HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI TẬP LỚN
HỌC PHẦN: QUẢN LÝ AN TOÀN THÔNG TIN
MÃ HỌC PHẦN: INT14106

ĐỀ TÀI: PHÂN TÍCH RỦI RO VỚI HỆ THỐNG THƯ VIỆN SỐ PTIT (DLIB.PTIT.EDU.VN)

Các sinh viên thực hiện:

B21DCAT006 - Cao Hữu Bảo Khánh

B21DCAT098 - Nguyễn Duy Hưng

B21DCAT090 - Nguyễn Minh Hiệu

B21DCAT102 - Nguyễn Mạnh Hưởng

B21DCAT106 - Nguyễn Xuân Khải

Tên nhóm: 06

Tên lớp: D21CQAT02-B

Giảng viên hướng dẫn: TS. Nguyễn Ngọc Điệp

HÀ NỘI 2024

PHÂN CÔNG NHIỆM VỤ NHÓM THỰC HIỆN

TT	Công việc / Nhiệm vụ	SV thực hiện	Thời hạn hoàn thành
1	- Tổ chức họp nhóm, phân chia nhiệm vụ; - Phân tích, đánh giá *"Các lỗ hổng truyền thống trong việc triển khai ứng dụng (có database) trên internet"* như chèn mã, brute-force mật khẩu, … - Hoàn thiện báo cáo.	Cao Hữu Bảo Khánh	- 4/5/2025 - 13/5/2025 - 16/5/2025
2	- Phân tích, đánh giá *"Các vấn đề về quản lý người dùng"* như xác thực không đủ mạnh, mật khẩu không đủ mạnh, … - Tìm hiểu tổng quan về hệ thống Dlib PTIT; - Viết báo cáo.	Nguyễn Duy Hưng	- 13/5/2025 - 15/5/2025 - 16/5/2025
3	- Phân tích, đánh giá *"Các vấn đề bị tấn công khi hoạt động trên Internet"* như DoS/DDoS, MiTM, Deface, … - Tìm hiểu tổng quan về OCTAVE và xác định các tiêu chuẩn đánh giá; - Viết báo cáo.	Nguyễn Minh Hiệu	- 13/5/2025 - 15/5/2025 - 16/5/2025
4	- Phân tích, đánh giá *"Các lỗ hổng truyền thống trong việc triển khai ứng dụng (có database) trên internet"* như forced browsing, path traversal, … - Kiểm nghiệm hệ thống với các luật, quy chuẩn và xác định rủi ro phi kỹ thuật	Nguyễn Mạnh Hưởng	- 13/5/2025 - 15/5/2025
5	- Phân tích, đánh giá *"Các vấn đề bị tấn công khi hoạt động trên Internet"* như phising, malware, … - Viết kết luận báo cáo	Nguyễn Xuân Khải	- 13/5/2025 - 16/5/2025

BIÊN BẢN HỌP NHÓM

Buổi 1:

* *Thời gian*: 9h30 ngày 4/5/2025 (Nhóm trưởng cho lùi lịch họp 1 chút để các bạn nghỉ lễ).

* *Hình thức*: Online qua Google Meet.

* *Nội dung cuộc họp*:

- Làm rõ các quy định của bài tập lớn;

- Lựa chọn trang web để thực hiện đánh giá;

- Xác định các yêu cầu quan trọng nhất cần thực hiện và tiến hành chia việc.

* *Đóng góp của các thành viên trong nhóm*:

- Cao Hữu Bảo Khánh, Nguyễn Minh Hiệu đề xuất 3 trang web là Portal PTIT, PTIT S-Link và Dlib PTIT. Sau khi hỏi thêm các nhóm khác để tránh bị trùng, lựa chọn cuối là Dlib PTIT.

- Khánh đề xuất hình thức trình bày phần lớn sẽ dựa trên báo cáo mẫu thầy gửi, bổ sung một số phần chẳng hạn như tổng quan về hệ thống DLib PTIT, các quy chuẩn thầy yêu cầu, … Sau đó, đề xuất tiến hành chia việc theo 3 "Yêu cầu xác định các rủi ro với hệ thống", trung bình 2 bạn 1 chủ đề.

- Nguyễn Duy Hưng nhận làm phần "Các vấn đề về quản lý người dùng".

- Nguyễn Xuân Khải, Hiệu nhận làm phần "Các vấn đề bị tấn công khi hoạt động trên Internet".

- Khánh, Nguyễn Mạnh Hưởng nhận làm phần "Các lỗ hổng truyền thống trong việc triển khai ứng dụng (có database) trên internet"

- Cuối cùng, với phần các quy chuẩn do Nhà nước quy định, cả nhóm quyết định sẽ xem xét cả hệ thống với các quy chuẩn đó, thay vì chia nhỏ theo từng loại rủi ro rồi mới đối sánh với các văn bản pháp luật.

* *Kết quả cuộc họp*:

- Hoàn thành việc chia việc;

- Xác định deadline đến 9h ngày 13/5/2025.

Buổi 2:

* *Thời gian*: 9h30 ngày 13/5/2025

* *Hình thức*: Online qua Google Meet

* *Nội dung cuộc họp*:

- Review lại những gì nhóm đã thực hiện được. Thực hiện sửa đổi, bổ sung nếu nhận ra những thiếu sót, vướng mắc.

- Chia nốt những phần việc còn lại: Làm biên bản, trình bày báo cáo, viết kết luận cho bài tập, …

** Đóng góp của các thành viên trong nhóm*:

- Các thành viên lần lượt trình bày những gì mình đã làm để cả nhóm nghe và nhận xét;

- Sau đó đến phần báo cáo, sau khi hội ý, các thành viên quyết định chia ra 3 chương;

- Sau đó, các thành viên lần lượt nhận những đầu việc còn lại:

+ Khánh: Làm biên bản, hoàn thiện báo cáo bản cuối cùng;

+ Hưng: Nhận viết chương 1 tổng quan về OCTAVE và hệ thống Dlib PTIT trong báo cáo;

+ Hiệu: Nhận viết chương 2 về từng bước trong quy trình OCTAVE;

+ Hưởng: Nhận viết phần đánh giá hệ thống DLib qua các luật, nghị định, quy chuẩn của Nhà nước;

+ Khải: Viết kết luận, đánh giá kết quả bài tập của nhóm.

** Kết quả cuộc họp*:

- Hoàn thiện nội dung của bài tập lớn;

- Thực hiện viết báo cáo;

- Deadline: Cố gắng đến trước 10h tối ngày 16/5/2025 hoàn thành.

NHÓM THỰC HIỆN TỰ ĐÁNH GIÁ

TT	SV thực hiện	Thái độ tham gia	Mức hoàn thành CV	Kỹ năng giao tiếp	Kỹ năng hợp tác	Kỹ năng lãnh đạo
1	Cao Hữu Bảo Khánh	5	4	4	3	3
2	Nguyễn Duy Hưng	5	4	4	3	
3	Nguyễn Minh Hiệu	4	4	3	3	
4	Nguyễn Mạnh Hưởng	3	4	3	3	
5	Nguyễn Xuân Khải	3	4	3	3	

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC BẢNG BIỂU

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation	Phương pháp đánh giá mối đe dọa, tài sản và lỗ hổng
API	Application Programming Interface	Giao diện lập trình ứng dụng
DDoS	Distributed Denial of Service	Tấn công từ chối dịch vụ phân tán
DoS	Denial of Service	Tấn công từ chối dịch vụ
CDN	Content Delivery Network	Mạng phân phối nội dung
WAF	Web Application Firewall	Tường lửa ứng dụng web
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập
IPS	Intrusion Prevention System	Hệ thống ngăn chặn xâm nhập
VPN	Virtual Private Network	Mạng riêng ảo
SQLi	SQL Injection	Tấn công chèn mã SQL
XSS	Cross -Site Scripting	Tấn công kịch bản chéo trang
HSTS	HTTP Strict Transport Security	Chính sách bảo mật truyền tải nghiêm ngặt HTTP
DMARC	Domain-based Message Authentication, Reporting and Conformance	Xác thực, báo cáo và tuân thủ dựa trên tên miền
SPF	Sender Policy Framework	Khung chính sách người gửi (email)
DKIM	DomainKeys Identified Mail	Thư điện tử xác thực khóa tên miền
CMS	Content Management System	Hệ thống quản lý nội dung
DR	Disaster Recovery	Khôi phục sau thảm họa
AES-256	Advanced Encryption Standard 256-bit	Tiêu chuẩn mã hóa tiên tiến 256 bit

MỞ ĐẦU

Hệ thống thư viện số dlib.ptit.edu.vn của Học viện Công nghệ Bưu chính Viễn thông (PTIT) là nền tảng trực tuyến quan trọng, cung cấp tài liệu học tập, nghiên cứu cho sinh viên, giảng viên và nghiên cứu sinh. Hệ thống lưu trữ các tài liệu nhạy cảm như giáo trình, luận văn, đề tài nghiên cứu, và thông tin người dùng, đòi hỏi mức độ bảo mật cao. Tuy nhiên, các rủi ro an ninh mạng như tấn công SQL Injection, DDoS, quản lý tài khoản yếu, và không tuân thủ các quy định pháp lý đang đe dọa tính bảo mật, toàn vẹn và sẵn dùng của hệ thống.

Báo cáo này áp dụng phương pháp OCTAVE để phân tích và đánh giá rủi ro an ninh thông tin cho dlib.ptit.edu.vn. Nhóm tập trung vào các lỗ hổng kỹ thuật truyền thống, vấn đề tấn công trên Internet, quản lý người dùng, và một lỗ hổng phi kỹ thuật, đồng thời đánh giá theo các quy chuẩn pháp lý bắt buộc (Luật An ninh mạng, Nghị định 13/2023/NĐ-CP, Nghị định 85/2016/NĐ-CP). Báo cáo đề xuất các biện pháp giảm thiểu hiệu quả, phù hợp với thực tiễn, nhằm đảm bảo an toàn và uy tín của Học viện.

CHƯƠNG 1. TỔNG QUAN VỀ PHƯƠNG PHÁP ĐÁNH GIÁ VÀ HỆ THỐNG THƯ VIỆN SỐ PTIT (DLIB PTIT)

1.1 Phương pháp đánh giá OCTAVE

1.1.1 Giới thiệu

Trong bối cảnh các mối đe dọa an ninh mạng ngày càng phức tạp và gia tăng về quy mô, việc quản lý rủi ro bảo mật thông tin trở thành một yêu cầu cấp thiết đối với mọi tổ chức. Để đối phó hiệu quả với thách thức này, các tổ chức cần một phương pháp đánh giá rủi ro toàn diện, không chỉ tập trung vào khía cạnh kỹ thuật mà còn phải gắn liền với mục tiêu vận hành và chiến lược phát triển của chính tổ chức. Một trong những khuôn khổ được áp dụng rộng rãi và hiệu quả hiện nay là OCTAVE – viết tắt của "Operationally Critical Threat, Asset, and Vulnerability Evaluation".

