ĐÁNH GIÁ MỨC ĐỘ AN TOÀN THÔNG TIN CỦA HỆ THỐNG PHẦN MỀM QUẢN LÝ DỰA TRÊN PHƯƠNG PHÁP THỰC NGHIỆM

Nguyễn Thị Phương Linh
Khoa Kỹ thuật Công nghệ, Trường Đại học Tiền Giang
Email: nguyenthiphuonglinh@tgu.edu.vn.

Tóm tắt: *Bài báo này tập trung đánh giá mức độ an toàn thông tin của một hệ thống phần mềm quản lý thông qua phương pháp kiểm thử thực nghiệm. Trước tiên là nghiên cứu được xây dựng dựa trên cơ sở lý thuyết về các mối đe dọa bảo mật phổ biến như SQL Injection, mã độc, nghe lén mạng và lỗi cấu hình hệ thống. Tiếp theo, các công cụ bảo mật gồm SQLMap, Malwarebytes, NetworkMiner, Nmap và Nessus được sử dụng để kiểm thử trong môi trường mô phỏng. Kết quả thực nghiệm cho thấy hệ thống vẫn tồn tại một số rủi ro bảo mật, bao gồm nguy cơ SQL Injection, truyền dữ liệu chưa được mã hóa đầy đủ và cấu hình cổng dịch vụ chưa tối ưu. Trên cơ sở đó, bài báo nhấn mạnh vai trò của kiểm thử bảo mật trong việc phát hiện sớm lỗ hổng và đề xuất các biện pháp cải thiện nhằm nâng cao mức độ an toàn cho hệ thống phần mềm quản lý.*
Từ khóa: *Đánh giá bảo mật, lỗ hổng hệ thống, kiểm thử thực nghiệm.*
Nhận bài: 14/1/2026; Biên tập: 15/1/2026; Phản biện: 16/1/2026; Duyệt đăng: 20/1/2026.

1. Đặt vấn đề

Sự phát triển nhanh chóng của công nghệ thông tin đã thúc đẩy việc ứng dụng phần mềm quản lý vào hoạt động kinh doanh bán lẻ. Các cửa hàng kinh doanh kinh doanh hiện nay thường sử dụng phần mềm để quản lý khách hàng, sản phẩm, hóa đơn và giao dịch tài chính. Những dữ liệu này mang tính nhạy cảm cao và có giá trị lớn đối với doanh nghiệp. Trong giáo dục, các nhà trường thường ứng dụng các phần mềm chung vào lĩnh vực giáo dục. Nguy cơ mất an toàn thông tin càng trở nên cao hơn.

Điều này có thể dẫn đến rò rỉ dữ liệu khách hàng, thất thoát tài chính và ảnh hưởng nghiêm trọng đến uy tín của doanh nghiệp.

Xuất phát từ thực tế đó, bài báo tập trung phân tích bảo mật cho một hệ thống phần mềm quản lý ở mức ứng dụng và hệ thống, thông qua kiểm thử thực nghiệm bằng các công cụ bảo mật thông dụng. Mục tiêu là đánh giá mức độ an toàn hiện tại của phần mềm và đề xuất các biện pháp cải thiện phù hợp với điều kiện triển khai tại các doanh nghiệp vừa và nhỏ ở Việt Nam.

2. Nội dung nghiên cứu

2.1. Cơ sở lý thuyết về an toàn thông tin trong kỷ nguyên số

2.1.1. Khái niệm về mức độ an toàn thông tin trong kỷ nguyên số

An toàn thông tin (ATTT) là trạng thái mà trong đó thông tin và các hệ thống thông tin được bảo vệ khỏi các mối đe dọa về truy cập trái phép, sử dụng sai mục đích, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại. Mục tiêu của ATTT là bảo đảm ba yếu tố cốt lõi: Tính bảo mật (Confidentiality), thông tin chỉ được truy cập bởi những người được phép. Tính toàn vẹn (Integrity), thông tin không bị thay đổi hoặc hư hại trong quá trình lưu trữ, xử lý, và truyền tải. Tính sẵn sàng (Availability), thông tin và hệ thống luôn sẵn sàng phục vụ khi người dùng hợp pháp cần đến.

