TRƯỜNG ĐẠI HỌC TƯ THỤC QUỐC TẾ SÀI GÒN **KHOA KỸ THUẬT& KHOA HỌC MÁY TÍNH** **PHÁT TRIỂN, VẬN HÀNH VÀ BẢO TRÌ PHẦN MỀM**	**Lab 5** **Phân tích Rủi ro và Lập Kế hoạch Đảm bảo Chất Lượng**	The Saigon International University

Mục tiêu

1. Hiểu cách phân tích rủi ro từ các ngữ cảnh thực tế trong hệ thống phần mềm.
2. Lập kế hoạch đảm bảo chất lượng để giảm thiểu rủi ro và nâng cao hiệu suất, bảo mật, tính ổn định.
3. Đánh giá kế hoạch đã thực hiện và đề xuất cải tiến cho hệ thống.

Tình huống mô tả

Ngữ cảnh 1: Hệ thống Quản lý Nhân sự Trực Tuyến

Công ty XYZ đã triển khai hệ thống Quản lý Nhân sự Trực Tuyến nhằm hỗ trợ quản trị và xử lý thông tin nhân sự. Hệ thống này cho phép:

- Nhân viên đăng nhập để kiểm tra bảng lương, hồ sơ cá nhân và lịch sử làm việc.
- Quản trị viên quản lý nhân viên, thực hiện các thao tác thêm, sửa, xóa thông tin và xuất báo cáo hiệu suất.

Trong vòng 6 tháng kể từ khi triển khai, công ty đã ghi nhận một số vấn đề đáng quan tâm. Quản trị viên thường xuyên phản ánh rằng hệ thống trở nên chậm chạp khi tìm kiếm nhân viên trong cơ sở dữ liệu lớn, đặc biệt khi lọc theo phòng ban hoặc chức vụ. Một số báo cáo hiệu suất nhân viên bị sai lệch do dữ liệu không đồng bộ giữa các module. Ngoài ra, đội bảo mật phát hiện có các nỗ lực tấn công brute-force vào chức năng đăng nhập, làm tăng nguy cơ tài khoản quản trị viên bị đánh cắp. Khi thêm hoặc chỉnh sửa hồ sơ nhân viên, nếu thiếu một số trường thông tin bắt buộc như địa chỉ email hoặc số điện thoại, hệ thống chỉ báo lỗi chung chung mà không chỉ rõ nguyên nhân, gây khó khăn cho người dùng.

Ngữ cảnh 2: Hệ thống Quản lý Thư viện Trực Tuyến

Hệ thống Quản lý Thư viện Trực Tuyến của công ty XYZ được thiết kế để cung cấp trải nghiệm thuận tiện cho cả độc giả và quản trị viên. Hệ thống hỗ trợ các tính năng như:

- Độc giả có thể tìm kiếm sách, gia hạn thời gian mượn và thanh toán phí trễ hạn.
- Quản trị viên quản lý thông tin sách, theo dõi tình trạng mượn trả, và xuất các báo cáo liên quan.

Tuy nhiên, hệ thống hiện đang đối mặt với một số vấn đề. Nhiều độc giả phản ánh rằng khi tìm kiếm các sách phổ biến, thời gian phản hồi của hệ thống kéo dài tới 20 giây, đặc biệt vào các khung giờ cao điểm. Một lỗi bảo mật nghiêm trọng được phát hiện khi độc giả có thể thay đổi URL trong trình duyệt để xem thông tin tài khoản của người khác. Quản trị viên cũng gặp khó khăn khi thêm sách mới: nếu thông tin như giá sách hoặc thể loại bị bỏ trống, hệ thống không đưa ra thông báo rõ ràng, khiến dữ liệu không được lưu. Khi xóa một đầu sách, các bản ghi liên quan đến mượn trả không được tự động xóa, dẫn đến sai lệch trong báo cáo thống kê.

Ngữ cảnh 3: Hệ thống Đặt Vé Máy Bay Trực Tuyến

Hãng hàng không ABC đã triển khai hệ thống đặt vé máy bay trực tuyến nhằm cung cấp trải nghiệm nhanh chóng và tiện lợi cho khách hàng. Hệ thống này hỗ trợ:

- Khách hàng tìm kiếm chuyến bay, đặt vé và thanh toán trực tuyến.
- Nhân viên hãng hàng không quản lý lịch bay, thông tin khách hàng và tình trạng ghế ngồi.

