

BIÊN BẢN
HỌP HỘI ĐỒNG CHẤM ĐỀ ÁN TỐT NGHIỆP THẠC SĨ

Căn cứ quyết định số Quyết định số 289/QĐ-HV ngày 06 tháng 03 năm 2024 của Giám đốc Học viện Công nghệ Bưu chính Viễn thông về việc thành lập Hội đồng chấm đề án tốt nghiệp thạc sĩ. Hội đồng đã họp vào hồi 10 giờ 00 phút, ngày 20 tháng 03 năm 2024 tại Học viện Công nghệ Bưu chính Viễn thông để chấm đề án tốt nghiệp thạc sĩ cho:

Học viên: **Đàm Tiến Đạt**

Tên đề án tốt nghiệp: **Phương pháp phát hiện lỗ hổng mã nguồn dựa trên tập luật**

Chuyên ngành: **Hệ thống thông tin** Mã số: **8.48.01.04**

Các thành viên của Hội đồng chấm đề án tốt nghiệp có mặt: 5 / 05

TT	HỌ VÀ TÊN	TRÁCH NHIỆM TRONG HĐ	GHI CHÚ
1	GS.TS. Từ Minh Phương	Chủ tịch	
2	TS. Trần Tiến Công	Thư ký	
3	PGS.TS. Hoàng Xuân Dậu	Phản biện 1	
4	PGS.TS. Nguyễn Long Giang	Phản biện 2	
5	PGS.TS. Phan Xuân Hiếu	Ủy viên	

Các nội dung thực hiện:

- Chủ tịch Hội đồng điều khiển buổi họp. Công bố quyết định của Giám đốc Học viện Công nghệ Bưu chính Viễn thông về việc thành lập Hội đồng chấm đề án tốt nghiệp thạc sĩ.
- Người hướng dẫn khoa học hoặc thư ký đọc lý lịch khoa học và các điều kiện bảo vệ đề án tốt nghiệp của học viên (Có bản lý lịch khoa học và kết quả các môn học cao học của học viên kèm theo).
- Học viên trình bày tóm tắt đề án tốt nghiệp.
- Phản biện 1 đọc nhận xét (có văn bản kèm theo)
- Phản biện 2 đọc nhận xét (có văn bản kèm theo)
- Các câu hỏi của thành viên Hội đồng:

Kết cấu bài báo không cân bằng, thiếu 3 ý nội dung
Bổ sung phần dẫn, phần của tăng cường để phân giải ảnh
chụp nano hình
Phân tích có nguyên tắc và luật, trình bày rõ ràng về tập luật?
hạn giải về thực nghiệm, đánh giá phần mềm cũng cần có và được gì?
Phát hiện lỗ hổng trên mã nguồn của đơn vị?

7. Trả lời của học viên:

- Ưu điểm của MobSF là dịch sẵn mã nguồn rồi phát hành lên, tạo kết quả trực quan, phân tích thêm các domain.
- Học viên chưa trả lời được câu hỏi về điểm của phát hiện là hệ thống nào.
- Học viên chưa trả lời được câu hỏi về thực.

8. Thư ký đọc nhận xét về quá trình thực hiện đề án tốt nghiệp của học viên (có văn bản kèm theo).

9. Hội đồng hợp riêng:

- Bầu Ban kiểm phiếu:

1. Trưởng Ban kiểm phiếu: PGS.TS Hoàng Xuân Việt
2. Ủy viên Ban kiểm phiếu: TS Trần Bình Công
3. Ủy viên Ban kiểm phiếu: PGS.TS Phan Xuân Kiên

- Hội đồng chấm đề án tốt nghiệp bằng bỏ phiếu kín.

- Ban kiểm phiếu làm việc:

- Trưởng Ban kiểm phiếu báo cáo kết quả kiểm phiếu (có Biên bản họp Ban kiểm phiếu kèm theo)

- Điểm trung bình của đề án tốt nghiệp: 7.5

Kết luận:

1. Các nội dung cần chỉnh sửa, hoàn thiện sau bảo vệ đề án tốt nghiệp:

• Bà sống và chữa của lại toàn bộ để an theo góp ý từ bên bên nhận xét của phía bên và các thành viên từ hội đồng

2. Đề nghị Học viện công nhận (hoặc không) và cấp bằng (hoặc không) thạc sĩ cho học viên:

3. Đề án tốt nghiệp có thể phát triển thành đề tài nghiên cứu cho NCS.....

Buổi làm việc kết thúc vào..... cùng ngày.

Chủ tịch

Alm

GS.TS. Từ Minh Phương

Thư ký

CG

TS. Trần Tiến Công

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

=====

BẢN NHẬN XÉT LUẬN VĂN TỐT NGHIỆP THẠC SĨ

(Dùng cho người phản biện)

Tên đề tài luận văn: Phương pháp phát hiện lỗ hổng mã nguồn dựa trên tập luật

Chuyên ngành: Hệ thống thông tin

Mã số: 8.48.01.04

Họ và tên học viên: Đàm Tiến Đạt

Họ và tên người nhận xét: PGS.TS. Nguyễn Long Giang

Cơ quan công tác: Viện Công nghệ thông tin, Viện Hàn Lâm KH&CN Việt Nam

Số điện thoại: 0904739189

Email: nlgiang@ioit.ac.vn

NỘI DUNG NHẬN XÉT

1. Cơ sở khoa học và thực tiễn, sự cần thiết lựa chọn đề tài

Phát hiện lỗ hổng bảo mật là chủ đề nghiên cứu quan trọng trong lĩnh vực an toàn thông tin. Luận văn nghiên cứu công cụ MobSF để giải quyết bài toán phát hiện lỗ hổng bảo mật mã nguồn dựa trên tập luật và thử nghiệm với rà quét và phát hiện lỗ hổng mã nguồn của phần mềm Egov Quảng Nam phiên bản Android. Chủ đề nghiên cứu của luận văn có ý nghĩa thực tiễn.

2. Nội dung của luận văn, các kết quả đã đạt được

Luận văn đạt được kết quả chính như sau:

- 1) Tìm hiểu bài toán phát hiện lỗ hổng bảo mật mã nguồn và công cụ MobSF phát hiện mã nguồn dựa trên tập luật
- 2) Thử nghiệm công cụ MobSF với bài toán và phát hiện lỗ hổng mã nguồn của phần mềm Egov Quảng Nam phiên bản Android

Tuy nhiên, phần tập luật chưa được làm rõ trong luận văn là thực hiện như thế nào (phần điều kiện/kết luận) và luận văn chỉ dừng lại ở việc sử dụng công cụ.

3. Những vấn đề học viên cần giải thích thêm

- Rà soát, chỉnh sửa luận văn về trình bày, các hình vẽ quá nhỏ và chụp quá nhiều giao diện, đặc biệt là phần 2.1.1 báo cáo kết quả công cụ MobSF và 2.3.1 về thành phần trong tập luật. Cần bổ sung trích dẫn tài liệu tham khảo (chưa có)

- Phần 1.2 chương 1 mô tả các công cụ phát hiện, tuy nhiên chưa có đánh giá các công cụ và mô tả vấn đề công cụ sử dụng ở chương 3, cần bổ sung tại sao lại sử dụng công cụ ở Chương 3 (MobSF)

- Phần chương 2, Mục 2.3.1 trình bày quá lan man về tính năng của MobSF mà thiếu tính cấu trúc hay đặc tả tính năng. Mục 2.3.2 chỉ trình bày các quy tắc (7 quy tắc) mà không mô tả rõ tập luật như thế nào (phân điều kiện/kết luận) và thực hiện trên MobSF như thế nào ?

- Phần Chương 3 thực nghiệm, phần kết quả thực hiện (mục 3.3) chưa đầy đủ như kịch bản /các bước đã mô tả. Chưa rõ việc phát hiện lỗ hổng dựa trên tập luật trên công cụ?

4. Kết luận

- Đồng ý cho phép học viên bảo vệ luận văn tốt nghiệp.
- Đề nghị học viên chỉnh sửa/bổ sung luận văn theo góp ý.

Câu hỏi: 1) Trình bày mô hình tập luật (ví dụ minh họa) và cách thực hiện cấu hình tập luật trên công cụ MobSF ?

Hà Nội, ngày 14 tháng 03 năm 2024

XÁC NHẬN CỦA CƠ QUAN

NGƯỜI NHẬN XÉT



Nguyễn Long Giang

BẢN NHẬN XÉT ĐỀ ÁN TỐT NGHIỆP THẠC SỸ
(Dùng cho người phản biện)

Tên đề tài đề án: Phương pháp phát hiện lỗ hổng mã nguồn dựa trên tập luật

Chuyên ngành: Hệ thống thông tin

Mã số: 60.48.01.04

Tên học viên: Đàm Tiến Đạt

Họ và tên người nhận xét: Hoàng Xuân Dâu

Học hàm, học vị: PGS. Tiến sỹ, Giảng viên cao cấp

Chuyên ngành: Khoa học máy tính

Cơ quan công tác: Khoa ATTT, Học viện Công nghệ BC-VT

NỘI DUNG NHẬN XÉT

I/ Cơ sở khoa học và thực tiễn, tính cấp thiết của đề tài:

- Đề tài có ý nghĩa thực tiễn trong việc phát hiện lỗ hổng bảo mật, nhằm tăng cường an toàn cho các phần mềm.

II/ Về nội dung, chất lượng của đề án, các kết quả đạt được (so với đề cương đã được duyệt):

*** Nội dung đề án:**

Đề án tốt nghiệp của học viên gồm 3 chương chính:

Chương 1 giới thiệu tổng quan về phát hiện lỗ hổng mã nguồn dựa trên tập luật.

Chương 2 mô tả quá trình phát hiện lỗ hổng mã nguồn dựa trên tập luật sử dụng công cụ MobSF.

Chương 3 mô tả quá trình thực nghiệm và một số kết quả phát hiện lỗ hổng của 1 phần mềm trên nền tảng Android.

*** Chất lượng đề án:** Trung bình

*** Các kết quả đạt được:** cơ bản đạt các kết quả theo đề cương được duyệt.

III/ Những vấn đề cần giải thích thêm:

- Đề án bố cục thành 3 chương là hợp lý, tuy nhiên kết cấu các chương không cân bằng, trong đó chương 3 quá ngắn chỉ khoảng 5 trang.

- Đề án quá lạm dụng cách viết sử dụng văn nói dẫn đến nội dung lắt nhắt, khó theo dõi. Ngoài ra đề án còn dùng lẫn lộn các từ “đề án”, “luận văn”
- Đề án có cung cấp danh sách tài liệu tham khảo, nhưng không hề có trích dẫn.
- Khá nhiều ảnh chụp màn hình chữ quá nhỏ, mờ, không thể đọc ở chương 2, 3.
- Đề án nêu vấn đề phát hiện lỗ hổng bảo mật phần mềm dựa trên mã nguồn sử dụng tập luật, nhưng không mô tả được rõ ràng tập luật là gì. Tập luật nêu ở mục 1.2.2 mới chỉ là các nguyên tắc.
- Phần mô tả ở Bảng 2.1 và phần text không thực sự phù hợp với Hình 2.12.
- Việc lựa chọn MobSF cho phát hiện lỗ hổng bảo mật phần mềm sử dụng mã nguồn không được luận giải, so sánh với các công cụ được liệt kê ở chương 1. Ngoài ra, gói APK trong phần mềm di động được thử nghiệm ở chương 3 là mã đã dịch, không phải là mã nguồn.
- Việc thử nghiệm chỉ được thực hiện trên duy nhất 1 phần mềm dẫn đến các đánh giá thử nghiệm có độ tin cậy thấp.
- Tên nhiệm vụ, mô tả nhiệm vụ và kết quả mong đợi trong bảng 3.1 trang 46 không phù hợp với nhau, chẳng hạn, Tên nhiệm vụ “Nhiệm vụ 1-1: Xác định mục đích” mà mô tả nhiệm vụ là “Rà quét lỗ hổng bảo mật của phần mềm Egov Quảng Nam phiên bản Android.” là không phù hợp.

Câu hỏi:

1. Công cụ phát hiện lỗ hổng MobSF có những ưu và nhược điểm gì so với các công cụ đã mô tả ở chương 1, như SonarQube?
2. Phát hiện lỗ hổng phần mềm dựa trên mã nguồn có những ưu điểm và nhược điểm gì so với phát hiện phát hiện dựa trên mã đã dịch/mã máy?

IV/ Kết luận:

Đề án đáp ứng các tiêu chuẩn của một đề án tốt nghiệp thạc sỹ kỹ thuật.

Đồng ý cho phép học viên bảo vệ đề án tốt nghiệp.

Hà nội, ngày 15 tháng 3 năm 2024

Người phản biện

(Ký ghi rõ họ tên)

Hoàng Xuân Dâu