OCTAVE được phát triển bởi Viện Kỹ nghệ Phần mềm (Software Engineering Institute - SEI) thuộc Đại học Carnegie Mellon, với mục tiêu cung cấp một cách tiếp cận có hệ thống để xác định, phân tích và giảm thiểu các rủi ro bảo mật thông tin. Không giống như các phương pháp đánh giá rủi ro chỉ tập trung vào công nghệ, OCTAVE nhấn mạnh đến yếu tố tổ chức, con người, quy trình và cách các yếu tố này tương tác với hạ tầng công nghệ để tạo ra rủi ro. Đây là một mô hình tự định hướng, cho phép tổ chức chủ động thực hiện đánh giá và đưa ra quyết định phù hợp với bối cảnh hoạt động riêng biệt.

Điểm nổi bật của OCTAVE là khả năng kết nối các mục tiêu bảo mật với định hướng kinh doanh và hoạt động cốt lõi của tổ chức. Phương pháp này giúp xác định các tài sản thông tin quan trọng cần được bảo vệ, đánh giá các mối đe dọa đến từ cả bên trong và bên ngoài, và nhận diện các lỗ hổng trong hệ thống kỹ thuật hoặc quy trình vận hành. Từ đó, tổ chức có thể xây dựng hồ sơ rủi ro cụ thể, ưu tiên biện pháp khắc phục phù hợp và đảm bảo duy trì hoạt động ổn định, an toàn.

Với sự phát triển qua các phiên bản như OCTAVE Classic, OCTAVE-S và OCTAVE Allegro, khuôn khổ này đã chứng minh tính linh hoạt và khả năng áp dụng rộng rãi cho nhiều loại hình tổ chức, từ doanh nghiệp nhỏ đến các cơ quan chính phủ và tổ chức lớn. Chính nhờ sự toàn diện, thực tiễn và định hướng chiến lược, OCTAVE đã trở thành một công cụ không thể thiếu trong việc xây dựng chiến lược an ninh thông tin bền vững trong kỷ nguyên số.

1.1.2 Cách hoạt động

OCTAVE là phương pháp đánh giá rủi ro linh hoạt và tự định hướng. Một nhóm nhỏ những người của các đơn vị hoạt động (hoặc doanh nghiệp) và bộ phận CNTT làm việc cùng nhau để giải quyết các nhu cầu bảo mật của tổ chức. Nhóm nghiên cứu rút ra kiến thức về nhiều nhân viên để xác định tình trạng an ninh hiện tại, xác định rủi ro đối với các tài sản quan trọng và thiết lập một chiến lược bảo mật. Nó có thể được điều chỉnh cho hầu hết các tổ chức.

Không giống như hầu hết các phương pháp đánh giá rủi ro khác, phương pháp OCTAVE được thúc đẩy bởi rủi ro hoạt động và thực tiễn bảo mật chứ không phải công nghệ. Nó được thiết kế để cho phép một tổ chức:

- Trực tiếp và quản lý đánh giá rủi ro an ninh thông tin cho chính họ.

- Đưa ra quyết định tốt nhất dựa trên những rủi ro duy nhất của họ.

- Tập trung vào việc bảo vệ tài sản thông tin quan trọng.

- Giao tiếp hiệu quả thông tin bảo mật quan trọng.

1.1.3 Cấu trúc của OCTAVE

Phương pháp OCTAVE dựa trên tám quy trình được chia thành ba giai đoạn. Trong các tổ chức giáo dục đại học, nó thường được bắt đầu bởi một giai đoạn thăm dò (được gọi là Giai đoạn Zero) để xác định các tiêu chí sẽ được sử dụng trong quá trình áp dụng phương pháp Octave.

1.1.3.1 Giai đoạn 1: Xác định hồ sơ mối đe dọa dựa trên tài sản

* *Quy trình 1:* Xác định các tài sản quan trọng

Mục tiêu: Liệt kê và mô tả chính xác các tài sản quan trọng của tổ chức (có thể là dữ liệu, phần mềm, phần cứng, con người, quy trình).

Cách làm:

- Tổ chức họp nhóm với các bộ phận liên quan.

- Thu thập danh sách tài sản.

- Đánh giá tầm quan trọng của từng tài sản dựa trên ảnh hưởng đến hoạt động, kinh doanh.

* *Quy trình 2:* Xác định các mối đe dọa đối với tài sản

Mục tiêu: Xác định ai/cái gì có thể gây hại cho các tài sản đó.

Cách làm:

- Phân loại các mối đe dọa thành các nhóm như: con người (nhân viên, hacker, đối thủ cạnh tranh), thiên nhiên (lũ lụt, cháy), kỹ thuật (lỗi phần mềm, phần cứng).

- Mô tả cách các mối đe dọa này có thể ảnh hưởng tới tài sản.

* *Quy trình 3*: Xác định các rủi ro liên quan đến mối đe dọa

Mục tiêu: Hiểu cách mối đe dọa khai thác các điểm yếu để gây tổn hại.

Cách làm:

- Phân tích kịch bản mối đe dọa xảy ra (ví dụ: hacker lợi dụng lỗ hổng để đánh cắp dữ liệu).

- Ghi lại mức độ ảnh hưởng có thể xảy ra.

1.1.3.2 Giai đoạn 2: Xác định các điểm yếu trong hạ tầng CNTT

* *Quy trình 4*: Xác định các rủi ro liên quan đến điểm yếu hạ tầng CNTT

Mục tiêu: Phát hiện các lỗ hổng kỹ thuật hoặc tổ chức có thể bị khai thác.

Cách làm:

- Kiểm tra các hệ thống, mạng, phần mềm hiện có.
- Sử dụng các công cụ quét điểm yếu (vulnerability scanner).
- Phỏng vấn nhân viên để hiểu các quy trình bảo mật hiện tại.

* *Quy trình 5*: Xác định các biện pháp kiểm soát hiện tại

Mục tiêu: Hiểu rõ các biện pháp bảo vệ hiện có và hiệu quả của chúng.

Cách làm:

- Kiểm tra các chính sách bảo mật, quy trình, phần mềm bảo vệ.
- Xem xét việc áp dụng tường lửa, mã hóa, kiểm soát truy cập.

* *Quy trình 6*: Xác định các điểm yếu chưa được xử lý

Mục tiêu: Tìm ra các điểm yếu chưa được bảo vệ hoặc bảo vệ chưa đủ.

Cách làm:

- So sánh các điểm yếu đã phát hiện với các biện pháp hiện có.
- Liệt kê các điểm yếu vẫn tồn tại.

1.1.3.3 Giai đoạn 3: Phát triển chiến lược quản lý rủi ro

* *Quy trình 7*: Đánh giá rủi ro và xác định ưu tiên

Mục tiêu: Xác định mức độ nghiêm trọng của từng rủi ro dựa trên khả năng xảy ra và tác động.

Cách làm:

- Dùng ma trận rủi ro (Risk Matrix) đánh giá xác suất xảy ra và mức độ ảnh hưởng.
- Xếp hạng ưu tiên các rủi ro để xử lý.

* *Quy trình 8*: Phát triển kế hoạch giảm thiểu rủi ro

Mục tiêu: Đề xuất các biện pháp cụ thể để giảm thiểu rủi ro đã ưu tiên.

Cách làm:

- Xây dựng các chính sách bảo mật, quy trình vận hành mới.
- Đề xuất các biện pháp kỹ thuật: cập nhật phần mềm, tăng cường kiểm soát truy cập ...
- Lập kế hoạch đào tạo nhân viên về bảo mật.
- Thiết lập kế hoạch giám sát và kiểm tra thường xuyên.

1.2 Hệ thống thư viện số PTIT

1.2.1 Giới thiệu chung

Hệ thống trang web tại địa chỉ https://dlib.ptit.edu.vn/ đóng vai trò là cổng thông tin trực tuyến chính thức cho Trung tâm Thư viện của Học viện Công nghệ Bưu chính Viễn thông (PTIT). Trang web này được thiết kế nhằm cung cấp một nền tảng tập trung để người dùng có thể khám phá, truy cập và tận dụng tối đa các nguồn tài liệu phong phú do thư viện của học viện quản lý. Trong bối cảnh giáo dục và nghiên cứu ngày càng phát triển, một thư viện số hiệu quả là yếu tố then chốt để hỗ trợ học viên, giảng viên và nhà nghiên cứu trong việc học tập, giảng dạy và tiến hành các công trình khoa học. Báo cáo này sẽ cung cấp một cái nhìn tổng quan về mục đích, các phần và tính năng quan trọng, cũng như các loại tài liệu có sẵn trên trang web này, giúp người dùng hiểu rõ hơn về cách thức khai thác hiệu quả nguồn tài nguyên quý giá này. Tuy nhiên, cần lưu ý rằng do các nguồn tài liệu nghiên cứu được cung cấp không liên quan trực tiếp đến trang web này, báo cáo sẽ dựa trên những thông tin có được từ chính yêu cầu của người dùng và những hiểu biết chung về các hệ thống thư viện số.

1.2.2 Chức năng của hệ thống

Trang web thư viện số PTIT cung cấp một loạt các phần và tính năng được thiết kế để tối ưu hóa trải nghiệm người dùng và giúp họ dễ dàng tìm kiếm, khám phá tài liệu.

- *Trang chủ*: Đây thường là điểm khởi đầu cho mọi người dùng khi truy cập trang web. Trang chủ có khả năng cung cấp một cái nhìn tổng quan về thư viện số, giới thiệu các tính năng nổi bật, thông báo mới nhất và có thể bao gồm thanh tìm kiếm nhanh để người dùng có thể bắt đầu tìm kiếm ngay lập tức.

- *Duyệt theo*: Tính năng này cho phép người dùng khám phá bộ sưu tập tài liệu theo nhiều tiêu chí khác nhau. Các tiêu chí phổ biến có thể bao gồm đơn vị và bộ sưu tập (ví dụ: khoa, phòng ban, loại tài liệu), năm xuất bản, tác giả, nhan đề, chủ đề và thậm chí là người hướng dẫn (đặc biệt hữu ích cho việc tìm kiếm khóa luận, luận văn). Việc phân loại tài liệu theo các tiêu chí này giúp người dùng thu hẹp phạm vi tìm kiếm và nhanh chóng tiếp cận các tài liệu liên quan đến lĩnh vực quan tâm của họ.

- *Hồ sơ tác giả*: Phần này cung cấp danh sách các tác giả có đóng góp tài liệu cho thư viện số. Người dùng có thể tìm kiếm theo tên tác giả để xem tất cả các công trình mà một tác giả cụ thể đã xuất bản hoặc đóng góp cho thư viện. Đây là một tính năng quan trọng cho những người quan tâm đến nghiên cứu của một cá nhân cụ thể trong học viện.

- *Các bộ sưu tập*: Trang web có thể tổ chức tài liệu thành các bộ sưu tập riêng biệt dựa trên loại hình tài liệu hoặc chủ đề. Theo thông tin từ yêu cầu, các bộ sưu tập có thể bao gồm bài giảng, bài trích báo - tạp chí, chương trình đào tạo, đề cương bài giảng, đề tài nghiên cứu khoa học, e-book chuyên ngành, giáo trình, khóa luận tốt nghiệp, luận án tiến sĩ, luận văn thạc sĩ, sách danh nhân, sách tâm lý - kỹ năng, sách tôn giáo tâm linh, thông tin - thư viện và tủ sách giải trí - giáo dục. Việc phân chia tài liệu thành các bộ

sưu tập rõ ràng giúp người dùng dễ dàng định hướng và tìm kiếm loại tài liệu mà họ đang cần. Ví dụ, một sinh viên có thể trực tiếp truy cập bộ sưu tập "Khóa luận tốt nghiệp" để tham khảo các công trình nghiên cứu trước đây của sinh viên trong trường.

