BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP.HCM
KHOA CÔNG NGHỆ THÔNG TIN

HCMUTE

BÁO CÁO THỰC TẬP TỐT NGHIỆP

Ngành: An Toàn Thông Tin

SVTH: Nguyễn Thắng Lợi

MSSV: 22162023

GVHD: ThS. Nguyễn Thị Thanh Vân

TP. Hồ Chí Minh, tháng 11 năm 2025

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc Lập - Tự Do - Hạnh Phúc

TP.HCM, ngày 11 tháng 11 năm 2025

PHIẾU NHẬN XÉT, ĐÁNH GIÁ THỰC TẬP TỐT NGHIỆP

Công ty: Công ty TNHH Phần mềm FPT Hồ Chí Minh
Thời gian thực tập: 23/07/2025 – 23/10/2025
Đơn vị thực tập: HCM.SAS
Cán bộ hướng dẫn: Võ Huỳnh Anh Nhật
Họ và tên sinh viên thực tập: Nguyễn Thắng Lợi
Trường: Đại học Sư phạm Kỹ thuật TP.HCM
Khoa: Công Nghệ Thông Tin
Ngành: An Toàn Thông Tin

❖ **Nhận xét:**

- Về mặt chuyên cần: Tốt ✓ Khá Trung bình yếu
- Ý thức tổ chức kỷ luật: Tốt ✓ Khá Trung bình yếu
- Khả năng chuyên môn: Tốt ✓ Khá Trung bình yếu
- Tính sáng tạo trong công việc: Tốt ✓ Khá Trung bình yếu

❖ **Đánh giá chung:**
- Nắm vững kiến thức nền tảng và hoàn thành tốt bài tập, công việc được giao
- Tận việc nhận trách
- Tổng thể tốt nhưng cần cải thiện thêm tiếng Anh giao tiếp

❖ **Điểm** (Thang điểm 10): 10

❖ **Xếp loại (Tốt, Khá, Trung bình, Yếu):** Tốt

Xác nhận của công ty

CÔNG TY TNHH PHẦN MỀM FPT TP HỒ CHÍ MINH
FPT Software

Trưởng phòng
Tuyển dụng & Hợp tác đào tạo Miền Nam
Vũ Thanh Tuân

Cán bộ hướng dẫn thực tập

Nhật

Võ Huỳnh Anh Nhật

LỜI CẢM ƠN

Lời đầu tiên, em xin được phép bày tỏ lòng biết ơn sâu sắc và chân thành nhất đến Thạc sĩ Nguyễn Thị Thanh Vân , giảng viên hướng dẫn đã luôn tận tâm định hướng, truyền đạt những kiến thức chuyên môn và trao đổi những kinh nghiệm quý báu để em có thể thực hiện và hoàn thành tốt kỳ thực tập tốt nghiệp này.

Em cũng xin trân trọng gửi lời cảm ơn đặc biệt đến Ban Lãnh đạo và các anh chị tại Công ty TNHH PHẦN MỀM FPT HỒ CHÍ MINH (FPT Software). Đặc biệt, em xin bày tỏ lòng cảm ơn chân thành tới anh Võ Huỳnh Anh Nhật (Mentor) và toàn thể các anh chị thuộc đơn vị SAS (Cyber Security Assurance Service), đã tạo điều kiện thuận lợi nhất, tận tình giúp đỡ và hỗ trợ em trong suốt quá trình thực tập, giúp em tích lũy kinh nghiệm thực tế quý báu tại vị trí Pentester.

Kính chúc quý Thầy/Cô, Ban Lãnh đạo cùng toàn thể cán bộ nhân viên công ty FPT Software luôn dồi dào sức khỏe và gặt hái nhiều thành công.

TP. HCM, ngày 20 tháng 11 năm 2025

Sinh viên thực hiện đề tài

Nguyễn Thắng Lợi

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc Lập - Tự Do - Hạnh Phúc

TP. HCM, ngày tháng 11 năm 2025

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

Giáo viên hướng dẫn: ThS. Nguyễn Thị Thanh Vân

Sinh viên thực tập: Nguyễn Thắng Lợi

- **Nhận xét:**

- Kiến thức sau thực tập:

- Trình bày báo cáo:

- **Đánh giá chung:**

- **Điểm số:** ……

Giảng viên hướng dẫn thực tập

LỜI MỞ ĐẦU

Đứng trước xu thế phát triển mạnh mẽ của công nghệ thông tin và sự gia tăng không ngừng của các mối đe dọa an ninh mạng, vai trò của An toàn Thông tin nói chung và Kiểm thử Xâm nhập (Penetration Testing - Pentest) nói riêng ngày càng trở nên quan trọng đối với mọi doanh nghiệp. Thực tập Tốt nghiệp là một học phần bắt buộc và vô cùng quan trọng đối với sinh viên Khoa Công nghệ Thông tin Trường Đại học Sư phạm Kỹ thuật TP.HCM, nhằm tạo điều kiện cho sinh viên vận dụng những kiến thức lý thuyết đã học vào môi trường làm việc thực tế.

