Trường Đại học Công nghệ Thông tin (UIT)
Đại Học Quốc Gia Tp. HCM

BÀI TẬP 02

Môn học: Lập trình an toàn & Khai thác lỗ hổng phần mềm

Tên chủ đề: **Quy trình phát triển phần mềm an toàn - Secure SDLC**

Mã môn học: NT521 – Năm học 2022-2023

1. NỘI DUNG THỰC HIỆN

Lưu ý chung:

+ ***Sinh viên chương trình Chất lượng cao***: bắt buộc thực hiện yêu cầu **1.1, 1.3**, (yêu cầu 1.2 là tự chọn).
+ ***Sinh viên chương trình tài năng***: **bắt buộc** thực hiện yêu cầu **1.1, 1.2, 1.3.**

1.1. Qui trình phát triển phần mềm an toàn.

Qui trình phát triển phần mềm an toàn là 01 cách tiếp cận nhằm đưa yếu tố an toàn, bảo mật vào tất cả các giai đoạn của SDLC. Dựa trên kiến thức đã học, và nhận định của bản thân, hãy thực hiện các yêu cầu sau:

a. *Yêu cầu bảo mật (security requirement) nào có giá trị nhất so với các yêu cầu bảo mật khác trong giai đoạn thu thập thông tin để viết bản đặc tả phần mềm? Tại sao nó lại đóng vai trò quan trọng trong các hệ thống phần mềm, hoặc các hệ thống thông tin bao gồm các phần mềm khác nhau của một tổ chức, cá nhân bất kỳ.*

b. *Nêu 05 loại tính năng bảo mật (security functionality) cần được trang bị trong các bộ khung (framework) phát triển phần mềm hiện đại. Giải thích vai trò của nó trong hệ thống phần mềm.*

1.2. Phân tích Lỗi Thiết kế không an toàn

Insecure Design - Một danh mục (category) mới của tiêu chuẩn Top 10 OWASP cho năm 2021 tập trung vào các rủi ro liên quan đến lỗi thiết kế và kiến trúc, với các khuyến nghị sử dụng nhiều hơn mô hình mối đe dọa (threat model), các mẫu thiết kế an toàn và kiến trúc tham chiếu. Với định hướng tới sự an toàn trong các phần mềm đưa ra thị trường, các tổ chức phát triển phần mềm cần phải áp dụng nguyên tắc "dịch chuyển sang trái" (pushing left) từ việc lập trình (coding) để chuyển sang các hoạt động tiền lập trình (pre-coding) an toàn theo như các nguyên tắc của Bảo mật theo thiết kế (Secure by Design).

Danh sách *tham khảo:* *https://owasp.org/Top10/A04_2021-Insecure_Design/*

Trong số các khuyến nghị ở danh mục này của OWASP, một số CWEs (Common Weakness Enumerations) nổi bật được đề cập như:

- CWE-209: Generation of Error Message Containing Sensitive Information,
- CWE-183 Permissive List of Allowed Inputs,
- CWE-256: Unprotected Storage of Credentials,
- CWE-501: Trust Boundary Violation,
- CWE-522: Insufficiently Protected Credentials.

Hãy chọn và phân tích nguyên nhân lỗ hổng đến từ thiết kế không an toàn dựa trên các các CWE điển hình như trên. Sau đó, lấy một ví dụ về 01 lỗ hổng bảo mật và phơi nhiễm phổ biến (Common Vulnerabilities and Exposures - CVE) tương ứng từ CWE đã chọn, thực hiện các bước demo tương ứng về lỗ hổng ứng với CWE đó.

1.3. Mô hình hóa tác nhân đe dọa – Threat modeling

Mục đích của bài tập này là để tạo cơ hội cho người học thực hành kỹ thuật mô hình hóa tác nhân đe dọa (threat modeling) trong giai đoạn thiết kế phần mềm an toàn, và làm quen với một trong những mô hình hóa tác nhân đe dọa phổ biến – mô hình STRIDE.

Yêu cầu:

