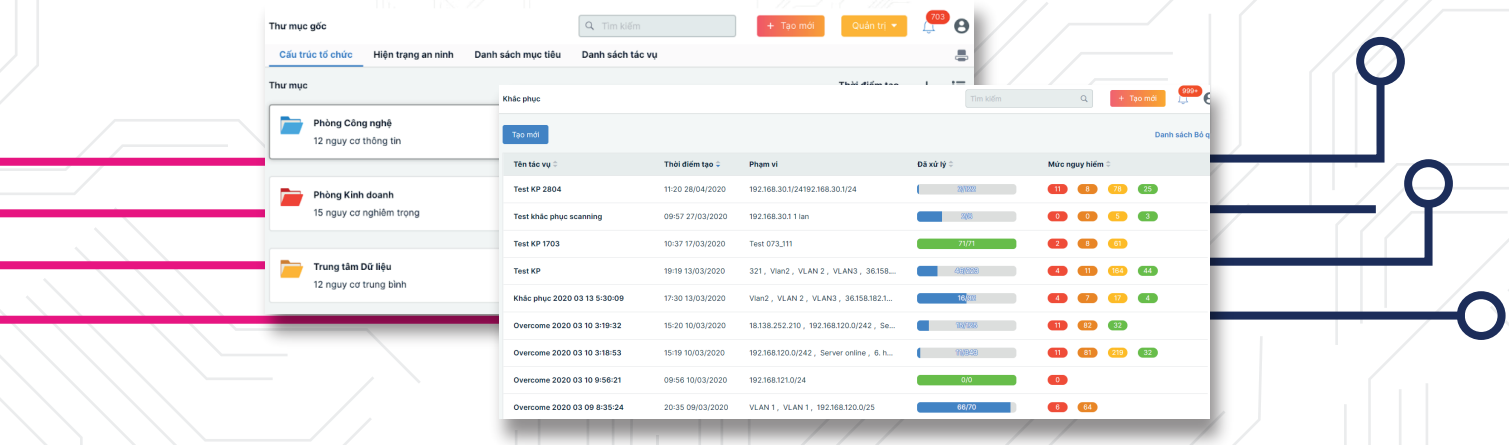
SecurityBox

GIẢI PHÁP QUẢN TRỊ NGUY CƠ AN NINH WEBSITE



4WEBSITE

SECURITYBOX 4WEBSITE LÀ GIẢI PHÁP QUẢN TRỊ NGUY CƠ AN NINH TOÀN DIỆN CHO HỆ THỐNG WEBSITE.

SecurityBox 4Website thực hiện rà quét, phát hiện và vẽ ra bức tranh toàn cảnh về tình trạng an ninh, số lượng điểm yếu, lỗ hổng của Website. Điều này cho phép quản trị viên nắm được thực trạng chi tiết an ninh, từ đó dễ dàng khoanh vùng và thực hiện các biện pháp xử lý, khắc phục để đảm bảo an toàn cho Website.

SecurityBox 4Website là giải pháp duy nhất hiện nay có khả năng cung cấp công nghệ tạo, quản lý và hướng dẫn khắc phục mọi nguy cơ an ninh của Website. Công nghệ này thiết kế một quy trình xử lý nguy cơ thông minh, cho phép khách hàng và đối tác dễ dàng khắc phục điểm yếu và lỗ hổng đã được cảnh báo và phát hiện.

NĂNG LỰC RÀ QUÉT VÀ PHÁT HIỆN NGUY CƠ AN NINH CỦA SECURITYBOX 4WEBSITE:

Tiêu chí	Thông số
Số lượng mã nhận diện lỗ hổng/điểm yếu an ninh	> 20.000
Số lượng script để phát hiện lỗ hổng đặc thù hoặc thực hiện kiểm thử xâm nhập tự động.	> 1.000
Số lượng mã nhận diện cập nhật hàng tháng	> 100

