BÁO CÁO BÀI TẬP

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

GVHD: Đỗ Thị Thu Hiền

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT521.O11.ANTT

STT	Họ và tên	MSSV	Email
1	Hoàng Anh Khoa	21522220	21522220@gm.uit.edu.vn
2	Đào Võ Hữu Hiệp	21522065	21522065@gm.uit.edu.vn
3	Nguyễn Đạo Ga Đô	21521955	21521955@gm.uit.edu.vn
4	Phạm Ngọc Thiện	21522627	21522627@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Câu 1	100%
2	Câu 2	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Các bước thực hiện/ Phương pháp thực hiện/Nội dung tìm hiểu (Ảnh chụp màn hình, có giải thích)

Đọc mô tả hệ thống phần mềm Hỗ trợ Bảo dưỡng Phi cơ cần được phát triển của hãng hàng không A 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. Thực hiện các yêu cầu:

1) 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.

- Tác nhân Spoofing :
Kẻ tấn công có thể sử dụng các kĩ thuật như social engineering, information gathering ... để có thể đánh lừa và thu thập các thông tin về nhân viên hoặc quản lý với mục đích giả mạo danh tính của nạn nhân nhằm truy cập vào hệ thống.
Ngoài ra, các nhân viên trong hãng hàng không A cũng có thể giả mạo danh tính của đồng nghiệp để thực hiện các hành động xấu.

-Tác nhân Tampering:
Kẻ tấn công thực hiện thay đổi các dữ liệu về hoạt động bảo dưỡng như thời gian, các tác vụ cần thực hiện, kết quả kiểm tra ... nhằm gây thiệt hại về tiền bạc (thêm các nhiệm vụ thay mới các bộ phận không cần thiết) hoặc gây nguy hiểm cho máy móc thiết bị (xóa các nhiệm vụ kiểm tra hoặc làm giả kết quả kiểm tra).

- Tác nhân Repudiation :
Nhân viên thực hiện giả mạo các đồng nghiệp khác để thực hiện các hành động xấu trong quy trình làm việc có thể đổ tội cho nạn nhân bị giả mạo và chối bỏ hoàn toàn trách nhiệm của bản thân đối với những hành động đã thực hiện.
Nhân viên cũng có thể giả mạo kết quả thực hiện công việc của họ khi đính kèm vào hồ sơ dịch vụ.