- *Đọc mô tả hệ thống phần mềm Hỗ trợ Bảo dưỡng Phi cơ cần được phát triển **của hãng hàng không BẦU TRỜI** như bên dưới. Vì lí do an toàn trong hoạt động bay, ứng dụng này cần được quan tâm tới độ an toàn, bảo mật nghiêm ngặt.*
- *Tìm và xác định các tác nhân đe dọa cho phần mềm sắp được phát triển theo **mô hình STRIDE** cho ngữ cảnh được chỉ định. Vẽ sơ đồ tác nhân đe dọa (threat modeling diagram) cho hệ thống phần mềm (người học có thể tham khảo chỉ dẫn quy trình thực hiện mô hình hóa tác nhân đe dọa của INFOSEC như liên kết gợi ý bên dưới).*
  - *Có thể tham khảo Top 10 OWASP 2021 hoặc OWASP Mobile Top 10*
  - *Khuyến khích sử dụng công cụ "Microsoft Threat Modeling Tool" để vẽ bản thiết kế phần mềm với các danh sách tác nhân đe dọa trong ở trên (threat modeling diagram), (tuy nhiên đây là yêu cầu không bắt buộc). Việc sử dụng công cụ này được xem là điểm cộng cho bài tập.*
- *Giả sử thay vì phát triển ứng dụng di động trên Apple iPad (native app), hãng hàng không muốn thay đổi sang phiên bản ứng dụng web (và đội bảo dưỡng máy bay vẫn dùng iPad để truy cập ứng dụng này). Trong ngữ cảnh này, các tác nhân đe dọa (threat model) đã xác định có thay đổi không? Thay đổi ở điểm nào? Giải thích lí do.*

Ngữ cảnh:

Việc bảo dưỡng máy bay là vô cùng quan trọng vì nếu máy bay gặp sự cố trong hành trình bay, ví dụ động cơ hỏng hóc, thường gây ra hậu quả thảm khốc. Do đó, trong lĩnh vực hàng không, có nhiều thủ tục và qui định liên quan đến cách bảo dưỡng máy bay.

Trong ngữ cảnh này, tổ chức của chúng tôi, **hãng hàng không BẦU TRỜI** cần phát triển một ứng dụng chạy trên các thiết bị Apple iPad để tạo và quản lý-duy trì các dữ liệu liên

quan tới hoạt động bảo dưỡng máy bay. Ứng dụng này có tên là "**Bảo Dưỡng Phi Cơ**", sẽ thay thế các hệ thống cũ đang vận hành vốn tồn tại nhiều lỗi, và chi phí vận hành khá đắt.

Các hồ sơ dữ liệu bảo trì cho máy bay liên quan với nhau nhiều hơn hầu hết các sản phẩm tiêu dùng thường ngày mà mọi người quen thuộc. Trước hết, mọi máy bay đều khác nhau về nhiều khía cạnh: ngay cả khi hai máy bay có cùng số hiệu nếu chúng được chế tạo vào những thời điểm khác nhau, nhà sản xuất có thể đã thay đổi nhà cung cấp cho một số bộ phận. Ngoài ra, nếu máy bay có hai cánh quạt, một trong số chúng có thể đã được thay thế nhưng không phải cùng loại như cánh quạt kia, và lượng thời gian mỗi cánh quạt đã sử dụng trong chuyến bay phải được theo dõi để có thể tiến hành kiểm tra và thay thế vào những thời điểm thích hợp.

Do đó, hồ sơ cho một chiếc máy bay bao gồm kiểu máy và số sê-ri của khung máy bay, từng động cơ, từng cánh quạt, v.v. Hồ sơ bao gồm thời điểm từng bộ phận này được lắp đặt, kiểm tra hoặc được bảo dưỡng và người đã chứng nhận rằng công việc được thực hiện đúng cách.

Khi bảo dưỡng máy bay, những người thực hiện công việc được cung cấp danh sách kiểm tra (checklist) các công việc phải hoàn thành. Người giám sát công việc phải có chứng chỉ thích hợp để thực hiện nhiệm vụ cụ thể đó, và phải ký tên ở cuối ghi rằng công việc đã được thực hiện một cách chính xác.

Ngoài ra, nhiều tổ chức, hay hãng hàng không coi hồ sơ máy bay của họ là bí mật. Họ có thể cung cấp các tài liệu sẵn có cho các cơ quan quản lý, nhưng vì nhiều lý do, họ không muốn đối thủ cạnh tranh của mình hoặc công chúng biết chi tiết về các chính sách và quy trình bảo dưỡng của họ hoặc chi tiết về máy bay cá nhân của họ.

Định kỳ, các cập nhật trong danh sách kiểm tra hoặc chính sách bảo trì thiết bị của máy bay được xem xét và điều chỉnh thích hợp bởi tổ chức, hãng hàng không. Đây là công việc thường xuyên để phòng chống các tai nạn có thể xảy ra – ví dụ như những người có trách nhiệm sẽ đưa ra quyết định một cách thích hợp để ngăn chặn một tai nạn tương tự tái diễn.

