

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 - SDLC

GVHD: Đỗ Thị Thu Hiền

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

A. Lớp: NT521.012.ATCL

STT	Họ và tên	MSSV	Email
1	Bùi Hoàng Trúc Anh	21521817	21521817@gm.uit.edu.vn
2	Lê Hoàng Oanh	21521253	21521253@gm.uit.edu.vn
3	Nguyễn Ngọc Trà My	21520353	21520353@gm.uit.edu.vn
4	Huỳnh Minh Tân Tiến	21521520	21521520@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:

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

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

BÁO CÁO CHI TIẾT

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.

Spoofing:

- Có thể truy cập bất hợp vào đường truyền wifi, tạo subnet ảo để bắt các gói tin, đánh cắp dữ liệu
- Tác nhân đe dọa có thể cố gắng giả mạo thiết bị iPad để truy cập vào ứng dụng "Bảo Dưỡng Phi Cơ".
- Người dùng không được xác thực một cách đầy đủ có thể mạo danh và truy cập vào dữ liệu bảo trì.

Tampering:

- Có thể truy cập bất hợp vào đường truyền wifi, tạo subnet ảo để bắt các gói tin, thay đổi dữ liệu

Information Disclosure:

- Nếu một người không có quyền truy cập vào dữ liệu bảo trì, họ có thể cố gắng thu thập thông tin về hướng dẫn sử dụng dịch vụ, danh sách kiểm tra hoặc thông tin khách hàng.
- Dữ liệu quan trọng về bảo trì máy bay có thể bị tiết lộ nếu có sự cố bảo mật.

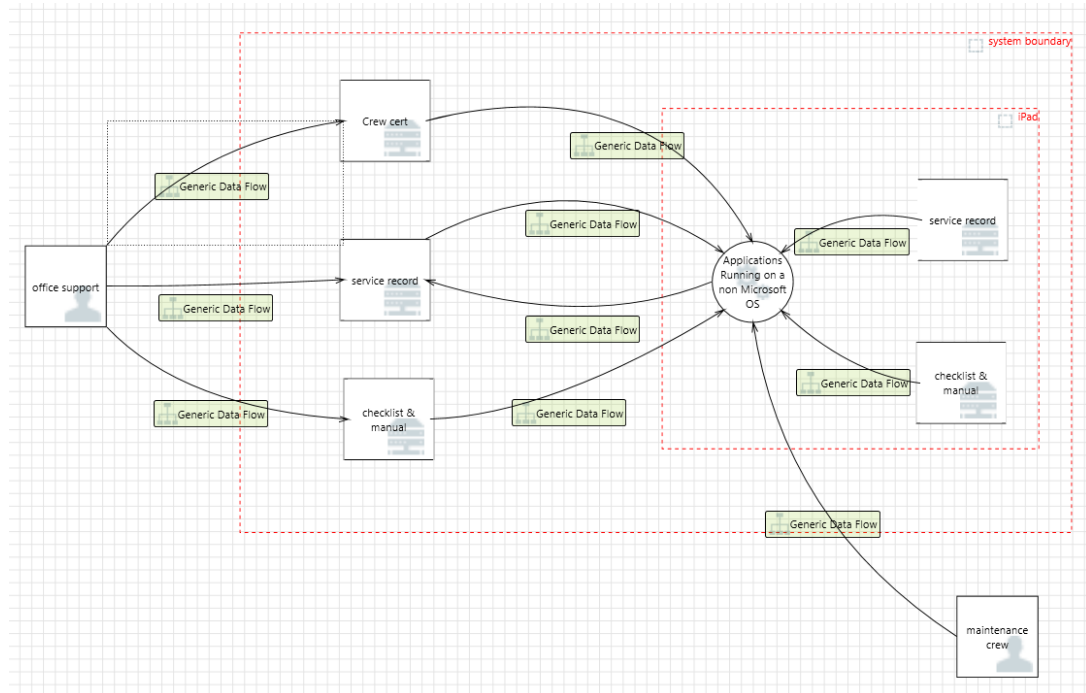
Denial of service (DOS):

- Sự không khả dụng của kết nối Wi-Fi ở ngoài sân bay hoặc trong khu vực động cơ của máy bay có thể gây ra sự cản trở trong việc sử dụng ứng dụng "Bảo Dưỡng Phi Cơ".
- Tấn công từ xa có thể tạo ra tình trạng quá tải trên hệ thống hoặc trên cơ sở dữ liệu, làm giảm hiệu suất hoặc làm cho dịch vụ không khả dụng.

