0.1 Đặt vấn đề

Hệ thống quản lý học tập trực tuyến (Learning Management System – LMS) là một nền tảng công nghệ đóng vai trò trung tâm trong việc hỗ trợ các hoạt động giảng dạy, học tập và quản lý đào tạo tại các cơ sở giáo dục đại học. Tại Đại học Bách khoa Hà Nội, hệ thống lms.hust.edu.vn được triển khai với mục tiêu cung cấp môi trường học tập trực tuyến cho giảng viên và sinh viên, cho phép quản lý học phần, phân phối tài liệu học tập, nộp và chấm bài, đồng thời hỗ trợ các hình thức tương tác học thuật trong suốt quá trình đào tạo. Với quy mô người dùng lớn cùng tần suất truy cập cao, hệ thống LMS trở thành một thành phần hạ tầng quan trọng, gắn liền với các hoạt động học tập và quản lý đào tạo của nhà trường.

Trong bối cảnh chuyển đổi số giáo dục đang diễn ra mạnh mẽ, các nền tảng học tập trực tuyến như LMS ngày càng phải xử lý và lưu trữ nhiều dữ liệu quan trọng, bao gồm thông tin tài khoản người dùng, kết quả học tập và các dữ liệu nội bộ phục vụ công tác đào tạo. Thực tế cho thấy, các mối đe dọa về an toàn thông tin đối với các ứng dụng web có xu hướng gia tăng, trong đó không ít sự cố bắt nguồn từ những lỗ hổng bảo mật chưa được phát hiện và khắc phục kịp thời. Những rủi ro này không chỉ ảnh hưởng trực tiếp đến quyền lợi của sinh viên và giảng viên mà còn có thể tác động tiêu cực đến tính liên tục của hoạt động đào tạo cũng như uy tín của đơn vị vận hành hệ thống.

Xuất phát từ thực tiễn đó, việc nhận diện và đánh giá các nguy cơ mất an toàn thông tin trên hệ thống lms.hust.edu.vn được đặt ra như một vấn đề nghiên cứu có ý nghĩa thực tiễn cao. Khi các nguy cơ này được phân tích và đánh giá một cách toàn diện, kết quả nghiên cứu có thể góp phần nâng cao nhận thức về an toàn thông tin cho người dùng, bảo vệ dữ liệu học tập và hỗ trợ nhà trường trong việc xây dựng và duy trì một môi trường đào tạo số an toàn, ổn định. Đồng thời, các kết quả và phương pháp nghiên cứu cũng có thể được tham khảo và mở rộng áp dụng cho các hệ thống quản lý học tập trực tuyến tương tự tại các cơ sở giáo dục khác, nơi yêu cầu về bảo mật ngày càng trở nên cấp thiết.

0.2 Mục tiêu và phạm vi đề tài

Mục tiêu của đồ án là áp dụng một quy trình kiểm thử phù hợp nhằm đánh giá mức độ an toàn bảo mật và xác định các lỗ hổng đang tồn tại trên hệ thống lms.hust.edu.vn – nền tảng quản lý học tập trực tuyến giữ vai trò quan trọng trong hoạt động giảng dạy và học tập của Trường Đại học Bách khoa Hà Nội. Thông qua việc thực hiện kiểm thử một cách có hệ thống, đồ án hướng tới việc phát hiện các điểm yếu bảo mật trong ứng dụng web, từ đó góp phần nâng cao mức độ an toàn và độ tin cậy của hệ thống.

Để đạt được mục tiêu này, đồ án tốt nghiệp được triển khai dựa trên phương pháp kiểm thử xâm nhập ứng dụng web theo khung hướng dẫn OWASP Web Security Testing Guide (WSTG). Khung hướng dẫn này đóng vai trò làm cơ sở định hướng cho toàn bộ quá trình nghiên cứu, từ giai đoạn chuẩn bị, thực hiện cho đến tổng hợp và báo cáo kết quả. Quá trình kiểm thử được thực hiện với sự hỗ trợ của các công cụ chuyên dụng như Burp Suite, kết hợp cùng các công cụ bổ trợ khác trên môi trường máy ảo Kali Linux nhằm phục vụ cho việc phát hiện, khai thác và phân tích các lỗ hổng bảo mật.

