0.1 Thu thập thông tin hệ thống

Giai đoạn Thu thập thông tin được thực hiện nhằm thu thập một cách có hệ thống và toàn diện các dữ liệu liên quan đến hệ thống mục tiêu, bao gồm các công nghệ và nền tảng được sử dụng, các endpoint có thể truy cập từ bên ngoài, sơ đồ chức năng trang web cũng như các thành phần tiềm ẩn nguy cơ gây ra rủi ro bảo mật.

0.1.1 Khảo sát hệ thống

Hoạt động khảo sát hệ thống tập trung vào việc xác định các công nghệ, nền tảng và thư viện được sử dụng, cũng như kiểm tra các yếu tố có khả năng làm lộ thông tin hoặc mở rộng bề mặt tấn công của ứng dụng web. Kết quả khảo sát hệ thống được tổng hợp và trình bày chi tiết trong bảng dưới đây

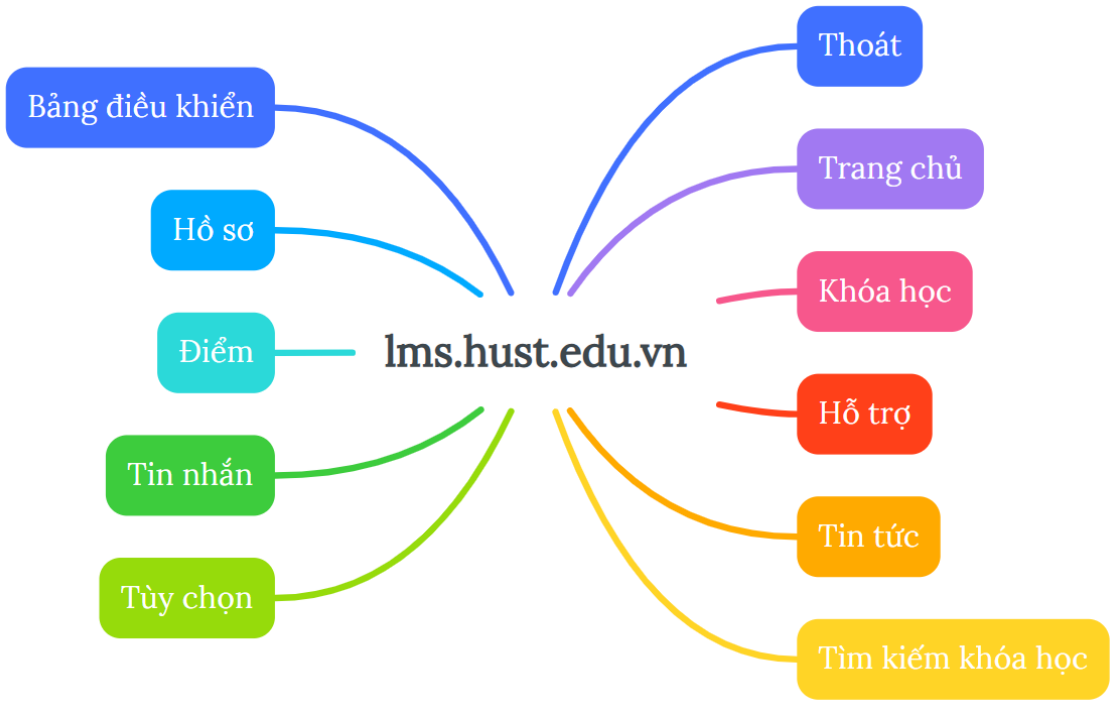
Bảng 1: Kết quả khảo sát hệ thống

STT	Nội dung	Công cụ	Kết quả	Tham chiếu WSTG
1	Xác định công nghệ web	Wappalyzer	JavaScript frameworks: RequireJS 2.3.5 Video players: VideoJS Font scripts: Font Awesome, Glyphicons Miscellaneous: HTTP/2, Babel LMS: Moodle Web servers: Nginx JavaScript graphics: MathJax 2.7.8 Programming languages: PHP JavaScript library: jQuery 3.4.1, OWL Carousel, core-js 2.6.1, YUI 3.17.2 Reverse proxies: Nginx UI frameworks: Bootstrap 4.3.1	WSTG-INFO-01 WSTG-INFO-02 WSTG-INFO-04 WSTG-INFO-05
2	Kiểm tra các tệp siêu dữ liệu	DevTools	Không phát hiện thẻ meta robots; không có dấu hiệu rò rỉ dữ liệu.	WSTG-INFO-03