Mức độ ATTT được hiểu là mức độ đáp ứng các tiêu chuẩn và yêu cầu bảo vệ thông tin trong một hệ thống nhất định, phản ánh khả năng chống chịu, ngăn ngừa, phát hiện và khắc phục các rủi ro, tấn công hoặc sự cố liên quan đến dữ liệu và công nghệ thông tin. Mức độ này có thể được đánh giá thông qua các tiêu chí như: Khả năng bảo vệ dữ liệu trước các cuộc tấn công mạng. Mức độ tuân thủ các quy định, tiêu chuẩn an toàn (ISO/IEC 27001, NIST, v.v.). Năng lực ứng phó và phục hồi sau sự cố an ninh mạng. Nhận thức và hành vi của người dùng đối với ATTT.

Trong kỷ nguyên số, khi hầu hết các hoạt động của con người, doanh nghiệp và chính phủ được số hóa, mức độ ATTT trở thành yếu tố sống còn, quyết định đến uy tín, hiệu quả hoạt động và niềm tin xã hội đối với hệ thống số.

2.1.2. Đặc điểm ATTT trong kỷ nguyên số

Phạm vi và quy mô rộng. Dữ liệu và hệ thống thông tin được kết nối toàn cầu, vượt khỏi biên giới quốc gia, dẫn đến phạm vi rủi ro mở rộng và khó kiểm soát.

Tốc độ phát triển công nghệ nhanh. Các công nghệ mới như trí tuệ nhân tạo (AI), Internet vạn vật (IoT), điện toán đám mây (Cloud Computing), và chuỗi khối (Blockchain) vừa mang lại tiện ích, vừa tạo ra lỗ hổng bảo mật mới.

Tấn công mạng ngày càng tinh vi. Tội phạm mạng sử dụng kỹ thuật cao, tự động hóa, và có khả năng tấn công quy mô lớn, gây thiệt hại nghiêm trọng cho cá nhân, tổ chức, thậm chí là quốc gia.

Phụ thuộc cao vào dữ liệu. Dữ liệu trở thành "tài sản số" quan trọng, nên mất mát hoặc rò rỉ dữ liệu ảnh hưởng trực tiếp đến lợi ích kinh tế, chính trị và an ninh quốc gia.

Yếu tố con người vẫn là mắt xích yếu. Dù công

nghệ bảo mật ngày càng tiên tiến, hành vi bất cẩn hoặc thiếu hiểu biết của người dùng vẫn là nguyên nhân chính dẫn đến vi phạm ATTT.

Đặc điểm trên đây đặt ra yêu cầu như sau: Xây dựng hệ thống chính sách và tiêu chuẩn bảo mật thống nhất. Mọi tổ chức, doanh nghiệp cần tuân thủ các tiêu chuẩn quốc tế về ATTT và có quy trình quản lý rủi ro rõ ràng.

Tăng cường năng lực giám sát, phát hiện và ứng phó sự cố. Áp dụng các công nghệ giám sát thời gian thực, phân tích hành vi bất thường, và có đội ngũ chuyên trách xử lý sự cố nhanh chóng.

Đảm bảo an ninh trong từng lớp hạ tầng số. Từ phần cứng, phần mềm, dữ liệu đến mạng truyền thông đều cần cơ chế bảo vệ thích hợp.

Đào tạo, nâng cao nhận thức cho người dùng. Xây dựng "văn hóa ATTT" trong toàn xã hội, đặc biệt trong môi trường giáo dục và cơ quan nhà nước.

