CyStack

DATA SHEET

Đánh giá lỗ hổng bảo mật với CyStack Web Security

Tự động quét và giám sát các lỗ hổng bảo mật trong hệ thống

Thách thức bảo mật

Đánh giá lỗ hổng bảo mật rất quan trọng trong công tác an ninh mạng doanh nghiệp, giúp các doanh nghiệp xác định và phân định mức độ ưu tiên các lỗ hổng trong hệ thống và mạng. Việc xác định và giải quyết các lỗ hổng giúp doanh nghiệp giảm nguy cơ bị tấn công mạng và bảo vệ khỏi các mối đe dọa tiềm ẩn.

Tuy nhiên, việc thực hiện đánh giá lỗ hổng không phải là điều dễ dàng đối với mọi doanh nghiệp bởi:

- Thiếu chuyên môn: Đánh giá lỗ hổng bảo mật đòi hỏi kiến thức và kỹ năng chuyên môn về bảo mật, hạ tầng mạng và phát triển phần mềm. Các công ty công nghệ không có đội ngũ an ninh mạng nội bộ đủ chuyên môn cần thiết để tiến hành đánh giá lỗ hổng kỹ lưỡng và hiệu quả.
- Tài nguyên hạn chế: Đánh giá lỗ hổng bảo mật thường là một quá trình tốn nhiều thời gian và tài nguyên, đặc biệt đối với các doanh nghiệp lớn có các hệ thống và hạ tầng mạng phức tạp. Các công ty phi bảo mật không có đủ nguồn tài nguyên hoặc nhân sự chuyên trách thực hiện đánh giá lỗ hổng bảo mật.
- Độ phức tạp của hệ thống và mạng: Đánh giá lỗ hổng bảo mật liên quan đến việc kiểm tra các hệ thống và hạ tầng mạng để phát hiện các lỗ hổng. Với các hệ thống và hạ tầng mạng phức tạp, việc xác định và đánh giá toàn bộ các lỗ hổng tiềm ẩn trở nên khó khăn.
- Thay đổi liên tục: Các hệ thống và hạ tầng mạng liên tục phát triển và các lỗ hổng mới luôn được phát hiện. Điều này có nghĩa là, đánh giá lỗ hổng bảo mật là quá trình liên tục, đòi hỏi giám sát và cập nhật thường xuyên. Các công ty không có nguồn lực hoặc chuyên môn để theo kịp những thay đổi liên tục này.

Lợi ích của khách hàng

- Tiết kiệm thời gian với các tác vụ tự động
- Xác định các vấn đề bảo mật đã biết hoặc ở cấp độ bề mặt và các lỗi cấu hình
- Thiết lập khung cơ sở về bảo mật
- Khắc phục tập trung các lỗ hổng được ưu tiên
- Xác thực chương trình vá lỗi/hardening

Giải pháp của CyStack

CyStack Web Security (CWS) là một công cụ quét và giám sát lỗ hổng bảo mật tự động dành cho các ứng dụng web được phát triển bởi CyStack. Sản phẩm này được xây dựng để đơn giản hóa và tự động hóa quy trình đánh giá lỗ hổng bằng cách tập trung vào:

- Xác định lỗ hổng: CWS giúp tự động quét các lỗ hổng tiềm ẩn trong ứng dụng web và máy chủ.
- Phân định mức độ ưu tiên các lỗ hổng: CWS giúp các doanh nghiệp ưu tiên các lỗ hổng dựa trên mức độ nghiêm trọng và tác động tiềm tàng của chúng. Điểm CVSS là một công cụ quan trọng hỗ trợ thực hiện đánh giá này. Phân định mức độ ưu tiên giúp các doanh nghiệp ưu tiên các nỗ lực để giải quyết các lỗ hổng nghiêm trọng nhất trước.
- Giám sát phát hiện các lỗ hổng mới: CWS quét và dò ra các lỗ hổng liên tục để cảnh báo ngay khi lỗ hổng mới được phát hiện, giúp các doanh nghiệp luôn cập nhật và chủ động giải quyết các rủi ro bảo mật.
- Theo dõi quá trình: CWS giúp các doanh nghiệp theo dõi quá trình xử lý các lỗ hổng theo thời gian, giúp các doanh nghiệp đảm bảo có các tiến triển nhất định trong việc giảm thiểu nguy cơ bị tấn công mạng.