STT	Nội dung	Công cụ	Kết quả	Tham chiếu WSTG
3	Phát hiện các đường dẫn web	dirsearch, gobuster, Burp Suite	Không phát hiện đường dẫn ẩn chứa thông tin nhạy cảm	WSTG-INFO-02 WSTG-INFO-05 WSTG-INFO-07
4	Địa chỉ IP	host	202.191.59.132	WSTG-INFO-02
5	Xác định dịch vụ đang chạy trên các cổng mạng	Nmap	Các cổng dịch vụ đang mở trên mục tiêu 80/TCP 443/TCP	WSTG-INFO-02

0.1.2 Sơ đồ chức năng trang web

Việc phát hiện cấu trúc sitemap của hệ thống là một trong những kết quả thu được trong quá trình thực hiện các hạng mục kiểm thử thuộc nhóm Information Gathering theo khung hướng dẫn OWASP Web Security Testing Guide. Trên cơ sở kinh nghiệm sử dụng ứng dụng LMS với vai trò người dùng sinh viên, kết hợp với sự hỗ trợ của các công cụ quét tự động, đồ án xác định được cấu trúc sitemap của hệ thống mục tiêu, được trình bày chi tiết ở phần dưới đây.



Hình 0.1: Sơ đồ toàn bộ chức năng Sinh viên của trang web

Từ sơ đồ tổng quan các chức năng chính của hệ thống LMS dành cho sinh viên được trình bày ở Hình 3.1, có thể thấy cấu trúc website được tổ chức theo nhiều nhóm chức năng khác nhau, phục vụ các nhu cầu học tập, quản lý học phần và tương tác của người dùng. Tuy nhiên, sơ đồ tổng quan chỉ phản ánh mối quan hệ và phạm vi chức năng ở mức khái quát, chưa thể hiện đầy đủ các chức năng cụ thể mà từng trang trong hệ thống cung cấp.

Do đó, để làm rõ hơn phạm vi và nội dung của từng chức năng, bảng dưới đây trình bày chi tiết các trang chính của hệ thống LMS, kèm theo mô tả và các chức năng tương ứng mà người dùng có thể thực hiện trên mỗi trang. Việc phân tích chi tiết này đóng vai trò quan trọng trong việc xác định các điểm cần kiểm thử và xây dựng các kịch bản đánh giá an toàn bảo mật trong các bước tiếp theo của đồ án.

Bảng 2: Mô tả chi tiết chức năng của các module phần mềm Sinh viên

Trang	Mô tả	Chi tiết chức năng
Đăng nhập	Đăng nhập hệ thống	Đăng nhập vào tài khoản cá nhân của người dùng.
Bảng Điều khiển	Các khóa học được truy cập gần đây	Xem thông tin các khóa học đã tham gia theo từng học kỳ.
	Tổng quan về khóa học	Xem tiến trình từng khóa học. Đánh dấu khóa học. Xóa khóa học khỏi danh sách.
	Lịch	Xem lịch. Xuất lịch biểu. Thêm và đồng bộ lịch từ bên ngoài vào hệ thống.
	Sự kiện sắp diễn ra	Xem sự kiện sắp diễn ra. Xuất lịch biểu. Thêm và đồng bộ lịch từ bên ngoài vào hệ thống.
Hồ sơ	Chi tiết người dùng	Xem, sửa thông tin cá nhân.
	Chi tiết khóa học	Xem mô tả sơ lược khóa học.
	Báo cáo	Xem thông tin các phiên đăng nhập. Xem điểm tổng quan các môn học phần.
	Hoạt động đăng nhập	Xem thông tin về lần đầu truy cập trang web và lần truy cập gần nhất vào trang.