- *Tài liệu mới cập nhật, Xem nhiều nhất, Tải xuống nhiều nhất*: Các phần này được thiết kế để giúp người dùng khám phá những tài liệu đang được quan tâm gần đây hoặc phổ biến nhất trong cộng đồng PTIT. "Tài liệu mới cập nhật" giúp người dùng không bỏ lỡ những bổ sung mới nhất vào thư viện số. "Xem nhiều nhất" và "Tải xuống nhiều nhất" phản ánh sự quan tâm và nhu cầu của cộng đồng người dùng, giúp người dùng khám phá những tài liệu có giá trị và được đánh giá cao.

- *Hướng dẫn tìm kiếm và Hòm thư góp ý*: Để hỗ trợ người dùng trong quá trình sử dụng trang web, phần "Hướng dẫn tìm kiếm" có thể cung cấp các mẹo và kỹ thuật tìm kiếm hiệu quả, giúp họ khai thác tối đa chức năng tìm kiếm của thư viện số. "Hòm thư góp ý" là một kênh quan trọng để người dùng có thể gửi phản hồi, đề xuất hoặc báo cáo các vấn đề liên quan đến trang web hoặc nội dung của thư viện số, góp phần vào việc cải thiện chất lượng dịch vụ.

- *Cơ sở dữ liệu trực tuyến*: Thư viện PTIT có khả năng đăng ký hoặc cung cấp quyền truy cập đến nhiều cơ sở dữ liệu trực tuyến chuyên ngành. Phần này của trang web sẽ liệt kê các cơ sở dữ liệu này và cung cấp các liên kết trực tiếp để người dùng có thể truy cập và tìm kiếm tài liệu từ các nguồn bên ngoài. Điều này mở rộng đáng kể phạm vi tài liệu mà người dùng PTIT có thể tiếp cận.

- *Liên kết trong Học viện và Liên kết các thư viện số khác*: Trang web có thể cung cấp các liên kết hữu ích đến các trang web khác trong hệ thống của Học viện PTIT (ví dụ: trang web của các khoa, phòng ban, trung tâm) cũng như các liên kết đến các thư viện số của các tổ chức hoặc trường đại học khác. Điều này tạo điều kiện thuận lợi cho người dùng trong việc tìm kiếm thông tin liên quan từ nhiều nguồn khác nhau.

- *Đăng nhập*: Tính năng đăng nhập cho phép người dùng tạo tài khoản cá nhân hoặc sử dụng tài khoản do học viện cung cấp để truy cập các tính năng cá nhân hóa. Các tính năng này có thể bao gồm trang cá nhân để lưu trữ lịch sử tìm kiếm hoặc các tài liệu yêu thích, khả năng đăng ký nhận thông báo qua email về các tài liệu mới trong lĩnh vực quan tâm, và có thể là quyền truy cập vào các tài liệu bị hạn chế chỉ dành cho thành viên của học viện.

- *Tìm kiếm*: Chức năng tìm kiếm là một trong những tính năng quan trọng nhất của bất kỳ thư viện số nào. Trang web thư viện số PTIT có khả năng cung cấp một công cụ tìm kiếm mạnh mẽ cho phép người dùng tìm kiếm tài liệu dựa trên nhiều tiêu chí khác nhau như tất cả các trường thông tin, nhan đề, tác giả, người hướng dẫn, chủ đề hoặc năm xuất bản. Một công cụ tìm kiếm hiệu quả giúp người dùng nhanh chóng xác định và truy cập các tài liệu phù hợp nhất với nhu cầu của họ.

1.2.3 Đối tượng sử dụng

Hệ thống được thiết kế phục vụ cho các nhóm đối tượng chính sau:

- *Sinh viên PTIT*: Truy cập tài liệu học tập, tham khảo luận văn/khóa luận, sử dụng tài nguyên cho đề tài nghiên cứu và báo cáo môn học.

- *Giảng viên và cán bộ nghiên cứu*: Tra cứu tài liệu giảng dạy, đề tài nghiên cứu trước đây, hỗ trợ trong quá trình xây dựng giáo trình, chuẩn bị bài giảng và định hướng sinh viên nghiên cứu khoa học.

- *Cán bộ thư viện/quản trị viên hệ thống*: Quản lý, cập nhật, phê duyệt và tổ chức hệ thống tài liệu trên nền tảng thư viện số. Đảm bảo tài liệu được lưu trữ đúng quy định, chính xác và đầy đủ.

1.3 Kết chương

Chương này đã giới thiệu một cách tổng quan về mô hình đánh giá OCTAVE và hệ thống Dlib PTIT, qua đó tạo kiến thức nền tảng trước khi áp dụng vào đánh giá thực tế.

CHƯƠNG 2. PHÂN TÍCH VÀ ĐÁNH GIÁ RỦI RO CHO HỆ THỐNG THƯ VIỆN SỐ PTIT

2.1 Khái quát

Hệ thống thư viện số dlib.ptit.edu.vn là nền tảng trực tuyến của PTIT, cung cấp quyền truy cập vào các tài liệu học thuật như giáo trình, luận văn, đề tài nghiên cứu, và sách tham khảo. Hệ thống sử dụng cơ sở dữ liệu (database) để lưu trữ tài liệu và thông tin người dùng (tên, email, lịch sử truy cập), với các API endpoints như /api/search, /api/download hỗ trợ tìm kiếm và tải tài liệu. Với lượng người dùng lớn (sinh viên, giảng viên, nghiên cứu sinh), hệ thống yêu cầu bảo mật cao và tuân thủ các quy định pháp lý nghiêm ngặt.

2.2 Thiết lập tiêu chuẩn đánh giá rủi ro

Tiêu chuẩn đánh giá rủi ro dựa trên bối cảnh hoạt động của hệ thống thư viện số dlib.ptit.edu.vn, tập trung vào 5 lĩnh vực: danh tiếng, tài chính, năng suất, an toàn thông tin và pháp luật/tuân thủ.

Bảng 1. Thiết lập tiêu chuẩn đánh giá rủi ro

Lĩnh vực	Thấp (1)	Trung bình (2)	Cao (3)
Danh tiếng	Mất < 5% niềm tin, không bị truyền thông đưa tin	Mất 5-20% niềm tin, truyền thông địa phương	Mất > 20% niềm tin, truyền thông quốc gia
Tài chính	Thiệt hại <100 triệu VND/năm	Thiệt hại 100-500 triệu VND/năm	Thiệt hại > 500 triệu VND/năm
Năng suất	Gián đoạn < 4 giờ, ảnh hưởng cục bộ	Gián đoạn 4-12 giờ, ảnh hưởng vừa phải	Gián đoạn > 12 giờ, ảnh hưởng diện rộng
An toàn thông tin	Lộ dữ liệu không nhạy cảm, không ảnh hưởng đến hệ thống	Lộ dữ liệu cá nhân hạn chế (tên, MSSV, email), hoặc ghi đè dữ liệu cục bộ	Lộ dữ liệu nhạy cảm (thông tin tài khoản, nhật ký hệ thống), bị chiếm quyền, xóa dữ liệu, truy cập trái phép hệ thống
Luật pháp	Cảnh báo nội bộ, không bị phạt	Phạt ≤ 50 triệu VND, yêu cầu khắc phục	Phạt > 50 triệu VND, đình chỉ dịch vụ

2.3 Xây dựng hồ sơ tài sản thông tin

Bảng 2. Xây dựng hồ sơ tài sản

Tài sản	Mô tả	Đối tượng Chứa tài sản	Mức độ nhạy cảm
Tài liệu số nội bộ	Giáo trình, luận văn, đề tài nghiên cứu	Máy chủ database, cloud storage	Cao (Mã hóa AES-256)
Metadata người dùng	Tên, email, lịch sử truy cập	Hệ thống xác thực, logs server	Trung bình(RBAC)
API endpoints	/api/search, /api/download	API Gateway, reverse proxy	Cao (Rate limiting)
Bản ghi DNS	Cấu hình domain, bản ghi MX	DNS server, registrar	Cao(DNSSEC)

2.4 Xác định đối tượng chứa tài sản

2.4.1 Tài sản nội dung học thuật

Bảng 3. Tài sản nội dung học thuật

Tài sản	Chủ sỡ hữu
Bài giảng, đề cương	Giảng viên các khoa, Phòng Đào tạo
Giáo trình, sách tham khảo	Học viện CNBCVT, Nhà xuất bản
Luận văn, luận án, khóa luận	Sinh viên, học viên cao học, nghiên cứu sinh
Đề tài nghiên cứu khoa học	Nhóm nghiên cứu, Phòng KHCN

2.4.2 Tài sản hệ thống công nghệ thông tin

Bảng 4. Tài sản hệ thống CNTT

Tài sản	Chủ sở hữu
Máy chủ web,database	Trung tâm CNTT, Học viện CNBCVT
Hệ thống mạng, firewall	Trung tâm thư viện, Nhà cung cấp phần mềm

Hệ thống backup, DR	Trung tâm dữ liệu, Phòng CNTT

2.4.3 Tài sản dữ liệu người dùng

Bảng 5. Tài sản dữ liệu người dùng

Tài sản	Chủ sở hữu
Cơ sở dữ liệu người dùng	Trung tâm thư viện, Phòng CNTT
Logs truy cập, hoạt động	Phòng An ninh mạng, Học viện CNBCVT
Thông tin xác thực	Phòng Quản lý người dùng, Học viện CNBCVT
Dữ liệu cá nhân sinh viên, cán bộ	Phòng Công tác sinh viên, Phòng tổ chức cán bộ

2.5 Xác định, phân tích các rủi ro hệ thống thư viện số PTIT

2.5.1 Tấn công chèn mã như SQL injection, XSS, …

** Một số thử nghiệm:*

- Điền thử tên một tác giả hợp lệ vào thanh tìm kiếm, ví dụ *"Hoàng Xuân Dậu"*, …
- Điền thử một số ký tự như *",", "--", "@"*, …
- Điền thử cụm *' OR '1'='1* vào thanh tìm kiếm.

** Kết quả thử nghiệm:*

- Khi nhập một cụm/chuỗi ký tự vào thanh tìm kiếm và click tìm kiếm, ta thấy URL sau khi search thông tin trong phần query đã được mã hóa UTF-8 (VD: *https://dlib.ptit.edu.vn/simple-search?location=&filtername=all&query=Ho%C3%A0ng+Xu%C3%A2n+D%E1%BA%ADu&filterquery=&rpp=10&sort_by=score&order=desc*) -> Có khả năng đã qua xử lý để tránh kẻ xấu lợi dụng. Tuy nhiên đây chỉ là phán đoán, do không được phép nên chúng em không dám thử nghiệm với một số query độc hại.