Elevation of privilege:

- Người dùng không có quyền có thể cố gắng truy cập vào dữ liệu hoặc hệ thống bảo trì bằng cách bỏ qua quyền truy cập.
- Sự xâm nhập có thể xảy ra từ bên trong tổ chức hoặc từ bên ngoài nếu người dùng không bảo mật thiết bị iPad của họ.

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.



Threat List										
ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Priority
1	Diagram 1		Generated	Not Started	The Crew cert D	Tampering	Data flowing ac		Generic Data Fl	High
2	Diagram 1		Generated	Not Started	Data Store Deni	Repudiation	Crew cert claim:		Generic Data Fl	High
3	Diagram 1		Generated	Not Started	Data Flow Gene	Denial Of Servic	An external age		Generic Data Fl	High
4	Diagram 1		Generated	Not Started	Data Store Inaci	Denial Of Servic	An external age		Generic Data Fl	High
5	Diagram 1		Generated	Not Started	Spoofing of Des	Spoofing	service record n		Generic Data Fl	High
6	Diagram 1		Generated	Not Started	The service recc	Tampering	Data flowing ac		Generic Data Fl	High
7	Diagram 1		Generated	Not Started	Data Store Deni	Repudiation	service record c		Generic Data Fl	High
8	Diagram 1		Generated	Not Started	Data Flow Gene	Denial Of Servic	An external age		Generic Data Fl	High
9	Diagram 1		Generated	Not Started	Data Store Inaci	Denial Of Servic	An external age		Generic Data Fl	High
10	Diagram 1		Generated	Not Started	Spoofing of Des	Spoofing	checklist & man		Generic Data Fl	High
11	Diagram 1		Generated	Not Started	The checklist &	Tampering	Data flowing ac		Generic Data Fl	High
12	Diagram 1		Generated	Not Started	Data Store Deni	Repudiation	checklist & man		Generic Data Fl	High
13	Diagram 1		Generated	Not Started	Data Flow Gene	Denial Of Servic	An external age		Generic Data Fl	High
14	Diagram 1		Generated	Not Started	Data Store Inaci	Denial Of Servic	An external age		Generic Data Fl	High
17	Diagram 1		Generated	Not Started	Spoofing of Sou	Spoofing	service record n		Generic Data Fl	High
18	Diagram 1		Generated	Not Started	Weak Access Cc	Information Dis	Improper data f		Generic Data Fl	High
19	Diagram 1		Generated	Not Started	Spoofing of Sou	Spoofing	checklist & man		Generic Data Fl	High
20	Diagram 1		Generated	Not Started	Weak Access Cc	Information Dis	Improper data f		Generic Data Fl	High
32	Diagram 1		Generated	Not Started	Spoofing the A	Spoofing	Applications Ru		Generic Data Fl	High
33	Diagram 1		Generated	Not Started	Spoofing the m	Spoofing	maintenance cr		Generic Data Fl	High
34	Diagram 1		Generated	Not Started	Potential Lack o	Tampering	Data flowing ac		Generic Data Fl	High
35	Diagram 1		Generated	Not Started	Potential Data F	Repudiation	Applications Ru		Generic Data Fl	High
36	Diagram 1		Generated	Not Started	Data Flow Sniffi	Information Dis	Data flowing ac		Generic Data Fl	High