Trong mùa cao điểm, hệ thống thường xuyên bị phản ánh bởi khách hàng. Khi có nhiều người tìm kiếm chuyến bay cùng lúc (hơn 500 lượt tìm kiếm), hệ thống thường xuyên bị treo, không thể phản hồi trong thời gian ngắn. Một số trường hợp khách hàng đặt vé thành công nhưng ghế vẫn hiển thị là còn trống, dẫn đến nhiều khiếu nại từ khách hàng. Tình trạng bảo mật cũng đáng lo ngại: hệ thống không tự động đăng xuất khách hàng sau thời gian dài không hoạt động, dẫn đến nguy cơ bị lạm dụng tài khoản. Nhân viên hãng hàng không gặp phải lỗi khi cố gắng chỉnh sửa thông tin chuyến bay đã có vé đặt trước, gây khó khăn trong việc cập nhật lịch trình bay.

Nội dung thực hành

Phần 1: Phân tích Rủi ro

1. Xác định các rủi ro:
    - Liệt kê các rủi ro tiềm ẩn dựa trên vấn đề mô tả.
    - Phân loại rủi ro thành 4 nhóm chính:
        - Hiệu suất
        - Bảo mật
        - Tính ổn định
        - Quản lý vận hành

2. Đánh giá rủi ro:
    - Phân tích mức độ nghiêm trọng (Severity) và khả năng xảy ra (Likelihood) của từng rủi ro.
    - Trình bày kết quả phân tích trong bảng Risk Matrix.

1. Hiệu suất tìm kiếm chậm - Hệ thống chậm khi tìm kiếm nhân viên trong CSDL lớn, đặc biệt khi lọc theo phòng ban/chức vụ - Hiệu suất
   Dữ liệu báo cáo sai lệch - Báo cáo hiệu suất nhân viên bị sai do dữ liệu không đồng bộ giữa các module - Tính ổn định
   brute-force - Có nỗ lực tấn công brute-force vào chức năng đăng nhập - Bảo mật

Thông báo lỗi không rõ rang - Khi thiếu trường bắt buộc (email, SĐT), hệ thống chỉ báo lỗi chung chung - Quản lý vận hành

Hệ thống ql nhân sự			
Rủi ro	Mức độ nghiêm trọng	Khả năng xảy ra	Mức độ ưu tiên
Hiệu suất tìm kiếm chậm			High
Dữ liệu báo cáo sai lệch			High
Tấn công brute-force			Critical
Thông báo lỗi không rõ			Med

2. Thời gian phản hồi tìm kiếm quá lâu - Tìm kiếm sách phổ biến mất tới 20 giây, đặc biệt giờ cao điểm - Hiệu suất
   Lỗ hổng bảo mật URL - Độc giả có thể thay đổi URL để xem thông tin tài khoản người khác - Bảo mật
   Validation dữ liệu kém - Khi thêm sách thiếu thông tin (giá, thể loại), không có thông báo rõ rang - Quản lý vận hành
   Dữ liệu không nhất quán - Khi xóa sách, bản ghi mượn trả không tự động xóa -> sai lệch báo cáo - Tính ổn định

Hệ thống ql thư viện			
Rủi ro	Mức độ nghiêm trọng	Khả năng xảy ra	Mức độ ưu tiên
Thời gian phản hồi chậm			C
Lỗ hổng bảo mật URL			C
Validation dữ liệu kém			H
Dữ liệu không nhất quán			H

3. Hệ thống bị treo khi quá tải - Khi >500 lượt tìm kiếm cùng lúc, hệ thống treo - Hiệu suất
   Bug đặt vé - Khách đặt vé thành công nhưng ghế vẫn hiển thị trống - Tính ổn định
   Không tự động đăng xuất - Hệ thống không logout sau thời gian idle -> nguy cơ lạm dụng tài khoản - Bảo mật
   Lỗi khi sửa chuyến bay đã có vé - Nhân viên không thể chỉnh sửa thông tin chuyến bay đã có vé đặt - Quản lý vận hành

Hệ thống đặt vé bay			
Rủi ro	Mức độ nghiêm trọng	Khả năng xảy ra	Mức độ ưu tiên
Hệ thống bị treo			C

khi quá tải			
Bug đặt vé			C
Không tự động đăng xuất			M
Lỗi khi sửa chuyến bay đã có vé			H

Ví dụ Risk Matrix:

Rủi ro	Severity	Likelihood	Vị trí
Hệ thống treo khi tìm kiếm dữ liệu	Cao	Trung bình	Cao-Trung bình
Lỗ hổng bảo mật URL	Cao	Cao	Cao-Cao
Dữ liệu không đồng bộ trong báo cáo	Trung bình	Trung bình	Trung bình-Trung bình

Phần 2: Lập Kế hoạch Đảm Bảo Chất Lượng

1. Lập kế hoạch giảm thiểu rủi ro:
    - Đưa ra các biện pháp cụ thể để giảm thiểu từng rủi ro.
    - Xác định thời gian thực hiện, công cụ/phương pháp sử dụng, và người chịu trách nhiệm.

Ví dụ Bảng Kế Hoạch:

Rủi ro	Hoạt động giảm thiểu	Công cụ/Phương pháp	Thời gian thực hiện	Người chịu trách nhiệm	Kết quả mong đợi
Tấn công brute-force	Thêm CAPTCHA và khóa tài khoản sau 5 lần đăng nhập sai	Google reCAPTCHA	2 ngày	Nhóm bảo mật	Ngăn chặn hoàn toàn brute-force.
Dữ liệu không đồng bộ	Tích hợp cơ chế kiểm tra và đồng bộ dữ liệu giữa các module	Sử dụng dịch vụ đồng bộ dữ liệu	3 ngày	Nhóm backend	Báo cáo trả về dữ liệu chính xác.
Thời gian phản hồi chậm	Tối ưu hóa truy vấn SQL, thêm index vào bảng cơ sở dữ liệu	EXPLAIN và INDEX trong SQL	3 ngày	Nhóm backend	Thời gian phản hồi <200ms.

2. Mô tả cách triển khai chi tiết một hoạt động giảm thiểu:
    - Chọn một rủi ro từ bảng kế hoạch và mô tả cách thực hiện biện pháp giảm thiểu.
    - Phần này cần nêu rõ:
        - Bối cảnh hiện tại
        - Giải pháp
        - Các bước triển khai

Rủi ro	Hoạt động giảm thiểu	Phương pháp	Thời gian	Người chịu trách nhiệm	Kết quả mong đợi
brute-force	Thêm Google reCAPTCHA Khóa tài khoản sau 5 lần đăng nhập sai rate limit	Google reCAPTCHA Redis Database triggers		Bảo mật	
Dữ liệu sai lệch	transaction management đồng bộ dữ liệu real-time			backend	
Tìm kiếm chậm	Tối ưu SQL queries database indexes	Database indexing		backend	
Thông báo lỗi	field-level validation error messages chi tiết Frontend validation			Be+fe	

Phần 3: Đánh giá và Cải tiến

1. Đánh giá hiệu quả kế hoạch:
    - So sánh kết quả trước và sau khi thực hiện kế hoạch.
    - Ghi nhận hiệu quả từng biện pháp giảm thiểu.

Ví dụ Bảng Đánh Giá:

Rủi ro	**Hoạt động**	**Kết quả trước**	**Kết quả sau**	**Đánh giá**
Thời gian phản hồi chậm khi tìm kiếm	Tối ưu hóa truy vấn SQL	10 giây phản hồi	150ms phản hồi	Đạt yêu cầu.
Tấn công brute-force	Thêm CAPTCHA và khóa tài khoản	10 tài khoản bị tấn công	Không còn tài khoản bị tấn công	Đạt yêu cầu.

2. Đề xuất cải tiến:
    - Nêu các biện pháp bổ sung để cải thiện chất lượng hệ thống, chẳng hạn:

- Tích hợp kiểm thử bảo mật tự động.
- Thực hiện kiểm tra hiệu suất định kỳ với lượng người dùng lớn hơn.

Rủi ro	**Hoạt động**	**Kết quả trước**	**Kết quả sau**	**Đánh giá**
Tìm kiếm chậm	Tối ưu SQL + indexing + Redis cache	- Thời gian: 8-12 giây - User complaints: 30/tuần	- Thời gian: 150ms average - User complaints: 0 - Cache hit rate: 85%	Đạt yêu cầu.
Tấn công brute-force	Thêm reCAPTCHA + rate limiting + account lockout	- 50 tài khoản bị tấn công/tuần - 10 account admin bị hack	- 0 tài khoản bị hack - 98% bot requests bị block - Failed attempts giảm 95%	Đạt yêu cầu.
Dữ liệu sai lệch	Transaction management + Message queue sync	- 15% báo cáo sai - 50 tickets/tuần về data inconsistency	- 0% báo cáo sai - Data sync real-time - Tickets giảm 100%	Đạt yêu cầu.
Error messages	Field-level validation + custom error messages	- Generic error: "Input invalid" - 40 support tickets/tuần	- Specific errors: "Email is required" - Support tickets giảm 85%	Đạt yêu cầu.

Yêu cầu Nộp Bài

1. Báo cáo phân tích rủi ro:
   - Danh sách rủi ro và bảng Risk Matrix.
   - Đánh giá mức độ nghiêm trọng và khả năng xảy ra.

2. Kế hoạch đảm bảo chất lượng:
   - Bảng kế hoạch chi tiết.
   - Mô tả cách thực hiện một hoạt động giảm thiểu.

3. Báo cáo đánh giá và cải tiến:
   - Kết quả thực hiện kế hoạch.
   - Đề xuất cải tiến để hoàn thiện hệ thống.