- Khi thử với *' OR '1'='1* (lưu ý ở đây là dán vào thanh tìm kiếm chứ không phải URL, và chỉ thử sau khi thấy phần query trên URL đã được mã hóa), ta không thấy có báo lỗi hay dấu hiệu gì về cảnh báo liên quan đến tấn công chèn mã, mà vẫn có kết quả trả về -> Vẫn có nguy cơ tiềm ẩn lợi dụng quá trình tìm kiếm, hay thậm chí là đăng nhập.

- Nhưng khi thử các ký tự đặc biệt như *"-"*, *"--"*, … thì hệ thống báo có lỗi xảy ra, từ khóa tìm kiếm không phù hợp -> Đã có áp dụng việc lọc các ký tự đầu vào. Như vậy chỉ nhận thấy có vấn đề khi thử nghiệm với chuỗi *' OR '1'='1*. Nếu được thử nghiệm sâu hơn thì có thể biết rõ hơn vấn đề.

** Bảng tổng kết:*

Bảng 6. Bảng tổng kết tấn công chèn mã vào hệ thống

<table>
<tr><td colspan="2">Thông tin tài sản</td><td colspan="5">Dữ liệu sách, tài khoản người dùng và kết quả truy vấn thư viện số</td></tr>
<tr><td colspan="2">Mối quan tâm</td><td colspan="5">Tham số tìm kiếm có thể bị lợi dụng để chèn mã độc nhằm truy xuất dữ liệu trái phép. Nếu chưa lọc kỹ đầu vào của khung này dẫn đến các lỗi như XSS, SQL Injection. Cần ngăn chặn các hành vi tác động đến cơ sở dữ liệu của những người không có thẩm quyền.</td></tr>
<tr><td rowspan="5">Tình huống đe dọa</td><td>Tài sản</td><td colspan="5">Cơ sở dữ liệu</td></tr>
<tr><td>Người tiến hành</td><td colspan="5">Hacker, người dùng độc hại</td></tr>
<tr><td>Phương tiện/Truy nhập</td><td colspan="5">Thanh tìm kiếm, các khung điền thông tin đăng nhập hay ý kiến phản hồi, công cụ như trình duyệt, Burp Suite, SQLMap, …</td></tr>
<tr><td>Động cơ</td><td colspan="5">Truy cập trái phép hoặc sửa đổi dữ liệu thư viện, trong đó có thông tin người dùng</td></tr>
<tr><td>Kết quả</td><td colspan="5">Phá hủy dữ liệu do bị hacker tấn công.</td></tr>
<tr><td colspan="2">Tác động</td><td colspan="5">Phân tích rủi ro</td></tr>
<tr><td colspan="2" rowspan="7">Việc bất kỳ ai cũng có thể tác động đến cơ sở dữ liệu thì website sẽ không thể hoạt động.</td><td>Lĩnh vực</td><td>Phân loại</td><td colspan="2">Giá trị tác động</td><td>Mức điểm</td></tr>
<tr><td>Danh tiếng/ Uy tín</td><td>4</td><td colspan="2">Cao (3)</td><td>12</td></tr>
<tr><td>Tài chính</td><td>2</td><td colspan="2">Trung bình (2)</td><td>4</td></tr>
<tr><td>Năng suất</td><td>2</td><td colspan="2">Trung bình (2)</td><td>4</td></tr>
<tr><td>An toàn thông tin</td><td>5</td><td colspan="2">Cao (3)</td><td>15</td></tr>
<tr><td>Luật pháp</td><td>3</td><td colspan="2">Cao (3)</td><td>9</td></tr>
<tr><td colspan="3">Tổng điểm</td><td>44</td></tr>
<tr><td colspan="3">Khả năng xảy ra</td><td colspan="3">Trung bình</td></tr>
<tr><td colspan="6">Lựa chọn giảm thiểu</td></tr>
</table>

Giảm thiểu	Giảm thiểu hay loại trừ	Loại trừ hay chấp nhận	Chấp nhận
	X		
Phương pháp loại bỏ			
Nhân viên kỹ thuật		- Sử dụng prepared statements hoặc ORM để truy vấn. - Kiểm tra, lọc toàn bộ đầu vào từ phía client và server. - Ghi log các truy vấn bất thường. - Bổ sung tính năng tự động chặn truy vấn có chứa từ khóa nghi ngờ (OR 1=1, ...)	
Người dùng (Giảng viên, sinh viên)		- Hạn chế sử dụng các ký tự đặc biệt.	

2.5.2 Tấn công dò mật khẩu người dùng

** Một số thử nghiệm:*

- Với cùng 1 email, thử nhập sai mật khẩu nhiều lần;

- Nhập nhiều tài khoản các nhau, kể cả dùng các mail bên ngoài không phải mail đăng ký với trường, đăng nhập sai liên tục.

** Kết quả thử nghiệm*:

- Kể cả khi đã nhập sai tài khoản và nhập khẩu nhiều lần, vẫn không bị giới hạn hay ngăn chặn. Hệ thống vẫn cho phép đăng nhập lại như bình thường -> Nguy cơ bị brute-force để dò tìm mật khẩu của người dùng hợp lệ.

- Cũng không có CAPTCHA hay một số hình thức khác để xác minh không phải robot, thời gian cho phép đăng nhập lại rất nhanh -> Gần như là không có bất kỳ hình thức hạn chế nào để đảm bảo an toàn cho quá trình đăng nhập của người dùng.

** Bảng tổng kết*:

Bảng 7. Bảng tổng kết tấn công dò mật khẩu người dùng

Thông tin tài sản		Tài khoản đăng nhập hệ thống thư viện số và cơ chế xác thực người dùng
Mối quan tâm		Hệ thống không giới hạn số lần đăng nhập sai, không CAPTCHA, có nguy cơ bị brute-force để chiếm quyền truy cập
Tình huống đe dọa	**Tài sản**	Tài khoản người dùng và quyền truy cập hệ thống
	Người tiến hành	Hacker

<table>
<tr><td rowspan="3"></td><td>Phương tiện/Truy nhập</td><td colspan="4">Biểu mẫu đăng nhập trên dlib.ptit.edu.vn; công cụ brute-force như Hydra, Burp Suite Intruder, …</td></tr>
<tr><td>Động cơ</td><td colspan="4">Chiếm quyền truy cập vào tài khoản người dùng hoặc quản trị viên</td></tr>
<tr><td>Kết quả</td><td colspan="4">Thông tin người dùng hợp lệ bị chiếm đoạt, có thể bị lợi dụng cho các mục đích xấu khác</td></tr>
<tr><td colspan="2">Tác động</td><td colspan="4">Phân tích rủi ro</td></tr>
<tr><td colspan="2" rowspan="7">Việc không giới hạn số lần đăng nhập sai cũng như không có các biện pháp hạn chế khác có thể khiến tài khoản người dùng bị chiếm đoạt, gây mất dữ liệu người dùng hoặc bị lợi dụng cho các tác vụ xấu.</td><td>Lĩnh vực</td><td>Phân loại</td><td>Giá trị tác động</td><td>Mức điểm</td></tr>
<tr><td>Danh tiếng/ Uy tín</td><td>3</td><td>Cao (3)</td><td>9</td></tr>
<tr><td>Tài chính</td><td>2</td><td>Trung bình (2)</td><td>4</td></tr>
<tr><td>Năng suất</td><td>2</td><td>Trung bình (2)</td><td>4</td></tr>
<tr><td>An toàn thông tin</td><td>5</td><td>Cao (3)</td><td>15</td></tr>
<tr><td>Luật pháp</td><td>3</td><td>Trung bình (2)</td><td>6</td></tr>
<tr><td colspan="3">Tổng điểm</td><td>38</td></tr>
<tr><td colspan="2">Khả năng xảy ra</td><td colspan="4">Cao</td></tr>
<tr><td colspan="6">Lựa chọn giảm thiểu</td></tr>
<tr><td colspan="2">Giảm thiểu</td><td>Giảm thiểu hay loại trừ</td><td colspan="2">Loại trừ hay chấp nhận</td><td>Chấp nhận</td></tr>
<tr><td colspan="2"></td><td>X</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="6">Phương pháp loại bỏ</td></tr>
<tr><td colspan="2">Nhân viên kỹ thuật</td><td colspan="4">- Giới hạn số lần đăng nhập sai;
- Khóa tạm thời tài khoản sau nhiều lần thất bại;
- Thêm CAPTCHA khi nghi ngờ; cảnh báo đăng nhập bất thường;
- Hỗ trợ xác thực hai yếu tố (2FA)</td></tr>
<tr><td colspan="2">Người dùng (Giảng viên, sinh viên)</td><td colspan="4">- Bảo vệ tài khoản, sử dụng mật khẩu mạnh</td></tr>
</table>

2.5.3 Tấn công vào cấu hình hệ thống (dò đường dẫn)

** Một số thử nghiệm*:

- Điền *"/admin"* vào cuối URL;

- Điền *"/login.php"* vào cuối URL.

** Kết quả thử nghiệm:*

- Web hiện thông báo đường dẫn không chính xác.

- Tuy vậy, không trả về thông báo lỗi HTTP mặc định, với mã lỗi + thông báo. Thì vẫn có nguy cơ hacker thử các URL khác để dò cấu trúc nội bộ, hay thử các endpoint ít người biết như */admin/config*, */koha/svc/admin*, ... để tìm điểm vào hệ thống quản trị nếu không được cấu hình bảo vệ đúng. Nhưng chúng em suy đoán rằng khả năng này xảy ra không cao.

** Bảng tổng kết*:

Bảng 8. Bảng tổng kết tấn công vào cấu hình hệ thống

<table>
<tr><td colspan="2">Thông tin tài sản</td><td colspan="5">Cấu trúc đường dẫn hệ thống thư viện số, điểm truy cập tới chức năng quản trị</td></tr>
<tr><td colspan="2">Mối quan tâm</td><td colspan="5">Hệ thống phản hồi lỗi thân thiện khi truy cập URL nội bộ như /admin, cho thấy có thể dò cấu trúc router hoặc endpoint nội bộ</td></tr>
<tr><td rowspan="5">Tình huống đe dọa</td><td>Tài sản</td><td colspan="5">Đường dẫn và giao diện quản trị hệ thống</td></tr>
<tr><td>Người tiến hành</td><td colspan="5">Hacker</td></tr>
<tr><td>Phương tiện/Truy nhập</td><td colspan="5">URL, công cụ dò quét như Gobuster, Burp Suite, Nikto, …</td></tr>
<tr><td>Động cơ</td><td colspan="5">Dò tìm điểm truy cập admin, chiếm quyền hoặc thực hiện Forced Browsing</td></tr>
<tr><td>Kết quả</td><td colspan="5">Trả về thông báo lỗi tùy chỉnh thay vì mã lỗi HTTP chuẩn, có thể bị lạm dụng để tiếp tục dò đoán endpoint quản trị</td></tr>
<tr><td colspan="2">Tác động</td><td colspan="5">Phân tích rủi ro</td></tr>
<tr><td colspan="2" rowspan="6">Trường hợp trang quản trị hệ thống bị xâm nhập có thể gây tê liệt hoạt động của hệ thống, dữ liệu bị ảnh hưởng, …</td><td>Lĩnh vực</td><td>Phân loại</td><td>Giá trị tác động</td><td>Mức điểm</td></tr>
<tr><td>Danh tiếng/ Uy tín</td><td>2</td><td>Trung bình (2)</td><td>4</td></tr>
<tr><td>Tài chính</td><td>2</td><td>Trung bình (2)</td><td>4</td></tr>
<tr><td>Năng suất</td><td>2</td><td>Trung bình (2)</td><td>4</td></tr>
<tr><td>An toàn thông tin</td><td>3</td><td>Cao (3)</td><td>9</td></tr>
<tr><td>Luật pháp</td><td>2</td><td>Trung bình (2)</td><td>4</td></tr>
</table>

