Thực hiện kiểm thử

1. Đặc điểm của ứng dụng web:

http://demo.sachmem.com/

* Chỉ cài đặt trên máy chủ
* Cần có hệ thống mạng nội bộ LAN
* Các máy trạm làm việc chỉ cần một trình duyệt web: CocCoc, Chrom, IE, FireFox
* Quản lý và bảo mật tốt

1. Quy trình thực hiện kiểm thử:
2. Kiểm thử giao diện.
3. Nội dung kiểm thử:

* Thông tin thể hiện như menu, kích thước, vị trí, màu sắc, font chữ thể hiện trên form
* Kiểm tra các điều khiển: Textbox, option (radio button), check boxes, command button, combo boxes, list boxes, Label, Dialog, Icon/Tooltip, Phím nóng/ tắt, các phím Tab/ Shift tab/ enter/ ESC, Focus con trỏ, Thông báo, Menu điều khiển, dấu hiệu của trường bắt buộc
* Giá trị mặc định

1. Phương pháp thực hiện:

Xác định số form cần test

Kiểm tra lần lượt các điều khiển trên cùng 1 form theo chiều:

* Từ trên xuống dưới
* Từ trái qua phải
* Từ mỗi điều khiển độc lập đến logic giữa các điều khiển

Kiểm tra các nội dung trên mỗi form:

* Màu sắc hài hoà hợp lý, vị trí các điều khiển đặt theo yêu cầu khách hàng(nếu có)
* Các nút hiển thị ở các Form tương tự nhau phải giống nhau trừ khi có yêu cầu riêng.
* Các tên thuộc tính dạng text tương ứng với các điều khiển trên Form đều phải đúng chính tả không dùng tiếng anh.
* Kiểm tra giao diện các Form trên các trình duyệt khác nhau đảm bảo phải như nhau.

1. Những lỗi thường gặp:

Form nỗi thường thấy: có thể check list theo cái này:

* Các Form giao diện không nhất quán về màu sắc, tên nút, các nút không cùng kích cỡ.
* Các câu thông báo thường sai chính tả hoặc là tiếng anh hoặc tiếng việt không dấu.
* Lỗi chính tả (tên Form, tên nút lệnh, tên trường thuộc tính...)
* Thiếu ký tự \* bên cạnh trường bắt buộc
* Câu thông báo không chính xác với thao tác đã thực hiện
* Sai trật tự Tab
* Khi một nút lệnh không được sử dụng trong 1 số thời điểm nó không được chuyển sang màu xám mờ
* Tên các nút lựa chọn mang tính kỹ thuật, không dễ hiểu với người dùng hệ thống.
* Không Focus con trỏ chuột tới thuộc tính đầu tiên của form.

1. Kiểm thử hàm và chức năng.
2. Nội dung kiểm thử:

* Việc xử lý các thao tác (action): Add, Update ,Delete ,Data type , Select , View, Search, Import/Export, Share/Send data
* Valid data: Việc xử lý các chức năng với việc nhập các bộ dữ liệu hợp lệ
* Invalid data:Việc xử lý các chức năng với việc nhập các bộ dữ liệu không hợp lệ
* Flow: Việc xử lý mối liên hệ giữa các chức năng theo luồng nghiệp vụ.

1. Phương pháp thực hiện:

Để test function, áp dụng tất các kỹ thuật test để phân tích ra các trường hợp hợp lệ và các trường hợp không hợp lệ, các luồng nghiệp vụ đúng ...

* Khi test valid data và invalid data thì áp dụng các kỹ thuật test phân tích giá trị biên, phân vùng tương đương để tạo dữ liệu.
* Khi test việc xử lý theo các action thì cần chú ý: với mỗi thao tác của người dùng đều làm cho hệ thống biến đổi sang một trạng thái khác.
* Khi test flow: cần phải hiểu và nắm được về luồng nghiệp vụ của mỗi phần mềm.

