Môn: Kiến trúc tích hợp hệ thống
Hồ Phúc Lâm - Thực hành 09 – 23/10/2024

Bài 8:

Web site phục vụ cho việc quảng bá thông tin cần thiết của trường bao gồm các hạng mục: tin tức, quảng cáo, công tác hỗ trợ, tuyển sinh và diễn đàn. Hệ thống phải chạy nhanh, đáp ứng 100 người truy cập cùng lúc và chạy 24/24 đảm bảo tính dự phòng và bảo mật. Để đảm bảo điều đó hệ thống phải có 4 máy chủ web server, 4 database server chạy SQL server/Oracle, và có 2 tường lửa để kiểm soát. Có 8 đường truyền tốc độ 100 Mbs (trong nước) và 10 Mbs(quốc tế) với hai nhà cung cấp khác nhau hoạt động theo cơ chế stand-by được dấu nối vào 4 thiết bị router khác nhau. Web site phải chia thành các module dựa theo yêu cầu. Dữ liệu trung bình 10TB/năm. Mục tin tức bao gồm các sự kiện liên quan đến hoạt động của trường; mục quảng cáo bao gồm các thông tin quảng cáo ví dụ như thành tích của nhà trường được báo đài khen tặng; mục công tác hỗ trợ nhằm giúp đỡ giảng viên, sinh viên của trường, những giảng viên hay sinh viên có thể vào đây xem thông tin về các khoản mục giúp đỡ sau đó liên hệ trực tiếp với phòng; công tác phục vụ tuyển sinh bao gồm các thông tin liên quan đến việc tuyển sinh các khóa khác nhau; và cuối cùng là phần diễn đàn cho phép mọi người có thể đăng tin (khi có tài khoản) và xem các mục tin trong diễn đàn. Liên quan đến việc quản lý các thông tin khác nhau trên web site được phân quyền như sau: việc quảng bá thông tin và quảng cáo sẽ do phòng PR của trường đảm nhiệm chỉ có các nhân viên trong phòng PR mới có quyền đăng bài, những người còn lại chỉ được xem mà thôi. Tương tự cho thông tin hỗ trợ chỉ có các nhân viên trong phòng Hỗ trợ mới có quyền đăng bài, còn lại chỉ được xem.Tất cả tài khoản sẽ do admin quản lý. Hệ thống có khả năng reset mật khẩu tự động khi có yêu cầu từ người dùng. Tất cả thông tin đăng trên web site đều có thể truy cập bên trong và ngoài trường. Mục thông tin tuyển sinh cũng được phân quyền chỉ có nhân viên phòng tuyển sinh mới có quyền đăng bài còn lại chỉ xem. Phần diễn đàn được quản lý như sau chỉ có tài khoản admin (quản trị web site) mới có quyền tạo các hạng mục khác nhau, có quyền xóa bài của những người khác, các tài khoản còn lại chỉ có quyền đăng bài khi có tài khoản (tài khoản do nguoi dùng tự tạo) và chỉ được xóa bài của mình đăng.

Yêu cầu:

Câu 1: Viết RFP (request for proposal) cho hệ thống Web site trên
Câu 2:

- **Functional testing**
- **Security testing**

THỰC HÀNH

Câu 1: viết RFP (request for proposal) cho hệ thống Web site trên

1.Kiểm tra chức năng

Cũng như bất kỳ một ứng dụng nào khác, việc kiểm thử xem ứng dụng web có được xây dựng đúng với yêu cầu (requirements) của khách hàng hay không là điều tiên quyết và quan trọng nhất.