		Tổng điểm	**25**
Khả năng xảy ra		Thấp	
Lựa chọn giảm thiểu			
Giảm thiểu	Giảm thiểu hay loại trừ	Loại trừ hay chấp nhận	Chấp nhận
		X	
Phương pháp loại bỏ			
Nhân viên kỹ thuật		- Trả về mã lỗi HTTP chuẩn (404/403) cho các đường dẫn không tồn tại; - Cấu hình server để không phản hồi khác biệt giữa URL có thật và không thật; - Ẩn hoặc đổi tên endpoint nhạy cảm (admin, config, ...) …	

2.5.4 Tấn công path traversal

Bảng 9. Bảng tổng kết tấn công path traversal

Thông tin tài sản	File cấu hình, dữ liệu nhạy cảm trên máy chủ				
Mối quan tâm	Hacker khai thác lỗ hổng nhập liệu để truy cập file/directory ngoài phạm vi cho phép, đọc file cấu hình, mã nguồn hoặc dữ liệu nhạy cảm.				
Tình huống đe dọa	**Tài sản**	Dữ liệu cấu hình, mã nguồn, dữ liệu người dùng			
	Người thực hiện	Hacker, đối tượng có kỹ năng kỹ thuật			
	Phương tiện/Truy nhập	Gửi request với tham số đường dẫn (../) để truy cập file hệ thống			
	Động cơ	Đánh cắp thông tin, khai thác sâu hơn vào hệ thống.			
	Kết quả	Lộ thông cấu hình, đánh cắp tài liệu học thuật có giá trị, truy cập trái phép dữ liệu người dùng			
Khả năng xảy ra		Trung Bình			
Tác động		**Phân tích rủi ro**			
Có thể truy cập các file hệ thống và tài liệu ngoài phạm vi được phép, đặc biệt nguy hiểm với luận		**Lĩnh vực**	**Phân loại**	**Giá trị tác động**	**Mức điểm**

văn/luận án chưa công bố hoặc tài liệu giảng dạy nội bộ	**Danh tiếng/ Uy tín**	4	Trung bình (3)	12
	Tài chính	2	Thấp (1)	2
	Năng suất	3	Trung Bình (2)	6
	Luật pháp	5	Cao (3)	15
	Tổng điểm			**35**
Mức độ ảnh hưởng	Trung bình			
Lựa chọn giảm thiểu				
Giảm thiểu	Giảm thiểu hay loại trừ	Loại trừ hay chấp nhận		Chấp nhận
X				
Phương pháp giảm thiểu				
Source của website	Kiểm tra, lọc và xác thực đầu vào. Giới hạn quyền truy cập file. Cấu hình web server chặn truy cập ngoài thư mục cho phép.			
Kiểm thử	Định kỳ kiểm tra lỗ hổng bảo mật, đặc biệt là API truy xuất tài liệu số			

2.5.5 Website bị ngừng hoạt động do DOS/Ddos và các biến thể Dos

Bảng 10. Bảng tổng kết tấn công DoS/DDoS

Thông tin tài sản		Tính sẵn dùng của website dlib.ptit.edu.vn
Mối quan tâm		Một cuộc tấn công DoS hoặc DDoS khiến hệ thống thư viện số bị gián đoạn, sinh viên, giảng viên không thể truy cập tài liệu học tập, nghiên cứu, ảnh hưởng lớn đến uy tín của Học viện.
Tình huống đe dọa	**Tài sản**	Tính sẵn dùng của website và các dịch vụ thư viện số
	Người thực hiện	Nhóm hacker, đối thủ cạnh tranh, hoặc cá nhân có động cơ phá hoại
	Phương tiện/Truy nhập	Hệ thống botnet, các công cụ tấn công DDoS như LOIC, XOIC, hoặc thuê dịch vụ DDoS, …
	Động cơ	Tấn công làm tê liệt website, gây mất tính sẵn dùng

<table>
<tr><td></td><td>Kết quả</td><td colspan="4">Website ngừng hoạt động từ vài phút đến nhiều giờ, gây ảnh hưởng lớn đến hoạt động học tập, nghiên cứu, uy tín của Học viện.</td></tr>
<tr><td colspan="2">Khả năng xảy ra</td><td colspan="4">Cao</td></tr>
<tr><td colspan="2">Tác động</td><td colspan="4">Phân tích rủi ro</td></tr>
<tr><td colspan="2" rowspan="6">Ảnh hưởng lớn đến việc truy cập các tài liệu học tập, nghiên cứu của sinh viên, giảng viên, đặc biệt nghiêm trọng trong mùa thi hoặc thời điểm nộp luận văn.</td><td>Lĩnh vực</td><td>Tác động</td><td>Giá trị tác động</td><td>Mức điểm</td></tr>
<tr><td>Danh tiếng/ Uy tín</td><td>4</td><td>Cao (3)</td><td>12</td></tr>
<tr><td>Tài chính</td><td>3</td><td>Cao (3)</td><td>9</td></tr>
<tr><td>Năng suất</td><td>5</td><td>Cao (3)</td><td>15</td></tr>
<tr><td>Luật pháp</td><td>2</td><td>Trung bình (2)</td><td>4</td></tr>
<tr><td colspan="3">Tổng điểm</td><td>39</td></tr>
<tr><td colspan="2">Mức độ ảnh hưởng</td><td colspan="4">Cao</td></tr>
<tr><td colspan="6">Lựa chọn giảm thiểu</td></tr>
<tr><td>Giảm thiểu</td><td>Giảm thiểu hay loại trừ</td><td colspan="3">Loại trừ hay chấp nhận</td><td>Chấp nhận</td></tr>
<tr><td></td><td>x</td><td colspan="3"></td><td></td></tr>
<tr><td colspan="6">Phương pháp giảm thiểu</td></tr>
<tr><td colspan="2">Source của website</td><td colspan="4">Chống Iframe: chèn 1 đoạn mã Javascript chống chèn iframe từ các website khác đến website.
Giới hạn số kết nối website tại một thời điểm.Hạn chế lưu lượng mạng để đảm bảo rằng lưu lượng truy cập tác vụ PBMS hợp lệ có thể đạt tới hệ thống PBMS</td></tr>
<tr><td colspan="2">Hệ thống Firewall</td><td colspan="4">- Sử dụng Firewall mềm trên VPS: cài đặt một số phần mềm firewall mã nguồn mở để bảo vệ VPS hoặc máy chủ của mình như:
https://en.wikipedia.org/wiki/List_of_router_and_firewall_distributions
- Triển khai WAF kết hợp dịch vụ anti-DdoS, sử dungj CDN như Cloudflare.</td></tr>
</table>

2.5.6 Website bị giả mạo bởi Man-in-the-middle, DNS Spoofing

Bảng 11. Bảng tổng kết tấn công giả mạo

<table>
<tr><td colspan="2">Thông tin tài sản</td><td colspan="5">Phiên đăng nhập, dữ liệu truyền tải</td></tr>
<tr><td colspan="2">Mối quan tâm</td><td colspan="5">Đánh chặn, nghe lén hoặc thay đổi dữ liệu khi người dùng đang truy cập thư viện số, đặc biệt nguy hiểm khi sinh viên sử dụng WiFi công cộng</td></tr>
<tr><td rowspan="4">Tình huống đe dọa</td><td>Tài sản</td><td colspan="5">Thông tin xác thực, dữ liệu truyền</td></tr>
<tr><td>Người thực hiện</td><td colspan="5">Hacker , đối tượng có khả năng kiểm soát mạng trung gian (WiFi công cộng, mạng nội bộ không bảo mật)</td></tr>
<tr><td>Phương tiện/Truy nhập</td><td colspan="5">ARP spoofing, DNS spoofing, SSL stripping, Wifi giả mạo</td></tr>
<tr><td>Động cơ</td><td colspan="5">Đánh cắp thông tin đăng nhập, theo dõi hoạt động người dùng</td></tr>
<tr><td colspan="2">Kết quả</td><td colspan="5">Mất quyền kiểm soát tài khoản, lộ thông tin cá nhân, thay đổi dữ liệu</td></tr>
<tr><td colspan="2">Tác động</td><td colspan="5">Phân tích rủi ro</td></tr>
<tr><td colspan="2" rowspan="6">Tài khoản người dùng bị chiếm quyền.</td><td>Lĩnh vực</td><td>Phân loại</td><td colspan="2">Giá trị tác động</td><td>Mức điểm</td></tr>
<tr><td>Danh tiếng/ Uy tín</td><td>4</td><td colspan="2">Cao (3)</td><td>12</td></tr>
<tr><td>Tài chính</td><td>3</td><td colspan="2">Trung Bình (2)</td><td>6</td></tr>
<tr><td>Năng suất</td><td>2</td><td colspan="2">Trung Bình (2)</td><td>4</td></tr>
<tr><td>Luật pháp</td><td>5</td><td colspan="2">Cao (3)</td><td>15</td></tr>
<tr><td colspan="3">Tổng điểm</td><td>37</td></tr>
<tr><td colspan="7">Lựa chọn giảm thiểu</td></tr>
<tr><td colspan="2">Giảm thiểu</td><td>Giảm thiểu hay loại trừ</td><td colspan="3">Loại trừ hay chấp nhận</td><td>Chấp nhận</td></tr>
<tr><td colspan="2"></td><td>X</td><td colspan="3"></td><td></td></tr>
<tr><td colspan="7">Phương pháp giảm thiểu</td></tr>
<tr><td colspan="2">Hệ thống web</td><td colspan="5">Sử dụng IDS: Một dạng hệ thống phát hiện dấu hiệu xâm nhập. Khi được đặt và triển khai trên hệ thống của web, nó có thể phát hiện các hình thức giả mạo ARP cache và giả mạo DNS.
Sử dụng DNSSEC: DNSSEC là một giải pháp thay thế mới cho DNS, sử dụng các bản ghi DNS có chữ ký (Signature) để bảo đảm sự hợp lệ hóa của đáp trả truy vấn. Giải pháp này đã có sự triển khai nhất định.
Triển khai HTTPS toàn diện, HSTS</td></tr>
</table>

Đào tạo	Nâng cao nhận thức cho người dùng về rủi ro khi sử dụng WiFi công cộng Hướng dẫn sử dụng VPN khi truy cập từ mạng không tin cậy

