CyStack

DATA SHEET

Kiểm thử bảo mật

Phát hiện lỗ hổng bảo mật trước khi hacker làm điều đó

Tổng quan

Kiểm thử bảo mật, hay Pentest, là quá trình giả lập một cuộc tấn công vào hệ thống máy tính, mạng hay ứng dụng web để xác định những lỗ hổng mà tin tặc có thể khai thác. Trong quá trình pentest, các chuyên gia bảo mật sử dụng những công cụ và kỹ thuật khác nhau để kiểm tra tính bảo mật của môi trường mục tiêu và xác định những điểm yếu an toàn thông tin.

Pentest rất quan trọng vì quy trình này giúp doanh nghiệp phát hiện và vá những lỗ hổng trong hệ thống và ứng dụng của họ trước khi bị tin tặc khai thác. Đây là một giải pháp hiệu quả để cải thiện tình trạng bảo mật của doanh nghiệp và đảm bảo doanh nghiệp tuân thủ các quy định và tiêu chuẩn của ngành.

Bên cạnh việc xác định những lỗ hổng, pentest còn giúp các doanh nghiệp đánh giá những rủi ro từ một cuộc tấn công thực tế, hiểu được hậu quả tiềm ẩn của việc bị tấn công, và phát triển các chiến lược để chống lại các cuộc tấn công này. Bên cạnh đó, pentest còn giúp doanh nghiệp xây dựng văn hóa bảo mật và cải thiện khả năng ứng phó với các sự cố an ninh thông tin.

Lợi ích của khách hàng

- Bảo vệ dữ liệu nhạy cảm
- Ngăn chặn các cuộc tấn công
- Duy trì tính toàn vẹn của hệ thống
- Đáp ứng các tiêu chuẩn và quy định

Giải pháp của CyStack

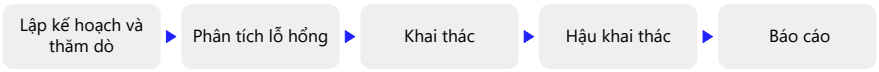
Đội ngũ kiểm thử bảo mật của CyStack bao gồm những chuyên gia tài năng giàu kinh nghiệm, thành thạo các phương pháp kiểm thử bám sát mục tiêu và tối ưu nhất. Họ là những chuyên gia có nền tảng vững chắc về phát triển phần mềm và nghiên cứu an ninh mạng, giúp đội ngũ CyStack đánh giá toàn diện nhất các rủi ro bảo mật trong sản phẩm số của doanh nghiệp. Các chuyên gia tại CyStack cũng thường xuyên tham gia các hội nghị an ninh mạng lớn trên thế giới với vai trò diễn giả hàng năm, đồng thời họ là những chuyên gia săn lỗi phần mềm với nhiều thành tích phát hiện ra các lỗ hổng bảo mật nghiêm trọng và được ghi danh trên Hall of Fame của các hãng công nghệ lớn toàn cầu như IBM, HP, Microsoft, Nokia, Alibaba, Sea Group, v.v.

Dịch vụ kiểm thử bảo mật của CyStack là một giải pháp hoàn hảo cho các doanh nghiệp đang tìm cách cải thiện tính bảo mật cho hệ thống và ứng dụng. Một trong những tính năng chính làm nên sự khác biệt của CyStack đó là việc kết hợp những phương thức kiểm thử truyền thống với bảo mật cộng đồng. Cách tiếp cận độc đáo này tận dụng kiến thức chuyên môn và kinh nghiệm của cộng đồng chuyên gia bảo mật trên toàn cầu để tăng hiệu quả của quá trình kiểm thử lên nhiều lần.

Ngoài ra, dịch vụ pentest tại CyStack cũng đi kèm với một nền tảng quản lý lỗ hổng được phát triển bởi chính đội ngũ kỹ sư nội bộ. Nền tảng này được trang bị các công cụ và tính năng mạnh mẽ cho phép các doanh nghiệp dễ dàng theo dõi, phân loại và đưa ra giải pháp khắc phục các lỗ hổng bảo mật được báo cáo. Hệ thống này cũng bao gồm khả năng giám sát trạng thái của các lỗ hổng theo thời gian thực, tạo báo cáo và cảnh báo cũng như tích hợp với các giải pháp quản lý công việc khác.

Phương pháp luận

Các bước cụ thể của một dự án Pentest có thể khác nhau tùy vào mục đích và mục tiêu của dự án, cũng như các đặc điểm của môi trường mục tiêu. Nhưng nhìn chung, quy trình kiểm thử bảo mật của CyStack tuân thủ nghiêm ngặt các bước sau:



1. **Lập kế hoạch và thăm dò**: Giai đoạn liên quan đến việc xác định phạm vi và mục tiêu của cuộc kiểm thử, xác định thông tin về mạng và các hệ thống mục tiêu, đồng thời thu thập thông tin về môi trường mục tiêu để hiểu rõ hơn về cách thức hoạt động của mục tiêu và những lỗ hổng tiềm ẩn.
2. **Phân tích lỗ hổng**: Trong giai đoạn này, các chuyên gia kiểm thử xác định các lỗ hổng tiềm ẩn trong hệ thống mục tiêu bằng cách sử dụng các kỹ thuật như dò quét lỗ hổng, dò quét hệ thống mạng, và đánh giá cấu hình. Ngoài ra, các lỗ hổng phổ biến (1-day flaws, CVEs) cũng sẽ được kiểm thử.
3. **Khai thác**: Đây là giai đoạn tấn công thực sự, tức là, các chuyên gia cố gắng khai thác một hoặc nhiều lỗ hổng đã xác định để có được quyền truy cập trái phép vào hệ thống.
4. **Sau khai thác**: Giai đoạn liên quan đến việc duy trì quyền truy cập vào hệ thống đã bị xâm nhập và leo thang đặc quyền trong hệ thống, nếu có thể.
5. **Báo cáo**: Giai đoạn cuối cùng liên quan đến việc chuẩn bị một báo cáo tóm tắt quá trình kiểm thử, các lỗ hổng được xác định và các khuyến nghị để cải thiện tính bảo mật của hệ thống.

