Trong mục này, nội dung sẽ trình bày mục đích của từng nội dung kiểm thử thuộc 11 nhóm trong quy trình kiểm thử xâm nhập chủ động.

a) Thu thập thông tin

Bảng 1: 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 web-site 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.
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.

Mã	Nội dung kiểm thử	Mục tiêu
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.

b) Kiểm thử cấu hình và quản lý triển khai

Bảng 2: 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 gỡ 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 nguy cơ 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 nhầm lẫn 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.

c) Kiểm thử quản lý định danh

Bảng 3: 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 yếu 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.

d) Kiểm thử xác thực

Bảng 4: 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 bỏ 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.

e) Kiểm thử phân quyền

Bảng 5: 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.

f) Kiểm thử quản lý phiên làm việc

Bảng 6: 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 rối 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.

g) Kiểm thử xác thực dữ liệu đầu vào

Bảng 7: 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.

h) Kiểm thử xử lý lỗi

Bảng 8: 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 lộ 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.

i) Kiểm thử mật mã yếu

Bảng 9: 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.

j) Kiểm thử phía máy khách

Bảng 10: 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.

k) Kiểm thử API

Bảng 11: Mục đích của nội dung kiểm thử API

Mã	Nội dung kiểm thử	Mục tiêu
WSTG-APIT-01	Thu thập thông tin API	Xác định toàn bộ các API endpoint được backend hỗ trợ, bao gồm cả các endpoint đã được tài liệu hóa và chưa được tài liệu hóa. Đồng thời xác định tất cả các tham số của từng endpoint mà backend xử lý và khám phá các dữ liệu liên quan đến API được nhúng trong HTML hoặc mã JavaScript gửi tới phía client.
WSTG-APIT-02	Kiểm thử kiểm soát truy cập theo đối tượng trong API	Đánh giá việc API có thực thi đầy đủ cơ chế phân quyền ở mức đối tượng hay không, nhằm đảm bảo rằng người dùng chỉ có thể truy cập và thao tác trên các đối tượng mà họ được phép tương tác.
WSTG-APIT-99	Kiểm thử GraphQL	Đánh giá việc triển khai GraphQL có được cấu hình an toàn và sẵn sàng cho môi trường sản xuất hay không, đồng thời xác thực tất cả các trường dữ liệu đầu vào trước các hình thức tấn công phổ biến và đảm bảo các cơ chế kiểm soát truy cập được áp dụng đầy đủ.