2.5.7 Website bị tấn công deface

Bảng 12. Bảng tổng kết tấn công deface

<table>
<tr><td>Thông tin tài sản</td><td colspan="5">Giao diện website, nội dung, danh tiếng của PTIT</td></tr>
<tr><td>Mối quan tâm</td><td colspan="5">Các vụ tấn công deface (thay đổi giao diện website) diễn ra rất phổ biến vì nó bắt nguồn từ nhiều lỗ hổng bảo mật khác nhau, và hầu hết là những lỗ hổng rất nghiêm trọng</td></tr>
<tr><td rowspan="4">Tình huống đe dọa</td><td>Tài sản</td><td colspan="4">Giao diện, nội dung website</td></tr>
<tr><td>Người thực hiện</td><td colspan="4">Hacker, nhóm tấn công có tổ chức</td></tr>
<tr><td>Phương tiện/Truy nhập</td><td colspan="4">Khai thác lỗ hổng CMS, file upload, SQLi, lỗi cấu hình</td></tr>
<tr><td>Động cơ</td><td colspan="4">Có rất nhiều động cơ khiến hacker thực thi một cuộc tấn công deface như: cảnh báo quản trị viên website đang tồn tại lỗ hổng bảo mật nghiêm trọng, chứng tỏ năng lực bản thân, thù hằn, tuyên truyền...</td></tr>
<tr><td>Kết quả</td><td colspan="4">Giao diện trang web bị thay đổi ảnh hưởng nghiêm trọng tới uy tín của công ty TMĐT</td></tr>
<tr><td colspan="2">Khả năng xảy ra rủi ro</td><td colspan="4">Cao</td></tr>
<tr><td colspan="2">Tác động</td><td colspan="4">Phân tích rủi ro</td></tr>
<tr><td colspan="2" rowspan="6">Thay đổi giao diện, nội dung website thư viện số, chèn thông tin sai lệch hoặc nội dung không phù hợp, ảnh hưởng nghiêm trọng đến uy tín của học viện</td><td>Lĩnh vực</td><td>Phân loại</td><td>Giá trị tác động</td><td>Mức điểm</td></tr>
<tr><td>Danh tiếng/ Uy tín</td><td>5</td><td>Cao (3)</td><td>15</td></tr>
<tr><td>Tài chính</td><td>4</td><td>Cao (3)</td><td>12</td></tr>
<tr><td>Năng suất</td><td>3</td><td>Trung bình (2)</td><td>6</td></tr>
<tr><td>Luật pháp</td><td>1</td><td>Trung bình (2)</td><td>2</td></tr>
<tr><td colspan="3">Tổng điểm</td><td>41</td></tr>
<tr><td colspan="6">Lựa chọn giảm thiểu</td></tr>
<tr><td>Giảm thiểu</td><td>Giảm thiểu hay loại trừ</td><td colspan="3">Loại trừ hay chấp nhận</td><td>Chấp nhận</td></tr>
<tr><td></td><td>x</td><td colspan="3"></td><td></td></tr>
<tr><td colspan="6">Phương pháp giảm thiểu</td></tr>
</table>

Giám sát truy cập hệ thống	Theo dõi các thông tin nhật ký, file log của máy chủ và truy tìm xem hacker đã làm gì và làm thế nào đối với hệ thống của mình.
Mã nguồn website	Kiểm tra và cập nhật bản vá các lỗ hổng như SQL injection, XSS, Remote file include, Local file include

2.5.8 Rủi ro phishing

Bảng 13. Bảng tổng kết rủi ro phising

<table>
<tr><td>Thông tin tài sản</td><td colspan="4">Thông tin xác thực người dùng (tên đăng nhập, mật khẩu), dữ liệu cá nhân (tên, email, lịch sử truy cập), phiên đăng nhập</td></tr>
<tr><td>Mối quan tâm</td><td colspan="4">Các cuộc tấn công phishing nhằm đánh cắp thông tin xác thực hoặc lừa người dùng cung cấp thông tin nhạy cảm thông qua email giả mạo, trang web giả mạo, hoặc các liên kết độc hại. Điều này có thể dẫn đến truy cập trái phép vào hệ thống thư viện số, làm lộ tài liệu học thuật hoặc thông tin cá nhân.</td></tr>
<tr><td rowspan="5">Tình huống đe dọa</td><td>Tài sản</td><td colspan="3">Thông tin xác thực, dữ liệu cá nhân, phiên đăng nhập</td></tr>
<tr><td>Người thực hiện</td><td colspan="3">Hacker, nhóm tội phạm mạng, hoặc cá nhân có động cơ đánh cắp thông tin</td></tr>
<tr><td>Phương tiện/Truy nhập</td><td colspan="3">Email giả mạo, trang web giả mạo (nhái giao diện dlib.ptit.edu.vn), liên kết độc hại qua mạng xã hội hoặc email</td></tr>
<tr><td>Động cơ</td><td colspan="3">Đánh cắp thông tin đăng nhập để truy cập trái phép, bán dữ liệu cá nhân, hoặc thực hiện các hành vi phá hoại</td></tr>
<tr><td>Kết quả</td><td colspan="3">Mất quyền kiểm soát tài khoản, lộ thông tin cá nhân, truy cập trái phép vào tài liệu học thuật, gây ảnh hưởng đến uy tín của Học viện</td></tr>
<tr><td colspan="2">Khả năng xảy ra rủi ro</td><td colspan="3">Cao</td></tr>
<tr><td colspan="2">Tác động</td><td colspan="3">Phân tích rủi ro</td></tr>
<tr><td colspan="2" rowspan="5">Thay đổi giao diện, nội dung website thư viện số, chèn thông tin sai lệch hoặc nội dung không phù hợp, ảnh hưởng nghiêm trọng đến uy tín của học viện</td><td>Lĩnh vực</td><td>Phân loại</td><td>Giá trị tác động</td><td>Mức điểm</td></tr>
<tr><td>Danh tiếng/ Uy tín</td><td>4</td><td>Cao (3)</td><td>12</td></tr>
<tr><td>Tài chính</td><td>3</td><td>Trung bình (2)</td><td>6</td></tr>
<tr><td>Năng suất</td><td>3</td><td>Trung bình (2)</td><td>6</td></tr>
<tr><td>An toàn và sức khỏe</td><td>1</td><td>Thấp (1)</td><td>1</td></tr>
</table>

		Luật pháp	5	Cao (3)	15
		Tổng điểm			**40**
Lựa chọn giảm thiểu					
Giảm thiểu	Giảm thiểu hay loại trừ	Loại trừ hay chấp nhận			Chấp nhận
Ưu tiên triển khai các biện pháp bảo vệ	x	Không áp dụng			Không áp dụng
Phương pháp giảm thiểu					
Hệ thống web		- Triển khai HTTPS toàn diện và HSTS để đảm bảo người dùng chỉ truy cập vào trang web chính thức. - Sử dụng DMARC, SPF, DKIM để kiểm tra tính hợp lệ của email gửi từ domain dlib.ptit.edu.vn, giảm nguy cơ email giả mạo. - Cảnh báo người dùng về các trang web giả mạo thông qua thông báo trên giao diện chính thức.			
Đào tạo		- Tổ chức các buổi đào tạo về nhận thức an ninh mạng, hướng dẫn sinh viên và giảng viên nhận biết email/liên kết phishing. - Khuyến khích sử dụng VPN khi truy cập từ mạng công cộng			
Kiểm tra định kỳ		Quét các trang web giả mạo nhái domain dlib.ptit.edu.vn bằng các công cụ như Google Safe Browsing hoặc dịch vụ giám sát thương hiệu			

2.5.9 Rủi ro Malware

Bảng 14. Bảng tổng kết rủi ro malware

Thông tin tài sản	Máy chủ web, cơ sở dữ liệu, tài liệu số, thiết bị người dùng	
Mối quan tâm	Malware (như ransomware, spyware, hoặc trojan) có thể được phát tán qua tài liệu tải xuống từ hệ thống, email giả mạo, hoặc lỗ hổng trên website. Điều này có thể làm tê liệt hệ thống, làm mất dữ liệu học thuật, hoặc ảnh hưởng đến thiết bị của người dùng	
Tình huống đe dọa	**Tài sản**	Máy chủ web, cơ sở dữ liệu, tài liệu số, thiết bị người dùng
	Người thực hiện	Hacker, tội phạm mạng, hoặc bot tự động phát tán malware
	Phương tiện/Truy nhập	Tệp tải xuống chứa mã độc, email đính kèm, khai thác lỗ hổng website (như XSS, file upload)

<table>
<tr><td rowspan="2"></td><td>Động cơ</td><td colspan="4">Tống tiền (ransomware), đánh cắp dữ liệu, hoặc phá hoại hệ</td></tr>
<tr><td>Kết quả</td><td colspan="4">Mất dữ liệu, mã hóa tài liệu học thuật, gián đoạn dịch vụ, lây nhiễm thiết bị người dùng, ảnh hưởng đến uy tín của Học viện</td></tr>
<tr><td colspan="2">Khả năng xảy ra rủi ro</td><td colspan="4">Trung bình</td></tr>
<tr><td colspan="2">Tác động</td><td colspan="4">Phân tích rủi ro</td></tr>
<tr><td colspan="2" rowspan="6">Thay đổi giao diện, nội dung website thư viện số, chèn thông tin sai lệch hoặc nội dung không phù hợp, ảnh hưởng nghiêm trọng đến uy tín của học viện</td><td>Lĩnh vực</td><td>Phân loại</td><td>Giá trị tác động</td><td>Mức điểm</td></tr>
<tr><td>Danh tiếng/ Uy tín</td><td>5</td><td>Cao (3)</td><td>15</td></tr>
<tr><td>Tài chính</td><td>4</td><td>Cao (3)</td><td>12</td></tr>
<tr><td>Năng suất</td><td>4</td><td>Cao (3)</td><td>12</td></tr>
<tr><td>An toàn và sức khỏe</td><td>2</td><td>Thấp(1)</td><td>2</td></tr>
<tr><td>Luật pháp</td><td>4</td><td>Cao (3)</td><td>12</td></tr>
<tr><td colspan="2">Lựa chọn giảm thiểu</td><td colspan="3">Tổng điểm</td><td>53</td></tr>
<tr><td>Giảm thiểu</td><td>Giảm thiểu hay loại trừ</td><td colspan="3">Loại trừ hay chấp nhận</td><td>Chấp nhận</td></tr>
<tr><td>Ưu tiên triển khai các biện pháp bảo vệ</td><td>x</td><td colspan="3">Không áp dụng</td><td>Không áp dụng</td></tr>
<tr><td colspan="6">Phương pháp giảm thiểu</td></tr>
<tr><td colspan="2">Hệ thống web</td><td colspan="4">- Cài đặt và cập nhật phần mềm diệt virus/malware trên máy chủ (ví dụ: ClamAV).
- Kiểm tra và quét tất cả các tệp tải lên để phát hiện mã độc trước khi lưu trữ.
- Áp dụng WAF (Web Application Firewall) để phát hiện và chặn các hành vi bất thường như tải lên tệp độc hại hoặc khai thác XSS.
- Cập nhật và vá lỗi CMS, plugin, và phần mềm liên quan định kỳ.</td></tr>
<tr><td colspan="2">Máy chủ và cơ sở dữ liệu</td><td colspan="4">- Sử dụng hệ thống phát hiện xâm nhập (IDS/IPS) để giám sát và chặn các hành vi đáng ngờ.
- Thực hiện backup định kỳ và kiểm tra khả năng khôi phục dữ liệu để giảm thiểu tác động của ransomware.</td></tr>
<tr><td colspan="2">Đào tạo người dùng</td><td colspan="4">- Hướng dẫn sinh viên và giảng viên không tải xuống các tệp từ nguồn không xác thực.</td></tr>
</table>

