BÁO CÁO BÀI TẬP

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

Tên chủ đề: Exercise 2

GVHD: Phan Thế Duy

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: ANTN2020

STT	Họ và tên	MSSV	Email
1	Nguyễn Bình Thục Trâm	20250815	20520815@gm.uit.edu.vn
2	Nguyễn Bùi Kim Ngân	20520648	20520648@gm.uit.edu.vn
3	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	1.1	100%
2	1.2	100%
3	1.3	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

III. Nội dung tìm hiểu:

1.1. Quy trình phát triển phần mềm an toàn

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.*

⇨ Theo nhóm chúng em thì yêu cầu 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 là Least Privilege bởi vì các mối đe dọa có thể đến từ bên trong, bên ngoài và phía cộng tác với doanh nghiệp hay cá nhân.

Lý do: Trong khi thực hiện thiết kế cho một công ty hoặc cá nhận thì cần phải giải quyết việc truy cập đến hệ thống hay phần mềm bởi rất nhiều người bởi nhiều thành phần khác nhau:

Phía bên ngoài thì đó là người dùng (quyền user)

Phía bên trong thì phải có quản trị (quyền administrator), team dev hay test (quyền edit), team reviewer (quyền view).

Phía cộng tác khi thực hiện dự án cùng công ty hay cá nhân mà công ty, cá nhân đó thuê outsource thì phải có thêm cả quyền cho bên cộng tác viên outsource (quyền collaborator)

Từ việc phân quyền hữu hạn bên trên có thể giúp chặn đứng một số vấn đề xảy ra từ ba bên trên, có thể là vô tình hoặc là cố ý thì một trong ba bên trên làm ảnh hưởng đến hệ thống hoặc phần mềm thì vẫn có khả năng quản lý, truy vết và phục hồi sau khi có vấn đề cũng như là dự đoán trước được những khả năng có thể xảy ra đối với hệ thống nhằm đảm bảo tính confidence cho công ty cũng như là cá nhân. Ví dụ, user chỉ được sử dụng một số tính năng dành cho người dùng chứ không được chỉnh sửa gì trong phần mềm hay hệ thống, còn editor chỉ có quyền code, add module,... chứ không được toàn quyền như phía admin. Còn về phía collaborator thì sẽ được cấp quyền hỗ trợ code hay test hoặc vận hành sau đó kết thúc việc cộng tác sẽ được thu hồi lại quyền vì vậy hạn chế được việc người đó đã hết cộng tác mà vẫn có nhiều việc can thiệp vào hệ thống.

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.*

⇨ 5 loại tính năng bảo mật cần có trong các framework hiện đại là: Identify, Protect, Detect, Respond, Recover.

(5 security functionality. Source: https://www.nist.gov/cyberframework/online-learning/five-functions)

⇨ Vai trò trong hệ thống phần mềm:

- Identify: Tính năng này đóng vai trò hỗ trợ trong việc nâng cao nhận thức về quản lý rủi ro an ninh mạng đối với hệ thống, con người, tài sản, dữ liệu trong nhiều trường hợp xảy ra. Từ đó tiến hành đánh giá và xây dựng chiến lược quản lí rủi ro trong hệ thống, xác định các chính sách bảo mật phù hợp với hệ thống.
- Protect: Tính năng này đóng vai trò vạch ra các biện pháp bảo vệ thích hợp để đảm bảo cung cấp các dịch vụ cơ sở hạ tầng quan trọng. Protect hỗ trợ việc ngăn chặn, hạn chế các tác động trong một sự kiện, một cuộc tấn công an ninh tiềm ẩn.
- Dectect: Tính năng này đóng vai trò xác định các hoạt động thích hợp để xác định sự xuất hiện của một sự kiện, cuộc tấn công an ninh mạng; cho phép phát hiện kịp thời các sự kiện an ninh mạng.
- Respond: Tính năng này đóng vai trò thực hiện hành động đáp lại liên quan đến sự cố an ninh mạng được phát hiện; hỗ trợ khả năng ngăn chặn sự tác động từ một sự cố an ninh mạng tiềm ẩn.
- Recover: Tính năng này đóng vai trò xác định các hoạt động cần thiết nhằm duy trì các kế hoạch có khả năng phục hồi và khôi phục bất kỳ tính năng hoặc dịch vụ nào đó đã bị suy giảm do sự cố an ninh mạng. Recover sẽ hỗ trợ khôi phục kịp thời để hệ thống có thể hoạt động bình thường, giảm tác động từ sự cố an ninh mạng.