Trong kỳ thực tập này, em đã có cơ hội làm việc tại **Công ty TNHH PHẦN MỀM FPT HỒ CHÍ MINH (FPT Software)**, một trong những doanh nghiệp công nghệ hàng đầu tại Việt Nam. Em đã đảm nhiệm vị trí **Pentester** (Chuyên viên kiểm thử xâm nhập) thuộc đơn vị **SAS (Cyber Security Assurance Service)**. Trong suốt quá trình thực tập, mục tiêu chính của em là làm quen, hiểu rõ quy trình làm việc chuẩn mực, và trực tiếp tham gia vào các dự án kiểm thử bảo mật đối với hệ thống web app. Kết quả thực tập không chỉ giúp em tích lũy kinh nghiệm chuyên môn mà còn là bước đệm quan trọng để em định hướng phát triển nghề nghiệp trong lĩnh vực an ninh mạng.

MỤC LỤC

Nội dung **Trang**

CHƯƠNG 1: GIỚI THIỆU TỔNG QUAN VỀ ĐƠN VỊ THỰC TẬP

1.1. Thông tin về đơn vị thực tập

1.1.1. Giới thiệu về FPT Software

FPT Software là một công ty thành viên trực thuộc Tập đoàn FPT – tập đoàn công nghệ hàng đầu Việt Nam với gần ba thập kỷ phát triển trong lĩnh vực Công nghệ Thông tin và Viễn thông. Được thành lập với định hướng đưa dịch vụ và sản phẩm công nghệ Việt Nam vươn tầm thế giới, FPT Software hiện nay đã trở thành một trong những doanh nghiệp cung cấp dịch vụ CNTT có quy mô lớn nhất Đông Nam Á. Công ty có **trụ sở chính tại Hà Nội**, đồng thời duy trì hệ thống văn phòng rộng khắp với **88 cơ sở tại 30 quốc gia**, từ châu Á, châu Âu cho đến châu Mỹ. Với hơn **33.000 nhân viên** trên toàn cầu, FPT Software sở hữu nguồn lực kỹ thuật và quản lý dồi dào, phục vụ nhu cầu của khách hàng doanh nghiệp đa ngành nghề ở quy mô quốc tế [1].

Về năng lực cạnh tranh, FPT Software xây dựng danh tiếng thông qua việc cung cấp dịch vụ chất lượng cao, đáp ứng nhu cầu của hơn **1.100 khách hàng**, trong đó có khoảng **96 công ty nằm trong danh sách Fortune 500** [1]. Đây đều là các tập đoàn lớn trong lĩnh vực tài chính, ngân hàng, sản xuất, năng lượng, công nghệ, hàng không và viễn thông. Mối quan hệ hợp tác với các khách hàng này cho thấy mức độ tin cậy cao mà FPT Software đạt được trên thị trường toàn cầu, đồng thời phản ánh năng lực cung cấp dịch vụ quy mô lớn, tiêu chuẩn quốc tế của công ty.

Hoạt động kinh doanh cốt lõi của FPT Software tập trung vào các mảng **Chuyển đổi số (Digital Transformation)**, **Tư vấn CNTT (IT Consulting)** và **Phát triển phần mềm theo yêu cầu (Software Development Outsourcing)**. Công ty luôn chú trọng ứng dụng các công nghệ tiên tiến như **Trí tuệ Nhân tạo (AI)**, **Máy học**, **Điện toán đám mây (Cloud Computing)**, **RPA – Tự động hóa quy trình bằng robot**, **Blockchain**, và nhiều công nghệ mới nổi khác nhằm tạo ra những giải pháp công nghệ toàn diện cho khách hàng [1]. Các sản phẩm và dịch vụ của FPT Software không chỉ hỗ trợ doanh nghiệp tối ưu vận hành, tiết kiệm chi phí mà còn thúc đẩy quá trình đổi mới sáng tạo, hướng tới mô hình doanh nghiệp số hiện đại.

Bên cạnh hoạt động kinh doanh, FPT Software đặc biệt coi trọng vấn đề **chất lượng dịch vụ** và **an toàn thông tin**. Công ty vận hành **Hệ thống Quản lý An toàn Thông tin (ISMS)** theo các tiêu chuẩn quốc tế và đã đạt nhiều chứng nhận quan trọng như **ISO/IEC 27001**, **CMMI**, và các chứng chỉ liên quan đến quản trị chất lượng và bảo mật trong phát triển phần mềm. Những tiêu chuẩn này đóng vai trò đảm bảo rằng toàn bộ quy trình vận hành, phát triển và cung cấp dịch vụ của công ty đều tuân thủ quy định nghiêm ngặt về bảo mật, góp phần bảo vệ tài sản dữ liệu của khách hàng và của chính FPT Software trước bối cảnh các mối đe dọa an ninh mạng ngày càng gia tăng.