Trang	Mô tả	Chi tiết chức năng
	Nội dung khác	Xem thông tin các mục blog của mình. Xem thông tin các bài viết diễn đàn. Xem thông tin các cuộc thảo luận trong diễn đàn. Xem thông tin Learning plans.
Điểm		Xem điểm tổng quan các môn học phần.
Tin nhắn	Tìm kiếm	Tìm người và tin nhắn.
	Nhắn tin	Nhắn tin cho người khác.
Tùy chọn	Tài khoản	Sửa hồ sơ cá nhân. Sửa đường dẫn trang nhà. Sửa ngôn ngữ ưa thích. Sửa các lựa chọn diễn đàn. Sửa trình soạn thảo ưu tiên. Cấu hình khóa học: Bật/tắt trình chọn hoạt động và tài nguyên. Cài đặt ưu tiên cho lịch. Tùy chọn tin nhắn: Chỉnh sửa quyền riêng tư, tùy chọn thông báo và thông tin chung. Tùy chọn thông báo: Bật/tắt vô hiệu hóa thông báo. Linked logins: Liên kết tài khoản bên ngoài thông qua dịch vụ OAuth 2.0 (HUST Login).
	Các blog	Tùy chọn: Chỉnh sửa số mục blog mỗi trang.
	Điểm badges	Quản lý các huy hiệu: tìm kiếm huy hiệu. Badge preferences: Bật/tắt tự động hiện các huy hiệu đã đạt được trên trang hồ sơ.
Khóa học	Semester Courses	Xem thông tin các khóa học theo từng kỳ.
	A-Z Courses	Xem thông tin toàn bộ các khóa học hiện có trên LMS.

Trang	Mô tả	Chi tiết chức năng
Hỗ trợ	Hỗ trợ Sinh viên	Hướng dẫn Sinh viên sử dụng hệ thống học tập trực tuyến HUST.
	Hỗ trợ Giảng viên	Hướng dẫn Giảng viên sử dụng hệ thống học tập trực tuyến HUST.
Tin tức		Xem các thông báo mới nhất từ hệ thống.
Tìm kiếm khóa học		Tìm kiếm các khóa học theo từ khóa.
Thoát		Đăng xuất khỏi tài khoản người dùng.

0.2 Kiểm thử cấu hình và triển khai

Trong phần này, hoạt động kiểm thử cấu hình và triển khai hệ thống được thực hiện dựa trên khung hướng dẫn OWASP Web Security Testing Guide (WSTG) nhằm đánh giá mức độ an toàn của các thiết lập hệ thống, nền tảng ứng dụng và các cơ chế bảo vệ ở tầng hạ tầng. Nội dung kiểm thử tập trung vào việc rà soát các cấu hình có nguy cơ làm lộ thông tin nhạy cảm, các chính sách bảo mật HTTP, cơ chế phân quyền truy cập tài nguyên, cũng như các sai sót trong quá trình triển khai có thể dẫn đến rủi ro mất an toàn thông tin.

Bảng 4.3 dưới đây tổng hợp kết quả kiểm thử đối với từng hạng mục thuộc nhóm WSTG-CONF, qua đó phản ánh các cấu hình đã đáp ứng yêu cầu an toàn bảo mật, các trường hợp chưa đạt, cũng như những hạng mục không thể tiến hành kiểm thử do giới hạn về quyền truy cập trong phạm vi đánh giá. Các kết quả này được sử dụng làm cơ sở cho việc nhận diện các vấn đề cấu hình tồn tại và đề xuất các biện pháp khắc phục phù hợp trong các phần tiếp theo của đồ án.

Bảng 3: Kết quả kiểm thử cấu hình và triển khai

ID	Nội dung	Kết luận
WSTG-CONF-01	Kiểm thử cấu hình hạ tầng mạng	Không thể tiến hành do tài khoản kiểm thử không có quyền truy cập tài nguyên liên quan.