	- Cảnh báo về các email đính kèm đáng ngờ hoặc liên kết không rõ nguồn gốc.
Kiểm tra định kỳ	Thực hiện kiểm tra bảo mật định kỳ (penetration testing) để phát hiện lỗ hổng liên quan đến file upload, XSS, hoặc các vector phát tán malware

2.5.10 Yếu tố xác thực không đủ mạnh

Bảng 15. Bảng tổng kết rủi ro yếu tố xác thực không đủ mạnh

<table>
<tr><td colspan="2">Thông tin tài sản</td><td colspan="5">Tài khoản người dùng hệ thống (giảng viên, sinh viên, quản trị viên)</td></tr>
<tr><td colspan="2">Mối quan tâm</td><td colspan="5">Hệ thống không có xác thực hai yếu tố (2FA), chỉ dùng mật khẩu đơn thuần dễ bị tấn công brute-force hoặc phishing.</td></tr>
<tr><td rowspan="5">Tình huống đe dọa</td><td>Tài sản</td><td colspan="5">Tài khoản người dùng</td></tr>
<tr><td>Người tiến hành</td><td colspan="5">Hacker, đối tượng giả mạo</td></tr>
<tr><td>Phương tiện/Truy nhập</td><td colspan="5">Brute-force, công cụ dò mật khẩu, tấn công phishing</td></tr>
<tr><td>Động cơ</td><td colspan="5">Chiếm quyền truy cập trái phép</td></tr>
<tr><td>Kết quả</td><td colspan="5">Vi phạm tính bí mật, toàn vẹn, cho phép thao tác trái phép trong hệ thống</td></tr>
<tr><td colspan="2">Tác động</td><td colspan="5">Phân tích rủi ro</td></tr>
<tr><td colspan="2" rowspan="7">Dễ bị chiếm quyền truy cập tài khoản cá nhân dẫn đến bị thay đổi thông tin, mất dữ liệu riêng tư, thao tác giả mạo.</td><td>Lĩnh vực</td><td colspan="2">Phân loại</td><td>Giá trị tác động</td><td>Mức điểm</td></tr>
<tr><td>Danh tiếng/ Uy tín</td><td colspan="2">5</td><td>Cao (3)</td><td>15</td></tr>
<tr><td>Tài chính</td><td colspan="2">3</td><td>Trung bình (2)</td><td>6</td></tr>
<tr><td>Năng suất</td><td colspan="2">3</td><td>Trung bình (2)</td><td>6</td></tr>
<tr><td>An toàn thông tin</td><td colspan="2">1</td><td>Thấp (1)</td><td>1</td></tr>
<tr><td>Luật pháp</td><td colspan="2">2</td><td>Trung bình (2)</td><td>2</td></tr>
<tr><td colspan="3">Tổng điểm</td><td>32</td></tr>
<tr><td colspan="3">Khả năng xảy ra</td><td colspan="3">Cao</td></tr>
<tr><td colspan="6">Lựa chọn giảm thiểu</td></tr>
<tr><td colspan="2">Giảm thiểu</td><td>Giảm thiểu hay loại trừ</td><td colspan="2">Loại trừ hay chấp nhận</td><td>Chấp nhận</td></tr>
<tr><td colspan="2"></td><td>X</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="6">Phương pháp loại bỏ</td></tr>
<tr><td colspan="3">Nhân viên kỹ thuật</td><td colspan="3">- Áp dụng xác thực 2 bước (2FA);
- Hạn chế đăng nhập sai quá nhiều lần;</td></tr>
</table>

	- Cảnh báo đăng nhập bất thường;

2.5.11 Mật khẩu không đủ mạnh

Bảng 16. Bảng tổng kết rủi ro mật khẩu không đủ mạnh

<table>
<tr><td colspan="2">Thông tin tài sản</td><td colspan="5">Tài khoản người dùng</td></tr>
<tr><td colspan="2">Mối quan tâm</td><td colspan="5">Người dùng được phép đặt mật khẩu yếu, ngắn, dễ đoán</td></tr>
<tr><td rowspan="5">Tình huống đe dọa</td><td>Tài sản</td><td colspan="5">Tài khoản người dùng</td></tr>
<tr><td>Người tiến hành</td><td colspan="5">Hacker, đối tượng giả mạo</td></tr>
<tr><td>Phương tiện/Truy nhập</td><td colspan="5">Brute-force, công cụ dò mật khẩu, tấn công phishing</td></tr>
<tr><td>Động cơ</td><td colspan="5">Truy cập trái phép vào hệ thống để đánh cắp dữ liệu</td></tr>
<tr><td>Kết quả</td><td colspan="5">Mất tính bí mật, tài khoản bị chiếm quyền điều khiển</td></tr>
<tr><td colspan="2">Tác động</td><td colspan="5">Phân tích rủi ro</td></tr>
<tr><td colspan="2" rowspan="7">Nếu người dùng đặt mật khẩu yếu, kẻ tấn công có thể dễ dàng truy cập dẫn tới rò rỉ thông tin cá nhân.</td><td>Lĩnh vực</td><td>Phân loại</td><td colspan="2">Giá trị tác động</td><td>Mức điểm</td></tr>
<tr><td>Danh tiếng/ Uy tín</td><td>4</td><td colspan="2">Trung bình (2)</td><td>8</td></tr>
<tr><td>Tài chính</td><td>3</td><td colspan="2">Trung bình (2)</td><td>6</td></tr>
<tr><td>Năng suất</td><td>2</td><td colspan="2">Thấp (1)</td><td>2</td></tr>
<tr><td>An toàn thông tin</td><td>1</td><td colspan="2">Thấp (1)</td><td>1</td></tr>
<tr><td>Luật pháp</td><td>1</td><td colspan="2">Thấp (1)</td><td>1</td></tr>
<tr><td colspan="3">Tổng điểm</td><td>18</td></tr>
<tr><td colspan="3">Khả năng xảy ra</td><td colspan="4">Cao</td></tr>
<tr><td colspan="7">Lựa chọn giảm thiểu</td></tr>
<tr><td colspan="2">Giảm thiểu</td><td>Giảm thiểu hay loại trừ</td><td colspan="2">Loại trừ hay chấp nhận</td><td colspan="2">Chấp nhận</td></tr>
<tr><td colspan="2"></td><td>X</td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="7">Phương pháp loại bỏ</td></tr>
<tr><td colspan="3">Nhân viên kỹ thuật</td><td colspan="4">- Thiết lập chính sách bắt buộc mật khẩu mạnh (dài, ký tự đặc biệt, số...);
- Cảnh báo người dùng khi sử dụng mật khẩu yếu;
- Buộc đổi mật khẩu định kỳ;</td></tr>
</table>

2.5.12 Quản lý phiên đăng nhập chưa an toàn

Bảng 17. Bảng tổng kết rủi ro quản lý phiên đăng nhập chưa an toàn

<table>
<tr><td colspan="2">Thông tin tài sản</td><td colspan="5">Phiên đăng nhập, cookie session</td></tr>
<tr><td colspan="2">Mối quan tâm</td><td colspan="5">Cookie không có thuộc tính bảo mật, thời gian sống phiên quá dài hoặc không tự động hết hạn</td></tr>
<tr><td rowspan="5">Tình huống đe dọa</td><td>Tài sản</td><td colspan="5">Session đăng nhập</td></tr>
<tr><td>Người tiến hành</td><td colspan="5">Hacker (qua XSS, chiếm quyền máy tính)</td></tr>
<tr><td>Phương tiện/Truy nhập</td><td colspan="5">Công cụ đánh cắp cookie, XSS</td></tr>
<tr><td>Động cơ</td><td colspan="5">Đăng nhập trái phép, chiếm quyền tài khoản</td></tr>
<tr><td>Kết quả</td><td colspan="5">Truy cập trái phép, đánh cắp dữ liệu, thao tác hệ thống sai lệch</td></tr>
<tr><td colspan="2">Tác động</td><td colspan="5">Phân tích rủi ro</td></tr>
<tr><td colspan="2" rowspan="7">Kẻ tấn công có thể lấy cắp session và đăng nhập như người dùng dẫn đến truy cập trái phép, đánh cắp thông tin.</td><td>Lĩnh vực</td><td colspan="2">Phân loại</td><td>Giá trị tác động</td><td>Mức điểm</td></tr>
<tr><td>Danh tiếng/ Uy tín</td><td colspan="2">5</td><td>Cao (3)</td><td>15</td></tr>
<tr><td>Tài chính</td><td colspan="2">4</td><td>Trung bình (2)</td><td>8</td></tr>
<tr><td>Năng suất</td><td colspan="2">3</td><td>Trung bình (2)</td><td>6</td></tr>
<tr><td>An toàn thông tin</td><td colspan="2">1</td><td>Thấp (1)</td><td>1</td></tr>
<tr><td>Luật pháp</td><td colspan="2">2</td><td>Trung bình (2)</td><td>4</td></tr>
<tr><td colspan="3">Tổng điểm</td><td>34</td></tr>
<tr><td colspan="3">Khả năng xảy ra</td><td colspan="4">Trung bình</td></tr>
<tr><td colspan="7">Lựa chọn giảm thiểu</td></tr>
<tr><td colspan="2">Giảm thiểu</td><td>Giảm thiểu hay loại trừ</td><td colspan="2">Loại trừ hay chấp nhận</td><td colspan="2">Chấp nhận</td></tr>
<tr><td colspan="2"></td><td>X</td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="7">Phương pháp loại bỏ</td></tr>
<tr><td colspan="2">Nhân viên kỹ thuật</td><td colspan="5">- Đặt HttpOnly, Secure, SameSite=Strict cho cookie;
- Tự động đăng xuất khi không hoạt động (idle timeout);
- Hạn chế thời gian sống của session;</td></tr>
</table>