Nhờ chiến lược phát triển bền vững, đầu tư mạnh mẽ vào nguồn nhân lực và công nghệ cốt lõi, FPT Software không chỉ giữ vững vị thế tại thị trường trong nước mà còn trở thành một trong những đại diện tiêu biểu của ngành CNTT Việt Nam trên trường quốc tế. Đối với sinh viên thực tập, môi trường tại FPT Software mang đến cơ hội tiếp cận mô hình làm việc chuyên nghiệp, học hỏi công nghệ tiên tiến, đồng thời rèn luyện tác phong và năng lực kỹ thuật trong môi trường doanh nghiệp quy mô lớn, tạo nền tảng vững chắc cho định hướng nghề nghiệp trong tương lai.

1.1.2. Giới thiệu về đơn vị SAS (Cyber Security Assurance Service)

SAS (Cyber Security Assurance Service) là đơn vị chuyên trách về **An toàn thông tin (ATTT)** trực thuộc FPT Software, được thành lập với mục tiêu nâng cao năng lực bảo mật trong toàn bộ hệ sinh thái sản phẩm và dự án của công ty. Bên cạnh việc hỗ trợ các dự án nội bộ, SAS còn cung cấp các dịch vụ bảo mật độc lập cho khách hàng bên ngoài, đặc biệt là các doanh nghiệp lớn đang trong quá trình chuyển đổi số [2]. Với vai trò là đơn vị hạt nhân trong chiến lược bảo mật của FPT Software, SAS được xây dựng như một trung tâm chuyên môn cao, hội tụ đội ngũ kỹ sư bảo mật, chuyên gia ứng phó sự cố và các nhà phân tích an ninh có kinh nghiệm.

Về chức năng, SAS tập trung triển khai các giải pháp và dịch vụ nhằm đảm bảo an toàn và tăng cường khả năng phòng vệ trước các mối đe dọa mạng hiện đại. Các lĩnh vực hoạt động chính bao gồm [2]:

- **Application Security (Bảo mật Ứng dụng):** Cung cấp dịch vụ tư vấn, đánh giá và kiểm thử để đảm bảo mức độ an toàn của ứng dụng trong suốt vòng đời phát triển. Đơn vị thực hiện nhiều phương pháp đánh giá như Secure Code Review, Security Architecture Review, Penetration Testing và Vulnerability Assessment nhằm phát hiện, mô phỏng và khai thác các lỗ hổng trước khi sản phẩm được triển khai thực tế.
- **Cyber Defense (Phòng thủ mạng):** Vận hành các dịch vụ bảo mật trọng yếu như **SOC as a Service** (dịch vụ Trung tâm Điều hành An ninh) và **MXDR – Managed Extended Detection and Response**, giúp khách hàng giám sát, phát hiện và ứng phó với mối đe dọa 24/7. Các hoạt động này đóng vai trò quan trọng trong việc đảm bảo tính liên tục của hệ thống và hạn chế thiệt hại từ những sự cố an ninh mạng.
- **Cloud & Data Security (Bảo mật Đám mây và Dữ liệu):** Cung cấp các giải pháp tăng cường tuân thủ, bảo vệ dữ liệu và cải thiện khả năng phục hồi trong môi trường đám mây. SAS hỗ trợ đánh giá kiến trúc, cấu hình an toàn, kiểm tra mức độ tuân thủ tiêu chuẩn quốc tế và triển khai các biện pháp bảo vệ tài sản dữ liệu cho doanh nghiệp.

Một trong những hoạt động cốt lõi của SAS là quản lý và vận hành **chương trình Software Security Assurance (SSA)** – chương trình đảm bảo an toàn thông tin xuyên suốt vòng đời phát triển phần mềm của FPT Software. Chương trình này tích hợp đồng bộ các công cụ tự động, quy trình chuẩn hóa và chuyên môn của đội ngũ kỹ sư nhằm thực hiện các hoạt động **Security Testing** cho hàng trăm dự án web và cloud mỗi năm. Thông qua SSA, SAS giúp giảm thiểu rủi ro bảo mật, tăng cường độ tin cậy của sản phẩm, đồng thời đáp ứng các yêu cầu nghiêm ngặt về tuân thủ của khách hàng quốc tế.

Với hệ sinh thái dịch vụ toàn diện và quy trình bảo mật chuẩn hóa, SAS đóng vai trò chiến lược trong việc xây dựng năng lực phòng thủ an ninh mạng của FPT Software. Đối với sinh viên thực tập, việc làm việc trong môi trường của SAS mang lại cơ hội tiếp cận các kiến thức thực tiễn, công nghệ tiên tiến và quy trình chuyên nghiệp trong lĩnh vực an toàn thông tin doanh nghiệp.

1.2. Nhiệm vụ thực tập

Vị trí thực tập của tôi là **Pentester**, thuộc bộ phận **Offensive Security** của đơn vị SAS. Trong vai trò này, tôi tham gia vào hoạt động **Penetration Testing as a Service**, với nhiệm vụ chính là mô phỏng các cuộc tấn công mạng thực tế nhằm phát hiện, khai thác và đánh giá mức độ rủi ro của các lỗ hổng bảo mật trên hệ thống của khách hàng. Công việc đòi hỏi khả năng phân tích kỹ thuật, hiểu biết sâu về các mô hình tấn công và khả năng vận dụng linh hoạt các công cụ kiểm thử.