Trường hợp sử dụng điển hình (Use case):

- Đội bảo dưỡng của hãng hàng không nhận một hoặc nhiều thiết bị iPad vào lúc bắt đầu mỗi ca làm việc.
- Họ sẽ tham khảo Ứng dụng "Bảo Dưỡng Phi Cơ" cho ca làm việc của mình, ứng dụng này sẽ hiển thị danh sách các công việc cần được thực hiện. Chú ý rằng, họ sẽ không cần phải hoàn thành tất cả các nhiệm vụ công việc trong ca làm việc của mình - thời gian thực hiện để bảo trì có thể khác nhau và vì vậy họ sẽ làm hết sức có thể trong ca làm việc của mình, sau đó, ca sau sẽ đảm nhận.

- Khi thực hiện một nhiệm vụ bảo trì, Ứng dụng "Bảo Dưỡng Phi Cơ" sẽ hiển thị cho đội bảo dưỡng các hồ sơ bảo trì cho chiếc máy bay đó, hướng dẫn sử dụng để thực hiện tác vụ cụ thể đó và danh sách kiểm tra chính xác.
- Khi một thành viên của đội bảo dưỡng hoàn thành một mục trong danh sách kiểm tra, họ phải thực hiện một số hành động (chẳng hạn như nhấn đúng nút trên màn hình) để kiểm tra, xác nhận lại rằng qui trình đã được hoàn thành. Đôi khi các mục trong danh sách kiểm tra sẽ yêu cầu điền thông tin như số sê-ri của một bộ phận thay thế cho một bộ phận cũ.
- Các thành viên đội bảo dưỡng có thể chụp ảnh công việc của họ bằng máy ảnh trên iPad và đính kèm chúng vào hồ sơ dịch vụ bảo trì phụ tùng máy bay.
- Khi một nhiệm vụ hoàn thành, Ứng dụng "Bảo Dưỡng Phi Cơ" sẽ có người chịu trách nhiệm về nhiệm vụ đó (người phải được chứng nhận hợp lệ) ký tên rằng nhiệm vụ đã được thực hiện đúng quy trình chuẩn.
- Đôi khi thực hiện một nhiệm vụ bảo dưỡng thiết bị máy bay sẽ dẫn đến việc tạo ra một nhiệm vụ mới. Ví dụ, một cuộc kiểm tra tình trạng thiết bị sẽ đưa ra kết luận rằng một bộ phận của máy bay cần được thay thế. Ứng dụng cũng sẽ hỗ trợ tính năng tạo mới nhiệm vụ bảo dưỡng này.
- Khi ca làm việc của họ kết thúc, đội bảo trì sẽ trả lại iPad mà họ đã sử dụng.

Cơ sở dữ liệu chính của tổ chức/hãng hàng không về hồ sơ của máy bay sẽ được cập nhật chính xác khi dịch vụ bảo dưỡng được thực hiện.

Đặc tả hệ thống:

Trung tâm dữ liệu (data center) của tổ chức/hãng hàng không sẽ đảm nhận lưu trữ:

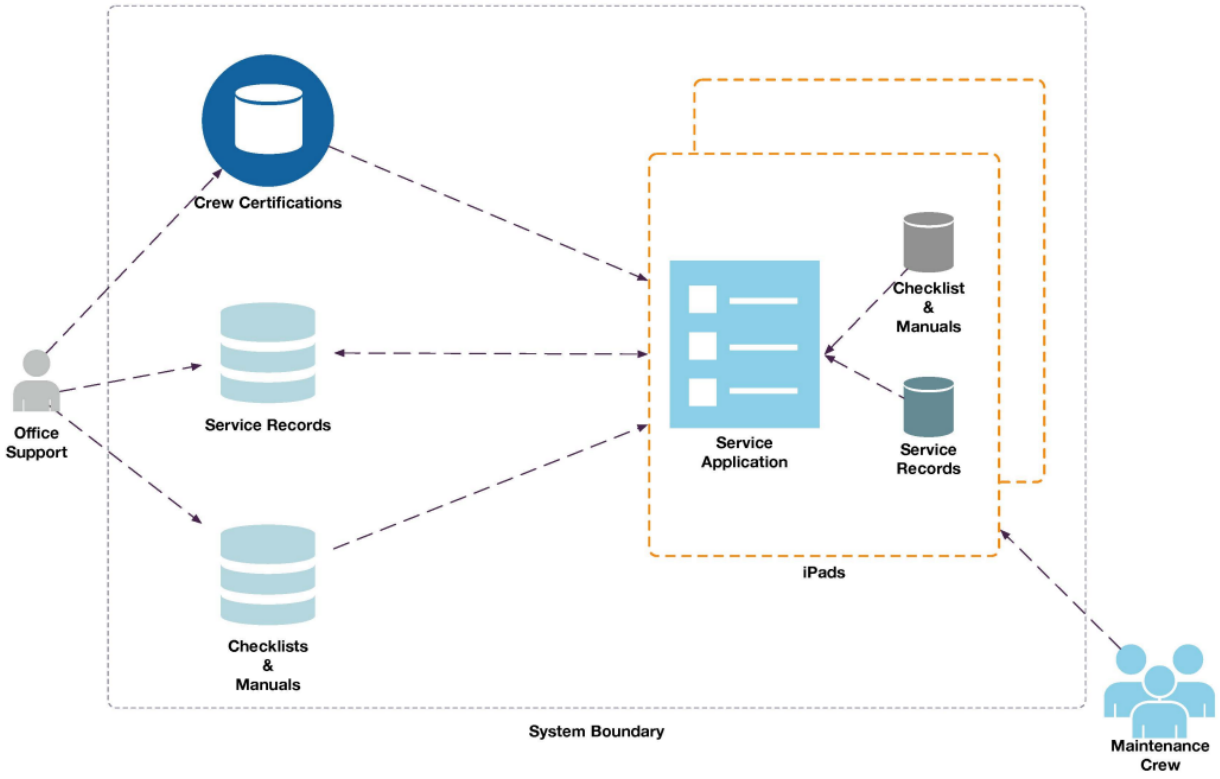
- Cơ sở dữ liệu chứa tất cả các hồ sơ dịch vụ cho máy bay của hãng. Cơ sở dữ liệu này đã tồn tại: Ứng dụng "Bảo Dưỡng Phi Cơ" sẽ phải xử lý các bản ghi được tạo bởi các hệ thống đã phát triển trước đó. Ngoài ra, hãng hàng không sẽ không thể thay thế đồng thời hệ thống bảo trì máy bay hiện có của mình, vì vậy ngay cả khi Ứng dụng "Bảo Dưỡng Phi Cơ" được đưa vào sử dụng, một số người trong tổ chức vẫn sẽ sử dụng các hệ thống cũ hơn.
- Cơ sở dữ liệu tổng thể của tất cả các hướng dẫn sử dụng dịch vụ và danh sách kiểm tra cho tất cả các thiết bị, phụ tùng máy bay được hãng hàng không BẦU TRỜI sử dụng.
- Cơ sở dữ liệu về các chứng chỉ do nhân viên dịch vụ của hãng hàng không BẦU TRỜI nắm giữ

Lưu ý:

Thiết bị iPad sẽ được kích hoạt wifi và wifi sẽ có sẵn trong văn phòng của tổ chức/hãng hàng không. Tuy nhiên, ở ngoài sân bay (hoặc bên trong khu vực động cơ của máy bay) tính khả dụng của wifi sẽ không được đảm bảo.

Ứng dụng "Bảo Dưỡng Phi Cơ" sẽ được cài đặt trên iPad. Tuy vậy, do có quá nhiều hướng dẫn sử dụng dịch vụ và danh sách kiểm tra trong hãng bay, nên tất cả thông tin này có thể không được tải hết xuống iPad. Do đó, Ứng dụng "Bảo Dưỡng Phi Cơ" sẽ có những hồ sơ/thông tin cần thiết, tuy nhiên không phải tất cả chúng. Tương tự, iPad không thể chứa tất cả hồ sơ dịch vụ cho tất cả các máy bay của hãng hàng không này.

Kiến trúc tổng thể của ứng dụng được mô tả như hình bên dưới.



2. GỢI Ý – THAM KHẢO

Một số gợi ý thực hiện:

- Tham khảo bài giảng môn học.
- Software Design Basics: https://www.tutorialspoint.com/software_engineering/software_design_basics.htm
- Software Analysis & Design Tools: https://www.tutorialspoint.com/software_engineering/software_analysis_design_tools.htm
- Threat Modeling, Step by Step: https://akademie.dw.com/docs/Handbook_Threat_Modeling_Guide.pdf

- **Threat modeling: Technical walkthrough and tutorial – INFOSEC resource:** https://resources.infosecinstitute.com/topic/threat-modeling-technical-walkthrough-and-tutorial/
- A Hybrid Threat Modeling Method: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2018_004_001_516627.pdf
- "Avoiding The Top 10 Software Security Design Flaws" by the IEEE Center for Secure Design: https://ieeecs-media.computer.org/media/technical-activities/CYBSI/docs/Top-10-Flaws.pdf
- "Tactical Threat Modeling" – SAFECode: https://safecode.org/wp-content/uploads/2017/05/SAFECode_TM_Whitepaper.pdf
- The Microsoft Threat Modeling Tool: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
- Microsoft Threat Modeling Tool threats: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
- OWASP Insecure Design: https://owasp.org/Top10/A04_2021-Insecure_Design

---

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung thực hiện, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

*Ví dụ: [*NT101.K11.ANTT*]-Ex01_Group03.*

- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT