0.1 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 **owasp**.

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 **owasp**.

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 **owasp**.

0.2 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 **owasp_guild**. 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.

0.2.1 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 **owasp_model**.

- 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 tiêu của quá trình kiểm thử bảo mật, thường được tiếp cận theo mô hình hộp đen.

0.2.2 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 **owasp_model**.

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.

0.2.3 Các giai đoạn kiểm thử

Quá trình kiểm thử bảo mật ứng dụng web bao gồm 11 giai đoạn chính **owasp_guild**, 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 kẻ 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.

0.3 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 kiêm 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.

0.4 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.

0.5 Giới thiệu các công cụ kiểm thử

0.5.1 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.

0.5.2 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.