Mục tiêu của vị trí này là cung cấp một đánh giá toàn diện về khả năng phòng thủ của hệ thống, đồng thời đề xuất các biện pháp khắc phục rõ ràng và hiệu quả giúp khách hàng nâng cao năng lực bảo mật, đáp ứng các tiêu chuẩn an ninh quốc tế. Đây cũng là vị trí phù hợp với định hướng nghề nghiệp của tôi, cho phép tôi rèn luyện kỹ năng chuyên môn và nắm vững quy trình kiểm thử xâm nhập chuyên nghiệp trong môi trường thực tế.

CHƯƠNG 2: NỘI DUNG CÔNG VIỆC THỰC TẬP

2.1. Tổng quan quá trình thực tập

Quá trình thực tập tại Công ty TNHH Phần mềm FPT (FPT Software), vị trí Pentester, đã được thực hiện trong **03 tháng** (từ 23/07 đến 23/10) và được chia thành ba giai đoạn chính, tập trung vào việc chuyển giao kiến thức lý thuyết sang kỹ năng thực hành chuyên nghiệp.

Bảng 1. Tóm tắt quá trình thực tập

Giai đoạn	Thời gian	Mục tiêu chính	Thành tựu nổi bật
GĐ-1	23/07 – 23/08	Đào tạo về nghiệp vụ, làm quen với quy trình Pentest và cơ cấu tổ chức của đơn vị SAS.	Nắm rõ quy trình pentest dành cho web app. Hoàn thành bài kiểm tra năng lực loại Khá.
GĐ-2	23/08 – 23/09	Nắm bắt và thực hiện các khâu cơ bản bao gồm: pre-assessment (chuẩn bị) và post-assessment (báo cáo và kiểm thử lại sau bản vá).	Hoàn thành tốt các đầu việc được giao, nắm rõ cách viết report (mô tả lỗ hổng và đề xuất khắc phục hiệu quả).
GĐ-3	23/09 – 23/10	Tham gia trực tiếp vào khâu quan trọng nhất: assessment (tìm kiếm lỗ hổng) cho các dự án web app thuộc chương trình SSA.	Nắm rõ toàn bộ quy trình pentest cho web app. Được đánh giá có tiến bộ tốt từ Mentor và PM, chính thức ghi tên vào danh sách nhân sự của đơn vị SAS.

Tổng thể, quá trình thực tập đã giúp sinh viên từ việc làm quen với quy trình chuẩn đến việc làm chủ kỹ năng kiểm thử và trực tiếp tham gia vào các dự án thực tế, từ đó đạt được mục tiêu trở thành một phần của đội ngũ nhân sự chuyên nghiệp tại FPT Software.

2.2. GĐ-1: Đào tạo nghiệp vụ và hội nhập môi trường doanh nghiệp

2.2.1. Mục tiêu giai đoạn

Giai đoạn đầu tiên đóng vai trò nền tảng, giúp sinh viên chuyển đổi tư duy từ môi trường học thuật sang môi trường làm việc chuyên nghiệp trong lĩnh vực An toàn thông tin. Mục tiêu cụ thể gồm:

- **Về kiến thức:** Hệ thống hóa, đối chiếu lại các kiến thức lý thuyết đã học với quy trình thực tế tại doanh nghiệp, đặc biệt trong mảng Application Security.
- **Về kỹ năng:** Làm chủ các công cụ kiểm thử (pentest tools) và nắm vững quy trình kiểm thử xâm nhập tiêu chuẩn (Pentest Methodology) được đơn vị SAS áp dụng hiện nay.
- **Về tuân thủ:** Hiểu và tuân thủ đầy đủ các quy định bảo mật, cam kết bảo mật thông tin (NDA) và văn hóa làm việc tại FPT Software.

2.2.2. Nội dung thực hiện chi tiết

Ngay khi bắt đầu thực tập, sinh viên được đào tạo về các yêu cầu tuân thủ liên quan đến bảo mật thông tin – yếu tố quan trọng hàng đầu đối với nhân sự trong lĩnh vực Cyber Security. Các nội dung đã hoàn thành gồm:

- **Tìm hiểu và cam kết tuân thủ Hệ thống Quản lý An toàn Thông tin (ISMS)** của FPT Software, bao gồm các quy định về xử lý dữ liệu, phân quyền truy cập và quản lý tài sản thông tin.
- **Nghiên cứu chính sách bảo mật dữ liệu khách hàng**, các quy tắc liên quan đến việc sử dụng thiết bị cá nhân, mạng nội bộ, cũng như các hành vi phải tránh để không xảy ra rò rỉ dữ liệu trong quá trình làm việc.
- **Tìm hiểu cơ cấu tổ chức và vai trò của đơn vị SAS**, nhận thức được nhiệm vụ của SAS như một đơn vị chuyên trách giúp bảo vệ các sản phẩm phần mềm của FPT và cung cấp dịch vụ an ninh mạng cho khách hàng toàn cầu.

Giai đoạn này giúp sinh viên hình thành tư duy làm việc nghiêm túc, có trách nhiệm với dữ liệu và tài sản thông tin – yếu tố cốt lõi của một Pentester chuyên nghiệp.

