Trong quá trình thực hiện đồ án, việc đánh giá an toàn bảo mật đối với nền tảng web LMS được thực hiện theo phương pháp kiểm thử hộp đen, kết hợp giữa kiểm thử thủ công và việc sử dụng các công cụ kiểm thử tự động. Quy trình kiểm thử được xây dựng dựa trên việc nghiên cứu và tham khảo khung hướng dẫn OWASP Web Security Testing Guide (WSTG), từ đó xác định các hạng mục kiểm thử phù hợp nhằm xây dựng kế hoạch kiểm thử bảo mật trong phạm vi đồ án.

Trên cơ sở kế hoạch kiểm thử đã được xây dựng, hệ thống LMS được phân tích nhằm làm rõ cấu trúc, chức năng và luồng xử lý của các module chính. Từ kết quả phân tích này, các điểm yếu và lỗ hổng bảo mật tiềm ẩn có khả năng bị khai thác được xác định và đánh giá một cách có hệ thống. Mỗi lỗ hổng được phát hiện đều được phân tích chi tiết, bao gồm mức độ ảnh hưởng, phương pháp chứng minh sự tồn tại của lỗ hổng, cũng như các khuyến nghị khắc phục tương ứng.

Thông qua quá trình nghiên cứu và triển khai, kết quả của đồ án cho thấy vai trò của hoạt động kiểm thử xâm nhập trong việc đánh giá và nâng cao mức độ an toàn cho các ứng dụng web. Các kết quả thu được phản ánh thực trạng an toàn bảo mật của hệ thống LMS tại thời điểm kiểm thử, đồng thời cung cấp cơ sở tham khảo cho việc cải thiện cơ chế bảo mật và định hướng cho các hoạt động nghiên cứu, kiểm thử an toàn bảo mật trong giai đoạn tiếp theo.

Trong phạm vi của đồ án, hoạt động kiểm thử an toàn bảo mật được thực hiện theo phương pháp kiểm thử hộp đen và giới hạn ở các chức năng dành cho người dùng có vai trò sinh viên. Mặc dù nhiều lỗ hổng bảo mật đã được phát hiện và phân tích, các kết quả đạt được không đồng nghĩa với việc hệ thống LMS được bảo đảm an toàn trước mọi hình thức tấn công. Trên thực tế, vẫn có khả năng tồn tại các điểm yếu bảo mật khác chưa được phát hiện do những hạn chế về phạm vi kiểm thử, vai trò người dùng được đánh giá và phương pháp tiếp cận được áp dụng.

Từ những hạn chế nêu trên, trong các hướng nghiên cứu và phát triển tiếp theo, việc mở rộng phạm vi kiểm thử là cần thiết nhằm đánh giá hệ thống một cách toàn diện hơn. Cụ thể, việc cung cấp quyền truy cập mã nguồn phục vụ kiểm thử và áp dụng các phương pháp kiểm thử hộp xám hoặc hộp trắng có thể giúp nâng cao độ sâu và độ chính xác của quá trình đánh giá, qua đó phát hiện các lỗ hổng liên quan đến logic xử lý, cơ chế phân quyền hoặc các đoạn mã lập trình không an toàn mà phương pháp kiểm thử hộp đen có thể chưa phát hiện. Bên cạnh đó, việc mở rộng hoạt động kiểm thử trên toàn bộ các mô-đun với đầy đủ các vai trò người dùng, đồng thời đánh giá thêm các thành phần khác của hệ thống như ứng dụng di động, hạ tầng mạng, hệ điều hành, các dịch vụ nền và API, sẽ giúp phản ánh đầy đủ và chính xác hơn mức độ an toàn tổng thể của hệ thống.