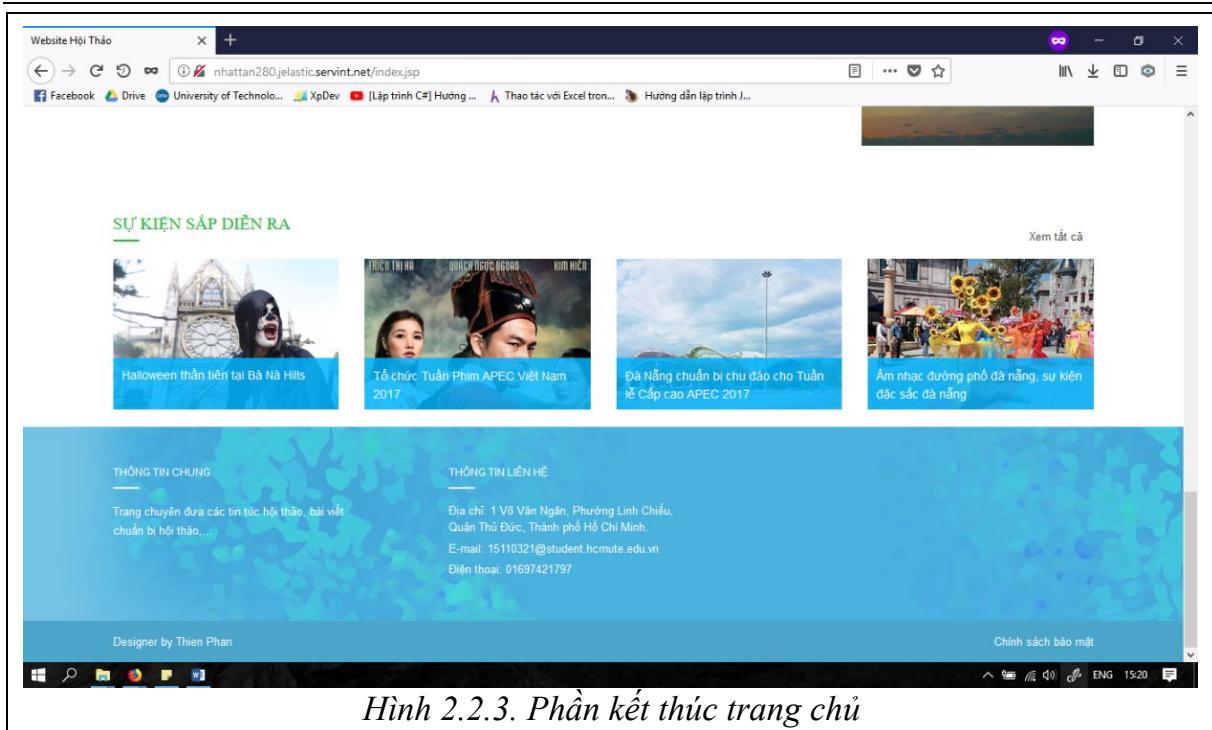
2.2.1. Trang chủ



Hình 2.2.1. Phần mở đầu

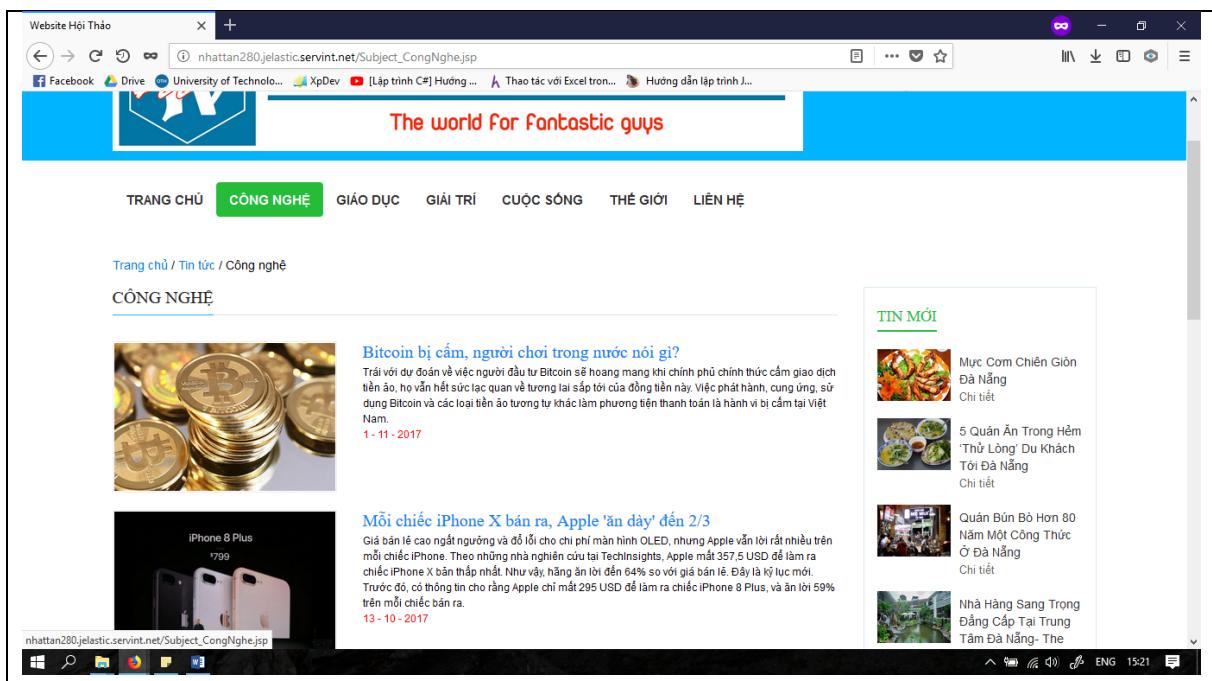


Hình 2.2.2. Phần phân loại nội dung trong trang chủ



Hình 2.2.3. Phần kết thúc trang chủ

2.2.2. Trang phân loại nội dung “Công nghệ”



2.2.3. Trang phân loại nội dung “Giáo dục”

Website Hội Thảo

The world For Fantastic guys

TRANG CHỦ CÔNG NGHỆ GIÁO DỤC GIẢI TRÍ CUỘC SỐNG THẾ GIỚI LIÊN HỆ

Trang chủ / Tin tức / Giáo dục

GIÁO DỤC



Lương thấp, giáo viên mầm non chất vật sống
Giáo viên mầm non làm việc hơn 8 tiếng mỗi ngày nhưng đang nhận mức lương thấp nhất. Với hệ số 1,86, nhiều giáo viên trẻ mới ra trường chỉ có mức lương hơn 3,2 triệu đồng, còn giáo viên sắp nghỉ hưu cũng chỉ nhận được hơn 5 triệu đồng/tháng.
1 - 11 - 2017



Jack Ma: Con người cần có chí sốt tình yêu để thành công
Trong buổi trò chuyện với sinh viên Việt Nam, Jack Ma khuyên người trẻ tìm cơ hội khi người khác than vãn, học cách làm khác biệt, không từ bỏ và chủ trọng vào chí sốt tình yêu.
13 - 10 - 2017

TIN MỚI

- Mực Corm Chiên Giòn Đà Nẵng Chi tiết
- 5 Quán Ăn Trong Hẻm 'Thủ Lòng' Du Khách Tới Đà Nẵng Chi tiết
- Quán Bún Bò Hòn 80 Năm Một Công Thức Ăn Đà Nẵng Chi tiết
- Nhà Hàng Sang Trọng Đẳng Cấp Tại Trung Tâm Đà Nẵng- The

2.2.4. Trang phân loại nội dung “Giải trí”

Website Hội Thảo

The world For Fantastic guys

TRANG CHỦ CÔNG NGHỆ GIÁO DỤC GIẢI TRÍ CUỘC SỐNG THẾ GIỚI LIÊN HỆ

Trang chủ / Tin tức / Giải trí

GIẢI TRÍ



Sao võ thuật trẻ trong phim của Jack Ma khiến Thành Long, Lý Liên Kiết phải nể phục
Mới đây, thông tin về bộ phim Công thủ đạo do tỷ phú Jack Ma đảm nhiệm nhân vật chính đã gây sốt trên cộng đồng mạng. Bộ phim hồi tự rất nhiều những cao thủ võ thuật để kết hợp với ông chủ của Alibaba nhằm quảng cáo cho môn võ cổ truyền của Trung Hoa. Một trong số đó, không thể không nhắc tới Huỳnh Tấn, chàng diễn viên trẻ khiến nhiều người phải kinh ngạc.
1 - 11 - 2017



Tổ chức Tuần Phim APEC Việt Nam 2017
TTO - Theo ban tổ chức, các phim được chọn trình chiếu trong Tuần phim APEC Việt Nam 2017 sẽ được chiếu miễn phí một lần tại Hà Nội và một lần tại Đà Nẵng.
13 - 10 - 2017

TIN MỚI

- Mực Corm Chiên Giòn Đà Nẵng Chi tiết
- 5 Quán Ăn Trong Hẻm 'Thủ Lòng' Du Khách Tới Đà Nẵng Chi tiết
- Quán Bún Bò Hòn 80 Năm Một Công Thức Ăn Đà Nẵng Chi tiết
- Nhà Hàng Sang Trọng Đẳng Cấp Tại Trung Tâm Đà Nẵng- The

2.2.5. Trang phân loại nội dung “Cuộc sống”

The screenshot shows a news article from a Vietnamese website. The header features a logo with the letters 'WY' and the text 'The world For Fantastic guys'. Below the header is a navigation bar with tabs: TRANG CHỦ, CÔNG NGHỆ, GIÁO DỤC, GIẢI TRÍ, CUỘC SỐNG (highlighted in green), THẾ GIỚI, and LIÊN HỆ. The main content area has a breadcrumb trail: Trang chủ / Tin tức / Cuộc sống. A sub-header 'CUỘC SỐNG' is followed by a large image of a person in a black hoodie and white face paint standing in front of a Gothic-style building. Below the image is the title 'Halloween thần tiên tại Bà Nà Hills' and a brief description: 'Điển ra từ ngày 1/10 đến hết ngày 31/10/2017, lễ hội Halloween tại Sun World Ba Na Hills với chủ đề "Xứ sở thần tiên" mang đến cho du khách những trải nghiệm khác lạ với cuộc hồi ức cùng các nhân vật cổ tích tưởng chừng chỉ có trong giấc mơ. Không tập trung khai thác yếu tố rùng rợn hay sử dụng...'. The date '1 - 11 - 2017' is also present. To the right, there's a sidebar titled 'TIN MỚI' with links to other news articles, each with a thumbnail image and a brief description.

2.2.6. Trang phân loại nội dung “Thế giới”

Website Hội Thảo

nhattan280.jelastic.servint.net/Subject_TheGioi.jsp

Facebook Drive University of Technolo... XpDev [Lập trình C#] Hướng ... Thao tác với Excel tron... Hướng dẫn lập trình J...