Tiếp đến là nội dung trọng tâm của giai đoạn 1, chiếm phần lớn thời gian đào tạo. Sinh viên được hướng dẫn chuyên sâu về quy trình kiểm thử xâm nhập ứng dụng web theo tiêu chuẩn nội bộ của SAS, dựa trên OWASP, OSSTMM và các best practices quốc tế.

- Nghiên cứu quy trình (Methodology)

- Tiếp cận ba phương pháp luận: **Black-box**, **Gray-box**, và **White-box**.
- Nghiên cứu chuyên sâu **OWASP Top 10** [3], bao gồm cách thức nhận diện, khai thác và biện pháp phòng chống cho các nhóm lỗ hổng phổ biến như SQL Injection, Cross-site Scripting (XSS), Broken Access Control, Security Misconfiguration…
- Hiểu cách kết hợp giữa kiểm thử tự động và kiểm thử thủ công, đặc biệt trong các tình huống yêu cầu phân tích logic ứng dụng.

- Làm quen và cấu hình công cụ (Tools)

- Thiết lập môi trường kiểm thử an toàn (lab environment) tránh ảnh hưởng đến hệ thống thật.
- Cài đặt và sử dụng thành thạo **Burp Suite Professional**, các bộ công cụ hỗ trợ scan lỗ hổng, cùng các script cần thiết trong quá trình khai thác.
- Hiểu rõ vai trò, giới hạn và khả năng của từng công cụ để hỗ trợ kiểm thử hiệu quả.

- Thực hành quy trình Pentest chuẩn

- **Reconnaissance (Thu thập thông tin):** Xác định công nghệ, đặc điểm nền tảng, bản đồ API/endpoint và cấu trúc hệ thống.
- **Vulnerability Analysis (Phân tích lỗ hổng):** Đánh giá kết quả scan kết hợp kiểm tra thủ công nhằm loại bỏ false positives và xác định mức độ ảnh hưởng thực tế.

- **Exploitation (Khai thác):** Thực hiện khai thác có kiểm soát để chứng minh khả năng gây ảnh hưởng (PoC) mà không làm gián đoạn hoặc gây hại đến hệ thống của khách hàng.

Cuối giai đoạn 1, sinh viên tham gia bài kiểm tra đánh giá năng lực nhằm xác định mức độ sẵn sàng trước khi tham gia vào giai đoạn thực hiện các dự án thực tế. Nội dung kiểm tra gồm:

- **Mô phỏng pentest** trên một ứng dụng web lab được thiết kế có chủ đích với nhiều dạng lỗ hổng.
- **Yêu cầu:** Phát hiện lỗ hổng, khai thác thành công và viết báo cáo sơ bộ mô tả quá trình khai thác và biện pháp khắc phục.
- Kết quả đánh giá đóng vai trò làm tiêu chí để đơn vị quyết định sinh viên có đủ điều kiện tham gia trong các dự án thực tế hay không.

2.2.3. Kết quả đạt được

Sau tháng thực tập đầu tiên, sinh viên đã đạt được các kết quả nổi bật sau:

- **Nắm vững và áp dụng thành thạo quy trình Web Application Pentest** theo tiêu chuẩn của SAS trong các bài tập mô phỏng.
- **Sử dụng thành thạo các công cụ kiểm thử**, đặc biệt là kỹ năng phân tích thủ công và đánh giá logic ứng dụng – yếu tố quan trọng trong việc phát hiện các lỗ hổng không thể scan tự động.
- **Hoàn thành bài kiểm tra năng lực với kết quả Khá**, đủ điều kiện để chuyển sang giai đoạn tham gia dự án thực tế.
- **Hình thành tác phong làm việc chuyên nghiệp**, nghiêm túc thực hiện các yêu cầu về bảo mật thông tin và đạo đức nghề nghiệp của một Pentester (Ethical Hacker).

2.3. GĐ-2: Tham gia thực hiện các khâu cơ bản trong dự án

2.3.1. Mục tiêu giai đoạn

Sau khi hoàn thành giai đoạn đào tạo nền tảng, sinh viên bước vào giai đoạn tiếp cận trực tiếp với các dự án pentest đang được triển khai tại đơn vị. Mục tiêu trung tâm của giai đoạn này là nắm bắt toàn diện quy trình vận hành của một dự án Pentest, đặc biệt là hai giai đoạn quan trọng:

- **Giai đoạn chuẩn bị (Pre-assessment):** Đảm bảo tất cả điều kiện kỹ thuật, phạm vi kiểm thử và tài nguyên liên quan được thiết lập chính xác trước khi tiến hành tấn công thử nghiệm.
- **Giai đoạn tổng kết (Post-assessment):** Đảm bảo chất lượng đầu ra của dự án, hỗ trợ khách hàng khắc phục lỗ hổng, thực hiện tái kiểm thử và đóng gói báo cáo tổng kết.

Giai đoạn này giúp sinh viên chuyển từ việc học kiến thức mô phỏng sang làm việc trong môi trường thực, hiểu cách vận hành của đội dự án, chuẩn hóa quy trình làm việc và tiếp cận các tình huống bảo mật thực tế.