1.2. Phân tích lỗi Thiết kế không an toàn (Insecure Design):

CWE-256: Unprotected Storage of Credentials, là lỗ hổng lưu trữ thông tin xác thực không được bảo vệ. Nguyên nhân đến từ việc mật khẩu được lưu trữ ở dạng plaintext và có thể dễ dàng lấy được như trong thuộc tính, cấu hình file hoặc trong memory của ứng dụng.

Ví dụ CVE-2022-34816, sản phẩm HPE Network Virtualization verson 1.0 của nhà cung cấp Jenkins, đã lưu trữ mật khẩu không được mã hoá trong global configuration file

trên Jenkins controller, nơi mà chúng có thể bị xem bởi user có quyền truy cập vào file system của Jenkins controller (source: https://www.cvedetails.com/cve/CVE-2022-34816/)

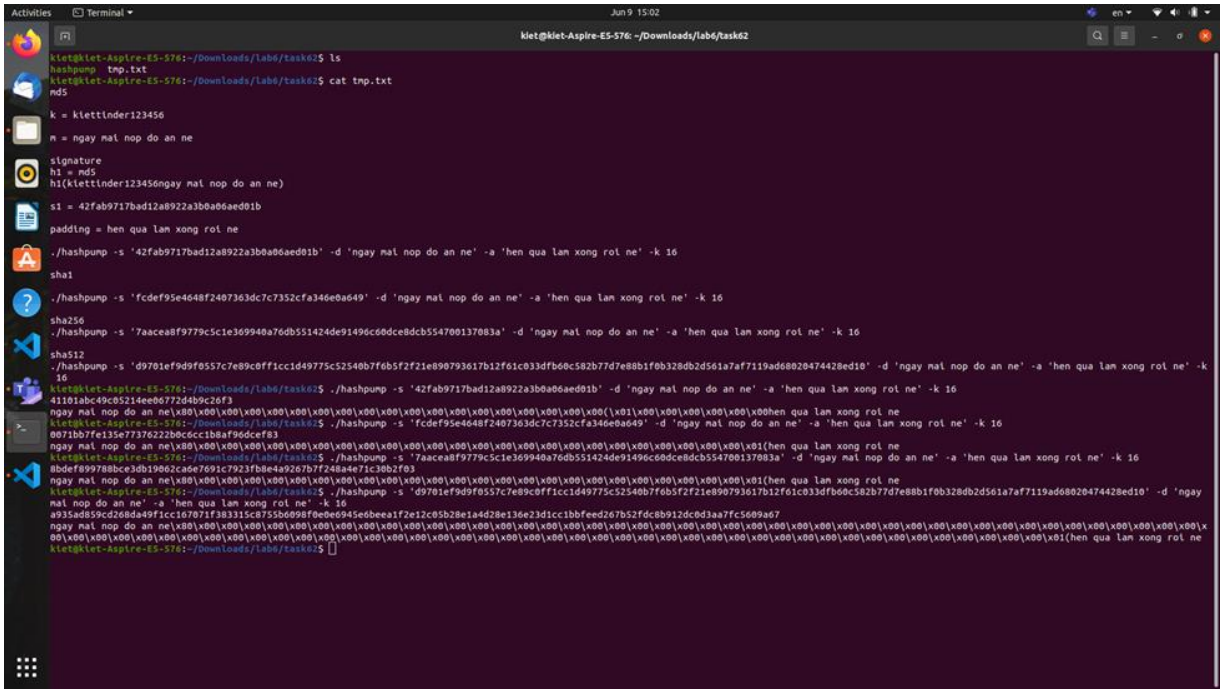
Demo:

Bảng các dạng lưu của mật khẩu

Mật khẩu plaintext	Mật khẩu với SHA256(K||M)	Mật khẩu với SHA256(K||SHA256(K||M))
VoAnhKiet!20520605	654b01fef41659754c564031be6665cf439059d8b4a10321855e34d5d41f2c86	670be9fe200b5e752fe08479300c9b37bdbfc3c240d8e2aa66ca0fad4f064546
NguyenBuiKimNgan!20520648	426f3f450dae3464d3558d38a06dce475d9f807d435184af512a059f781402d2	8090db317f8792a3aeffe2338f2197dff220a3cd9817009b1eb8a97c9362fd54
NguyenBinhThucTram!20520815	cf30fb892102446773ba62f450d106d01e47e2a2747e257f330627a147897d24	646f2c07be2e5e3e40f3029eba2b85d464a81335b0c92a804b1716473b240478

Giả sử như những mật khẩu được lưu trong configuration file trên Jenkins controller tương tự như mật khẩu plaintext (cột 1 "bảng các dạng lưu của mật khẩu") có thể là một mối đe dọa đến vấn đề confidentiality.

Gợi ý: có thể lưu dưới dạng băm với những hàm băm đời 2 hoặc đời 3 trong cột 2 trong "bảng các dạng lưu của mật khẩu" đó là kiểu hàm băm đời 2 sha256, nhưng có thể xảy ra vấn đề về việc bị tấn công theo kiểu "Length extension attacks on MAC in form" với các hàm băm bằng cách add thêm các padding vào mà trong đó có thể là các câu lệnh SQL nguy hiểm. Dưới đây là một ví dụ minh họa



Như vậy có thể chống lại cuộc tấn công bằng các cách:

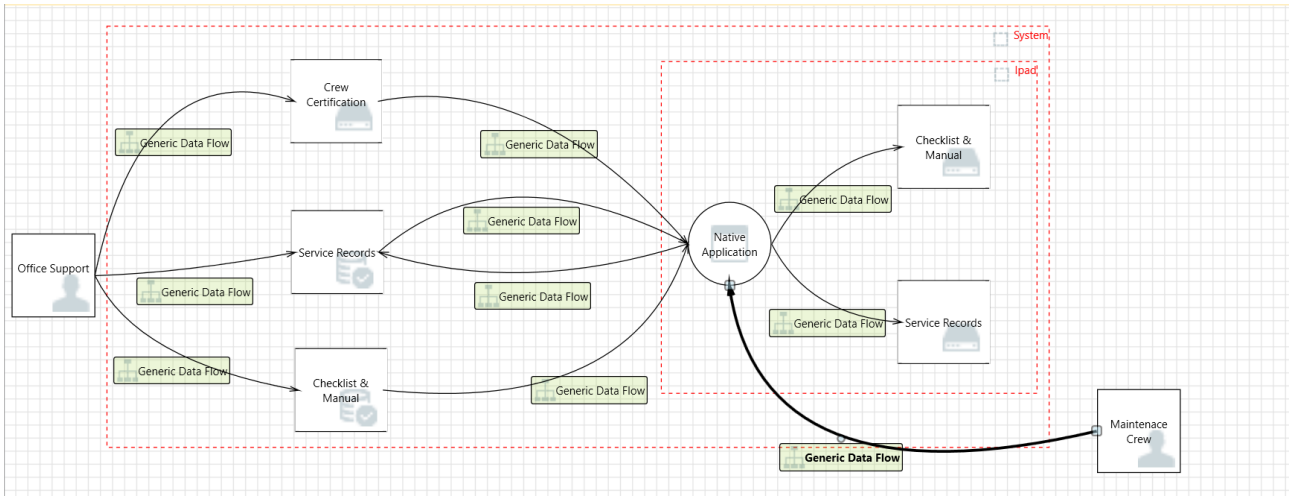
Cách 1: cài đặt SHA256(M||K) thay vì SHA256(K||M)

Cách 2: cài đặt SHA256(K||SHA256(K||M)

Cách 2 được trình bày như cột 3 trong "bảng các dạng lưu của mật khẩu"

1.3. Mô hình hóa tác nhân đe dọa (Thread Modeling)

Thread Modeling diagram native app "Bảo dưỡng phi cơ":

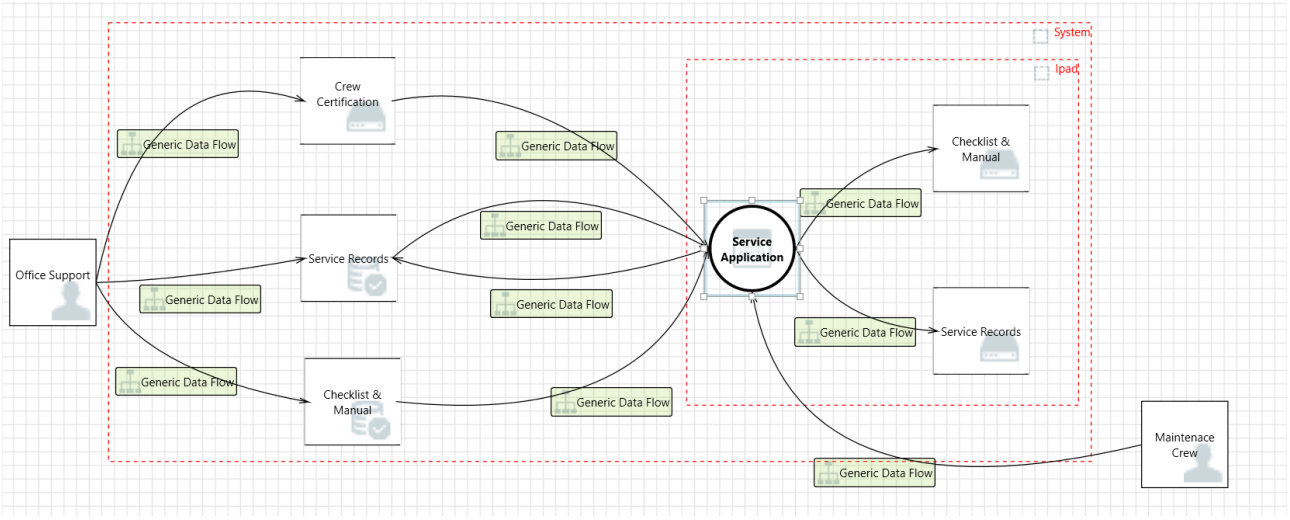


Thread List mà Microsoft Threat Modeling tool phát hiện được:

Threat List

ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Priority
4	Diagram 1		Generated	Not Started	Spoofing of Des	Spoofing	Crew Certificati		Generic Data Fl	High
5	Diagram 1		Generated	Not Started	Spoofing of Des	Spoofing	Checklist & Mar		Generic Data Fl	High
6	Diagram 1		Generated	Not Started	Possible SQL Inj	Tampering	SQL injection is		Generic Data Fl	High
7	Diagram 1		Generated	Not Started	Spoofing of Des	Spoofing	Service Records		Generic Data Fl	High
8	Diagram 1		Generated	Not Started	Possible SQL Inj	Tampering	SQL injection is		Generic Data Fl	High
80	Diagram 1		Generated	Not Started	Spoofing of Des	Spoofing	Checklist & Mar		Generic Data Fl	High
81	Diagram 1		Generated	Not Started	Potential Excess	Denial Of Servic	Does Native Ap		Generic Data Fl	High
82	Diagram 1		Generated	Not Started	Spoofing of Des	Spoofing	Service Records		Generic Data Fl	High
83	Diagram 1		Generated	Not Started	Potential Excess	Denial Of Servic	Does Native Ap		Generic Data Fl	High
84	Diagram 1		Generated	Not Started	Spoofing of Sou	Spoofing	Crew Certificati		Generic Data Fl	High
85	Diagram 1		Generated	Not Started	Weak Access Co	Information Dis	Improper data p		Generic Data Fl	High
86	Diagram 1		Generated	Not Started	Spoofing of Sou	Spoofing	Service Records		Generic Data Fl	High
87	Diagram 1		Generated	Not Started	Weak Access Co	Information Dis	Improper data p		Generic Data Fl	High
88	Diagram 1		Generated	Not Started	Spoofing of Des	Spoofing	Service Records		Generic Data Fl	High
89	Diagram 1		Generated	Not Started	Potential SQL In	Tampering	SQL injection is		Generic Data Fl	High
90	Diagram 1		Generated	Not Started	Potential Excess	Denial Of Servic	Does Native Ap		Generic Data Fl	High
91	Diagram 1		Generated	Not Started	Spoofing of Sou	Spoofing	Checklist & Mar		Generic Data Fl	High
92	Diagram 1		Generated	Not Started	Weak Access Co	Information Dis	Improper data p		Generic Data Fl	High
93	Diagram 1		Generated	Not Started	Spoofing the M	Spoofing	Maintenace Cre		Generic Data Fl	High
94	Diagram 1		Generated	Not Started	Elevation Using	Elevation Of Pri	Native Applicati		Generic Data Fl	High