The world For fantastic guys

TRANG CHỦ CÔNG NGHỆ GIÁO DỤC GIẢI TRÍ CUỘC SỐNG THẾ GIỚI LIÊN HỆ

Trang chủ / Tin tức / Thế giới

THẾ GIỚI



Việt Nam đã đón gần 140 lượt máy bay dự hội nghị APEC

Tính đến chiều 7/11, 3 sân bay Đà Nẵng, Nội Bài, Tân Sơn Nhất đã đón tổng cộng gần 140 lượt máy bay phục vụ APEC. Con số này tiếp tục tăng lên trong những ngày tới. Chiều 7/11, trao đổi với Zing.vn, ông Võ Huy Cường, Cục phó Cục Hàng không, cho biết theo thống kê sân bay Đà Nẵng đã đón 119 lượt máy bay vận chuyển hàng hóa và các quan chức dự hội nghị APEC. Trong khi đó, sân bay Nội Bài đón 15 lượt, Tân Sơn Nhất 4 lượt.

1 - 11 - 2017



Thủ tướng phát biểu tại hội nghị cấp cao ASEAN - Ấn Độ

Thủ tướng Nguyễn Xuân Phúc hôm qua tham dự các lãnh đạo ASEAN kiểm điểm hợp tác, định hướng quan hệ ASEAN - Ấn Độ tại hội nghị ở Philippines.

13 - 10 - 2017

TIN MỚI



Mực Corm Chiên Giòn
Đà Nẵng
Chi tiết



5 Quán Ăn Trong Hẻm
Thủ Lĩnh Du Khách
Tại Đà Nẵng
Chi tiết



Quán Bún Bò Hon 80
Năm Một Công Thức
Ở Đà Nẵng
Chi tiết



Nhà Hàng Sang Trọng
Đẳng Cấp Tại Trung
Tâm Đà Nẵng- The

2.2.7. Trang liên hệ

The screenshot shows a Microsoft Edge browser window displaying the contact page of a website. The URL in the address bar is nhattan280.jelastic.servint.net/Subject_LienHe.jsp. The page title is "LIÊN HỆ". The main content area contains a form with fields for "Họ và tên", "Địa chỉ email", "Tiêu đề", and "Thông điệp", followed by a "GỬI ĐI" button. To the right, there is a sidebar titled "TIN MỚI" featuring five news items with small thumbnail images and titles:

- Mực Corm Chiên Giòn Đà Nẵng Chi tiết
- 5 Quận Ăn Trong Hẻm 'Thủ Lòng' Du Khách Tới Đà Nẵng Chi tiết
- Quán Bún Bò Hòn 80 Năm Một Công Thức Ăn Đà Nẵng Chi tiết
- Nhà Hàng Sang Trọng Đẳng Cấp Tại Trung Tâm Đà Nẵng- The Garden House Chi tiết
- Mì Quảng Éch Đà Nẵng Chi tiết

2.2.8. Cửa sổ đăng nhập

The screenshot shows a Microsoft Edge browser window displaying the login page of the website. The URL in the address bar is nhattan280.jelastic.servint.net/index.jsp. The page title is "ĐĂNG NHẬP". The login form has fields for "Tài Khoản" (username) and "Password" (password), a "Ghi nhớ tài khoản" (remember account) checkbox, and a "Đăng Nhập" (Login) button. The background features a banner for "APEC VIET NAM 2017".

2.2.9. Cửa sổ đăng ký

ĐĂNG KÝ THÀNH VIÊN

Tài Khoản: _____
Mật Khẩu: _____
Nhập Lại Mật Khẩu: _____
Họ Tên: _____
Giới Tính: Nam Nữ
Ngày sinh: _____
Email: _____
Số Điện Thoại: _____
Địa Chỉ: _____

APEC VIET NAM 2017

2.2.10. Trang quản lý bài viết của Writer

STT	Tên bài viết	Thời gian	Thể loại	Tình trạng	Thao tác
12	Việt Nam đã đón gần 140 lượt máy bay dự hội nghị APEC	2017-12-27	công nghệ	chưa duyệt	Xem nội dung
13	Chiều 7/11, trao đổi với Zing.vn	2017-12-27	Giáo Dục	Duyệt	Xem nội dung
14	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27	Công Nghệ	chưa duyệt	Xem nội dung
15	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27	Giải Trí	chưa duyệt	Xem nội dung
16	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27	Giải Trí	Tu chối	Xem nội dung
17	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27	Công Nghệ	Duyệt	Xem nội dung
18	demo	2017-12-24	Khác	chưa duyệt	Xem nội dung

2.2.11. Trang thêm bài viết của Writer

Website Hội Thảo

BÀI VIẾT | Bài viết mới

Tên Bài viết
Nhập tên bài viết

Ngày viết
mm / dd / yyyy

Thể loại
Công nghệ

Nội dung
Nhập nội dung bài viết

Tôi chắc chắn về nội dung đăng tải là hợp pháp và đảm bảo tuân phong mĩ tục.

Gửi bài viết | Hủy

2.2.12. Trang quản lý bài viết chờ phê duyệt của Reviewer

Website Hội Thảo

FANTASTIC WORLD
The world For Fantastic guys

Cá nhân | Đăng xuất | Kiểm duyệt

TRANG CHỦ CÔNG NGHỆ GIÁO DỤC GIẢI TRÍ CUỘC SỐNG THẾ GIỚI LIÊN HỆ

KIỂM DUYỆT | Bài viết chờ xử lý

Số	Tên bài viết	Thời gian	Thể loại	Người gửi	Thao tác
12	Việt Nam đã đón gần 140 lượt máy bay dự hội nghị APEC	2017-12-27	công nghệ	phanthien@gmail.com	Xem nội dung
14	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27	Công Nghệ	phanthien@gmail.com	Xem nội dung
15	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27	Giải Trí	phanthien@gmail.com	Xem nội dung
18	demo	2017-12-31	Khác	phanthien@gmail.com	Xem nội dung

THÔNG TIN CHUNG | THÔNG TIN LIÊN HỆ

2.2.13. Logo trang web



2.2.14. Trang quản lý bài viết của Adminitrator

The screenshot shows a web browser window titled 'Website Hội Thảo'. The address bar shows the URL: nhattan280.jelastic.servint.net/Login. The page content is for a website titled 'FANTASTIC WORLD' with the tagline 'The world For Fantastic guys'. The top navigation bar includes links for 'Cá nhân', 'Đăng xuất', 'Bài viết', 'Kiểm duyệt', and 'Quản lý tài khoản'. Below the navigation is a horizontal menu with links: TRANG CHỦ, CÔNG NGHỆ, GIÁO DỤC, GIẢI TRÍ, CUỘC SỐNG, THẾ GIỚI, and LIÊN HỆ. The main content area is titled 'BÀI VIẾT |Quản lý bài viết' and features a green button labeled 'Bài viết mới'. A table lists 7 posts with columns: STT, Tên bài viết, Thời gian, Thể loại, Tình trạng, and Thao tác. The posts are:

STT	Tên bài viết	Thời gian	Thể loại	Tình trạng	Thao tác
12	Việt Nam đã đón gần 140 lượt máy bay dự hội nghị APEC	2017-12-27	công nghệ	chưa duyệt	Xem nội dung
13	Chiều 7/11, trao đổi với Zing.vn	2017-12-27	Giáo Dục	Duyệt	Xem nội dung
14	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27	Công Nghệ	chưa duyệt	Xem nội dung
15	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27	Giải Trí	chưa duyệt	Xem nội dung
16	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27	Giải Trí	Tu choi	Xem nội dung
17	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27	Công Nghệ	Duyệt	Xem nội dung

2.2.15. Trang quản lý phê duyệt bài viết của Adminitrator

The screenshot shows a web browser window titled 'Website Hội Thảo'. The address bar shows the URL: nhattan280.jelastic.servint.net/Admin_Manager_Check.jsp. The page content is for a website titled 'FANTASTIC WORLD' with the tagline 'The world For Fantastic guys'. The top navigation bar includes links for 'Cá nhân', 'Đăng xuất', 'Bài viết', 'Kiểm duyệt', and 'Quản lý tài khoản'. Below the navigation is a horizontal menu with links: TRANG CHỦ, CÔNG NGHỆ, GIÁO DỤC, GIẢI TRÍ, CUỘC SỐNG, THẾ GIỚI, and LIÊN HỆ. The main content area is titled 'KIỂM DUYỆT |Bài viết chờ xử lý' and features a green button labeled 'Bài viết chờ xử lý'. A table lists 4 posts with columns: STT, Tên bài viết, Thời gian, Thể loại, Người gửi, and Thao tác. The posts are:

STT	Tên bài viết	Thời gian	Thể loại	Người gửi	Thao tác
12	Việt Nam đã đón gần 140 lượt máy bay dự hội nghị APEC	2017-12-27	công nghệ	phanthien@gmail.com	Xem nội dung
14	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27	Công Nghệ	phanthien@gmail.com	Xem nội dung
15	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27	Giải Trí	phanthien@gmail.com	Xem nội dung
18	demo	2017-12-31	Khac	phanthien@gmail.com	Xem nội dung

2.2.16. Trang quản lý tải khoản của Adminitrator

The screenshot shows a web browser window titled "Website Hội Thảo". The URL is nhattan280.jelastic.servint.net/Admin_Account_Manager.jsp. The page header features a logo with the letters "FW" and the text "FANTASTIC WORLD" and "The world For Fantastic guys". Navigation links include TRANG CHỦ, CÔNG NGHỆ, GIÁO DỤC, GIẢI TRÍ, CUỘC SỐNG, THẾ GIỚI, and LIÊN HỆ. On the right, there are buttons for Cá nhân, Đăng xuất, Bài viết, Kiểm duyệt, and Quản lý tài khoản. A green button labeled "Thêm tài khoản" is visible. Below the header is a table listing five users:

STT	Username	Password	Họ và tên	Vai trò	Thông tin chi tiết	Thao tác
1	ThienPhan	123456	Phan Minh Thiện	Admin	Xem chi tiết	Xóa
2	PhieuHuynh	123456	Trần Huỳnh Phiêu	Reviewer	Xem chi tiết	Xóa
3	Tantran	123456	Trần Nhật Tân	Admin	Xem chi tiết	Xóa
4	ThuyHuynh	123456	Huỳnh Thị Thuý	Writer	Xem chi tiết	Xóa
5	NghiaLam	123456	Lâm Thành Nghĩa	Writer	Xem chi tiết	Xóa

2.2.17. Trang thêm tài khoản dành cho Admininitrator

The screenshot shows a web browser window titled "Website Hội Thảo". The URL is nhattan280.jelastic.servint.net/Admin_Account_New.jsp. The page header features a logo with the letters "FW" and the text "FANTASTIC WORLD | Tài khoản mới". The form fields include:

- Username:** Nhập Username
- Password:** Nhập Password
- Nhập lại Password:** Nhập lại Password
- Họ và tên:** Nhập Họ tên người dùng
- Ngày sinh:** mm / dd / yyyy
- Thể loại:** Nam (dropdown menu)
- Số điện thoại:** Nhập Số điện thoại
- Mail:** Nhập địa chỉ e-mail
- Thể loại:** Administrator (dropdown menu)

At the bottom are two buttons: "Thêm tài khoản" (in green) and "Hủy" (in red).