Trên cơ sở nghiên cứu có hệ thống các nhóm lỗ hổng được mô tả trong từng hạng mục của OWASP WSTG, đồ án tiến hành thu thập thông tin về hệ thống mục tiêu và xây dựng kế hoạch kiểm thử chi tiết, trong đó xác định rõ các chức năng cần được đánh giá cũng như các kịch bản kiểm thử tương ứng. Khi phát hiện lỗ hổng, đồ án xây dựng các minh chứng khai thác nhằm xác thực sự tồn tại của các lỗ hổng này, đồng thời đề xuất các biện pháp khắc phục phù hợp để giảm thiểu rủi ro trong các phiên bản hệ thống tiếp theo. Cuối cùng, đồ án thực hiện đánh giá rủi ro nhằm phân tích mức độ ảnh hưởng của từng lỗ hổng, từ đó đề xuất các định hướng cải thiện và nâng cao mức độ an toàn bảo mật cho hệ thống.

0.3 Định hướng giải pháp

Hoạt động kiểm thử xâm nhập có thể được tiến hành trong ba mô hình kiểm thử khác nhau, bao gồm:

- **Kiểm thử hộp đen**: là hình thức kiểm thử trong đó kiểm thử viên không có bất kỳ thông tin nào về kiến trúc và cơ chế hoạt động nội bộ của hệ thống. Phương pháp này phản ánh sát nhất các kịch bản tấn công thực tế và được xem là thách thức nhất đối với người kiểm thử.
- **Kiểm thử hộp trắng**: cung cấp cho kiểm thử viên toàn quyền truy cập và hiểu biết đầy đủ về hệ thống mục tiêu, bao gồm mã nguồn, cấu hình và kiến trúc hệ thống, từ đó cho phép đánh giá bảo mật một cách toàn diện hơn.
- **Kiểm thử hộp xám**: là sự kết hợp giữa hai phương pháp trên, trong đó kiểm thử viên chỉ được cung cấp một phần thông tin về hệ thống. Tùy vào phạm vi kiểm thử, lượng thông tin này có thể bao phủ toàn bộ hệ thống ở mức tổng quan hoặc tập trung chi tiết vào một thành phần cụ thể.

Xuất phát từ việc phân tích các mô hình kiểm thử nêu trên, đồng thời cân nhắc đến phạm vi quyền truy cập hạn chế của kiểm thử viên, em quyết định lựa chọn phương pháp kiểm thử hộp đen dựa trên khung kiểm thử OWASP Web Security Testing Guide (WSTG) làm hướng tiếp cận chính trong đồ án này.

Tiếp theo, em tiến hành nghiên cứu chi tiết khung WSTG, đồng thời tìm hiểu và sử dụng các công cụ kiểm thử xâm nhập chuyên dụng cho ứng dụng web. Trên cơ sở đó, em xây dựng một kế hoạch kiểm thử chi tiết và triển khai quá trình kiểm thử theo đúng lộ trình đã đề ra. Kết quả cuối cùng là tổng hợp các lỗ hổng bảo mật được phát hiện và đánh giá mức độ ảnh hưởng của chúng đối với hệ thống.

Trong suốt quá trình thực hiện, em kết hợp sử dụng các công cụ quét tự động và các kỹ thuật kiểm thử thủ công nhằm đảm bảo phạm vi đánh giá toàn diện cho từng hạng mục trong WSTG. Cách tiếp cận này cho phép phát hiện có hệ thống các lỗ hổng phổ biến, đồng thời giúp em xác minh và phân tích sâu hơn các vấn đề do công cụ tự động cảnh báo.

0.4 Bố cục đồ án

Phần còn lại của báo cáo đồ án tốt nghiệp này được tổ chức như sau.

- **Chương 2: Xây dựng kế hoạch kiêm thử**: Trình bày phương pháp kiểm thử xâm nhập được áp dụng trong Đồ án tốt nghiệp, dựa trên khung kiểm thử OWASP Web Security Testing Guide (WSTG).
- **Chương 3: Kiểm thử hệ thống**: Tổng hợp và trình bày kết quả kiểm thử, bao gồm các hạng mục kiểm thử đạt yêu cầu và các trường hợp phát sinh lỗ hổng. Các phân tích và minh chứng chi tiết được trình bày trong phần phụ lục.
- **Chương 4: Các đóng góp nổi bật**: Phân tích các kết quả trọng tâm của Đồ án tốt nghiệp, đánh giá mức độ ảnh hưởng của các lỗ hổng được phát hiện
- **Chương 5: Kết luận và hướng phát triển**: Đánh giá tổng thể mức độ hiệu quả của phương pháp thực hiện, đồng thời đề xuất các định hướng cải tiến và mở rộng cho nghiên cứu cũng như ứng dụng thực tế trong tương lai.