ID	Nội dung	Kết luận
WSTG-CONF-02	Kiểm thử cấu hình nền tảng ứng dụng	Đạt. Không có mã debug, tệp hoặc phần mở rộng nhạy cảm nào còn sót lại trong môi trường production. Tuy nhiên, việc kiểm tra bằng cách xem mã nguồn sẽ đánh giá chính xác hơn so với kiểm thử hộp đen.
WSTG-CONF-03	Kiểm thử xử lý phần mở rộng tệp đối với thông tin nhạy cảm	Đạt. Không phát hiện tệp tin nhạy cảm hoặc dữ liệu nội bộ thông qua các phần mở rộng phổ biến (như .bak, .log, .php, .json, .zip, .env, v.v.).
WSTG-CONF-04	Rà soát các bản sao lưu cũ và tệp không được tham chiếu để tìm thông tin nhạy cảm	Không thể tiến hành do tài khoản kiểm thử không có quyền truy cập tài nguyên liên quan.
WSTG-CONF-05	Liệt kê giao diện quản trị của hạ tầng và ứng dụng	Đạt. Không tìm thấy chức năng ẩn dành cho vai trò khác trong giao diện người dùng của sinh viên.
WSTG-CONF-06	Kiểm thử các phương thức HTTP	Cho phép sử dụng các phương thức HTTP sau: GET, POST, HEAD.
WSTG-CONF-07	Kiểm thử cơ chế HTTP Strict Transport Security	Thiếu tiêu đề HSTS.
WSTG-CONF-08	Kiểm thử chính sách Cross Domain của RIA	Không thể tiến hành do tài khoản kiểm thử không có quyền truy cập tài nguyên liên quan.
WSTG-CONF-09	Kiểm thử quyền truy cập tệp	Không thể tiến hành do tài khoản kiểm thử không có quyền truy cập tài nguyên liên quan.
WSTG-CONF-10	Kiểm thử khả năng chiếm quyền tên miền phụ	Không thể tiến hành do tài khoản kiểm thử không có quyền truy cập tài nguyên liên quan.
WSTG-CONF-11	Kiểm thử cấu hình lưu trữ đám mây	Đạt.
WSTG-CONF-12	Kiểm thử chính sách bảo mật nội dung	Thiếu tiêu đề CSP (Content Security Policy).
WSTG-CONF-13	Kiểm thử nhầm lẫn đường dẫn	Đạt.

ID	Nội dung	Kết luận
WSTG-CONF-14	Kiểm thử sai cấu hình các header bảo mật HTTP khác	X-Frame-Options và Cache-Control bị trùng lặp có thể gây xung đột.

0.3 Kiểm thử quản lý định danh

Trong phần này, hoạt động kiểm thử quản lý định danh được thực hiện nhằm đánh giá mức độ an toàn của các cơ chế liên quan đến việc xác định và quản lý danh tính người dùng trên hệ thống. Nội dung kiểm thử tập trung vào các vấn đề như định nghĩa vai trò người dùng, quy trình đăng ký và cấp tài khoản, khả năng liệt kê hoặc suy đoán tài khoản, cũng như chính sách đặt tên người dùng. Việc đánh giá các hạng mục này giúp xác định những điểm yếu có thể bị lợi dụng để thu thập thông tin người dùng hoặc làm tiền đề cho các hình thức tấn công tiếp theo.

Bảng 4.4 dưới đây tổng hợp kết quả kiểm thử đối với từng hạng mục thuộc nhóm WSTG-IDNT, qua đó thể hiện các cơ chế quản lý định danh đã đáp ứng yêu cầu an toàn bảo mật cũng như các vấn đề còn tồn tại cần được lưu ý và khắc phục.

Bảng 4: Kết quả kiểm thử quản lý định danh

ID	Nội dung	Kết luận
WSTG-IDNT-01	Kiểm thử định nghĩa vai trò	Đạt. Không tìm được biến vai trò trong cookie, cũng như các thư mục/tệp ẩn.
WSTG-IDNT-02	Kiểm thử quy trình đăng ký người dùng	Ứng dụng không cung cấp chức năng này.
WSTG-IDNT-03	Kiểm thử quy trình cấp tài khoản	Không thể thực hiện do thiếu quyền truy cập tài nguyên và không có tài nguyên thuộc vai trò khác.
WSTG-IDNT-04	Kiểm thử khả năng liệt kê tài khoản và tài khoản dễ đoán	Tài khoản người dùng có thể đoán được, do sử dụng email của đại học làm tên đăng nhập.
WSTG-IDNT-05	Kiểm thử chính sách tên người dùng yếu hoặc không được áp dụng	Tài khoản người dùng có cấu trúc nhất quán, do sử dụng email của đại học làm tên đăng nhập.