2.3.2. Nội dung thực hiện chi tiết

Giai đoạn Tiền đánh giá (Pre-assessment): Đây là bước khởi tạo quan trọng của mỗi dự án, yêu cầu sự chính xác và tỉ mỉ để đảm bảo phạm vi kiểm thử (Scope) được xác định đúng ngay từ đầu. Các tác vụ thường bao gồm:

- Kiểm tra môi trường (Environment health check)

- Tiếp nhận và rà soát thông tin bàn giao từ khách hàng, bao gồm **URL**, **tài khoản truy cập**, **VPN**, tài liệu kỹ thuật và các điều kiện đặc thù khác.
- Thực hiện kiểm tra kết nối (connectivity check), xác thực quyền truy cập vào môi trường Staging/UAT và đảm bảo môi trường hoạt động ổn định, không gặp lỗi hệ thống trước khi tiến hành pentest.

- Thu thập và rà soát API (API crawling & reconnaissance)

- Sử dụng kỹ thuật Crawling để thu thập bản đồ ứng dụng, nhận diện cấu trúc và các điểm đầu vào.
- Tổng hợp danh sách API endpoints cần kiểm thử, đối chiếu với tài liệu kỹ thuật (Swagger, API documentation) nhằm đảm bảo rằng không bỏ sót chức năng quan trọng.
- Đánh giá sơ bộ độ về phức tạp, mức độ rủi ro cũng như các khu vực cần ưu tiên kiểm thử.

- Quản lý tiến độ dự án

- Đồng bộ danh sách hạng mục kiểm thử lên công cụ theo dõi tiến độ nội bộ của SAS - Night Wolf Tracking.
- Hỗ trợ Project Manager theo dõi sát sao trạng thái dự án, đảm bảo các hạng mục được cập nhật chính xác và đúng thời hạn.

Giai đoạn Hậu đánh giá (Post-assessment): Sau khi hoàn tất việc kiểm thử và phát hiện lỗ hổng, dự án chuyển sang giai đoạn tổng kết và hỗ trợ khách hàng khắc phục các vấn đề còn chưa xử lý dứt điểm.

- Tái kiểm thử (Re-test)

- Khi khách hàng hoặc đội phát triển thông báo hoàn tất bản vá, sinh viên tiến hành tái kiểm thử các lỗ hổng đã phát hiện.
- Đánh giá hoạt động hệ thống sau khi vá để đảm bảo không xuất hiện lỗi mới hoặc hành vi bất thường.

- Đánh giá bản vá (Patch validation)

- Phân tích cơ chế bản vá để xác định lỗ hổng đã được xử lý triệt để, tránh tình trạng khắc phục bề mặt (bypassable fix).
- Kiểm tra tính hiệu quả và sự phù hợp của biện pháp bảo mật khách hàng đã áp dụng.

- Lập báo cáo tổng kết (Final reporting)

- Tổng hợp tất cả phát hiện, biên soạn báo cáo cuối cùng của dự án (Final Report).
- Nội dung báo cáo bao gồm: Mô tả chi tiết từng lỗ hổng; Bằng chứng khai thác (PoC); Điểm đánh giá mức độ rủi ro (CVSS); Khuyến nghị khắc phục (Remediation)

Báo cáo là tài liệu chính thức gửi cho khách hàng và ảnh hưởng trực tiếp đến chất lượng cuối cùng của dự án, vì vậy yêu cầu mức độ chính xác, rõ ràng và chuyên nghiệp cao.

2.3.3. Kết quả đạt được

Kết thúc giai đoạn tham gia dự án thực tế, sinh viên đạt được nhiều tiến bộ rõ rệt:

- **Kỹ năng quản lý công việc:** Hoàn thành tốt các nhiệm vụ được giao trong team, đảm bảo sự liền mạch và đúng tiến độ của từng dự án.
- **Kỹ năng báo cáo:** Nắm vững cách viết một báo cáo Pentest chuẩn, với mô tả kỹ thuật rõ ràng, có tính hệ thống, và đặc biệt là khả năng đưa ra khuyến nghị thực tiễn giúp khách hàng khắc phục lỗ hổng hiệu quả.
- **Hiểu sâu quy trình dự án Pentest:** Từ khâu chuẩn bị, rà soát, kiểm thử, tái kiểm thử cho đến tổng kết và bàn giao.
- **Nâng cao kỹ năng làm việc nhóm:** Có khả năng phối hợp nhịp nhàng với Project Manager, Mentor và các thành viên khác trong dự án.