2.2.18. Trang phê duyệt bài viết

Website Hội Thảo

BÀI VIẾT | Thông tin bài viết

Tên Bài viết
Việt Nam đã đón gần 140 lượt máy bay dự hội nghị APEC

Ngày viết
12 / 27 / 2017

Thể loại
công nghệ

Nội dung

Tính đến chiều 7/11, 3 sân bay Đà

Danh giá bài viết:
Bài viết chưa đủ nội dung

Chấp nhận Từ chối

2.2.19. Trang thông tin cá nhân của các tài khoản

Website Hội Thảo

The world For Fantastic guys

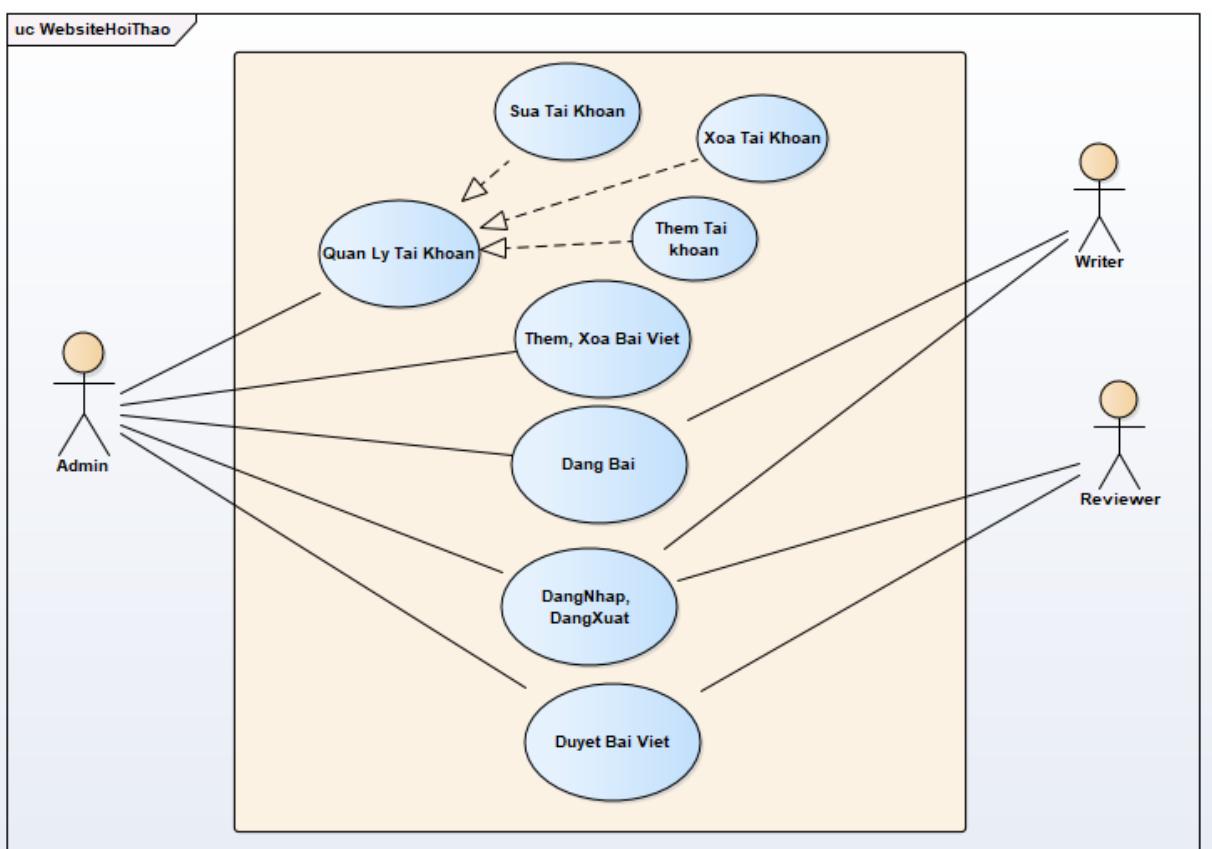
TRANG CHỦ CÔNG NGHỆ GIÁO DỤC GIÁI TRÍ CUỘC SỐNG THẾ GIỚI LIÊN HỆ

THÔNG TIN CÁ NHÂN | Thông tin tài khoản

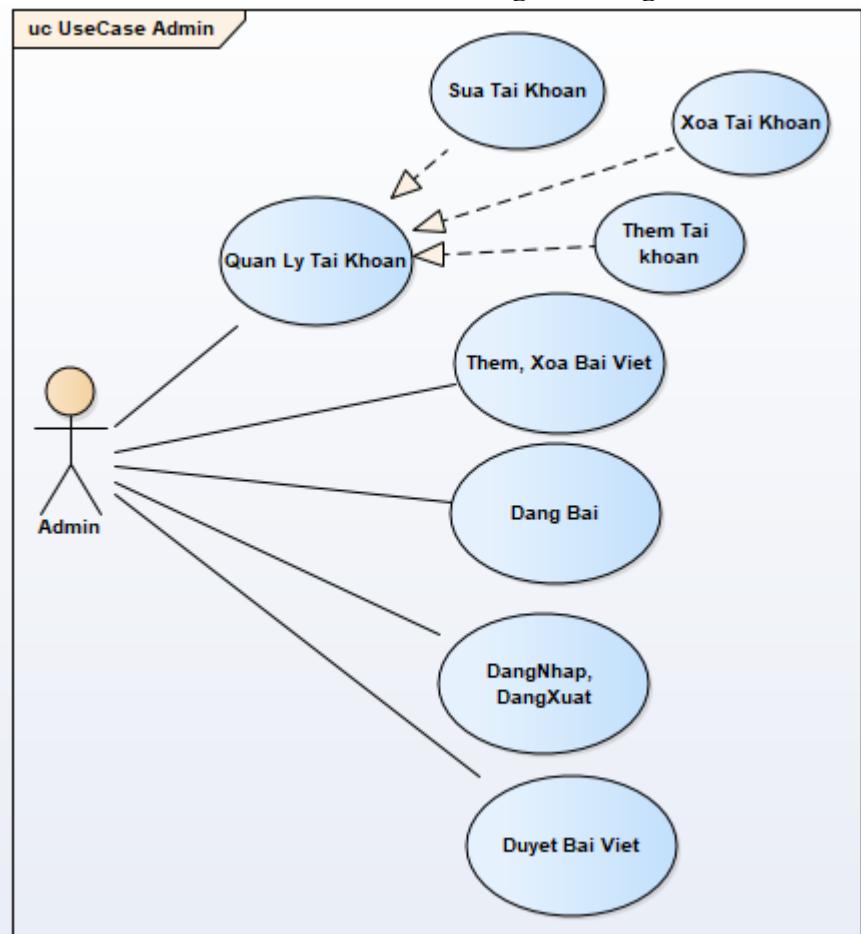
Username: ThienPhan
Password: *****
Họ và tên: Phan Minh Thiện
Ngày Sinh: 01 / 02 / 1997
Số điện thoại: 01697421797
Vai trò: Admin Lưu Thay Đổi

2.3. Đặc tả phần mềm

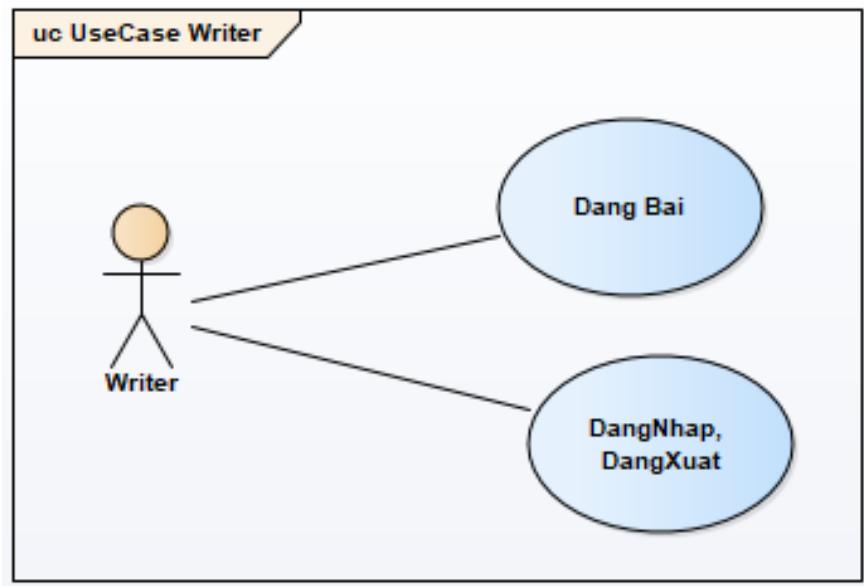
2.3.1. Usecase chức năng phần mềm



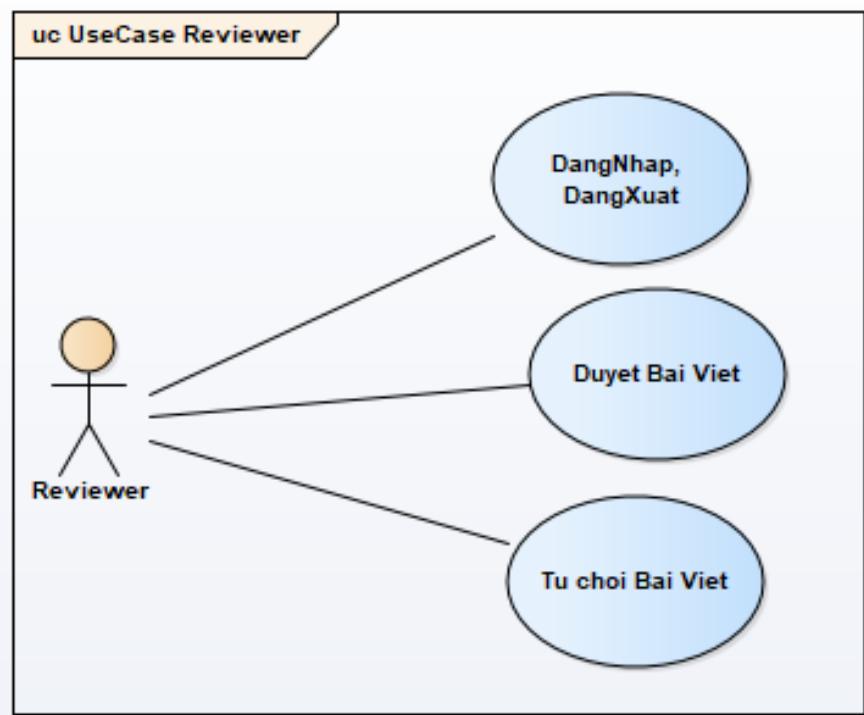
UseCase chung hệ thống



UseCase Admin



UseCase Writer



UseCase Reviewer

2.3.2. Đặc tả Usecase

STT	Tên use case	Mô tả
1	Đăng nhập Đăng xuất	Cho phép người dùng đăng nhập vào hệ thống để sử dụng quyền của mình, đồng thời đăng xuất khỏi hệ thống khi kết thúc công việc.
2	Thêm tài khoản	Cho phép Administrator thêm một tài khoản mới với chức năng do Administrator quy định vào hệ thống

3	Cập nhật tài khoản	Cho phép cập nhật thông tin cá nhân của người dùng sử dụng các chức năng website, tuy nhiên không thể cập nhật quyền hạn trong website khi đã lựa chọn.
4	Xóa tài khoản	Cho phép Administrator xóa một tài khoản đã có khỏi hệ thống tài khoản của website.
5	Thêm bài viết mới	Cho phép Administrator và Writer thêm bài viết vào trạng thái chờ kiểm duyệt của trang web.
6	Sửa bài viết đã có	Cho phép Administrator và Writer cập nhật lại thông tin bài viết đã có và đang ở trạng thái chờ kiểm duyệt để chính xác hơn về mặt nội dung của bài viết.
7	Duyệt bài viết	Cho phép Admin và Reviewer kiểm duyệt bài viết khi Writer đã gửi bài về hệ thống.
8	Tù chối bài viết	Cho phép Admin và Reviewer từ chối bài viết khi không đủ yêu cầu của website.