Phạm vi đối tượng

- Domain
- Dải IP
- CIDR
- URL

Deep Scan

Lỗ hổng bảo mật là nguyên nhân hàng đầu khiến các ứng dụng web bị tội phạm mạng tấn công. CWS giúp phát hiện và giải quyết những lỗ hổng bảo mật nghiêm trọng trong ứng dụng web để mang lại trải nghiệm an toàn cho người dùng cuối và hệ thống của doanh nghiệp.

Intelligence Gathering

Intelligence Gathering là một phần quan trọng của CWS liên quan đến quá trình thu thập thông tin về tech stack, dải mạng, và cơ sở hạ tầng của đối tượng. Bằng cách kết hợp công cụ thu thập thông tin độc đáo và các công nghệ thăm dò tự động, CWS thu thập toàn bộ thông tin liên quan đến mục tiêu để chuẩn bị cho giai đoạn phân tích lỗ hổng.

Fuzzing

Fuzzing là một kỹ thuật được sử dụng để phát hiện các lỗ hổng trong phần mềm bằng cách nhập một lượng lớn dữ liệu ngẫu nhiên, hay "fuzz", vào phần mềm và thử khiến phần mềm đó sập hoặc xảy ra các hành vi trái mong muốn. CWS đã triển khai công nghệ này để khám phá các lỗ hổng 0-day và lỗ hổng chưa biết trong mục tiêu.

Cơ sở dữ liệu về lỗ hổng

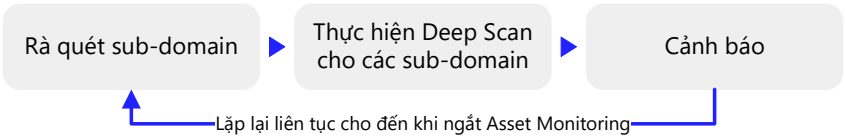
Bên cạnh Fuzzing, đội ngũ chuyên gia tại CyStack xây dựng và duy trì cơ sở dữ liệu các lỗ hổng phổ biến và đã được công khai, thực hiện bằng cách liên tục thu thập ID CVE mới, các lỗ hổng 1-day và các lỗ hổng hay được khai thác qua các nguồn tin cậy; sau đó viết mã tái hiện lỗ hổng cho các lỗ hổng rồi thêm vào CWS. Cơ sở dữ liệu lỗ hổng của CWS được cập nhật tại https://web.cystack.net/vulnerability/.

Kiểm thử có xác thực

Hầu hết các ứng dụng web đều có cả các yếu tố công khai lẫn nội bộ. Bất kỳ ai cũng có thể truy cập các yếu tố công khai, trong khi các yếu tố nội bộ chỉ dành cho những người dùng có tài khoản như Dashboard hoặc Admin page truy cập. Khi kiểm thử một ứng dụng web bằng tài khoản được xác thực, có nhiều khả năng tìm thấy các lỗ hổng và truy cập các yếu tố bị hạn chế của trang web hơn so với thử nghiệm mà không có xác thực. CWS cung cấp hai tùy chọn để quét có xác thực: thay đổi header của gói tin (cookie và token xác thực) hoặc Basic authentication.

Asset Monitoring

Asset Monitoring giúp cải thiện tính bảo mật cho hệ thống bằng cách liên tục khai thác các sub-domain, địa chỉ IP trong cùng một dải mạng và cảnh báo về các tệp bị lộ, lỗ hổng hoặc lỗi cấu hình. Với Asset Monitoring, doanh nghiệp sẽ được đảm bảo an toàn cho hệ thống và ngăn chặn các vi phạm bảo mật tiềm ẩn.



DevSecOps

Là một phần của CI/CD

CWS hỗ trợ đầy đủ các API call để quá trình quét lỗ hổng được bắt đầu ngay khi có một Git commit mới thông qua việc thực hiện request tới API. Kết quả sẽ được phản hồi trong vài phút giúp các nhà phát triển nhận biết các lỗi và khắc phục trước khi chính thức thực hiện merge hoặc triển khai ứng dụng.