Chi tiết chức năng

Giải pháp giám sát tình trạng an ninh hệ thống

- Đánh giá hiện trạng an ninh của toàn hệ thống hoặc của từng phòng ban/tổ chức trong hệ thống theo tiêu chí An toàn/Nguy hiểm.
- Quản lý nguy cơ an ninh theo từng phòng ban, tổ chức.
- Phát hiện, cảnh báo thông tin lỗ hổng/điểm yếu trên toàn hệ thống.
- Phát hiện, cảnh báo thông tin lỗ hổng/điểm yếu cho từng phòng ban, tổ chức.
- Phát hiện, cảnh báo một số các bất thường xảy ra với hệ thống Website.
- Phát hiện, cảnh báo tức thời các lỗ hổng/nguy cơ có khả năng khai thác thông qua Email/SMS/Slack.
- Tổng hợp và thống kê các nguy cơ an ninh của Website theo thời gian.
- Giám sát trạng thái hoạt động của website bao gồm: Trạng thái Ping, Thời gian tải trang hay kiểm tra domain của website có nằm trong blacklist của các tổ chức hàng đầu thế giới vì bị nghi ngờ độc hại.
- Giám sát lịch sử đánh giá an ninh của website qua thời gian.
- Giám sát lịch sử kiểm tra trạng thái của website theo 07 ngày hoặc 24 giờ gần nhất.
- Thống kê lại toàn bộ lịch sử quá trình giám sát, đánh giá nguy cơ an ninh mạng.

Rà quét an ninh website, web service

- Phát hiện các thông tin liên quan tới máy chủ Web, hệ điều hành máy chủ, phiên bản phần mềm.
- Phát hiện ngôn ngữ lập trình: PHP, Java, .Net, JS.
- Phát hiện thông tin về cổng và dịch vụ.
- Phát hiện các thông tin liên quan tới nền tảng phát triển Website: Joomla, CakePHP, Wordpress, Sharepoint, Drupal.
- Rà quét thông tin cấu trúc website, liệt kê toàn bộ các đường dẫn có thể thu thập được đối với website đó.
- Rà quét các lỗ hổng nguy hiểm nhất của Website: SQL injection, Blind SQL injection, Command injection, PHP Code injection, Directory Traversal, XSS.
- Phát hiện lộ lọt các thông tin nhạy cảm (tài khoản mặc định, mật khẩu yếu).
- Phát hiện các lỗi có nguy cơ lộ lọt thông tin: Directory Listing, Script Source Code Disclosure, Application Error Message, .htaccess File Readable.
- Kiểm tra cấu hình an ninh của một Webserver.
- Kiểm tra các nguy cơ liên quan tới upload dữ liệu và nguy cơ bị Hacker upload mã độc để chiếm quyền điều khiển hệ thống.
- Rà quét, phát hiện Malware, các Shell trên Website.
- Rà quét nguy cơ với các Website cần đăng nhập.
- Xem kết quả dựa theo đường dẫn hoặc theo nguy cơ.
- Cơ chế học và dạy thiết bị thông minh để lọc bỏ dần các cảnh báo sai (false positive) trong thời gian đầu triển khai thiết bị.
- Lập lịch rà quét an ninh định kì.

Chi tiết chức năng

Tấn công kiểm thử

- Tấn công thử nghiệm với các lỗ hổng có khả năng tấn công khai thác.

Khắc phục lỗ hổng điểm yếu

- Đề xuất các biện pháp khắc phục tương ứng với các lỗ hổng và các thông tin đã thu thập được.
- Theo dõi số lượng lỗ hổng điểm yếu đã khắc phục, chưa khắc phục, chưa xử lý thông qua giao diện quản trị.
- Ghi dấu, theo dõi, giám sát quá trình khắc phục lỗ hổng điểm yếu. Hỗ trợ phương thức ghi chú trên từng lỗ hổng trong quá trình khắc phục.

Tự động hóa quy trình kiểm tra an ninh

- Toàn bộ việc kiểm tra an ninh được thực hiện tự động theo lịch đã đặt sẵn.

Báo cáo

- Tạo báo cáo sau mỗi lần thực hiện rà quét (báo cáo cơ bản, báo cáo chi tiết).
- Tạo báo cáo hỗ trợ sửa lỗi tương ứng với từng mục tiêu đã thực hiện rà quét (báo cáo hỗ trợ sửa lỗi).
- Hỗ trợ báo cáo theo các chuẩn an ninh khác nhau.
- Hỗ trợ báo cáo theo các mức độ khác nhau (báo cáo cơ bản, báo cáo chi tiết theo thiết bị, báo cáo chi tiết theo nguy cơ).
- Hỗ trợ báo cáo theo nhiều định dạng khác nhau như Word, Excel.

Phương thức vận hành

- Quản trị thông qua giao diện Website.
- Hỗ trợ tiếng Việt.
- Cấu hình mạng và các thông số cho thiết bị thông qua giao diện quản trị.