- ***Kiểm tra nội dung giao diện trên trang web:*** Mỗi thành phần button, textbox, image, link trên page và bố cục page cần tuân theo chính xác kích thước và vị trí mà bản thiết kế UI quy định. Đa số các bản thiết kế đều kèm theo mockup/wireframe để chỉ rõ kích thước và vị trí, màu sắc, cỡ chữ và bố cục từng trang web. Bạn cần so sánh đối chiếu giữa mockup và nội dung thực sự hiển thị trên browser.
- ***Kiểm tra các link & menu***: Kiểm tra tất cả link nội bộ (internal link) và link ngoại bộ (external link) xem chúng có hoạt động không, có trỏ đến đúng địa chỉ mong muốn không. Bạn cần bảo đảm các link email sẽ mở ra trình soạn email mặc định khi user click vào. Ngoài ra, các link không được tự trỏ đến vị trí của chính nó và không tồn tại các orphan page.
- ***Kiểm tra các form nhập dữ liệu:*** Đảo đảm các trường (field) dữ liệu được thiết kế đúng dạng, luôn có giá trị mặc định, luôn có bộ lọc kiểm tra (validation) những thông tin user nhập vào xem có hợp lệ không trước khi submit. Ngoài ra, quá trình chuyển tải thông tin từ browser đến server cũng cần bảo đảm là thông tin gửi đi khớp với những gì user nhập vào, không thất lạc và bị sai lệch.
- ***Kiểm tra lỗi cú pháp html/css:*** Xác định các tag CSS 404 trả lại hoặc lỗi tải khác CSS. Xác định trên HTML id, class, và các thuộc tính tên không phù hợp với bất kỳ thẻ CSS nào.
- ***Kiểm tra cookie (browser) & session (server)*** Kiểm tra các ứng dụng đăng nhập trong phiê n bằng cách cho phép và vô hiệu hóa các tập tin cookie. Cookie thử nghiệm ti êu c ực bằng cách sử dụng một tên miền không phối hợp. Kiểm tra xem cookie phiên thiết lập lại giữa các phiên trình duyệt. Kiểm tra bảo mật ứng dụng bằng cách xóa các tập tin cookie có chọn lọc trong khi ki ểm tra hoạt động .

- ***Kiểm tra bản dịch (localization):*** Nếu ứng dụng của bạn hỗ trợ đa ngôn ngữ, test bản dịch từng ngôn ngữ là cần thiết để bảo đảm quá trình dịch và gắn ráp không có sự cố "râu ông này cắm cằm bà kia", hoặc bản dịch không sát nghĩa, bị tràn dòng khi dịch, v…v..
- ***Kiểm tra database:*** Kiểm tra dữ liệu thống nhất trong các hình thức web cơ sở dữ liệu theo định hướng Kiểm tra chức năng tạo, chỉnh sửa, xóa, cập nhật công việc . Kiểm tra dữ liệu cung cấp dữ liệu chính xác . Xác định kết nối cơ sở dữ liệu và các lỗi truy vấn .

2.Kiểm tra khả năng sử dụng

Việc thiết kế và trình bày của một ứng dụng có ảnh hưởng lớn đến thành công người dùng của bạn sẽ có trong việc sử dụng các ứng dụng Web.

- ***Kiểm tra nội dung***
    - Kiểm tra nội dung là hợp lý sắp xếp và dễ dàng cho người sử dụng hiểu.
    - Kiểm tra lỗi chính tả.
    - Kiểm tra xem trang adhear đến m àu s ắc và hoa văn hướng dẫn phong cách, bao gồm phông chữ, khung hình, và biên giới.
    - Kiểm tra xem các h ình ảnh tải một cách chính xác và có kích thước phù hợp.
- ***Kiểm tra các logic liên kết và hướng dẫn***
    - Người dùng luôn cần hướng dẫn và liên kết ở mọi nơi, mọi lúc và càng súc tích cô đọng càng tốt. Nên bảo đảm mọi thao tác trên trang web đều được hướng dẫn và gợi ý thông qua các tooltip, các thông báo, sitemap, các liên kết và hình ảnh nếu cần.
- ***Kiểm tra văn hóa khu vực và đối tượng sử dụng***
    - Điều này bắt nguồn từ đặc điểm riêng của từng lĩnh vực (ví dụ y khoa thường dùng màu sáng để thể hiện sự sạch sẽ), hoặc văn hóa riêng từng khu vực (người châu á thường chuộng tông màu nóng và cầu kỳ hơn châu âu).
    - Thêm vào đó, trong quá trình test, bạn hãy luôn bảo đảm rằng chuẩn thiết kế web app của bạn có thể được tìm thấy phổ biến ở nhiều web app khác. Vd

như button login, logout thường nằm ở góc trên bên phải và menu chính luôn nằm ở trên cho tất cả trang web con. Nếu một trang web khoa học trình bày bằng font chữ cách điệu lòe loẹt, tiêu đề chạy ngang dọc, hoặc một trang web dành cho trẻ em lại chỉ dùng 2 tông màu đen trắng buồn tẻ thi nên góp ý với bộ phận thiết kế.

3. Kiểm tra sự tương thích

Với đặc điểm hỗ trợ trên nhiều thiết bị, nhiều môi trường và công nghệ thay đổi chóng mặt, kiểm thử độ tương thích với web app là một thử thách không nhỏ vì trải dài và tốn nhiều công sức (lại có rủi ro cao).

• Kiểm thử tương thích theo thiết bị & hệ điều hành

- Ngày nay, các browser được ứng dụng rộng rãi trên máy tính cá nhân, máy tính xách tay, máy tính bảng, smartphone và nhiều loại thiết bị ngoại vi hỗ trợ hệ điều hành. . Không có phần mềm nào chạy hoàn hảo trên tất cả môi trường nên hãy đặt ưu tiên cho những môi trường cần hỗ trợ.
- Hai điều cần lưu tâm nhất khi kiểm thử web với thiết bị : khung hình và khả năng hỗ trợ của thiết bị với các phiên bản html. Hãy truy cập tất cả nội dung web bạn có thể trên từng loại thiết bị và thay đổi zoom hình, quay ngang dọc để xem nội dung web thay đổi thế nào. Hãy chạy thử từng chức năng trên trang web để bảo đảm chúng chạy đúng.

• Trình duyệt tương thích

- Thử nghiệm ứng dụng web của bạn cho chức năng chính xác trên một số trình duyệt như Firefox, IE, Chrome, Opera, và Safari.
- Kiểm tra chức năng ứng dụng với một loạt các cài đặt cấu hình bảo mật trình duyệt.
- Kiểm tra chức năng ứng dụng với các tính năng trình duyệt bật - tắt (JavaScript, cookies).
- Kiểm tra dựng hình trình duyệt của giao diện người dùng ứng dụng của bạn.
- Kiểm tra các thiết lập bảo mật của trình duyệt cho tên miền chéo truy cập và hack.

- Kiểm tra chức năng ứng dụng nhất quán trên nhiều phiên bản của một trình duyệt.

4.Kiểm thử hiệu suất

- ***Kiểm thử trọng tải (load test)***
  - Tuyến tính khả năng mở rộng - nơi hiệu suất của một ứng dụng không thay đổi khi số lượng người dùng tăng lên. Kiểm tra tải trọng xác định một chỉ số Khả năng mở rộng cho hiệu suất ứng dụng web
  - Kiểm tra phản ứng máy chủ để dưới dạng trình duyệt gửi yêu cầu
  - Xác định thay đổi hoạt động trong một khoảng thời gian .
  - Thử nghiệm cho các chức năng mà ngừng làm việc ở các cấp độ cao hơn của người sử dụng tải.
  - Xác định các vấn đề về độ trễ mạng về chức năng ứng dụng Web
- ***Kiểm thử sức chịu đựng (stress test)***
  - Xác định cách thức ứng dụng đáp ứng theo mức độ tải .
  - Xác định các phần của ứng dụng web mà không theo mức độ tải .
  - Xác định các chức năng ứng dụng sau khi một vụ tai nạn hệ thống hoặc thành phần thất bại.
  - Xác định các hình th ức v à các liên k ết hoạt động khác nhau theo mức độ tải.

5.Kiểm thử bảo mật

- Bảo vệ dữ liệu ứng dụng Web và duy trì chức năng như thiết kế.
- Kiểm tra các hoạt động mà không cần loging .
- Kiểm tra xác thực cơ bản sử dụng tên giả và các thông tin mật khẩu
- Kiểm tra giấy chứng nhận X.509 an ninh an toàn trên các trang web
- Thử nghiệm cho các chức năng ứng dụng chính xác dựa trên các giá trị thuộc tính không hợp lệ URL.
- Kiểm tra các chức năng ứng dụng với các lĩnh vực đầu vào không hợp lệ, bao gồm các lĩnh vực văn bản.
- Kiểm tra bảo vệ máy chủ web của các thư mục web không thể truy cập hoặc các tập tin.

- Kiểm tra để xác định ứng dụng Web vi phạm an ninh, bao gồm cả thông báo l ỗi và vi phạm an ninh nỗ lực đang được đăng nhập.
- Kiểm tra các lĩnh vực CAPTCHA cho các hình th ức web và đăng nhập.
- Kiểm tra các thiết lập bảo mật trình duyệt để di chuyển từ an toàn vào các trang web không an toàn.

6. Backup hệ thống

- Sao lưu dữ liệu (backup) 1 tuần/ lần hoặc 2 ngày/lần để giúp dữ liệu web luôn an toàn khi nhà cung cấp có sự cố xảy ra.
- Tổ chức, bố cục lại website sao cho các danh mục được sắp xếp hợp lý giúp khách hàng tìm kiếm thông tin dễ dàng hơn
- Xử lý khi hệ thống gặp sự cố về website, domain, hosting.

Câu 2:

FUNCTIONAL TESTING

Mã kiểm thử	Kịch bản kiểm thử	Các bước kiểm thử	Dữ liệu	Kết quả mong đợi	Kết quả thực tế	Đạt/ không đạt
F01	Kiểm thử chức năng người dùng đăng nhập vào tài khoản của mình	1.Truy cập trang đăng nhập 2.Nhập tên đăng nhập 3.Nhập mật khẩu 4.Nhấn nút đăng nhập	Tên đăng nhập: user1 Mật khẩu: password1	Đăng nhập thành công và chuyển đến trang chính	Như mong đợi	Đạt
F02	Kiểm thử người dùng đăng ký tài khoản mới	1.Truy cập trang đăng ký 2.Nhập tên tài khoản 3.Nhập mật khẩu 4.Nhập thông tin cá nhân vào các trường dữ liệu tương ứng 3.Nhấn nút "Đăng ký"	Tên đăng nhập: newuser Mật khẩu: password123 Họ tên: Nguyễn Văn An	Tạo tài khoản thành công và thông báo thành công	Như mong đợi	Đạt
F03	Kiểm thử người dùng có thể xem các bài viết trong mục tin tức	1.Truy cập trang tin tức 2.Kiểm tra danh sách bài viết 3. Chọn một bài viết ngẫu nhiên để xem chi tiết	Không có dữ liệu đầu vào	Hiển thị danh sách bài viết và thông tin chi tiết	Như mong đợi	Đạt

F04	Kiểm thử nhân viên Phòng PR có thể đăng bài quảng cáo	1.Đăng nhập vào tài khoản của nhân viên phòng PR 2.Truy cập trang đăng bài. 3.Nhập thông tin bài đăng quảng cáo 4.Nhấn "Đăng"	Nội dung: "Thành tích xuất sắc của Trường năm 2024"	Bài đăng quảng cáo được đăng thành công	Như mong đợi	Đạt
F05	Kiểm thử sinh viên có thể xem các thông tin hỗ trợ	1.Đăng nhập vào tài khoản sinh viên 2.Truy cập trang hỗ trợ 3.Kiểm tra danh sách thông tin hỗ trợ.	Không có dữ liệu đầu vào	Hiển thị thông tin hỗ trợ đầy đủ	Như mong đợi	Đạt
F06	Kiểm thử Nhân viên phòng tuyển sinh có thể đăng bài tuyển sinh	1.Đăng nhập vào tài khoản nhân viên phòng Tuyển sinh. 2.Truy cập trang đăng bài tuyển sinh. 3.Nhập thông tin nội dung. 4.Nhấn "Đăng"	Nội dung: "Tuyển sinh khóa 2024"	Bài tuyển sinh đã được đăng thành công. Và xuất hiện trong trang đầu của mục tuyển sinh	Như mong đợi	Đạt

F07	Kiểm thử người dùng có thể đăng bài trong diễn đàn	1.Đăng nhập vào tài khoản người dùng đã tạo. 2.Truy cập vào diễn đàn. 3.Nhập bài viết mới 4.Nhấn nút "Đăng bài"	Nội dung: "Cho mình hỏi về thông tin và quy trình xét học bổng của trường"	Bài đăng đã được đăng thành công và xuất hiện trong dánh sách của bài đăng diễn đàn	Như mong đợi	Đạt
F08	Kiểm thử quản trị viên có thể quản lý tài khoản bao gồm, xóa và sửa đổi thông tin tài khoản	1.Đăng nhập vào tài khoản quản trị viên 2.Truy cập trang quản lý tài khoản 3.Chọn tài khoản 4.Nhấn nút "Sửa" 5.Sửa thông tin 6.Nhấn xác nhận 7.Nhấn nút "Xóa" 8.Nhấn nút xác nhận xóa	Tài khoản quản trị viên: admin123 Mật khẩu: admin@123 Đổi tên tài khoản Nguyễn Văn A thành Nguyễn A Văn	Tài khoản Nguyễn Văn A đã đổi thành Nguyễn A Văn. Tiếp đó là tài khoản này đã được xóa khỏi hệ thống do người quản trị thực hiện	Như mong đợi	Đạt
F09	Kiểm thử hệ thống có chức năng reset mật khẩu tự dộng khi có yêu cầu từ người dùng	1.Truy cập trang đăng nhập 2.Nhấn "Quên mật khẩu" 3.Nhập email đã đăng kí tài khoản 4.Nhấn xác nhận gửi yêu cầu.	Emai: user1@example.com	Thông báo gửi yêu cầu reset mật khẩu từ hệ thống đến email người dùng thành công.	Như mong đợi	Đạt

SECURITY TESTING

Mã kiểm thử	Kịch bản kiểm thử	Các bước kiểm thử	Dữ liệu	Kết quả mong đợi	Kết quả thực tế	Đạt /Không đạt
S01	Kiểm thử tấn công SQL Injection	1. Truy cập trang đăng nhập. 2. Nhập chuỗi SQL tấn công vào trường tên đăng nhập hoặc mật khẩu. 3. Nhấn "Đăng nhập".	Tên đăng nhập: ' OR '1'='1'	Hệ thống không cho phép truy cập và thông báo lỗi.	Như mong đợi	Đạt
S02	Kiểm thử tấn công XSS (Cross-Site Scripting)	1. Truy cập trang đăng ký. 2. Nhập mã độc vào trường nhập liệu. 3. Nhấn "Đăng ký".	Tên đăng nhập: <script>alert(1)</script>	Hệ thống không chạy mã độc và thông báo lỗi.	Như mong đợi	Đạt
S03	Kiểm tra quyền truy cập	1. Đăng nhập vào tài khoản không có quyền quản trị. 2. Thử truy cập trang quản lý tài khoản.	Tài khoản không có quyền quản trị	Hệ thống từ chối truy cập và thông báo lỗi.	Như mong đợi	Đạt
S04	Kiểm tra tính mạnh của mật khẩu	1. Truy cập trang đăng ký. 2. Nhập mật khẩu yếu. 3. Nhấn "Đăng ký".	Mật khẩu: 12345	Hệ thống từ chối và thông báo mật khẩu không đủ mạnh.	Như mong đợi	Đạt

S05	Kiểm tra chức năng reset mật khẩu	1. Truy cập trang đăng nhập. 2. Nhấn "Quên mật khẩu". 3. Nhập email không hợp lệ và gửi yêu cầu.	Email: invalid@example.com	Hệ thống thông báo lỗi không tìm thấy email.	Như mong đợi	Đạt
S06	Kiểm tra bảo mật thông tin	1. Kiểm tra xem dữ liệu nhạy cảm có được mã hóa khi lưu trữ không. 2. Thực hiện truy vấn trên cơ sở dữ liệu.	Không cần dữ liệu đầu vào	Dữ liệu nhạy cảm được mã hóa và không thể truy cập dễ dàng.	Như mong đợi	Đạt
S07	Kiểm tra tường lửa	1. Thực hiện các cuộc tấn công giả lập như DDoS. 2. Theo dõi phản hồi của hệ thống.	Không cần dữ liệu đầu vào	Tường lửa chặn tất cả các cuộc tấn công không hợp lệ.	Như mong đợi	Đạt

---Kết thúc Bài Lab08 ---