Threat List										
ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Priority
36	Diagram 1		Generated	Not Started	Data Flow Sniffi	Information Dis	Data flowing ac		Generic Data Fl	High
37	Diagram 1		Generated	Not Started	Potential Proce	Denial Of Servic	Applications Ru		Generic Data Fl	High
38	Diagram 1		Generated	Not Started	Data Flow Gene	Denial Of Servic	An external age		Generic Data Fl	High
39	Diagram 1		Generated	Not Started	Elevation Using	Elevation Of Pri	Applications Ru		Generic Data Fl	High
40	Diagram 1		Generated	Not Started	Applications Ru	Elevation Of Pri	maintenance cr		Generic Data Fl	High
41	Diagram 1		Generated	Not Started	Elevation by Chi	Elevation Of Pri	An attacker ma		Generic Data Fl	High
42	Diagram 1		Generated	Not Started	Cross Site Requ	Elevation Of Pri	Cross-site requ		Generic Data Fl	High
43	Diagram 1		Generated	Not Started	Spoofing the A	Spoofing	Applications Ru		Generic Data Fl	High
44	Diagram 1		Generated	Not Started	Spoofing of Sou	Spoofing	Crew cert may k		Generic Data Fl	High
45	Diagram 1		Generated	Not Started	Potential Data F	Repudiation	Applications Ru		Generic Data Fl	High
46	Diagram 1		Generated	Not Started	Weak Access Co	Information Dis	Improper data f		Generic Data Fl	High
47	Diagram 1		Generated	Not Started	Potential Proce	Denial Of Servic	Applications Ru		Generic Data Fl	High
48	Diagram 1		Generated	Not Started	Data Flow Gene	Denial Of Servic	An external age		Generic Data Fl	High
49	Diagram 1		Generated	Not Started	Data Store Inac	Denial Of Servic	An external age		Generic Data Fl	High
50	Diagram 1		Generated	Not Started	Applications Ru	Elevation Of Pri	Crew cert may k		Generic Data Fl	High
51	Diagram 1		Generated	Not Started	Elevation by Chi	Elevation Of Pri	An attacker ma		Generic Data Fl	High
52	Diagram 1		Generated	Not Started	Spoofing the A	Spoofing	Applications Ru		Generic Data Fl	High
53	Diagram 1		Generated	Not Started	Spoofing of Sou	Spoofing	service record n		Generic Data Fl	High
54	Diagram 1		Generated	Not Started	Potential Data F	Repudiation	Applications Ru		Generic Data Fl	High
55	Diagram 1		Generated	Not Started	Weak Access Co	Information Dis	Improper data f		Generic Data Fl	High
56	Diagram 1		Generated	Not Started	Potential Proce	Denial Of Servic	Applications Ru		Generic Data Fl	High
57	Diagram 1		Generated	Not Started	Data Flow Gene	Denial Of Servic	An external age		Generic Data Fl	High
58	Diagram 1		Generated	Not Started	Data Store Inac	Denial Of Servic	An external age		Generic Data Fl	High

Threat List										
ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Priority
56	Diagram 1		Generated	Not Started	Potential Proce	Denial Of Servic	Applications Ru		Generic Data Fl	High
57	Diagram 1		Generated	Not Started	Data Flow Gene	Denial Of Servic	An external age		Generic Data Fl	High
58	Diagram 1		Generated	Not Started	Data Store Inac	Denial Of Servic	An external age		Generic Data Fl	High
59	Diagram 1		Generated	Not Started	Applications Ru	Elevation Of Pri	service record n		Generic Data Fl	High
60	Diagram 1		Generated	Not Started	Elevation by Chi	Elevation Of Pri	An attacker ma		Generic Data Fl	High
61	Diagram 1		Generated	Not Started	Spoofing the A	Spoofing	Applications Ru		Generic Data Fl	High
62	Diagram 1		Generated	Not Started	Spoofing of Des	Spoofing	service record n		Generic Data Fl	High
63	Diagram 1		Generated	Not Started	The service recc	Tampering	Data flowing ac		Generic Data Fl	High
64	Diagram 1		Generated	Not Started	Data Store Deni	Repudiation	service record c		Generic Data Fl	High
65	Diagram 1		Generated	Not Started	Data Flow Sniffi	Information Dis	Data flowing ac		Generic Data Fl	High
66	Diagram 1		Generated	Not Started	Potential Excess	Denial Of Servic	Does Applicatio		Generic Data Fl	High
67	Diagram 1		Generated	Not Started	Data Flow Gene	Denial Of Servic	An external age		Generic Data Fl	High
68	Diagram 1		Generated	Not Started	Data Store Inac	Denial Of Servic	An external age		Generic Data Fl	High
69	Diagram 1		Generated	Not Started	Spoofing the A	Spoofing	Applications Ru		Generic Data Fl	High
70	Diagram 1		Generated	Not Started	Spoofing of Sou	Spoofing	checklist & man		Generic Data Fl	High
71	Diagram 1		Generated	Not Started	Potential Data F	Repudiation	Applications Ru		Generic Data Fl	High
72	Diagram 1		Generated	Not Started	Weak Access Co	Information Dis	Improper data f		Generic Data Fl	High
73	Diagram 1		Generated	Not Started	Potential Proce	Denial Of Servic	Applications Ru		Generic Data Fl	High
74	Diagram 1		Generated	Not Started	Data Flow Gene	Denial Of Servic	An external age		Generic Data Fl	High
75	Diagram 1		Generated	Not Started	Data Store Inac	Denial Of Servic	An external age		Generic Data Fl	High
76	Diagram 1		Generated	Not Started	Applications Ru	Elevation Of Pri	checklist & man		Generic Data Fl	High
77	Diagram 1		Generated	Not Started	Elevation by Chi	Elevation Of Pri	An attacker ma		Generic Data Fl	High
78	Diagram 1		Generated	Not Started	Spoofing of Des	Spoofing	Crew cert may k		Generic Data Fl	High

[Export Csv](#) 65 Threats Displayed, 65 Total

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: *[NT521.011.ATCL]-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