Phối hợp quốc tế và pháp lý chặt chẽ. Các quốc gia cần hợp tác trong chia sẻ thông tin, phòng chống tấn công mạng, và hoàn thiện khung pháp lý về bảo vệ dữ liệu cá nhân, an ninh mạng.

Tóm lại, mức độ ATTT trong kỷ nguyên số không chỉ phản ánh năng lực kỹ thuật của hệ thống, mà còn là chỉ số niềm tin số của xã hội. Đảm bảo ATTT là yêu cầu thiết yếu để phát triển chính phủ số, kinh tế số và công dân số một cách bền vững. Vì vậy, việc nâng cao mức độ ATTT cần được xem là nhiệm vụ chiến lược của mọi tổ chức và cá nhân trong thời đại chuyển đổi số toàn cầu.

2.1.3. Đặc điểm về mức độ ATTT trong lĩnh vực giáo dục

Trong lĩnh vực giáo dục, ATTT không chỉ liên quan đến bảo vệ dữ liệu cá nhân của học sinh, sinh viên, giảng viên và cán bộ quản lý mà còn bao gồm việc bảo vệ dữ liệu học tập, kết quả nghiên cứu, hệ thống học trực tuyến và hạ tầng công nghệ thông tin của các cơ sở giáo dục. Mức độ ATTT trong lĩnh vực này có những đặc điểm riêng biệt, chịu ảnh hưởng bởi đặc thù môi trường sư phạm, tính mở của thông tin học thuật và quá trình chuyển đổi số trong quản lý - giảng dạy.

Đặc điểm 1: Khối lượng dữ liệu lớn và đa dạng

Ngành giáo dục lưu trữ và xử lý một lượng dữ liệu khổng lồ, bao gồm: Dữ liệu cá nhân của học sinh, sinh viên, giảng viên (hồ sơ, điểm số, thông tin định danh, sức khỏe, học phí,...). Dữ liệu học tập, nghiên cứu, khóa luận, tài liệu học liệu số. Dữ liệu quản lý đào tạo, tuyển sinh, và hoạt động học thuật.

Đặc điểm 2: Mức độ nhận thức về ATTT chưa đồng đều

Đối tượng sử dụng công nghệ trong giáo dục rất đa dạng - từ cán bộ quản lý, giảng viên đến học sinh, sinh viên. Một bộ phận người dùng chưa có ý thức và kỹ năng bảo mật thông tin, thường xuyên sử dụng mật khẩu yếu, chia sẻ tài khoản, hoặc truy cập vào các trang web, đường dẫn không an toàn. Nhiều cơ sở giáo dục chưa chú trọng đào tạo kỹ năng ATTT cơ bản cho người học và giáo viên, khiến hệ thống dễ bị tấn công hoặc khai thác lỗ hổng từ yếu tố con người.

Đặc điểm 3: Hệ thống công nghệ thông tin chưa đồng bộ và còn hạn chế

Ở nhiều trường học, đặc biệt là cấp phổ thông và các cơ sở giáo dục vùng sâu vùng xa, hạ tầng công nghệ thông tin còn yếu, thiếu đầu tư cho máy chủ, tường lửa, thiết bị bảo mật. Nhiều phần mềm quản lý học tập, thi trực tuyến, cổng thông tin điện tử chưa được kiểm định an toàn, dẫn đến lỗ hổng dễ bị khai thác. Việc sử dụng nhiều nền tảng học trực tuyến của bên thứ ba (Google Classroom, Zoom, Microsoft Teams, Moodle, v.v.) làm tăng nguy cơ rò rỉ dữ liệu nếu không có biện pháp bảo vệ bổ sung.