0.4 Kiểm thử xác thực

Trong phần này, hoạt động kiểm thử xác thực được thực hiện nhằm đánh giá mức độ an toàn của các cơ chế xác thực người dùng trên hệ thống, bao gồm cơ chế quản lý phiên làm việc, chính sách mật khẩu và các phương thức xác thực thay thế. Nội dung kiểm thử tập trung vào việc xác định các điểm yếu có thể ảnh hưởng đến

khả năng bảo vệ tài khoản người dùng, cũng như các nguy cơ rò rỉ thông tin xác thực trong quá trình sử dụng hệ thống.

Bảng 4.5. dưới đây trình bày tổng hợp kết quả kiểm thử đối với từng hạng mục thuộc nhóm WSTG-ATHN, qua đó phản ánh các cơ chế xác thực đã đáp ứng yêu cầu an toàn bảo mật, các chức năng không được triển khai, cũng như những vấn đề còn tồn tại cần được xem xét và khắc phục.

Bảng 5: Kết quả kiểm thử xác thực

ID	Nội dung	Kết luận
WSTG-ATHN-01	Kiểm thử việc truyền thông tin xác thực qua kênh đã mã hóa	Đã được chuyển sang mục 4.9 — Kiểm thử mật mã yếu.
WSTG-ATHN-02	Kiểm thử tài khoản mặc định	Ứng dụng không cung cấp chức năng này.
WSTG-ATHN-03	Kiểm thử cơ chế khóa tài khoản yếu	
WSTG-ATHN-04	Kiểm thử việc vượt qua sơ đồ xác thực	Đạt. Mỗi phiên làm việc được gắn với 1 mã Session có cơ chế hết hạn.
WSTG-ATHN-05	Kiểm thử tính năng “Ghi nhớ mật khẩu” dễ bị khai thác	Ứng dụng không cung cấp chức năng này.
WSTG-ATHN-06	Kiểm thử lỗ hổng bộ nhớ cache của trình duyệt	Không đạt. Sau khi người dùng đăng xuất, nếu nhấn nút “Back”, trình duyệt vẫn hiển thị thông tin nhạy cảm đã xem trước đó.
WSTG-ATHN-07	Kiểm thử phương thức xác thực yếu	Ứng dụng chỉ yêu cầu mật khẩu có 8 ký tự mà không có thêm yêu cầu khác về độ phức tạp (ký tự thường, ký tự hoa, số, ký tự đặc biệt).
WSTG-ATHN-08	Kiểm thử câu hỏi bảo mật dễ đoán	Ứng dụng không cung cấp chức năng này.
WSTG-ATHN-09	Kiểm thử chức năng thay đổi hoặc đặt lại mật khẩu yếu	Ứng dụng cho phép đặt lại mật khẩu mới trùng với mật khẩu cũ.
WSTG-ATHN-10	Kiểm thử các kênh xác thực thay thế có bảo mật kém	Đạt. Xác thực OAuth thông qua Office 365 là an toàn.
WSTG-ATHN-11	Kiểm thử xác thực đa yếu tố (MFA)	Ứng dụng không cung cấp chức năng này.

0.5 Kiểm thử phân quyền

Trong phần này, hoạt động kiểm thử phân quyền được thực hiện nhằm đánh giá mức độ an toàn của các cơ chế kiểm soát truy cập và phân quyền người dùng trên hệ thống. Nội dung kiểm thử tập trung vào việc xác định khả năng vượt qua cơ chế phân quyền, truy cập trái phép vào tài nguyên không được phép, leo thang đặc quyền, cũng như các lỗ hổng liên quan đến tham chiếu trực tiếp đối tượng không an toàn và các điểm yếu trong quá trình tích hợp OAuth.

Bảng 4.6 dưới đây tổng hợp kết quả kiểm thử đối với từng hạng mục thuộc nhóm WSTG-ATHZ, qua đó phản ánh các cơ chế phân quyền đã đáp ứng yêu cầu an toàn bảo mật cũng như các lỗ hổng còn tồn tại cần được xem xét và khắc phục nhằm hạn chế nguy cơ truy cập trái phép vào hệ thống.