Bằng cách tích hợp tính năng quét lỗ hổng bảo mật vào quá trình phát triển và triển khai, các doanh nghiệp sẽ đảm bảo được các ứng dụng an toàn và tuân thủ các tiêu chuẩn ngành cũng như các khuyến nghị bảo mật tốt nhất.

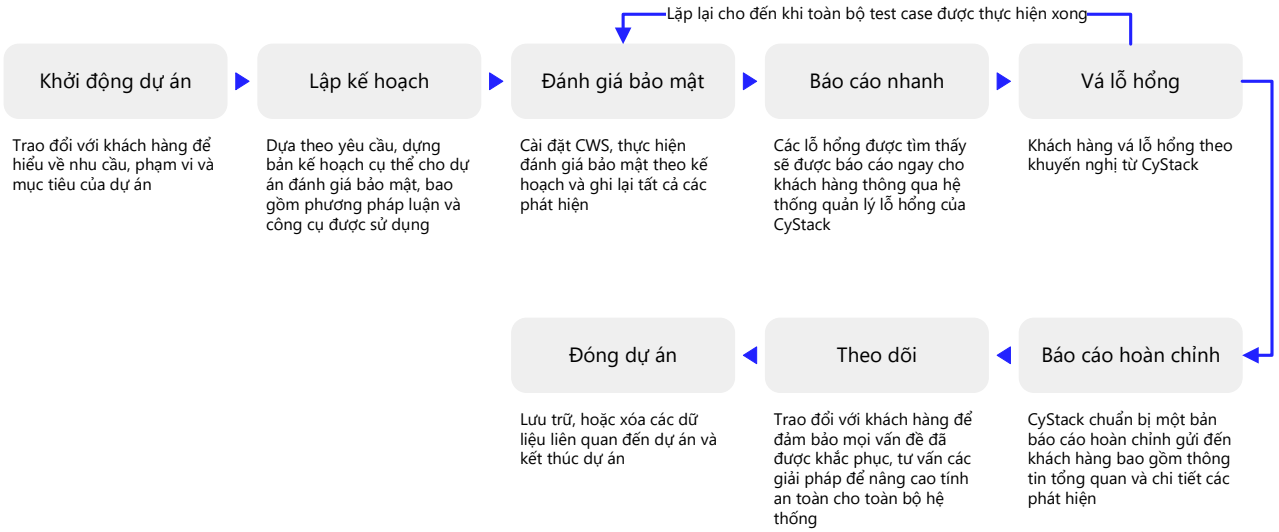
Tích hợp liền mạch CWS với các công cụ yêu thích

- **Slack**: Nhận những cập nhật về trạng thái quét, trạng thái xuất báo cáo cũng như cập nhật về phát hiện lỗ hổng dựa trên cài đặt và tùy chọn.
- **Jira**: Tạo issue và giao cho kỹ sư chịu trách nhiệm khi có phát hiện lỗ hổng mới.

Tính năng chính

- Rà quét các sub-domain và địa chỉ trong mạng nội bộ
- Phát hiện lỗ hổng bằng kỹ thuật fuzzing và cơ sở dữ liệu về lỗ hổng riêng của CyStack
- Giám sát và cảnh báo các vấn đề mới tự động và liên tục
- Quản lý, theo dõi, phân định mức độ ưu tiên và khắc phục các phát hiện trên một nền tảng đặc biệt
- Tích hợp chức nâng quét với các công cụ CI/CD và các công cụ cải thiện hiệu suất

Quy trình làm việc với khách hàng



Về CyStack

CyStack là một công ty đổi mới sáng tạo trong lĩnh vực an ninh mạng tại Việt Nam, chúng tôi tiên phong xây dựng các sản phẩm bảo mật thế hệ mới cho cả doanh nghiệp và cá nhân. Các giải pháp của CyStack tập trung vào bảo vệ dữ liệu, phòng chống tấn công mạng và quản lý lỗ hổng bảo mật.

Để biết thêm chi tiết, liên lạc tới hotline **(+84) 247 109 9656** hoặc gửi mail tới **contact@cystack.net** để trao đổi cùng các chuyên gia bảo mật tại CyStack.
cystack.net