Đặc điểm 4: Tính mở và tính chia sẻ thông tin cao

Giáo dục là lĩnh vực đòi hỏi mở, minh bạch và chia sẻ tri thức, do đó thông tin thường xuyên được trao đổi giữa các cá nhân, tổ chức, quốc gia. Việc mở truy cập học liệu, nghiên cứu khoa học, cơ sở dữ liệu học tập có thể dẫn đến nguy cơ mất kiểm soát nguồn thông tin. Tính mở của môi trường học thuật khiến ranh giới giữa chia sẻ học thuật và bảo mật dữ liệu trở nên mong manh, đặc biệt khi áp dụng công nghệ điện toán đám mây hoặc hệ thống quản lý học tập trực tuyến.

Đặc điểm 5: Sự phụ thuộc ngày càng lớn vào nền tảng số và dịch vụ trực tuyến

Quá trình chuyển đổi số giáo dục làm cho hoạt động dạy - học, quản lý và đánh giá phụ thuộc nhiều vào hạ tầng số: cổng học tập, hệ thống LMS, phần mềm quản lý thi, tuyển sinh, v.v. Khi các nền tảng này gặp sự cố hoặc bị tấn công (ví dụ: tấn công DDoS, mã độc, rò rỉ dữ liệu), hoạt động giáo dục bị gián đoạn hoặc tê liệt. Do đó, mức độ ATTT trong giáo dục gắn liền với độ ổn định và khả năng phục hồi của hệ thống công nghệ.

Đặc điểm 6: Liên quan chặt chẽ đến yếu tố pháp lý và đạo đức nghề nghiệp

Dữ liệu giáo dục chứa nhiều thông tin nhạy cảm về cá nhân và kết quả học tập, vì vậy việc bảo mật không chỉ là yêu cầu kỹ thuật mà còn là nghĩa vụ pháp lý và đạo đức của nhà trường và giáo viên. Việc tuân thủ các quy định như Luật An ninh mạng 2018, Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, cùng các chính sách của Bộ Giáo dục và Đào tạo là yêu cầu bắt buộc.

Đặc điểm 7: Nhu cầu cấp thiết xây dựng "văn hóa ATTT học đường"

Trong môi trường học đường, cần hình thành văn hóa ứng xử an toàn trên không gian mạng, giúp học sinh - sinh viên có thói quen không chia sẻ thông tin cá nhân trên mạng xã hội. Biết nhận diện và phòng tránh tin giả, lừa đảo trực tuyến. Biết bảo vệ tài khoản học tập và dữ liệu cá nhân. Việc này góp phần nâng cao mức độ ATTT bền vững từ gốc - từ nhận thức đến hành vi.

Tóm lại, mức độ ATTT trong lĩnh vực giáo dục phản ánh năng lực số và khả năng bảo vệ dữ liệu học đường trong bối cảnh chuyển đổi số quốc

gia. Với đặc thù là môi trường mở, đa đối tượng và có yêu cầu cao về tính chia sẻ, lĩnh vực giáo dục cần chú trọng đầu tư đồng bộ về hạ tầng kỹ thuật, thể chế quản lý, và giáo dục nhận thức để đảm bảo ATTT toàn diện và bền vững.

2.2. Các mối đe dọa ATTT trong kỷ nguyên số

2.2.1. Các lỗ hổng và kỹ thuật tấn công phổ biến

Hệ thống quản lý quản lý có thể đối mặt với nhiều dạng tấn công khác nhau, trong đó nổi bật như sau:

Thứ nhất, SQL Injection. Kẻ tấn công chèn mã SQL độc hại vào dữ liệu đầu vào của ứng dụng nhằm thay đổi logic truy vấn, từ đó đọc, sửa hoặc xóa dữ liệu trái phép trong cơ sở dữ liệu. Các biến thể như blind SQL Injection, time-based hay second-order SQL Injection làm tăng mức độ nguy hiểm do khó phát hiện bằng các cơ chế thông thường.

Thứ hai, phần mềm độc hại và tấn công chuỗi cung ứng. Ứng dụng có thể bị cài cắm trojan, backdoor hoặc bị nhiễm mã độc thông qua thư viện bên thứ ba không an toàn, bộ cài bị chỉnh sửa hoặc môi trường build không được bảo vệ chặt chẽ.