2.3.3. Xác định và mô tả Actor

STT	Tên Actor	Mô tả
1	Administrator	<ul style="list-style-type: none"> - Quản lý tài khoản (thêm, sửa, xóa tài khoản, cấp quyền cho tài khoản) - Quản lý bài viết (Thêm bài viết, Cập nhật bài viết,...). - Kiểm duyệt bài viết (Phê duyệt, Từ chối)
2	Reviewer	<ul style="list-style-type: none"> - Kiểm duyệt bài viết (Phê duyệt, Từ chối)
3	Writer	<ul style="list-style-type: none"> - Quản lý bài viết ứng với tài khoản tương ứng (Thêm bài viết, Cập nhật bài viết,...)
4	Viewer	<ul style="list-style-type: none"> - Khách vãng lai xem các bài đăng trên trang web

2.4. Thiết kế code

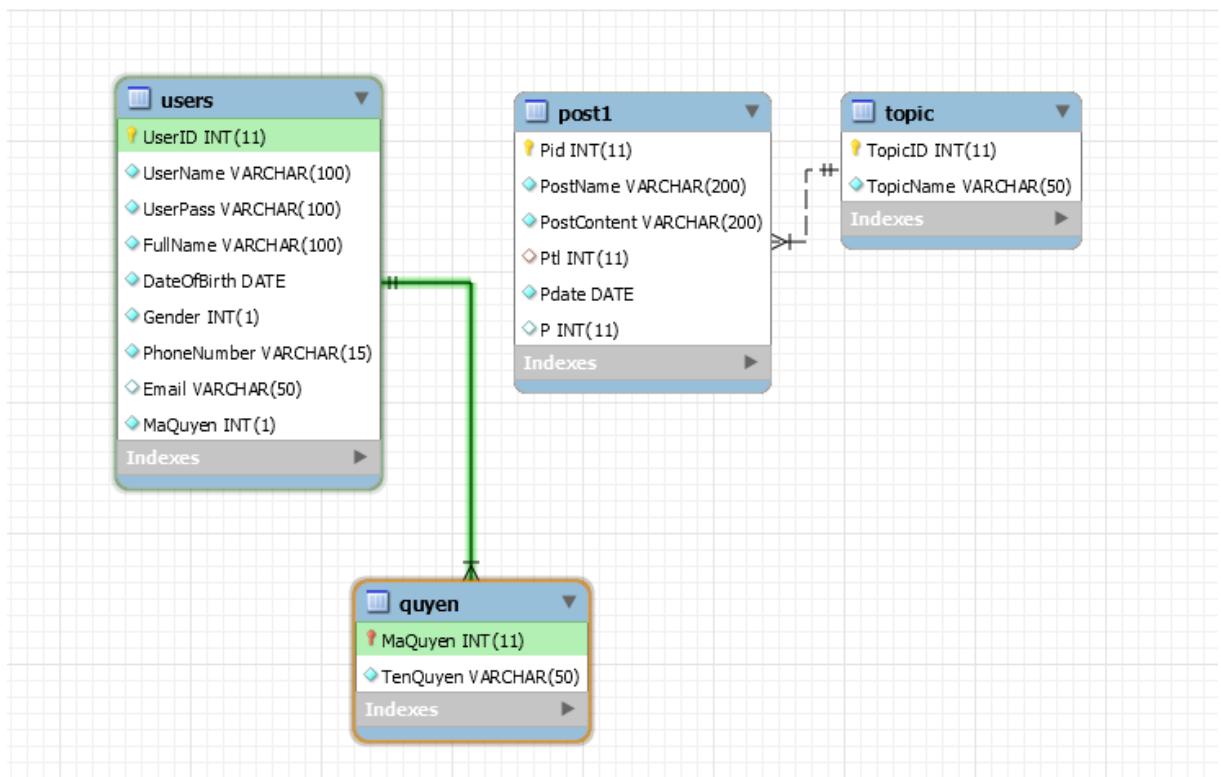
2.4.1. Bảng mô tả các lớp trong chương trình

STT	Tên lớp	Mô tả
1	DBConnection.java	Giải quyết việc kết nối giữa cơ sở dữ liệu và các serverlet xử lý
2	User.java	Lớp trung gian để trao đổi dữ liệu giữa cơ sở dữ liệu và giao diện website
3	Login.java	Xử lý việc đăng nhập vào các trang dành cho

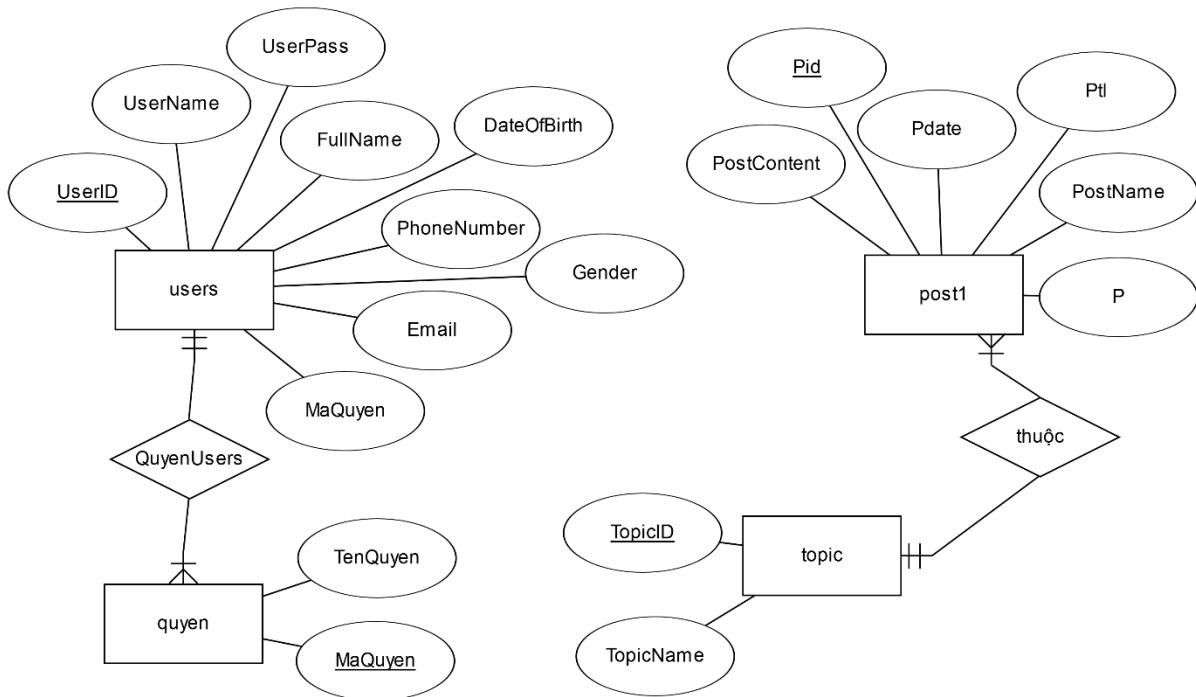
		các tài khoản chức năng của trang web
4	NewAccount.java	Xử lý việc tạo tài khoản mới.
5	Newad.java	Xử lý việc tạo bài viết mới chuyển hướng về khu vực làm việc của administrator
6	Newpost.java	Xử lý việc tạo bài viết mới chuyển hướng về khu vực làm việc của writer
7	Post.java	Lớp trung gian để trao đổi dữ liệu giữa cơ sở dữ liệu và giao diện website
8	Duyet.jsp	Xử lý duyệt bài viết đang chờ
9	Huy.jsp	Xử lý hủy bài viết đang chờ.
10	Xoa.jsp	Xử lý xóa tài khoản

2.5. Thiết kế cơ sở dữ liệu

2.5.1. Mô hình Diagram



2.5.2. Mô hình ERD



2.5.3. Mô tả các bảng trong cơ sở dữ liệu

STT	Tên bảng	Mô tả
1	Users	Lưu trữ thông tin về một tài khoản đăng nhập vào hệ thống. Các thông tin lưu trữ bao gồm username, password, quyền để đăng nhập vào và các thông tin cá nhân khác của người dùng đã đăng ký
2	Post	Lưu trữ các bài viết hiện hữu trong trang web, bao gồm cả bài viết được duyệt và chưa được duyệt.
3	Topic	Danh mục các nội dung chính của trang web được quy định sẵn.

2.5.4. Mô tả các trường trong các bảng

Bảng		User
STT	Trường	Mô tả
1	UserID	Mã người dùng (Số thứ tự) Đây là trường sinh tự động và được dùng làm khóa chính của bảng.
2	Username	Tên người dùng dùng đăng nhập
3	UserPass	Password dùng đăng nhập

4	Fullname	Tên đầy đủ của người dùng tài khoản
5	Phonenumber	Số điện thoại của người dùng (Đây là trường thông tin thêm, số thẻ để giá trị null)
6	Email	Email của người dùng (Đây là trường thông tin thêm, số thẻ để giá trị null)
7	Quyen	Quyền hạn của người dùng trong trang web Bao gồm 3 giá trị cố định tương ứng với Admin, Writer và Reviewer

Bảng		Post
STT	Trường	Mô tả
1	Pid	Mã bài viết Đây là trường khóa chính của bảng
2	Pname	Tên bài viết được người dùng đặt khi tạo bài viết Trường này có số lượng ký tự nhập vào giới hạn.
3	Pcontent	Nội dung của toàn bộ bài viết
4	Pdate	Thời gian bài viết được viết
5	Pstatus	Trạng thái của bài viết bao gồm: Chưa duyệt, Đã duyệt.
6	Ptl	Thể loại của bài viết, được quy định trong danh mục quy định sẵn. Đây là trường khóa ngoại từ bảng Topic
7	Puser	ID của người dùng viết bài viết. Đây là trường khóa ngoại từ bảng Users