2.5.13 Không tuân thủ Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân (Lỗ hổng phi kỹ thuật)

Bảng 18. Bảng tổng kết lỗ hổng phi kỹ thuật

<table>
<tr><td colspan="2">Thông tin tài sản</td><td colspan="5">Dữ liệu cá nhân người dùng trên hệ thống thư viện số dlib.ptit.edu.vn (họ tên, email, lịch sử truy cập, thông tin xác thực, v.v.)</td></tr>
<tr><td colspan="2">Mối quan tâm</td><td colspan="5">Việc hệ thống không tuân thủ Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân có thể dẫn đến vi phạm pháp luật, bị xử phạt hành chính, đình chỉ hoạt động, gây mất uy tín của Học viện và ảnh hưởng quyền lợi người dùng.</td></tr>
<tr><td colspan="2" rowspan="5">Tình huống đe dọa</td><td>Tài sản</td><td colspan="4">Dữ liệu cá nhân người dùng: thông tin định danh, tài khoản, lịch sử truy cập, email, số điện thoại, v.v.</td></tr>
<tr><td>Người thực hiện</td><td colspan="4">Cơ quan quản lý nhà nước (kiểm tra tuân thủ), hacker (khai thác lỗ hổng quản trị dữ liệu)</td></tr>
<tr><td>Phương tiện/Truy nhập</td><td colspan="4">Thanh tra, kiểm tra tuân thủ pháp lý; truy cập dữ liệu không được mã hóa hoặc không có biện pháp bảo vệ phù hợp</td></tr>
<tr><td>Động cơ</td><td colspan="4">Kiểm tra việc tuân thủ pháp luật, đánh cắp hoặc lạm dụng dữ liệu cá nhân</td></tr>
<tr><td>Kết quả</td><td colspan="4">Bị phạt hành chính, đình chỉ hoạt động hệ thống, rò rỉ dữ liệu cá nhân, mất uy tín của tổ chức</td></tr>
<tr><td colspan="2">Khả năng xảy ra rủi ro</td><td colspan="5">Trung Bình</td></tr>
<tr><td colspan="2">Tác động</td><td colspan="5">Phân tích rủi ro</td></tr>
<tr><td colspan="2" rowspan="6">Thay đổi giao diện, nội dung website thư viện số, chèn thông tin sai lệch hoặc nội dung không phù hợp, ảnh hưởng nghiêm trọng đến uy tín của học viện</td><td>Lĩnh vực</td><td>Phân loại</td><td colspan="2">Giá trị tác động</td><td>Mức điểm</td></tr>
<tr><td>Danh tiếng/ Uy tín</td><td>4</td><td colspan="2">Cao (3)</td><td>12</td></tr>
<tr><td>Tài chính</td><td>3</td><td colspan="2">Cao (3)</td><td>9</td></tr>
<tr><td>Năng suất</td><td>2</td><td colspan="2">Trung bình(2)</td><td>4</td></tr>
<tr><td>Luật pháp</td><td>4</td><td colspan="2">Cao (3)</td><td>12</td></tr>
<tr><td colspan="3">Tổng điểm</td><td>37</td></tr>
<tr><td colspan="6">Lựa chọn giảm thiểu</td></tr>
<tr><td>Giảm thiểu</td><td>Giảm thiểu hay loại trừ</td><td colspan="3">Loại trừ hay chấp nhận</td><td>Chấp nhận</td></tr>
<tr><td></td><td>x</td><td colspan="3"></td><td></td></tr>
<tr><td colspan="6">Phương pháp giảm thiểu</td></tr>
<tr><td colspan="2">Chính sách & Quy trình</td><td colspan="4">Ban hành chính sách bảo vệ dữ liệu cá nhân tuân thủ nghị định 13/2023/NĐ-CP

Xây dựng quy trình xin ý kiến đồng thuận của người dùng khi thu thập thông tin cá nhân

Thiết lập quy trình đáp ứng yêu cầu truy cập, chỉnh sửa, xóa dữ liệu từ chủ thể dữ liệu.</td></tr>
</table>

Kỹ thuật	Mã hóa dữ liệu cá nhân trên hệ thống Áp dụng kiểm soát truy cập chặt chẽ, phân quyền hợp lý cho cán bộ quản trị dữ liệu Giám sát, ghi log truy cập dữ liệu cá nhân và kiểm tra định kỳ
Đào tạo & Nhận thức	Đào tạo cán bộ, nhân viên về quy định bảo vệ dữ liệu cá nhân Nang cao nhận thức cho người dùng về quyền và trách nhiệm đối với dữ liệu cá nhân
Kiểm tra và giám sát	Đánh giá tuân thủ định kỳ theo Nghị định 13/2023/NĐ-CP. Báo cáo và xử lý kịp thời các vi phạm liên quan đến dữ liệu cá nhân.

2.6 Kết chương

Chương 2 này đã trình bày chi tiết quá trình phân tích và đánh giá rủi ro cho hệ thống thư viện số PTIT dựa theo khuôn mẫu của OCTAVE. Những rủi ro được nhận được ở nhiều loại, từ những loại truyền thống đối với các website thông thường, những vấn đề khi hoạt động trên Internet, những vấn đề liên quan đến quản lý người dùng, cả những rủi ro phi kỹ thuật và khả năng áp dụng các Nghị định, quy chuẩn của Nhà nước trong xây dựng hệ thống.

CHƯƠNG 3. KẾT QUẢ VÀ ĐÁNH GIÁ

Qua quá trình thực hiện đánh giá rủi ro hệ thống trang web thư viện số PTIT (https://dlib.ptit.edu.vn) bằng phương pháp OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), nhóm đã có cơ hội áp dụng một cách hệ thống các kiến thức về quản lý an toàn thông tin, từ lý thuyết đến thực tiễn, nhằm xây dựng một kế hoạch bảo vệ thông tin toàn diện, phù hợp với đặc thù của hệ thống.

Phương pháp OCTAVE được lựa chọn và triển khai như một khung phân tích rõ ràng, chuyên biệt, dựa trên việc xác định tài sản quan trọng, điểm yếu, cũng như mối đe dọa tiềm ẩn ảnh hưởng đến hoạt động của hệ thống thư viện số. Thông qua ba giai đoạn chính của OCTAVE, nhóm đã thực hiện các bước sau:

Xác định và phân loại tài sản quan trọng: Bao gồm dữ liệu tài liệu số, thông tin người dùng, hệ thống xác thực, hạ tầng máy chủ và giao diện truy cập. Việc nhận diện đúng các tài sản này giúp tập trung nguồn lực bảo vệ hiệu quả.

Nhận diện các mối đe dọa và điểm yếu: Đánh giá các nguy cơ phổ biến như tấn công SQL Injection, Cross-Site Scripting, truy cập trái phép, tấn công từ chối dịch vụ và nguy cơ mất dữ liệu do sai sót hoặc tấn công. Đồng thời, nhóm nhận thấy các điểm yếu như kiểm soát đầu vào chưa chặt chẽ, hệ thống xác thực còn đơn giản, và thiếu cơ chế mã hóa dữ liệu đầy đủ.

Phân tích và quản lý rủi ro: Dựa trên ma trận rủi ro được xây dựng, nhóm đánh giá mức độ ưu tiên xử lý các rủi ro, đồng thời đề xuất các biện pháp kiểm soát kỹ thuật và tổ chức nhằm giảm thiểu khả năng và tác động của các sự cố bảo mật.

Kết quả của bài tập là một danh sách rủi ro đã được ưu tiên xử lý, đi kèm các giải pháp cụ thể như tăng cường kiểm tra và lọc đầu vào, áp dụng xác thực đa yếu tố, triển khai mã hóa dữ liệu nhạy cảm, nâng cao giám sát truy cập và sao lưu dữ liệu định kỳ. Ngoài ra, nhóm cũng nhấn mạnh sự cần thiết của việc xây dựng chính sách an toàn thông tin rõ ràng, đào tạo nâng cao nhận thức cho người dùng, và phát triển quy trình phản ứng sự cố cũng như kế hoạch khôi phục dữ liệu sau thảm họa.

Việc áp dụng OCTAVE không chỉ giúp nhóm có một công cụ phân tích rủi ro khoa học, minh bạch mà còn tạo điều kiện cho tổ chức dễ dàng xác định và ưu tiên các vấn đề bảo mật cần giải quyết trước, phù hợp với quy mô và nguồn lực của hệ thống thư viện số PTIT. Đây là bước đầu quan trọng để nâng cao mức độ an toàn thông tin và đảm bảo hệ thống vận hành ổn định, phục vụ tốt nhu cầu nghiên cứu và học tập của cộng đồng.

Bài tập lớn cũng là cơ hội quý báu để nhóm thực hành và nâng cao năng lực vận dụng lý thuyết bảo mật thông tin vào tình huống thực tế. Qua đó, nhóm không chỉ làm chủ các nguyên tắc cốt lõi trong bảo vệ thông tin mà còn hiểu sâu về cách triển khai một phương pháp đánh giá rủi ro cụ thể như OCTAVE, từ đó góp phần xây dựng các giải pháp quản lý rủi ro phù hợp, hiệu quả cho từng điều kiện tổ chức riêng biệt.

KẾT LUẬN

Các kết quả đạt được:

Nhóm thực hiện đề tài "Phân tích rủi ro với hệ thống thư viện số PTIT (DLIB.PTIT.EDU.VN)" đã hoàn thành việc thu thập thông tin, phân tích và đánh giá một cách hệ thống các rủi ro bảo mật tiềm ẩn trong hệ thống thư viện số của Học viện Công nghệ Bưu chính Viễn thông. Đề tài đã thực hiện đầy đủ các nội dung đã đăng ký theo đề cương, bao gồm:

- Nghiên cứu và áp dụng phương pháp OCTAVE để đánh giá rủi ro thông tin trong tổ chức.

- Xây dựng hồ sơ tài sản thông tin của hệ thống thư viện số.

- Phân tích các mối đe dọa và điểm yếu trong hệ thống dựa trên thực nghiệm và các tiêu chuẩn kỹ thuật.

- Đánh giá rủi ro định lượng theo 5 lĩnh vực: danh tiếng, tài chính, năng suất, an toàn thông tin, và tuân thủ pháp luật.

- Đối chiếu với các quy chuẩn pháp lý như Luật An ninh mạng, Nghị định 13/2023/NĐ-CP và Nghị định 85/2016/NĐ-CP để xác định các rủi ro phi kỹ thuật.

- Đề xuất các biện pháp giảm thiểu và phương án xử lý phù hợp với mức độ ưu tiên của từng rủi ro.

Kết quả của bài tập là một bộ hồ sơ rủi ro hoàn chỉnh, minh bạch, có thể hỗ trợ cán bộ kỹ thuật và quản trị thư viện trong việc hoạch định chính sách bảo mật phù hợp.

Hướng phát triển:

Đề tài này có thể được mở rộng và phát triển theo các hướng sau:

- Tích hợp công cụ kiểm thử bảo mật tự động (Security Scanner, SIEM) để phát hiện lỗ hổng định kỳ trong hệ thống thư viện số.

- Nghiên cứu và triển khai mô hình quản lý an toàn thông tin theo tiêu chuẩn ISO/IEC 27001 cho hệ thống thư viện và các hệ thống nội bộ khác của PTIT.

- Thực hiện đánh giá rủi ro định kỳ kết hợp với phân tích chi phí - lợi ích cho từng phương án xử lý rủi ro.

- Xây dựng các plugin cảnh báo, giám sát truy cập và tự động hóa phản ứng sự cố (SOAR) cho hệ thống thư viện số.

- Mở rộng phạm vi đánh giá với các hệ thống thông tin khác trong học viện (hệ thống đào tạo, email, quản lý sinh viên, ...).

TÀI LIỆU THAM KHẢO

[1] Thư viện pháp luật, "Luật An ninh mạng 2018", https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx?, truy cập tháng 5.2025.

[2] Thư viện pháp luật, "Nghị định 13/2023/NĐ-CP", https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx?, truy cập tháng 5.2025

[3] Thư viện pháp luật, "Nghị định 85/2016/NĐ-CP", https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-85-2016-ND-CP-bao-dam-an-toan-he-thong-thong-tin-theo-cap-do-317475.aspx?f, truy cập tháng 5.2025.

[4] Báo cáo QLATTT, nhóm 9, nhóm lớp 3, khóa D16, đề tài "Đánh giá rủi ro cho hệ thống website sử dụng trong thương mại/kinh doanh điện tử", truy cập tháng 5.2025.