Thứ ba, nghe lén và tấn công mạng, Việc truyền dữ liệu không mã hóa hoặc cấu hình TLS yếu có thể dẫn đến rò rỉ thông tin đăng nhập và dữ liệu nhạy cảm thông qua các kỹ thuật sniffing hay Man-in-the-Middle.

Thứ tư, các lỗi cấu hình và kiểm soát truy cập. Bao gồm mở cổng dịch vụ không cần thiết, phân quyền không chặt chẽ (IDOR, Broken Access Control), hoặc thiếu cơ chế giám sát và ghi log.

2.2.2. Công cụ hỗ trợ phân tích và kiểm thử bảo mật

Để đánh giá toàn diện ATTT cho hệ thống, bài báo sử dụng kết hợp nhiều công cụ:

Một là, SQLMap là công cụ mã nguồn mở dùng để tự động phát hiện và kiểm tra lỗ hổng SQL Injection trong các ứng dụng sử dụng cơ sở dữ liệu.

Hai là, Malwarebytes là công cụ hỗ trợ phát hiện và loại bỏ mã độc, đồng thời ngăn chặn các phần mềm không mong muốn nhằm đảm bảo an toàn cho hệ thống.

Ba là, NetworkMiner là công cụ hỗ trợ phân tích lưu lượng mạng nhằm phát hiện và đánh giá nguy cơ rò rỉ thông tin trong quá trình truyền dữ liệu.

Bốn là, Nmap là công cụ dùng để quét mạng, phát hiện các thiết bị, cổng dịch vụ đang mở và hỗ trợ đánh giá tình trạng bảo mật của hệ thống mạng.

Năm là, Nessus là công cụ dùng để quét và đánh giá lỗ hổng bảo mật trong hệ thống, giúp phát hiện các điểm yếu và rủi ro ATTT.

2.3. Phương pháp nghiên cứu và thực nghiệm

2.3.1. Quy trình nghiên cứu

Quy trình nghiên cứu gồm các bước chính sau:

Một là, nghiên cứu lý thuyết về các mối đe dọa ATTT thường gặp đối với hệ thống phần mềm quản lý, bao gồm tấn công SQL Injection, phần mềm độc hại, nghe lén mạng, quét cổng và khai thác lỗ hổng hệ thống.

Hai là, lựa chọn các công cụ kiểm thử bảo mật phù hợp đã được trình bày trong hai file tài liệu, bao gồm SQLMap, Malwarebytes, NetworkMiner, Nmap và Nessus.

Ba là, xây dựng kịch bản thực nghiệm dựa trên chức năng và luồng dữ liệu điển hình của một hệ thống phần mềm quản lý.

Bốn là, thu thập kết quả, phân tích dữ liệu đầu ra từ các công cụ và đối chiếu với các tiêu chuẩn, khuyến nghị ATTT.

2.3.2. Môi trường và đối tượng thực nghiệm

Thực nghiệm được tiến hành trong môi trường kiểm thử nhằm đảm bảo an toàn và không ảnh hưởng đến hệ thống thực tế, trong đó hệ thống phần mềm quản lý được triển khai thử nghiệm trên nền tảng Windows, sử dụng môi trường phát triển Visual Studio và hệ quản trị cơ sở dữ liệu SQL Server. Các công cụ bảo mật được cài đặt và sử dụng đúng quy trình, đồng thời quá trình kiểm thử được thực hiện trên dữ liệu mô phỏng, đồng thời quá trình kiểm thử được thực hiện trên dữ liệu mô phỏng, phù hợp với các chuẩn mực nghiên cứu và yêu cầu về bảo mật thông tin.

2.3.3. Nội dung và quy trình thực nghiệm

Một là, kiểm thử lỗ hổng SQL Injection bằng SQLMap: Đầu tiên, tiến hành xác định các điểm nhập liệu và tham số truy vấn trong hệ thống phần mềm quản lý. Công cụ SQLMap được sử dụng để tự động kiểm tra khả năng tồn tại lỗ hổng SQL Injection thông qua các kỹ thuật như boolean-based, error-based và time-based.

Quy trình kiểm thử SQL Injection bằng SQLMap được thực hiện như sau:

Đầu tiên là lệnh khởi chạy: Sử dụng lệnh sqlmapu [URL] --batch để bắt đầu quét tự động tham số mục tiêu.

Tiếp theo là phân tích tự động: SQLMap tự động gửi các payload (Boolean, Time-based, Union...) để kiểm tra phản hồi từ máy chủ và nhận diện Hệ quản trị cơ sở dữ liệu (MySQL, Oracle, SQL Server...).

Kết quả nếu có lỗi: Hiển thị thông báo vulnerable kèm loại payload đã khai thác thành công. Đồng thời, người dùng có thể dùng thêm lệnh --dbs (liệt kê database) hoặc --dump (trích xuất dữ liệu) để kiểm tra mức độ ATTT.

Hai là, phân tích và phát hiện mã độc bằng Malwarebytes: Hệ thống được quét bằng phần mềm Malwarebytes nhằm phát hiện các phần mềm độc hại, trojan hoặc các chương trình không mong muốn. Quá trình quét được thực hiện ở chế độ quét toàn bộ để đảm bảo kiểm tra toàn diện. Sau khi quét xong sẽ xuất hiện các mối đe dọa đến hệ thống hoặc phần mềm. Đồng thời, Malwarebytes sẽ đưa ra những lời khuyên để người dùng bảo mật hệ thống tốt hơn. Từ đó giúp đánh giá mức độ an toàn của môi trường triển khai phần mềm.

Ba là, phân tích lưu lượng mạng bằng NetworkMiner. Để đánh giá nguy cơ rò rỉ thông tin qua mạng, lưu lượng dữ liệu trao đổi giữa các thành phần của hệ thống được thu thập và phân tích bằng NetworkMiner. Công cụ này cho phép trích xuất thông

tin đăng nhập, dữ liệu truyền ở dạng plaintext và các tệp được truyền qua mạng. Qua đó cho thấy một số dữ liệu được truyền ở dạng không mã hóa, tiềm ẩn nguy cơ rò rỉ thông tin trong quá trình trao đổi dữ liệu.

Bốn là, quét cổng và dịch vụ bằng Nmap: Công cụ Nmap được sử dụng để quét các cổng mạng và dịch vụ đang hoạt động trên hệ thống. Mục đích của bước này là xác định các cổng mở không cần thiết hoặc các dịch vụ tiềm ẩn nguy cơ mất an toàn.

Năm là, quét lỗ hổng hệ thống bằng Nessus: Nessus được sử dụng để quét và đánh giá các lỗ hổng đã biết trên hệ thống. Công cụ cung cấp danh sách chi tiết các lỗ hổng, mức độ nghiêm trọng và khuyến nghị khắc phục.

2.3.4. Kết quả thực nghiệm

Kết quả thực nghiệm cho thấy hệ thống vẫn còn tồn tại một số rủi ro về ATTT cần được khắc phục. Cụ thể, phần mềm có khả năng bị tấn công SQL Injection tại một số điểm nhập liệu nếu không sử dụng truy vấn tham số, làm tăng nguy cơ mất an toàn dữ liệu. Tiếp theo, trong một số kịch bản truyền dữ liệu, lưu lượng mạng chưa được mã hóa đầy đủ, dẫn đến nguy cơ bị nghe lén hoặc đánh cắp thông tin. Mặt khác, hệ thống chưa phát hiện mã độc ở mức độ nghiêm trọng, nhưng vẫn có khả năng phát sinh các phần mềm không mong muốn khi người dùng cài đặt thêm các công cụ từ bên ngoài. Cuối cùng, việc một số cổng dịch vụ được mở không cần thiết cho thấy cấu hình hệ thống chưa được tối ưu, cần được siết chặt hơn để nâng cao mức độ bảo mật tổng thể.