2.4. GĐ-3: Tham gia vào khâu Assessment trong dự án

2.4.1. Mục tiêu giai đoạn

Giai đoạn này là bước chuyển quan trọng nhất trong toàn bộ kỳ thực tập, đánh dấu việc sinh viên chính thức tham gia vào chu trình kiểm thử bảo mật thực tế với vai trò trực tiếp thực hiện nhiệm vụ. Từ việc chỉ hỗ trợ kỹ thuật ở các giai đoạn trước, sinh viên bắt đầu đảm nhiệm toàn bộ quy trình đánh giá bảo mật (Assessment) dưới sự giám sát của Mentor và chuyên gia an toàn thông tin. Mục tiêu của giai đoạn bao gồm:

- **Nâng cao năng lực chuyên môn**, đặc biệt là kỹ năng phát hiện và khai thác lỗ hổng trên các hệ thống Web App.
- **Vận dụng kiến thức lý thuyết** vào môi trường thực tế với yêu cầu khắt khe về tiến độ, chất lượng và tính chính xác của từng phát hiện kỹ thuật.
- **Rèn luyện tư duy phân tích** để xử lý các tình huống nghiệp vụ phức tạp và các lỗi logic không thể phát hiện bằng công cụ tự động.
- **Tiếp cận công nghệ bảo mật tiên tiến**, đặc biệt là các công cụ AI hỗ trợ trong kiểm thử được phát triển nội bộ tại FPT Software.

2.4.2. Nội dung thực hiện chi tiết

Trong suốt một tháng, sinh viên được phân công trực tiếp vào các dự án kiểm thử của đơn vị SAS, được cấp quyền truy cập đầy đủ vào môi trường đánh giá và chịu trách nhiệm tìm kiếm, phân tích, phân loại và ghi nhận lỗ hổng bảo mật.

- *Thực hiện kiểm thử xâm nhập toàn diện (Comprehensive Assessment):* Sinh viên tiến hành pentest dựa trên **Checklist tiêu chuẩn của SAS**, bao gồm nhiều nhóm kiểm thử quan trọng như:

- Thực hiện đánh giá bảo mật trên từng API Endpoint.
- Kiểm tra các cơ chế xác thực (Authentication) và phân quyền (Authorization).
- Xác định các điểm yếu liên quan đến truyền tải dữ liệu như: Thiếu xác thực đầu vào, truy cập trái phép dữ liệu,...

Việc kiểm thử API đóng vai trò quan trọng vì đa số ứng dụng hiện nay vận hành theo mô hình Frontend – Backend tách biệt, dữ liệu đều đi qua API nên nguy cơ rủi ro rất cao. Sinh viên tiến hành rà soát chuyên sâu các nhóm lỗ hổng kỹ thuật phổ biến như: Injection (SQL Injection, XSS,...), Misconfiguration, Sever-side Request Forgery và nhiều nhóm lỗi thuộc OWASP Top 10. Quá trình tìm kiếm bao gồm cả kỹ thuật **manual testing** và **sử dụng công cụ hỗ trợ**, kết hợp phân tích giao thức và quan sát hành vi ứng dụng.

Bên cạnh đó, cũng quan trọng không kém, là phân tích lỗ hổng nghiệp vụ (Logical Vulnerabilities). Đây là nhóm lỗi khó phát hiện nhất vì liên quan đến luồng xử lý nghiệp vụ và không tuân theo mẫu cố định. Sinh viên tập trung phân tích logic ứng dụng để tìm ra các tình huống bất thường như:

- Bypass quy trình thanh toán
- Tác động trái phép lên tài khoản người dùng khác
- Thay đổi tham số trên client để bỏ qua giới hạn hệ thống
- Lạm dụng chức năng để tạo lợi thế sai lệch (Function Misuse)

Nhóm lỗi này yêu cầu tư duy phân tích độc lập, kỹ năng quan sát chi tiết, và hiểu sâu về hoạt động của hệ thống.

- *Ứng dụng công nghệ mới trong kiểm thử:* Ngoài các phương pháp truyền thống, sinh viên được làm việc với các hệ thống hỗ trợ tiên tiến tại FPT Software, đặc biệt là làm quen với hệ thống AI Agent nội bộ với tên gọi "PentestOne". Đây là nền tảng được đội ngũ SAS phát triển để hỗ trợ cho việc kiểm thử bảo mật. Sinh viên được hướng dẫn cách sử dụng AI để phân tích và gợi ý các điểm nghi vấn, sinh tự động các Testcase giúp mở rộng phạm vi kiểm thử và tối ưu hóa thời gian kiểm thử bằng việc tự động hóa các tác vụ lặp lại.

Các công cụ AI hỗ trợ tăng hiệu suất và độ bao phủ kiểm thử nhờ Rút ngắn thời gian thu thập thông tin (Reconnaissance), tự động gợi ý payload phù hợp với từng loại lỗ hổng và hân tích hành vi ứng dụng và dự đoán điểm tấn công tiềm năng. Nhờ đó, chất lượng và tốc độ đánh giá được cải thiện đáng kể.

2.4.3. Kết quả đạt được

Qua một tháng làm việc với cường độ cao, sinh viên đã đạt được nhiều tiến bộ chuyên môn quan trọng:

- *Làm chủ quy trình Pentest của đơn vị:* Sinh viên đã nắm rõ toàn bộ chu trình kiểm thử của SAS, từ phân tích ban đầu đến ghi nhận lỗ hổng và đề xuất hướng khắc phục, thích ứng nhanh với quy trình chuyên nghiệp của doanh nghiệp lớn.