Bảng 6: Kết quả kiểm thử phân quyền

ID	Nội dung	Kết luận
WSTG-ATHZ-01	Kiểm thử Directory Traversal File Include	Đạt. Không tìm thấy lỗ hổng Directory Traversal File Include.
WSTG-ATHZ-02	Kiểm thử vượt qua cơ chế phân quyền	Đạt.
WSTG-ATHZ-03	Kiểm thử leo thang đặc quyền	Đạt.
WSTG-ATHZ-04	Kiểm thử tham chiếu trực tiếp đối tượng không an toàn	Không đạt. Ứng dụng có lỗ hổng tham chiếu trực tiếp đối tượng không an toàn ở chức năng “linked login”.
WSTG-ATHZ-05	Kiểm thử các điểm yếu OAuth	Đạt. Xác thực OAuth thông qua Office 365 là an toàn.

0.6 Kiểm thử quản lý phiên

Trong phần này, hoạt động kiểm thử quản lý phiên được thực hiện nhằm đánh giá mức độ an toàn của các cơ chế quản lý phiên làm việc của người dùng trên hệ thống. Nội dung kiểm thử tập trung vào việc phân tích cách thức tạo và quản lý phiên, cấu hình và thuộc tính của cookie, cơ chế kết thúc và hết hạn phiên, cũng như các nguy cơ liên quan đến chiếm đoạt hoặc lạm dụng phiên làm việc.

Bảng 4.7 dưới đây tổng hợp kết quả kiểm thử đối với từng hạng mục thuộc nhóm WSTG-SESS, qua đó phản ánh các cơ chế quản lý phiên đã đáp ứng yêu cầu an toàn bảo mật, các vấn đề cấu hình chưa phù hợp và những rủi ro tiềm ẩn cần được xem xét và khắc phục trong các phần tiếp theo.

Bảng 7: Kết quả kiểm thử quản lý phiên

ID	Nội dung	Kết luận
WSTG-SESS-01	Kiểm tra sơ đồ quản lý phiên	Đạt. Cookie định danh người dùng MoodleSession có đủ tính ngẫu nhiên, khó bị dò đoán, phân tích.
WSTG-SESS-02	Kiểm tra các thuộc tính của cookie	Cookie không được cấu hình thuộc tính HttpOnly.
WSTG-SESS-03	Kiểm tra lỗ hổng cố định phiên	Đạt. Cơ chế phân quyền phiên có thời gian hiệu lực và chức năng kết thúc phiên để chấm dứt phiên bất cứ khi nào người dùng đăng xuất.
WSTG-SESS-04	Kiểm tra các biến phiên bị lộ	Đạt. Cơ chế `Cache-Control` được bảo mật, tuy nhiên header `Expires` nên để là "0" thay vì để trống.
WSTG-SESS-05	Kiểm tra lỗ hổng CSRF	
WSTG-SESS-06	Kiểm tra chức năng đăng xuất	Đạt. Thời gian chờ phiên và cơ chế hủy phiên sau khi đăng xuất được thực hiện đúng cách.
WSTG-SESS-07	Kiểm tra cơ chế hết hạn phiên	Đạt. Thời gian hết hạn phiên khoảng 1 giờ hoạt động đúng cách.
WSTG-SESS-08	Kiểm tra lỗ hổng Session Puzzling	
WSTG-SESS-09	Kiểm tra lỗ hổng chiếm đoạt phiên	Cookie không có cờ `HttpOnly`, điều này có thể dẫn đến lỗ hổng chiếm đoạt phiên.
WSTG-SESS-10	Kiểm tra JWT (JSON Web Tokens)	Không tiến hành kiểm thử do ứng dụng không sử dụng JWT.
WSTG-SESS-11	Kiểm tra phiên đăng nhập đồng thời	

0.7 Kiểm thử xác thực đầu vào

Trong phần này, hoạt động kiểm thử xác thực đầu vào được thực hiện nhằm đánh giá khả năng kiểm soát và xử lý dữ liệu do người dùng cung cấp trước khi được đưa vào các thành phần xử lý phía máy chủ. Nội dung kiểm thử tập trung vào việc xác định các lỗ hổng phổ biến phát sinh từ việc thiếu hoặc thực hiện không đầy đủ cơ

chế kiểm tra dữ liệu đầu vào, bao gồm các dạng tấn công như XSS, Injection, giả mạo yêu cầu HTTP và các kỹ thuật khai thác liên quan đến xử lý tham số.