Ví dụ: Đối với trường nhận giá trị text thì sẽ có thể có những case sau:

* characters: " abc "
* number: "123"
* special character: "!@#$%"
* html tags:<script> the material is publish for all person </script>
* html tags: <script>alert("xss error") </script>
* html tags: <script> window.open("http://dantri.vn") </script>

1. Kiểm thử đường link.
2. Nội dung kiểm thử:

* Kiểm tra các links liên kết ngoài trang web
* Kiểm tra tất cả các links nội bộ
* Kiểm tra các links tới các vị trí trong cùng trang
* Kiểm tra các links sử dụng để gửi mail tới admin hoặc ngườidùng khác từ trang web
* Kiểm tra xem có trang trống nào không
* Kiểm tra các links bể trong tất cả các links nói trên

1. Phương thức thực hiện

* Vào công cụ hỗ trợ Link checker: <http://validator.w3.org/>
* Nhập địa chỉ trang web:
* Kết quả trả về về những trang bị broken

1. Kiểm thử tính tương thích.
2. Nội dung kiểm thử

* Kiểm thử sự tương thích với trình duyệt
* Kiểm thử sự tương thích với hệ điều hành
* Kiểm thử sự tương tích với thiết bị di động
* Kiểm thử sự tương thích với tùy chọn các thiết bị ngoại vi ( máy in …): không cần với trang http://demo.sachmem.com/

1. Phương pháp thực hiện

* Khi test một web thì cần phải có các yêu cầu:

Chạy trên hệ điều hành: Window, Ubuntu, MAC,…

Chạy các trình duyệt : CocCoc, Firefox, Chrome, IE,...

* Chạy trên các trình duyệt của các thiết bị di động có hệ điều hành là androin hoặc ios.
* Có thể kết nối với máy in để in bài

1. Kiểm thử tính ổn định.
2. Nội dung kiểm thử:

* Kiểm thử cho chuyển hướng
* Kiểm thử tính khả dụng
* Kiểm thử nội dung
* Các thông tin hỗ trợ người dùng

1. Phương pháp thực hiện:

* Trên các grid list ở hình phải sort được theo các cột thông tin
* Số lượng người tham dự từ lớn xuống bé
* Số lượng vé từ thấp lên cao

1. Kiểm thử an ninh và bảo mật.
2. Nội dung kiểm thử:

* Kiểm tra lỗi SQL Injection:
* Kiểm tra lỗi XSS
* Kiểm tra lỗ hổng CSRF
* Kiểm tra lỗi Path Traversal
* Kiểm tra lỗi mã hóa dữ liệu
* Kiểm tra lỗi xác thực/phân quyền
* Kiểm tra lỗi User enumeration
* Kiểm tra lỗi Session fixation
* Kiểm tra lỗ hổng cho phép dò đoán mật khẩu, thu thập danh sách, thông tin người dùng: Các ứng dụng không có cơ chế bảo vệ sử dụng captcha, lock account khi đăng nhập sai quá số lần quy định đều có khả năng bị mắc lỗi này.

1. Phương pháp thực hiện:

* Ví dụ 1: Kiểm tra lỗi sql injection: Nhập vào form đăng nhập chuỗi ký tự đặc biệt: test' or '1'='1. Hệ thống đăng nhập thành công => bị lỗi sql injection
* Ví dụ 2: Kiểm tra lỗi xss: Nhập vào chuỗi kí tự ***<script>alert(“ XSS”)</script>*** vào những nơi có thể nhập được dữ liệu. Sau đó, kích nút Lưu => Nếu ứng dụng lưu lại và cho phép thực thi script thì trên trình duyệt sẽ xổ ra cửa sổ có dòng chữ “XSS”, khi đó ứng dụng bị mắc lỗi XSS.
* Ví dụ 3: Kiểm tra lỗi xác thực/phân quyền: Sử dụng 2 user, 1 user có quyền thấp và 1 user có quyền cao hơn. Khi sử dụng user có quyền cao truy cập vào các chức năng dành riêng ta ghi lại các đường dẫn trên URL, sau đó đăng nhập vào bằng user quyền thấp và thử truy cập vào link đó. Nếu ứng dụng cho phép user truy cập thì cơ chế xác thực phân quyền của ứng dụng không có tác dụng.
* Ví dụ 4: kiểm tra lỗi User enumeration : Đăng nhập vào ứng dụng (cố tình nhập sai user hoặc password sai). Nếu ứng dụng trả về câu thông báo cụ thể là “sai mật khẩu” hoặc “sai user” thì ứng dụng mắc lỗi. Còn nếu trả về câu thông báo chung ví dụ “Username hoặc password không đúng.” thì không bắt lỗi.
* Ví dụ 5: Kiểm tra lỗi lỗ hổng cho phép dò đoán mật khẩu, thu thập danh sách, thông tin người dùng: Các ứng dụng không có cơ chế bảo vệ sử dụng captcha, lock account khi đăng nhập sai quá số lần quy định đều có khả năng bị mắc lỗi này.