Bên cạnh đó còn có những hạn chế như: Thực nghiệm được tiến hành trên phiên bản demo với quy mô nhỏ, chưa phản ánh đầy đủ các kịch bản triển khai thực tế lớn. Đồng thời, chưa đánh giá sâu các cơ chế bảo mật nâng cao như phát hiện xâm nhập (IDS/IPS) hoặc phân tích hành vi người dùng.

3. Kết luận

Bài báo tập trung nghiên cứu và đánh giá mức độ ATTT của một hệ thống phần mềm quản lý thông qua phương pháp kiểm thử thực nghiệm kết hợp nhiều công cụ bảo mật thông dụng. Nghiên cứu được xây dựng trên nền tảng lý thuyết về các mối đe dọa ATTT và triển khai kiểm thử trong môi trường mô phỏng các hình thức tấn công phổ biến. Các công cụ như SQLMap, Malwarebytes, NetworkMiner, Nmap và Nessus được sử dụng để phát hiện lỗ hổng SQL Injection, kiểm tra mã độc, phân tích lưu lượng mạng và đánh giá cấu hình hệ thống. Kết quả cho thấy hệ thống có thể tồn tại nhiều rủi ro bảo mật nếu không được thiết kế và vận hành đúng theo các nguyên tắc an toàn, qua đó nhấn mạnh tầm quan trọng của việc kiểm thử bảo mật và tích hợp ATTT ngay từ giai đoạn phát triển phần mềm ■

Tài liệu tham khảo

[1]. Bộ Thông tin và Truyền thông - Cục An toàn Thông tin (2025). *Hướng dẫn kiểm tra an toàn thông tin*, *Tài liệu kỹ thuật quốc gia*.

[2]. Bộ Giáo dục và Đào tạo (2024). *Quyết định số 477/QĐ-BGDĐT ngày 31/01/2024 - Hướng dẫn đảm bảo an toàn thông tin và tham gia môi trường mạng an toàn đối với hoạt động giáo dục*.

[3]. Casmiry, E., Mduma, N., & Sinde, R (2025). *Enhanced SQL Injection Detection using chisquare feature selection and machine learning classifiers*, *Frontiers in Big Data*.

[4]. Sheng, Z. (2025). *A Survey of Vulnerability Detection Techniques and Insights*, *ACM Computing Surveys*.

[5]. Huy Vũ (2023). *Shoppertainment ở Việt Nam sẽ đạt hơn 8 tỉ USD vào năm 2025*. Tạp chí Nhịp Cầu Đầu Tư.

Assessing the information security level of a management software system based on experimental methods.

Nguyen Thi Phuong Linh
Faculty of Engineering and Technology, Tien Giang University
Email: nguyenthiphuonglinh@tgu.edu.vn.

Abstract: *This paper assesses the information security level of a management software system through an experimental security testing approach. First, the study is developed based on a theoretical analysis of common security threats, including SQL Injection, malware, network eavesdropping, and system configuration vulnerabilities. Subsequently, a set of widely used security tools namely SQLMap, Malwarebytes, Network Miner, Nmap, and Nessus was applied to conduct security testing in a controlled experimental environment. The experimental results reveal that the system still suffers from several security risks, such as potential SQL Injection vulnerabilities, unencrypted data transmission, and suboptimal service port configurations. Therefore, these findings demonstrate the necessity of systematic security testing for early vulnerability detection. Finally, the paper proposes appropriate mitigation measures to enhance the overall security level of management software systems.*

Keywords: *Security assessment, system vulnerabilities, experimental testing.*