Bảng 4.8 dưới đây trình bày tổng hợp kết quả kiểm thử đối với từng hạng mục thuộc nhóm WSTG-INPV, qua đó phản ánh các cơ chế kiểm soát dữ liệu đầu vào đã đáp ứng yêu cầu an toàn bảo mật, đồng thời chỉ ra các trường hợp chưa đạt và những lỗ hổng còn tồn tại có thể bị khai thác nếu không được khắc phục kịp thời.

Bảng 8: Kết quả kiểm thử xác thực đầu vào

ID	Nội dung	Kết luận
WSTG-INPV-01	Kiểm thử XSS phản chiếu	Đạt
WSTG-INPV-02	Kiểm thử XSS lưu trữ	Không đạt. Chức năng "Tạo sự kiện mới", "Chỉnh sửa hồ sơ cá nhân" có lưu trữ và hiển thị lại dữ liệu phía client.
WSTG-INPV-03	Kiểm thử giả mạo phương thức HTTP	Đạt
WSTG-INPV-04	Kiểm thử ô nhiễm tham số HTTP	Đạt
WSTG-INPV-05	Kiểm thử SQL Injection	
WSTG-INPV-06	Kiểm thử LDAP Injection	Đạt
WSTG-INPV-07	Kiểm thử XML Injection	Đạt
WSTG-INPV-08	Kiểm thử SQL Server	Đạt
WSTG-INPV-09	Kiểm thử Xpath Injection	Đạt
WSTG-INPV-10	Kiểm thử IMAP SMTP Injection	Đạt
WSTG-INPV-11	Kiểm thử Code Injection	Đạt
WSTG-INPV-12	Kiểm thử File Inclusion	Đạt

ID	Nội dung	Kết luận
WSTG-INPV-13	Kiểm thử Format String Injection	Đạt
WSTG-INPV-14	Kiểm thử lỗ hổng ẩn	Đạt
WSTG-INPV-15	Kiểm thử HTTP Splitting / Smuggling	Không đạt. Ứng dụng có tồn tại lỗ hổng HTTP Smuggling có thể lấy được request của người khác bao gồm cả phiên đăng nhập
WSTG-INPV-16	Kiểm thử xử lý yêu cầu HTTP đến	Đạt
WSTG-INPV-17	Kiểm thử Host Header Injection	Đạt
WSTG-INPV-18	Kiểm thử Server-side Template Injection	Đạt
WSTG-INPV-19	Kiểm thử Server-Side Request Forgery	Đạt
WSTG-INPV-20	Kiểm thử Mass Assignment	Đạt

0.8 Kiểm thử xử lý lỗi

Trong phần này, hoạt động kiểm thử xử lý lỗi được thực hiện nhằm đánh giá cách thức hệ thống phản hồi và xử lý các tình huống lỗi phát sinh trong quá trình vận hành. Nội dung kiểm thử tập trung vào việc xác định khả năng làm lộ thông tin nội bộ thông qua thông báo lỗi không phù hợp, stack trace hoặc các phản hồi chi tiết từ phía máy chủ, vốn có thể bị kẻ tấn công lợi dụng để thu thập thông tin phục vụ cho các bước tấn công tiếp theo.

Bảng 4.9 dưới đây tổng hợp kết quả kiểm thử đối với từng hạng mục thuộc nhóm WSTG-ERRH, qua đó phản ánh mức độ an toàn của cơ chế xử lý lỗi hiện tại cũng như khả năng kiểm soát thông tin được trả về cho người dùng khi xảy ra lỗi.

Bảng 9: Kết quả kiểm thử xử lý lỗi

ID	Nội dung	Kết luận
WSTG-ERRH-01	Kiểm thử xử lý lỗi không đúng cách	Đạt.
WSTG-ERRH-02	Kiểm thử việc lộ Stack trace	Đạt.

0.9 Kiểm thử mật mã yếu

Trong phần này, hoạt động kiểm thử các cơ chế mật mã được thực hiện nhằm đánh giá mức độ an toàn của các giải pháp mã hóa được sử dụng trong quá trình truyền tải và xử lý dữ liệu trên hệ thống. Nội dung kiểm thử tập trung vào việc xác định các điểm yếu liên quan đến lớp bảo mật truyền tải, việc sử dụng các thuật toán hoặc bộ mã hóa không còn an toàn, cũng như nguy cơ rò rỉ thông tin nhạy cảm khi dữ liệu được truyền qua các kênh không được mã hóa đầy đủ.

Bảng 4.10 dưới đây trình bày tổng hợp kết quả kiểm thử đối với từng hạng mục thuộc nhóm WSTG-CRYP, qua đó phản ánh mức độ tuân thủ các yêu cầu bảo mật về mật mã của hệ thống, đồng thời chỉ ra các trường hợp chưa đạt do tồn tại các cấu hình hoặc cơ chế mã hóa yếu cần được xem xét và khắc phục.

Bảng 10: Kết quả kiểm thử mật mã yếu

ID	Nội dung	Kết luận
WSTG-CRYP-01	Kiểm thử bảo mật lớp truyền tải yếu	Đạt.
WSTG-CRYP-02	Kiểm thử lỗ hổng Padding Oracle	Đạt.
WSTG-CRYP-03	Kiểm thử thông tin nhạy cảm được gửi qua kênh không được mã hóa	Đạt.
WSTG-CRYP-04	Kiểm thử mã hóa yếu	Không đạt. Giao thức TLS 1.2 sử dụng các bộ mã hóa yếu.

0.10 Kiểm thử phía máy người dùng

Trong phần này, hoạt động kiểm thử phía máy người dùng được thực hiện nhằm đánh giá mức độ an toàn của các cơ chế xử lý và hiển thị dữ liệu trên trình duyệt. Nội dung kiểm thử tập trung vào việc xác định các lỗ hổng phát sinh từ việc thực thi mã phía client, thao tác với DOM, lưu trữ dữ liệu trên trình duyệt, cũng như các cơ chế bảo vệ liên quan đến chia sẻ tài nguyên và tương tác giữa các thành phần phía client.

Bảng 4.11 dưới đây tổng hợp kết quả kiểm thử đối với từng hạng mục thuộc nhóm WSTG-CLNT, qua đó phản ánh các chức năng phía client đã đáp ứng yêu cầu an toàn bảo mật, các trường hợp chưa đạt hoặc còn tồn tại rủi ro, cũng như những hạng mục chưa thể đánh giá đầy đủ do giới hạn của mô hình kiểm thử hộp đen.

Bảng 11: Kết quả kiểm thử phía máy người dùng

ID	Nội dung	Kết luận
WSTG-CLNT-01	Kiểm thử lỗ hổng Cross-Site Scripting dựa trên DOM (DOM-Based XSS)	Đạt.
WSTG-CLNT-02	Kiểm thử khả năng thực thi mã JavaScript phía trình duyệt	Không đạt. Chức năng "Tạo sự kiện mới", "Chỉnh sửa hồ sơ cá nhân" có lưu trữ và hiển thị lại dữ liệu phía client.
WSTG-CLNT-03	Kiểm thử lỗ hổng chèn mã HTML (HTML Injection)	Đạt.
WSTG-CLNT-04	Kiểm thử lỗ hổng chuyển hướng URL phía client	Đạt.
WSTG-CLNT-05	Kiểm thử lỗ hổng chèn mã CSS (CSS Injection)	Đạt.
WSTG-CLNT-06	Kiểm thử thao túng tài nguyên phía client	Đạt.
WSTG-CLNT-07	Kiểm thử chia sẻ tài nguyên chéo nguồn (Cross-Origin Resource Sharing - CORS)	
WSTG-CLNT-09	Kiểm thử lỗ hổng Clickjacking	Đạt.
WSTG-CLNT-12	Kiểm thử lưu trữ dữ liệu trên trình duyệt (Browser Storage)	Đạt. Không phát hiện thông tin nhạy cảm được lưu trữ trong bộ nhớ trình duyệt của người dùng.
WSTG-CLNT-13	Kiểm thử Cross-Site Script Inclusion (XSSI)	Khó kiểm thử trong mô hình kiểm thử xâm nhập hộp đen

ID	Nội dung	Kết luận
WSTG-CLNT-14	Kiểm thử tấn công Reverse Tabnabbing	Khó kiểm thử trong mô hình kiểm thử xâm nhập hộp đen do không có quyền truy cập cần thiết vào tài nguyên.