Bảng		Topic
STT	Trường	Mô tả
1	TopicID	Mã Topic

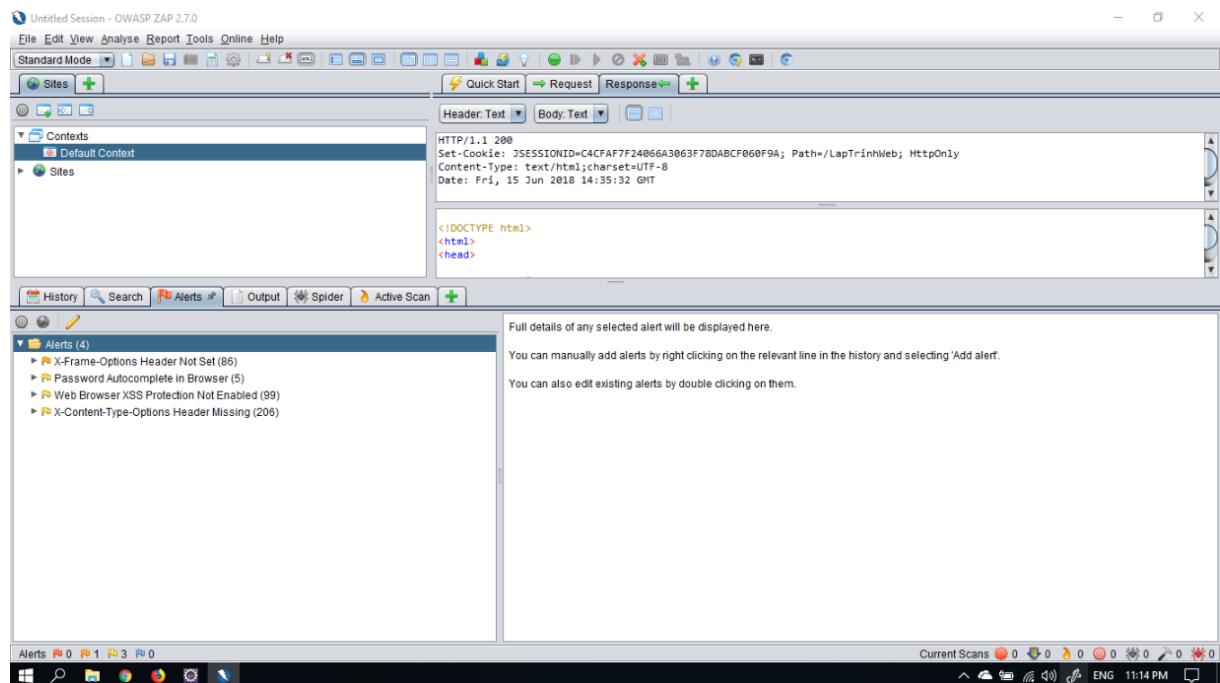
		Đây là trường khóa chính của bảng
2	TopicName	Tên topic

2.6. Chạy Demo

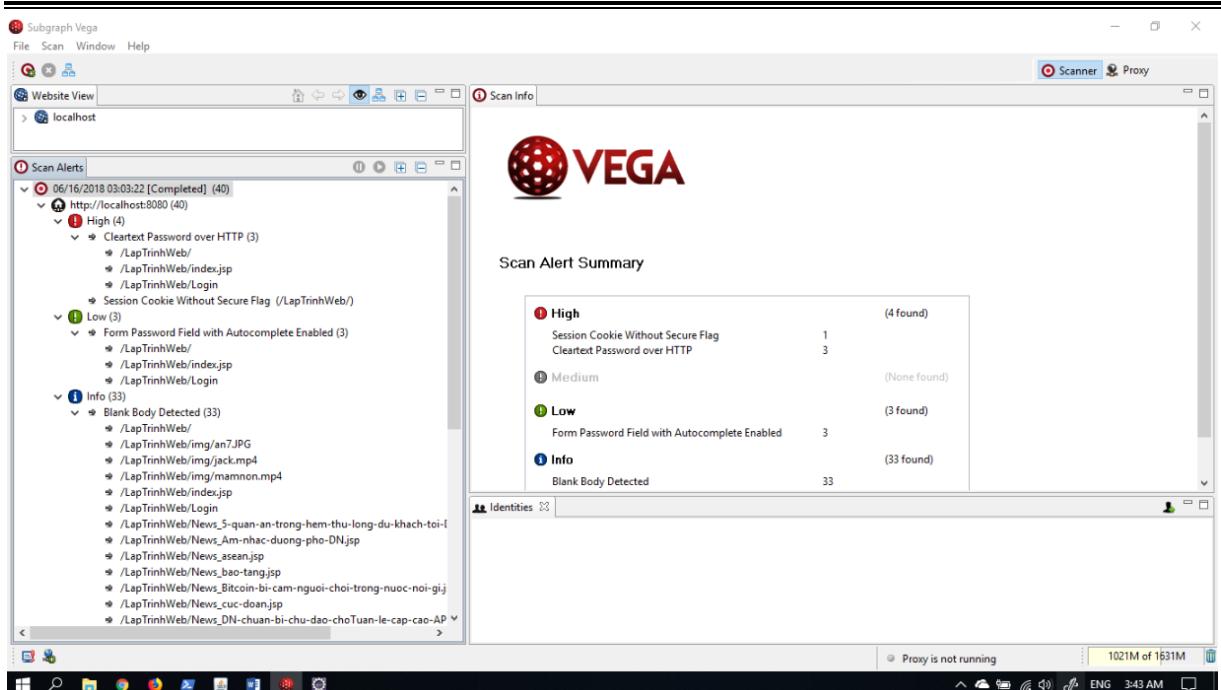
STT	Tên chức năng	Link video demo
1	Chức năng thêm bài viết mới	https://www.youtube.com/watch?v=umBrArFoLLg
2	Chức năng kiểm duyệt bài viết	
3	Chức năng Thêm tài khoản mới	https://youtu.be/Nxj3zoIjLIC
4	Chức năng Xóa tài khoản	https://youtu.be/GIOuu_fXdpo
5	Chức năng xem thông tin tài khoản	https://youtu.be/tfjQmERidi8
6	Chức năng load trang và đăng nhập	https://youtu.be/QMc6z7zn-5Y
7	Load giao diện trang chủ và responsive	https://youtu.be/_MkltoIHW6o

3. BẢO MẬT WEBSITE

3.1. Sử dụng các công cụ quét lỗ hổng bảo mật



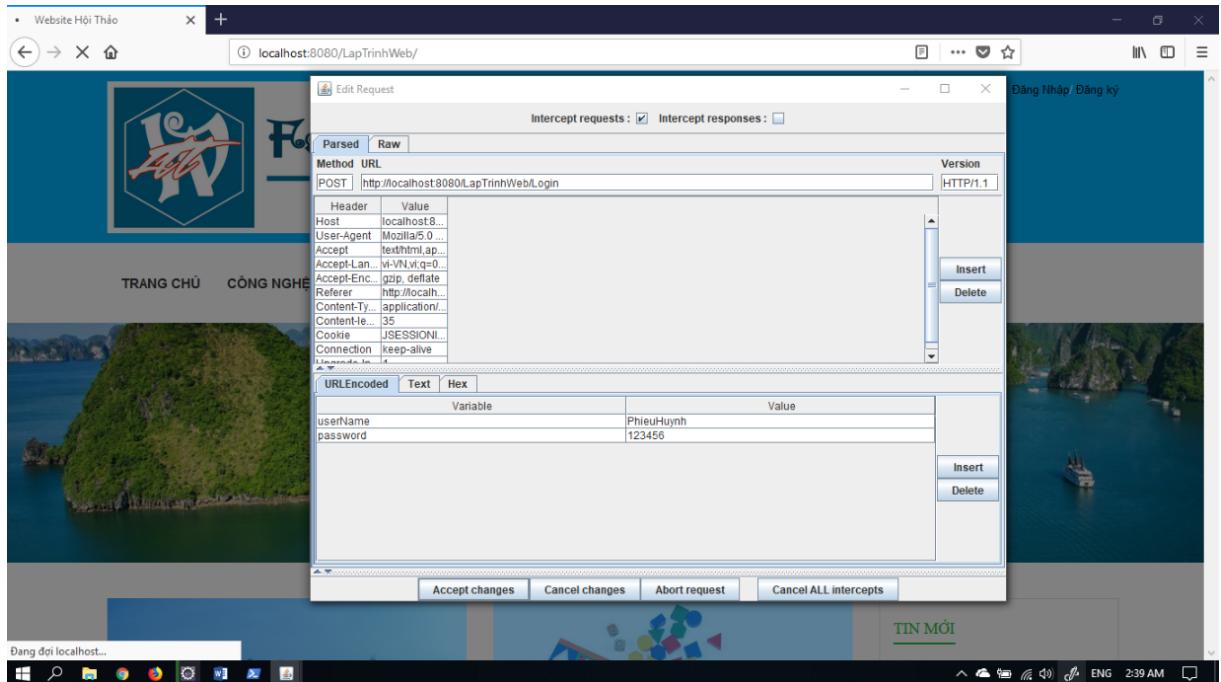
Các lỗi bảo mật kiểm tra thông qua ZAP



Các lỗi bảo mật kiểm tra thông qua VEGA

3.2. Vấn đề bảo mật về chặn gói tin qua mạng thông thường

- Vấn đề:** Khi người dùng nhập thông tin thực hiện đăng nhập tại màn hình đăng nhập và ấn Login, kẻ tấn công có thể đánh chặn gói tin và biết được thông tin username password của người dùng thông qua các thông tin trong request.

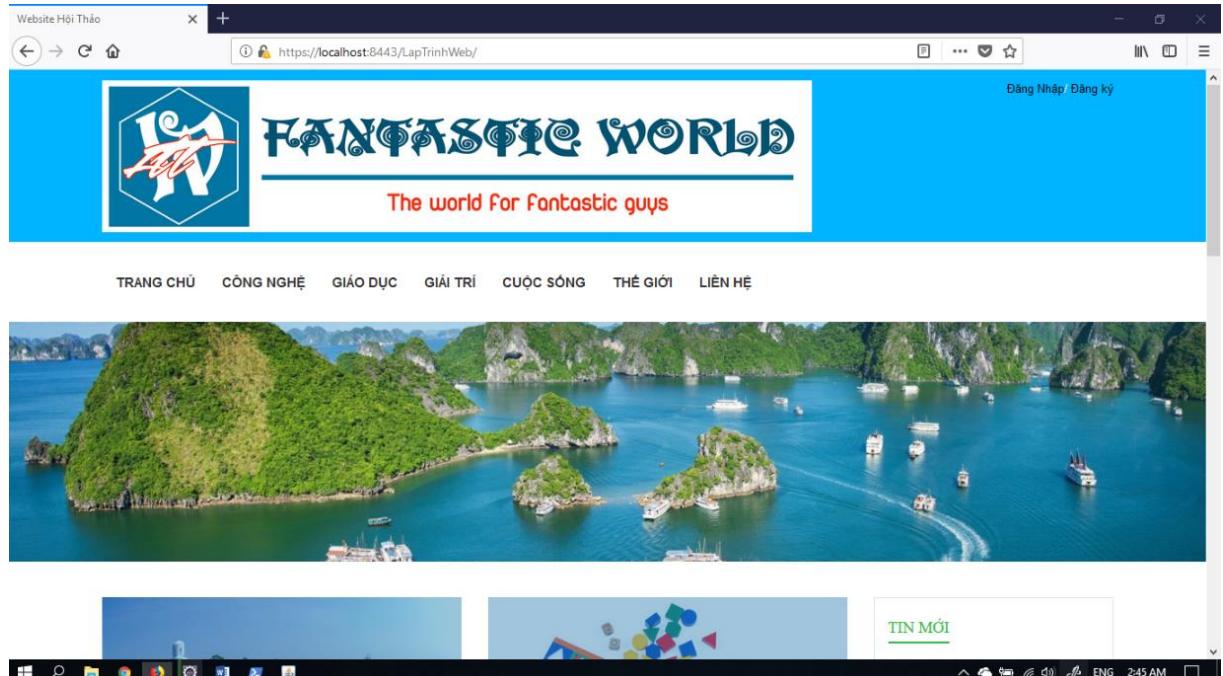


- Nhận định:** Đây là vấn đề cực kỳ quan trọng trong việc bảo mật của trang web. Người dùng có thể dễ dàng bị lấy cấp thông tin tin quan trọng chỉ thông qua một vài thao tác tấn công của hacker.

- Khắc phục:** Đối với vấn đề về đánh chặn gói tin để lấy cấp thông tin tiêu biểu là username, password của người dùng trên trang web đơn giản có 2 phương án khắc phục đơn giản:

+ Mã hóa password gửi đi qua các hàm mã hóa, băm dữ liệu: Việc này có thể thực hiện được và có tỉ lệ cao trong việc đảm bảo an toàn cho thông tin password của người dùng vì việc giải mã mất rất nhiều thời gian và tài nguyên.

+ Sử dụng giao thức mạng bảo mật HTTPS để đảm bảo an toàn cho tất cả gói tin gửi đi và tiếp nhận. Việc này dễ thực hiện và an toàn cho nhiều thông tin khác nhau không chỉ là mật khẩu nhưng lại tốn chi phí cho các chứng chỉ mạng.



Hình trang web sử dụng giao thức HTTPS

3.3. Về Access Control Flaws

3.3.1. Admin đã đăng nhập có quyền xem và xóa tài khoản bất kỳ

- **Vấn đề:** Khi một user được cấp quyền Admin đã đăng nhập vào hệ thống có thể đến trang quản lý tài khoản và kiểm tra thông tin của toàn bộ user trong hệ thống (bao gồm cả tất cả các user - Admin khác). Đồng thời user này có thể chỉnh sửa hoặc xóa hẳn đi thông tin của một user bất kỳ (kể cả admin khác) ra khỏi database nếu sử dụng chức năng xóa.

STT	Username	Password	Họ và tên	Vai trò	Thông tin chi tiết	Thao tác
1	ThienPhan	123456	Phan Minh Thiên	Admin	Xem chi tiết	<button>Xóa</button>
2	PhieuLy	123456	Trần Huỳnh Phiếu	Admin	Xem chi tiết	<button>Xóa</button>
4	ThuyLy	123456	Huỳnh Thị Thúy	Writer	Xem chi tiết	<button>Xóa</button>
5	NghiaLam	123456	Lâm Thành Nghĩa	Writer	Xem chi tiết	<button>Xóa</button>
6	HanhTran	123456	Trần Thị Thuý Hạnh	Writer	Xem chi tiết	<button>Xóa</button>

Hình Danh sách toàn bộ các user được lấy về khi một admin chọn quản lý tài khoản

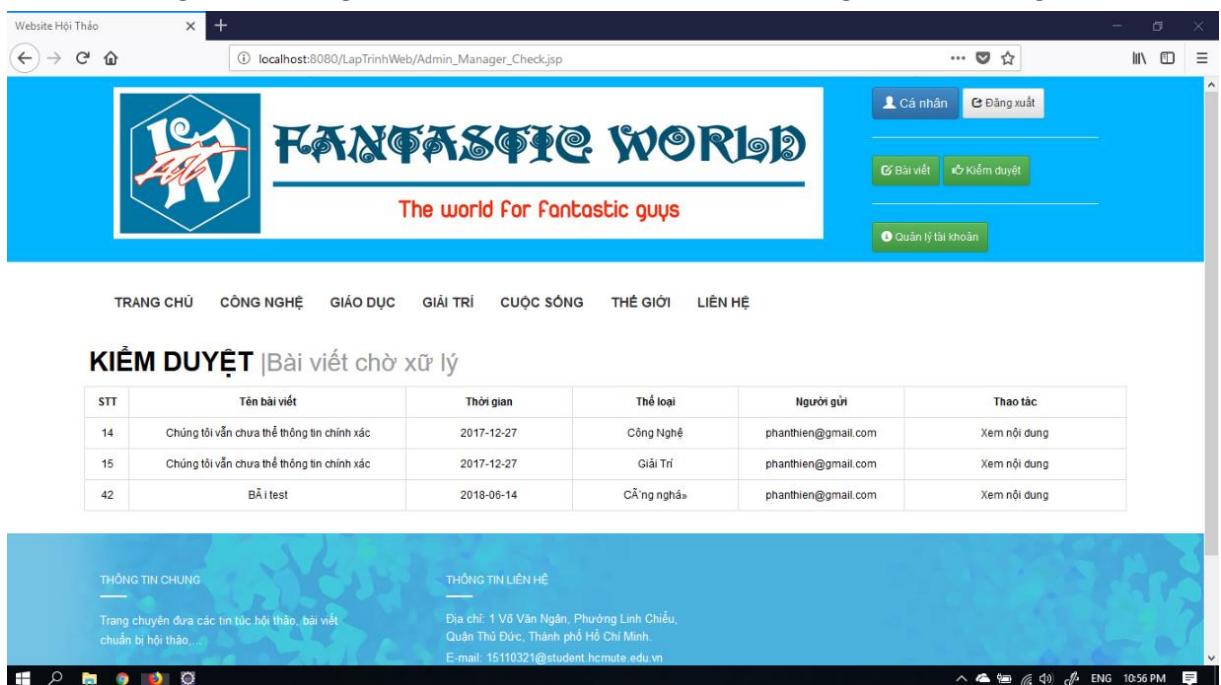
- **Nhận định:** Đây là vấn đề có thể cho qua ở các hệ thống nhỏ (gia đình dùng chung) tuy nhiên lại cực kỳ quan trọng ở các hệ thống lớn ảnh hưởng đến vấn đề phân quyền và bảo mật thông tin của từng người dùng, một tài khoản được cấp quyền admin vô tình hoặc cố ý có thể xóa một hoặc toàn bộ các user khác để chiếm quyền quản lý trang web.

- **Khắc phục:** Bổ sung thêm thuộc tính [ManagerID] vào từng bảng users và thuộc tính này sẽ được lưu thêm vào thông tin từng user khi một Admin tạo tài khoản cho một người dùng bất kỳ (Admin - Reviewer - Writer). Khi xây dựng thuộc tính này dữ liệu thông tin người dùng sẽ được tổ chức theo mô hình đa cấp với một user (có thể là admin) được quản lý bởi một admin (trừ admin đầu tiên của hệ thống) và một admin quản lý nhiều user do mình tạo ra.

3.4. Về Authentication Flaws

3.4.1. Truy suất đến các trang quản lý thông qua URL

- **Vấn đề:** Người dùng bất kỳ (UnAuthentication) có thể truy cập vào các trang quản lý của các người dùng phân quyền như Admin, Reviewer hay Writer nếu có URL đến các trang đó và đồng thời có thể thực hiện các chức năng trên các đang đến được.



The screenshot shows a web browser window titled "Website Hội Thảo". The address bar displays "localhost:8080/LapTrinhWeb/Admin_Manager_Check.jsp". The main content area features a logo with a stylized 'W' and the text "FANTASTIC WORLD" in large blue letters, with the tagline "The world For Fantastic guys" below it. On the right side, there are navigation links for "Cá nhân" (Personal), "Đăng xuất" (Logout), "Bài viết" (Posts), "Kiểm duyệt" (Review), and "Quản lý tài khoản" (Manage account). Below the header, there is a menu bar with links to "TRANG CHỦ", "CÔNG NGHỆ", "GIÁO DỤC", "GIẢI TRÍ", "CUỘC SỐNG", "THẾ GIỚI", and "LIÊN HỆ". The main content area is titled "KIỂM DUYỆT | Bài viết chờ xử lý" and contains a table with the following data:

STT	Tên bài viết	Thời gian	Thể loại	Người gửi	Thao tác
14	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27	Công Nghệ	phanthien@gmail.com	Xem nội dung
15	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27	Giải Trí	phanthien@gmail.com	Xem nội dung
42	BÀI test	2018-06-14	CÔNG NGHỆ	phanthien@gmail.com	Xem nội dung

At the bottom of the page, there are two sections: "THÔNG TIN CHUNG" (General Information) and "THÔNG TIN LIÊN HỆ" (Contact Information). The "THÔNG TIN CHUNG" section includes a note about the site being a news portal where users can post and review articles. The "THÔNG TIN LIÊN HỆ" section provides the address: 1 Võ Văn Ngân, Phường Linh Chiểu, Quận Thủ Đức, Thành phố Hồ Chí Minh, and the email: 15110321@student.hcmute.edu.vn. The browser status bar at the bottom shows the date and time as 10:56 PM.

Giao diện truy cập thành công mặc dù không đăng nhập

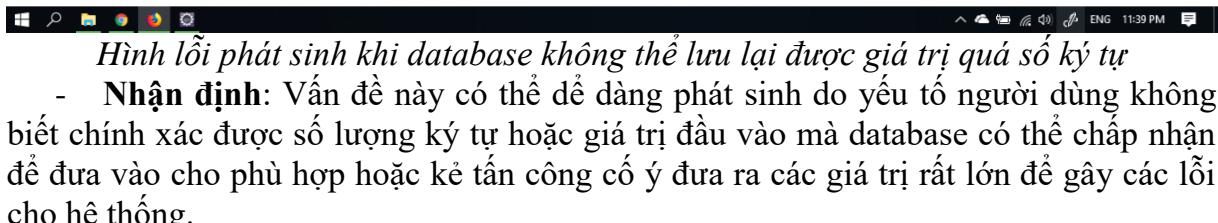
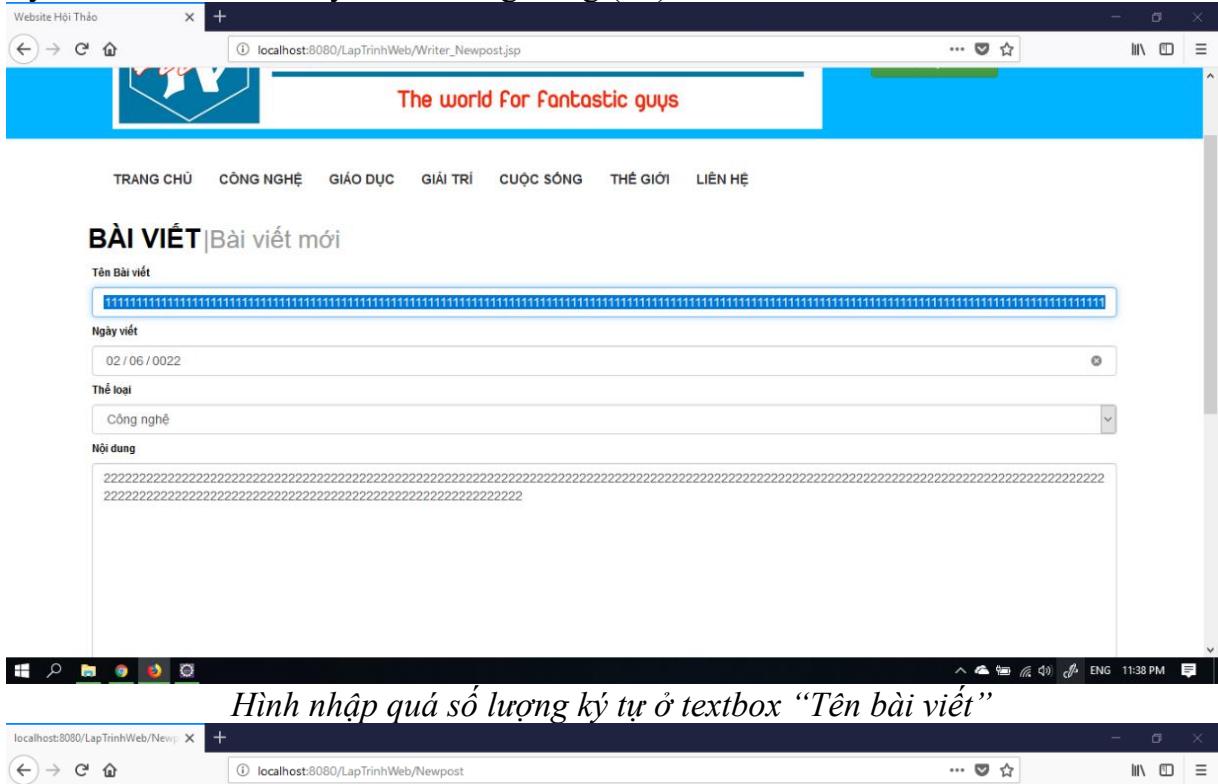
- Nhận định: Ở các trang có quản lý thông qua tài khoản dành riêng cho các nhóm người dùng nhất định chưa có kiểm tra lại phiên đăng nhập của các tài khoản truy suất đến từ đó mà bất cứ người dùng nào cũng có thể truy cập vào các trang quản lý nếu có URL.

- Khắc phục: Bổ sung thêm Controller **CheckPower** với chức năng kiểm tra ba yếu tố [username + password + quyền] khi có một truy cập bất kỳ đến với một trang chức năng bất kỳ. Nếu đảm bảo ba yếu tố trên là khớp nhau thì có thể truy cập vào trang và tiếp tục thực hiện các chức năng, sai một trong ba phải được chuyển hướng về trang chủ hoặc báo lỗi. Thực hiện thông qua việc kiểm tra HttpSession với các thông số yêu cầu nêu trên.

3.5. Về Buffer Overflows

3.5.1. Vuột số lượng ký tự quy định của các trường trong database

- **Vấn đề:** Database đã cố định một số lượng ký tự nhất định cho các trường trong các bảng. Tuy nhiên nếu nhiều dùng nhập quá số lượng ký tự này trong các textbox và gửi đi (thêm, sửa nội dung bài viết hoặc tài khoản) sẽ dẫn đến việc hệ thống không xử lý được dữ liệu và chuyển đến trang trống (lỗi)



-
- **Khắc phục:** Bổ sung việc kiểm tra giá trị đầu vào từng textbox trước khi cho phép người dùng gửi đi request thêm hoặc cập nhật database hoặc gán các giá trị vượt quá về một giá trị cố định trong phạm vi cho phép để tránh phát sinh lỗi do vượt quá số lượng cho phép này.

3.5.2. Giới hạn độ dài các textbox hoặc textarea không tác dụng với những kẻ tấn công

- **Vấn đề:** Mặc dù đã giới hạn độ dài các textbox, kẻ có ý định tấn công có thể chặn gói tin trước khi gửi lên server và thêm ký tự vào gói tin gửi đi với độ dài tùy ý. Khi tới server, gói tin có kích thước rất lớn vừa làm tràn bộ nhớ, tràn bộ đệm, vừa gây ra lỗi khi lưu xuống cơ sở dữ liệu mà không qua kiểm tra

- **Khắc phục:**

- + Ngoài việc giới hạn độ dài ở các textbox để tránh lỗi sai của người dùng, cần kiểm tra lại tại server để đảm bảo không bị lỗi stack/buffer overflows
- + Tiến hành kiểm tra theo hai bước:

Bước 1 là kiểm tra độ dài của request trước khi đọc dữ liệu từ request, nếu thấy kích thước request lớn quá mức cho phép, ngưng xử lý với request đó

```
@Override  
protected void doPost(HttpServletRequest req, HttpServletResponse resp) throws IOException {  
    System.out.println("/NewPost");  
    // kiểm tra nếu dữ liệu đầu vào trong request quá lớn  
    if (req.getContentLengthLong() > 50000) {  
        System.out.println("/NewPost: dữ liệu đầu vào quá lớn, trả lại trang chủ");  
        resp.sendRedirect(req.getContextPath() + "/");  
        return;  
    }  
}
```

Bước 2 là kiểm tra các giá trị dữ liệu trước khi lưu vào database để đảm bảo các ràng buộc dữ liệu trong database không bị sai

```
String PostName = req.getParameter("P_name");  
String PostContent = req.getParameter("txtcontent");  
String Pdate = req.getParameter("P_date");  
String Ptl = req.getParameter("P_tl");  
if (PostName.length() > 100) {  
    System.out.println("/NewAd: error vượt quá kích thước của PostName");  
    return;  
} else if (PostContent.length() > 20000) {  
    System.out.println("/NewAd: error vượt quá kích thước của PostContent");  
    return;  
} else if (Pdate.length() > 10) {  
    System.out.println("/NewAd: error vượt quá kích thước của Pdate");  
    return;  
} else if (Ptl.length() > 15) {  
    System.out.println("/NewAd: error vượt quá kích thước của Ptl");  
    return;  
}
```

3.6. Về Code Quality

- **Nhận định:** Trang web không gấp phai vấn đề về chất lượng code, không có các ghi chú để lại thông tin user trong nội dung trang web, không có đặt cố định các giá trị đăng nhập sử dụng trong quá trình rút ngắn thời gian kiểm thử phần mềm, không có các giá trị session, cookie được ghi sẵn,....

3.7. Về Concurrency

- **Nhận định:** Trang web không gặp phải các vấn đề bảo mật về việc truy cập đồng thời do sử dụng các phương thức để cơ sở dữ liệu đơn giản và nhiều thao tác đã xử lý dữ liệu ở phía client và gửi đi chứ không dùng thuộc tính để nhiều client truy cập đồng thời. Cụ thể tại các phương thức như sau
 - Phương thức Login: Khi yêu cầu login được gửi đi thông qua phương thức POST các thông tin người dùng sẽ được lấy về máy client và so sánh với các đối số thu được từ giao diện đăng nhập ở dạng thuộc tính ký tự nên không thể có sự truy cập đồng thời đến việc đăng nhập gây sai khác dữ liệu.
 - Phương thức NewAccount và phương thức NewPost: Tất cả các giá trị trên form tạo mới được lưu lại dưới dạng thuộc tính - biến hàm và trở thành các đối số cho câu lệnh SQL nên không thể diễn ra sự thay đổi dữ liệu ở các truy cập khác dù là cùng một user truy cập ở các thiết bị độc lập khác.

3.8. Về Cross site Scripting

3.8.1. Stored XSS

- **Nhận định:** Trang web gặp phải vấn đề về kiểu tấn công Cross-site Scripting khi lưu vào cơ sở dữ liệu (Stored XSS). Dẫn đến người đọc dữ liệu ra sẽ bị tấn công XSS

The screenshot shows a Microsoft Edge browser window with the URL `localhost:9999/WebSecurity/Admin_Newpost.jsp`. The page title is "BÀI VIẾT | Bài viết mới". There are several input fields: "Tên Bài viết" containing "`Bai viet tan cong XSS <script>prompt('vui long dang nhap lai');</script>`", "Ngày viết" set to "06 / 15 / 2018", "Thể loại" set to "Giáo dục", and a large "Nội dung" text area. At the bottom, there is a note: "Tôi chắc chắn về nội dung đăng tải là hợp pháp và đảm bảo tuân phong mỹ tục." and two buttons: "Gửi bài viết" (in green) and "Hủy".

The screenshot shows a Windows taskbar at the bottom and a table titled "PostName" with columns "Pid" and "PostName". The table contains the following data:

Pid	PostName
12	Việt Nam đã đón gần 140 lượt máy bay du hoi nahi APEC
13	Chiều 7/11, trao đổi với Zing.vn
14	Chúng tôi vẫn chưa thể thông tin chính xác
15	Chúng tôi vẫn chưa thể thông tin chính xác
16	Chúng tôi vẫn chưa thể thông tin chính xác
17	Chúng tôi vẫn chưa thể thông tin chính xác
56	Bai viet tan cong XSS <script>prompt('vui long dang nhap lai');</script>
NULL	NULL

Kết quả khi hacker lưu được đoạn mã tấn công XSS vào database

- **Khắc phục:** Tiến hành kiểm tra các request bằng servlet filter. Gắn filter vào trước các controller cần kiểm tra, filter có nhiệm vụ lọc bỏ các đoạn mã có khả năng là mã độc dạng html, java script...

```

// Avoid null characters
cleanValue = cleanValue.replaceAll("\0", "");
// Avoid anything between script tags
Pattern scriptPattern = Pattern.compile("<script>(.*)</script>", Pattern.CASE_INSENSITIVE);
cleanValue = scriptPattern.matcher(cleanValue).replaceAll("");
// Avoid anything in a src='...' type of expression
scriptPattern = Pattern.compile("src[\r\n]*=[\r\n]*\\'(.*)\\'", Pattern.CASE_INSENSITIVE | Pattern.MULTILINE | Pattern.DOTALL);
cleanValue = scriptPattern.matcher(cleanValue).replaceAll("");
scriptPattern = Pattern.compile("src[\r\n]*=[\r\n]*\\\"(.*)\\\"", Pattern.CASE_INSENSITIVE | Pattern.MULTILINE | Pattern.DOTALL);
cleanValue = scriptPattern.matcher(cleanValue).replaceAll("");
// Remove any lonesome </script> tag
scriptPattern = Pattern.compile("</script>", Pattern.CASE_INSENSITIVE);
cleanValue = scriptPattern.matcher(cleanValue).replaceAll("");
// Remove any lonesome <script ...> tag
scriptPattern = Pattern.compile("<script(.*)>", Pattern.CASE_INSENSITIVE | Pattern.MULTILINE | Pattern.DOTALL);
cleanValue = scriptPattern.matcher(cleanValue).replaceAll("");
// Avoid eval(...) expressions
scriptPattern = Pattern.compile("eval\\((.*?)\\)", Pattern.CASE_INSENSITIVE | Pattern.MULTILINE | Pattern.DOTALL);
cleanValue = scriptPattern.matcher(cleanValue).replaceAll("");
// Avoid expression(...) expressions
scriptPattern = Pattern.compile("expression\\((.*?)\\)", Pattern.CASE_INSENSITIVE | Pattern.MULTILINE | Pattern.DOTALL);