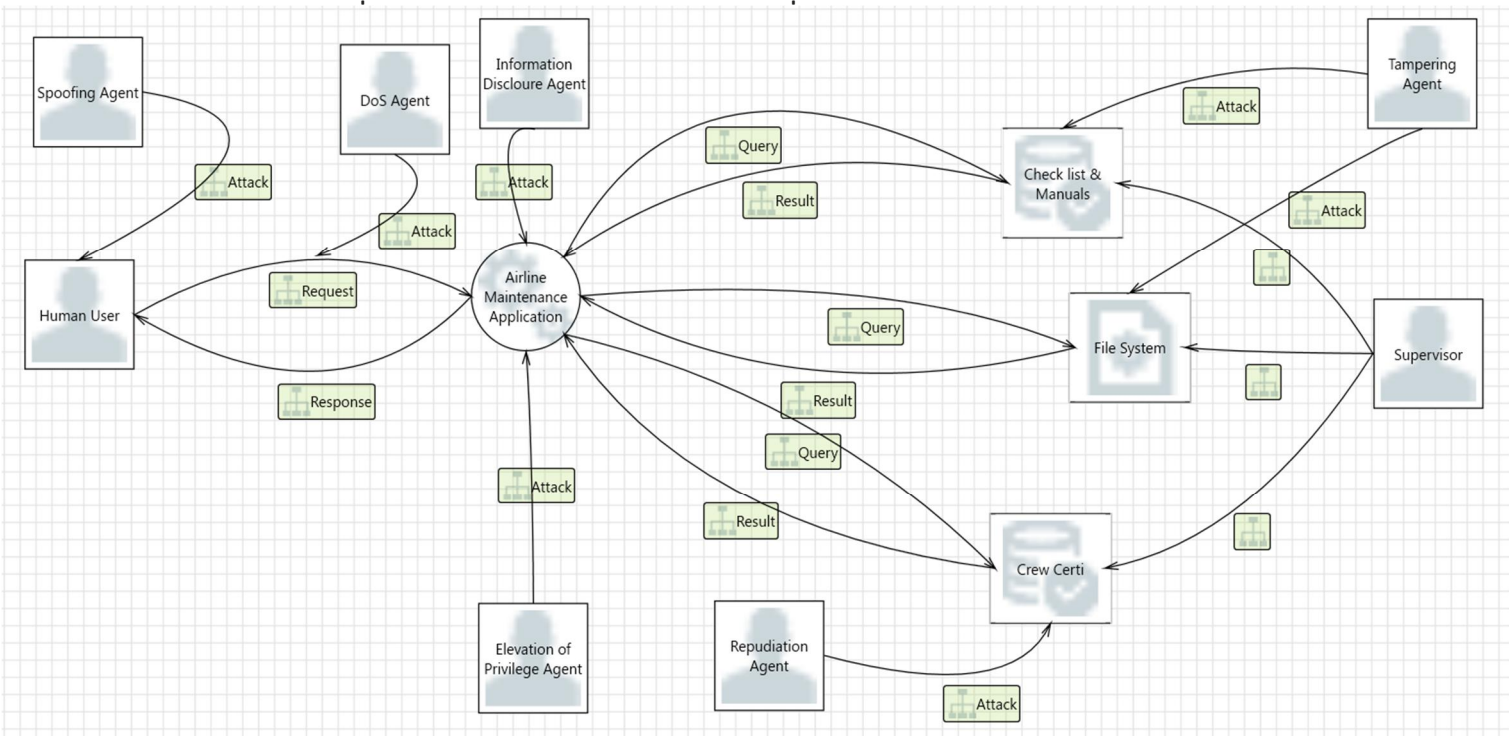
- Tác nhân Information Disclosure :
Kẻ tấn công cố gắng truy cập vào cơ sở dữ liệu nơi lưu trữ dữ liệu về bảo dưỡng máy bay và tiết lộ thông tin quan trọng về cấu trúc, quy trình bảo dưỡng hoặc chi tiết về máy bay cá nhân, thông tin về nhân sự hãng hàng không A (tên tuổi, chức vụ, chứng chỉ...).

Nhân viên một khi có được ipad có thể tải xuống tất các các thông tin về nhiệm vụ bảo dưỡng và những hồ sơ/thông tin chi tiết ... → Việc quản lý thông tin, phân quyền chưa hợp lý → lộ thông tin là việc hiển nhiên.
Ngoài ra, các lỗ hổng bảo mật trong ứng dụng cũ được sử dụng song song với ứng dụng mới có thể dẫn đến việc rò rỉ thông tin quan trọng cho các tác nhân đe dọa.

-Tác nhân Denial of Service :
Bởi vì nhiệm vụ bảo dưỡng được diễn ra ở sân bay (hoặc bên trong khu vực động cơ) nơi wifi không được đảm bảo. Do đó, kẻ tấn công có thể tập trung tấn công vào hệ thống mạng, làm ảnh hưởng đến đường truyền và tín hiệu -> gây ảnh hưởng đến việc sử dụng ứng dụng trên Ipad cho các nhân viên bảo dưỡng. Các nhiệm vụ có thể không thực hiện đúng, đầy đủ do thiếu sự hỗ trợ của ứng dụng.

- Tác nhân Elevation of Privilege :
Kẻ tấn công hoặc một thành viên của đội bảo dưỡng hoặc một người sử dụng có quyền truy cập vào ứng dụng. Bằng cách khai thác các lỗ hổng bảo mật hoặc sử dụng các kỹ thuật tấn công, tác nhân E có thể cố gắng tăng quyền truy cập và đặt mình vào vị trí có đặc quyền hơn trong hệ thống. Từ đó gây ra các thay đổi trên hệ thống.

2) Sử dụng công cụ "Microsoft Threat Modeling Tool" để vẽ bản thiết kế phần mềm và hiển thị các danh sách tác nhân đe dọa.



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 nộp bài theo thời gian quy định trên course.

Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Đặt tên theo định dạng: **[Mã lớp]-AssignmentX_NhomY** (trong đó X là Thứ tự Assignment, Y là số thứ tự nhóm đồ án theo danh sách đã đăng ký).

  Ví dụ: [NT521.O11.ANTT]-Assignment01_Nhom03.pdf.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.

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