- *Củng cố năng lực chuyên môn:* Trong các dự án được giao, sinh viên đã: chủ động phát hiện nhiều lỗ hổng với đa dạng mức độ nghiêm trọng, hoàn thành báo cáo kỹ thuật với chất lượng tốt, được Mentor đánh giá cao. Ngoài ra còn đảm nhận được cả khâu kỹ thuật và xử lý tình huống phát sinh trong quá trình đánh giá.

- Đạt được tín nhiệm của đội ngũ quản lý: dựa trên sự cố gắng, tinh thần học hỏi và kết quả đạt được, sinh viên đã nhận được phản hồi tích cực từ Mentor và PM dự án. Đồng thời chính thứcghi tên vào danh sách nhân sự của đơn vị Cyber Security Assurance Service (SAS) sau kỳ thực tập, tiếp tục làm việc với vai trò Pentester.

CHƯƠNG 3: KẾT LUẬN

Kỳ thực tập tốt nghiệp tại Công ty TNHH Phần mềm FPT (FPT Software) không chỉ là yêu cầu quan trọng để hoàn thành chương trình đào tạo tại Trường Đại học Sư phạm Kỹ thuật TP.HCM, mà còn là một dấu mốc có ý nghĩa đặc biệt đối với quá trình chuyển đổi từ nền tảng kiến thức học thuật sang năng lực làm việc thực tế trong môi trường doanh nghiệp của bản thân em.

Trong suốt ba tháng thực tập tại đơn vị **SAS – Cyber Security Assurance Service**, em đã có cơ hội tiếp cận một môi trường chuyên nghiệp, cường độ làm việc cao và đòi hỏi sự chính xác tuyệt đối trong từng hạng mục kỹ thuật. Nhờ sự hướng dẫn tận tình từ Mentor và sự hỗ trợ của các anh/chị trong nhóm, em đã hoàn thành xuất sắc những mục tiêu đề ra ban đầu:

3.1. Về chuyên môn

Em đã nắm vững và vận dụng thành thạo quy trình **kiểm thử xâm nhập (Pentest) cho ứng dụng Web** theo các tiêu chuẩn quốc tế mà SAS đang áp dụng. Trong quá trình tham gia các dự án thực tế, em đã trực tiếp thực hiện:

- Rà soát và khai thác các lỗ hổng kỹ thuật phổ biến (Technical Vulnerabilities).
- Phân tích và phát hiện các lỗi logic nghiệp vụ phức tạp (Business Logic Flaws) đòi hỏi tư duy phân tích sâu và khả năng quan sát chi tiết.
- Tham gia đầy đủ các giai đoạn của quy trình Pentest: từ Pre-assessment, Assessment đến Post-assessment.

Nhờ đó, em đã củng cố vững chắc nền tảng chuyên môn và tự tin hơn khi xử lý các tình huống kỹ thuật thực tế.

3.2. Về kỹ năng mềm

Môi trường làm việc tại FPT Software giúp em rèn luyện tác phong chuẩn mực của một kỹ sư An toàn thông tin chuyên nghiệp:

- Kỹ năng làm việc nhóm và trao đổi thông tin hiệu quả.
- Kỹ năng quản lý thời gian, sắp xếp công việc theo ưu tiên và đáp ứng đúng tiến độ dự án.
- Kỹ năng viết báo cáo kỹ thuật (Security Report) rõ ràng, mạch lạc và đúng chuẩn của doanh nghiệp.

Những kỹ năng này đóng vai trò then chốt trong việc đảm bảo chất lượng đầu ra của các dự án kiểm thử bảo mật.

3.3. Về kết quả thực tế

Em đã tham gia và đóng góp trực tiếp vào thành công của nhiều dự án Pentest do đơn vị SAS phụ trách. Các nhiệm vụ được giao đều được hoàn thành đúng tiến độ, đảm bảo chất lượng kỹ thuật và tính đầy đủ trong báo cáo đánh giá. Những kết quả này đã được Mentor và Ban quản lý dự án ghi nhận.

Thành tựu ý nghĩa nhất đối với em trong đợt thực tập này chính là việc được **Ban lãnh đạo và Mentor tin tưởng, chính thức ghi danh vào đội ngũ nhân sự của đơn vị SAS** sau khi kỳ thực tập kết thúc. Đây là sự ghi nhận rõ ràng nhất cho những nỗ lực mà em đã bỏ ra và là động lực mạnh mẽ để em tiếp tục phát triển sự nghiệp trong lĩnh vực An toàn thông tin, Bước sang giai đoạn tiếp theo, em đặt mục tiêu tiếp tục trau dồi kiến thức, mở rộng sang mảng **Mobile Application Pentest** và sẵn sàng tham gia các dự án bảo mật quy mô lớn với khách hàng quốc tế.

TÀI LIỆU THAM KHẢO

[1] FPT được vinh danh Doanh nghiệp Công nghệ số Việt Nam 2025 thể hiện tinh thần Công tư đồng kiến quốc

[2] Cyber Security | FPT Software

[3] OWASP. (2021). *OWASP Top 10: The Ten Most Critical Web Application Security Risks*. Open Web Application Security Project. https://owasp.org/Top10/