Thread Modeling diagram web app "Bảo dưỡng phi cơ":



Thread List mà Microsoft Threat Modeling tool phát hiện được:

4	Diagram 1	Generated	Not Started	Spoofing of Des	Spoofing	Crew Certificati	Generic Data Fl	High
5	Diagram 1	Generated	Not Started	Spoofing of Des	Spoofing	Checklist & Mar	Generic Data Fl	High
6	Diagram 1	Generated	Not Started	Possible SQL Inj	Tampering	SQL injection is	Generic Data Fl	High
7	Diagram 1	Generated	Not Started	Spoofing of Des	Spoofing	Service Records	Generic Data Fl	High
8	Diagram 1	Generated	Not Started	Possible SQL Inj	Tampering	SQL injection is	Generic Data Fl	High
95	Diagram 1	Generated	Not Started	Spoofing of Des	Spoofing	Checklist & Mar	Generic Data Fl	High
96	Diagram 1	Generated	Not Started	Potential Excess	Denial Of Servic	Does Service Ap	Generic Data Fl	High
97	Diagram 1	Generated	Not Started	Spoofing of Des	Spoofing	Service Records	Generic Data Fl	High
98	Diagram 1	Generated	Not Started	Potential Excess	Denial Of Servic	Does Service Ap	Generic Data Fl	High
99	Diagram 1	Generated	Not Started	Spoofing of Sou	Spoofing	Crew Certificati	Generic Data Fl	High
100	Diagram 1	Generated	Not Started	Cross Site Script	Tampering	The web server	Generic Data Fl	High
101	Diagram 1	Generated	Not Started	Persistent Cross	Tampering	The web server	Generic Data Fl	High
102	Diagram 1	Generated	Not Started	Weak Access Co	Information Dis	Improper data p	Generic Data Fl	High
103	Diagram 1	Generated	Not Started	Spoofing of Sou	Spoofing	Service Records	Generic Data Fl	High
104	Diagram 1	Generated	Not Started	Cross Site Script	Tampering	The web server	Generic Data Fl	High
105	Diagram 1	Generated	Not Started	Persistent Cross	Tampering	The web server	Generic Data Fl	High
106	Diagram 1	Generated	Not Started	Weak Access Co	Information Dis	Improper data p	Generic Data Fl	High
107	Diagram 1	Generated	Not Started	Spoofing of Des	Spoofing	Service Records	Generic Data Fl	High
108	Diagram 1	Generated	Not Started	Potential SQL In	Tampering	SQL injection is	Generic Data Fl	High
109	Diagram 1	Generated	Not Started	Potential Excess	Denial Of Servic	Does Service Ap	Generic Data Fl	High
110	Diagram 1	Generated	Not Started	Spoofing of Sou	Spoofing	Checklist & Mar	Generic Data Fl	High
111	Diagram 1	Generated	Not Started	Cross Site Script	Tampering	The web server	Generic Data Fl	High
112	Diagram 1	Generated	Not Started	Persistent Cross	Tampering	The web server	Generic Data Fl	High
113	Diagram 1	Generated	Not Started	Weak Access Co	Information Dis	Improper data p	Generic Data Fl	High
114	Diagram 1	Generated	Not Started	Spoofing the M	Spoofing	Maintenace Cre	Generic Data Fl	High
115	Diagram 1	Generated	Not Started	Cross Site Script	Tampering	The web server	Generic Data Fl	High
116	Diagram 1	Generated	Not Started	Elevation Using	Elevation Of Pri	Service Applicat	Generic Data Fl	High

- Khi thay đổi sang web app, threat list đã có sự thay đổi.

- Cụ thể, từ hình trên có thể thấy số lượng threat khi sử dụng web app tăng lên, chủ yếu là lỗ hổng liên quan đến web server và truyền dữ liệu qua web server. Vì thế, có thể xác định khi từ một native app chuyển sang web app thì sẽ gặp nhiều vấn đề bảo mật hơn, vì web app sẽ dễ bị tấn công hơn (do phải giao tiếp với internet) so với native app.

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, 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*]-Exe01_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