```

Một số code dùng lọc bỏ các dạng mã XSS

```

<filter>
    <filter-name>XSSFilter</filter-name>
    <filter-class>xssFilter.XSSFilter</filter-class>
</filter>

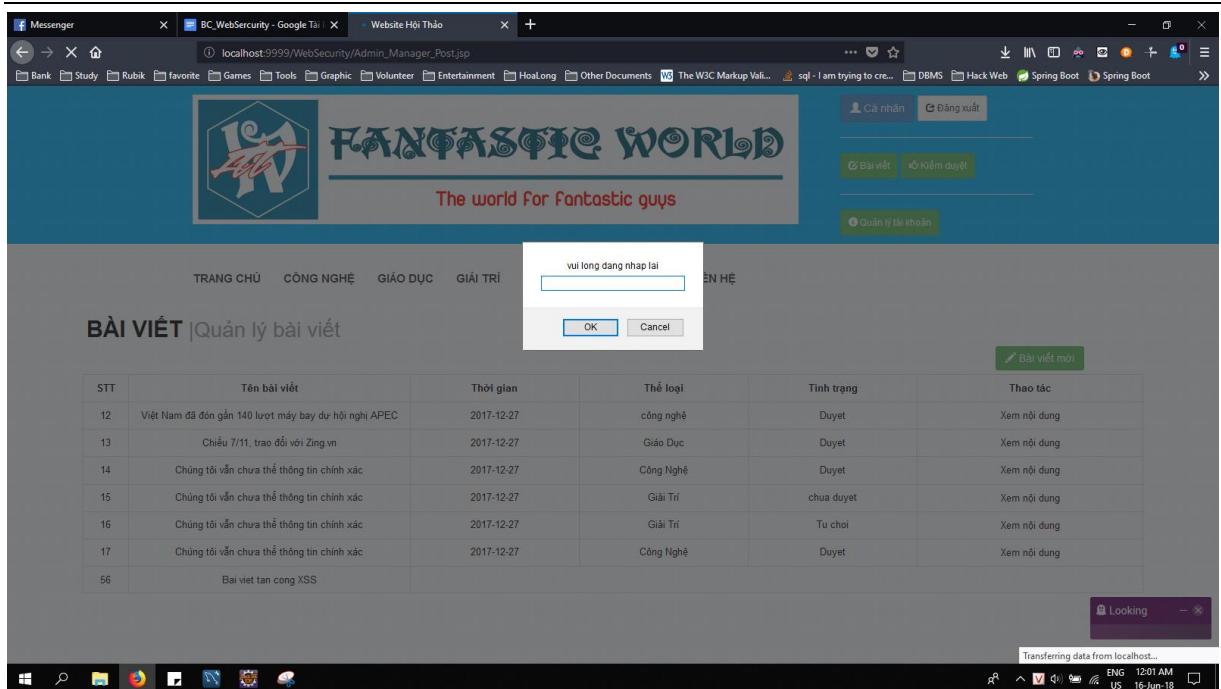
<filter-mapping>
    <filter-name>XSSFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>

```

Khai báo sử dụng filter

3.8.2. Đọc dữ liệu có sẵn mã độc tấn công XSS

- **Nhận định:** Dữ liệu trong database nếu đang có khả năng tấn công XSS, người dùng đọc nó từ cơ sở dữ liệu sẽ bị tấn công XSS



Hình ảnh bị tấn công XSS khi đọc dữ liệu từ hệ thống

- **Khắc phục:** Ngoài việc kiểm tra khi lưu vào cơ sở dữ liệu bằng Filter. Cơ sở dữ liệu có thể bị thay đổi không thông qua ứng dụng web và vẫn có khả năng bị tấn công XSS. Vì vậy cần kiểm tra khi đọc dữ liệu từ cơ sở dữ liệu để chống tấn công XSS

```
public class HtmlEncoder {
    public static String escapeHTML(String s) {
        StringBuilder out = new StringBuilder(Math.max(16, s.length()));
        for (int i = 0; i < s.length(); i++) {
            char c = s.charAt(i);
            if (c > 127 || c == '"' || c == '<' || c == '>' || c == '&') {
                out.append("&#");
                out.append((int) c);
                out.append(';');
            } else {
                out.append(c);
            }
        }
        return out.toString();
    }
}
```

Hàm lọc bỏ kí tự html

```

<td><%=HtmlEncoder.escapeHTML(resultset.getString(1))%></td>
<td><%=HtmlEncoder.escapeHTML(resultset.getString(2))%></td>
<td><%=HtmlEncoder.escapeHTML(resultset.getString(3))%></td>
<td><%=HtmlEncoder.escapeHTML(resultset.getString(4))%></td>
<td><%=HtmlEncoder.escapeHTML(resultset.getString(5))%></td>

<%-- <td><%=resultset.getString(1)%></td>
<td><%=resultset.getString(2)%></td>
<td><%=resultset.getString(3)%></td>
<td><%=resultset.getString(4)%></td>
<td><%=resultset.getString(5)%></td> --%>

```

Chỉnh sửa, thêm phần kiểm tra ở những chỗ đọc dữ liệu ra

BÀI VIẾT |Quản lý bài viết

STT	Tên bài viết	Thời gian
12	Việt Nam đã đón gần 140 lượt máy bay dự hội nghị APEC	2017-12-27
13	Chiều 7/11, trao đổi với Zing.vn	2017-12-27
14	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27
15	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27
16	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27
17	Chúng tôi vẫn chưa thể thông tin chính xác	2017-12-27
56	Bài viết tan cong XSS <script>prompt("vui long dang nhap lai");</script>	2018-06-15

Không còn chạy đoạn script khi đọc dữ liệu

3.9. Về Injection Flaws

- Nhận định: Trang web có gặp phải một vài vấn đề về việc tiêm nhiễm các câu lệnh SQL vào các phương thức có truy vấn đến database. Việc này xuất phát từ việc đã sử dụng các đối số cho câu lệnh truy vấn SQL dưới dạng ký tự “?” ở phần lớn các câu lệnh truy vấn SQL nhưng một số truy vấn khác lại không được thực hiện (chủ yếu ở các trang .jsp) nên trang web không thể bị tấn công thông qua việc tiêm nhiễm ở các phương thức trong package Controller nhưng vẫn có thể bị tấn công ở các câu lệnh viết ngay trong trang jsp truyền trực tiếp dữ liệu.

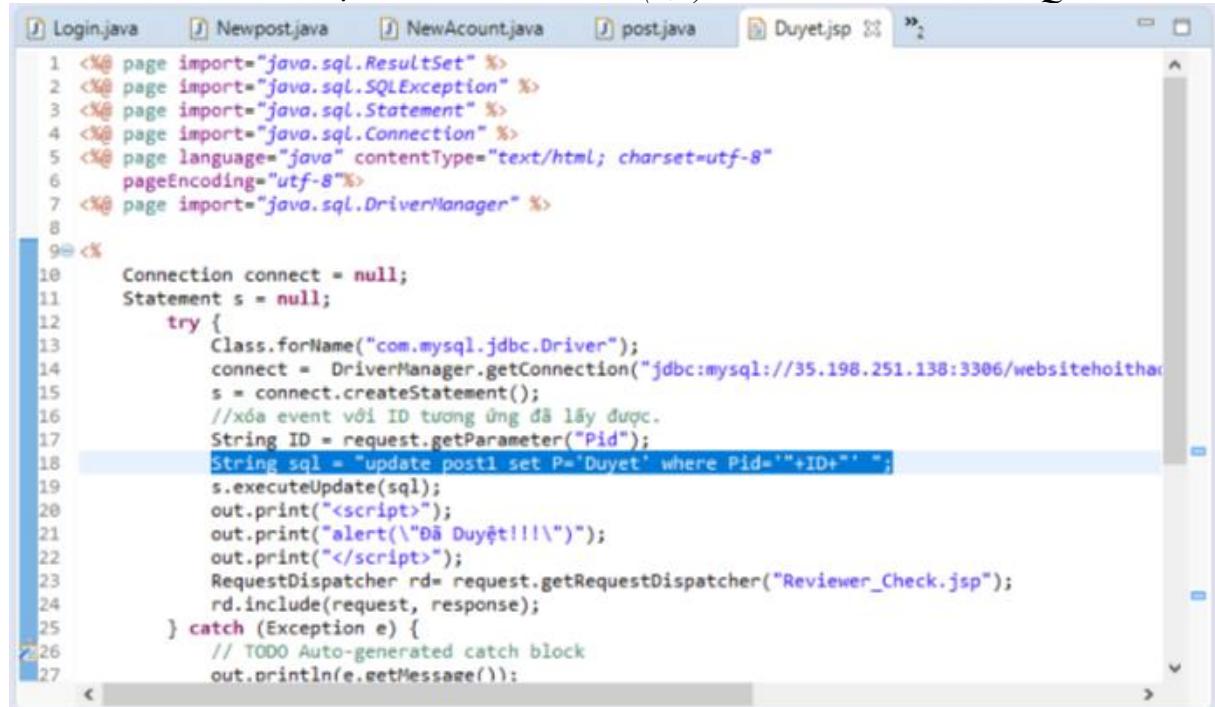
- Việc xác định này khó khăn hơn cho những người tấn công vì không biết chính xác cấu trúc trang web ở phương thức xử lý nào thì có thể tấn công SQL Injection, tuy nhiên vẫn là vẫn đề phải được khắc phục để đảm bảo tất cả các vấn đề liên quan đến SQL Injection

```

1 package DAO;
2
3
4 import java.sql.PreparedStatement;
5
6
7 public class post {
8     public static Integer add(String PostName, String PostContent) throws SQLException, ClassNotFoundException {
9         try {
10             String str= "insert into post(PostName,PostContent) values (?,?)";
11
12             PreparedStatement pst = DBConnection.connect().prepareStatement(str);
13             pst.setString(1, PostName);
14             pst.setString(2, PostContent);
15             int i= pst.executeUpdate();
16             return i;
17         }catch(SQLException se) {
18             return -1;
19         }
20     }
21 }
22
23

```

Hình câu lệnh Insert với “value (?,?)” để tránh tiêm nhiễm SQL



```

1 <%@ page import="java.sql.ResultSet" %>
2 <%@ page import="java.sql.SQLException" %>
3 <%@ page import="java.sql.Statement" %>
4 <%@ page import="java.sql.Connection" %>
5 <%@ page language="java" contentType="text/html; charset=utf-8"
6 pageEncoding="utf-8"%>
7 <%@ page import="java.sql.DriverManager" %>
8
9 <%
10 Connection connect = null;
11 Statement s = null;
12 try {
13     Class.forName("com.mysql.jdbc.Driver");
14     connect = DriverManager.getConnection("jdbc:mysql://35.198.251.138:3306/websitehoithao");
15     s = connect.createStatement();
16     //xóa event với ID tương ứng đã lấy được.
17     String ID = request.getParameter("Pid");
18     String sql = "update post1 set P='Duyet' where Pid='"+ID+"'";
19     s.executeUpdate(sql);
20     out.print("<script>");
21     out.print("alert(\"Đã Duyệt!!!\"');");
22     out.print("</script>");
23     RequestDispatcher rd= request.getRequestDispatcher("Reviewer_Check.jsp");
24     rd.include(request, response);
25 } catch (Exception e) {
26     // TODO Auto-generated catch block
27     out.println(e.getMessage());

```

Hình Một số câu lệnh SQL vẫn chưa được truyền đổi số tránh Injection