Tính năng chính

- Nhận được sự đảm bảo về tính bảo mật của hạ tầng và ứng dụng
- Được đánh giá bởi các chuyên gia bảo mật từ CyStack và hơn 3000 nhà nghiên cứu từ cộng đồng của CyStack
- Quản lý, phân loại và nhận hướng dẫn khắc phục lỗ hổng thông qua Nền tảng quản lý lỗ hổng của CyStack
- Nhận các tư vấn để tăng cường bảo mật cho toàn hệ thống
- Giảm thiểu rủi ro và nâng cao hiệu quả hoạt động của hệ thống

Hướng tiếp cận của CyStack

CyStack đưa ra 3 cách tiếp cận kiểm thử bảo mật. Đội ngũ sẽ kiểm thử hộp đen cho các dự án nếu không có yêu cầu khác từ khách hàng:

	Hộp đen tức kiểm thử xâm nhập hộp kín	**Hộp xám** sự kết hợp giữa kiểm thử hộp đen và hộp trắng	**Hộp trắng** tức kiểm thử xâm nhập hộp mở
Mục tiêu	Mô phỏng tấn công mạng ngoài đời thật	Đánh giá lỗ hổng của tổ chức trước các mối đe dọa bên trong	Mô phỏng cuộc tấn công khi hacker chiếm được quyền truy cập của một tài khoản có đặc quyền
Mức độ truy cập	Không có quyền truy cập nội bộ hoặc thông tin hạ tầng	Có một số quyền truy cập nội bộ và thông tin hạ tầng	Có quyền truy cập trực tiếp toàn bộ ứng dụng và hệ thống
Ưu điểm	Chân thực nhất Kiểm thử dưới góc nhìn của hacker	Hiệu quả hơn phương pháp hộp đen, tiết kiệm thời gian cũng như chi phí Kiểm thử dưới góc nhìn của hacker	Toàn diện nhất, khó bỏ sót lỗ hổng và nhanh hơn Kiểm thử dưới góc nhìn của hacker
Khuyết điểm	Cần nhiều thời gian và dễ bỏ sót lỗ hổng	Không thực sự có khuyết điểm đáng kể	Lượng lớn thông tin (ví dụ, mã nguồn) cần phải cung cấp cho tester và tốn kém

Đối tượng kiểm thử bảo mật

Ứng dụng web

Ứng dụng web đóng vai trò rất quan trọng, là phương tiện để các doanh nghiệp tương tác với internet, khách hàng, đối tác và nhà cung cấp. Các ứng dụng này là một phần quan trọng của doanh nghiệp và được sử dụng để quảng bá công ty, tạo thu nhập và tăng doanh thu. Thật không may, điều này cũng khiến các ứng dụng web trở thành mục tiêu của tội phạm mạng và cũng thường là nguồn gốc của các cuộc tấn công.
CyStack cam kết tuân theo những phương pháp và tiêu chuẩn ngành tốt nhất khi kiểm thử bảo mật cho các ứng dụng web. Một trong những tài nguyên chính đội ngũ chuyên gia dựa vào là OWASP Testing Guide. Đây là bộ tiêu chuẩn được công nhận rộng rãi trong lĩnh vực bảo mật web, cung cấp một tập hợp toàn diện các quy trình kiểm thử và đề xuất để xác định và giảm thiểu các lỗ hổng ứng dụng web phổ biến. Cụ thể, các test case sử dụng bao gồm:

- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Testing for Error Handling
- Testing for Weak Cryptography
- Business Logic Testing
- Client-side Testing
- API Testing

Các tiêu chuẩn

- OWASP Testing Guide
- The Penetration Testing Execution Standard
- REST API security guidelines
- NIST SP 800-95

Ứng dụng di động

Các ứng dụng di động là một phần quan trọng trong cuộc sống hiện đại và được sử dụng cho nhiều mục đích khác nhau, bao gồm liên lạc, giải trí, ngân hàng và mua sắm. Do vậy các doanh nghiệp phải đảm bảo rằng các ứng dụng di động do họ phát triển luôn an toàn để bảo vệ dữ liệu, ngăn chặn các cuộc tấn công và duy trì niềm tin của người dùng.

OWASP Mobile Application Security Testing Guide (MASTG) được sử dụng làm tiêu chuẩn cơ bản khi thực hiện dự án kiểm thử cho các ứng dụng di động. OWASP MASTG là một tài liệu toàn diện cung cấp các hướng dẫn và khuyến nghị để kiểm thử tính bảo mật của ứng dụng di động, bao quát nhiều chủ đề, gồm tối ưu kiến trúc ứng dụng, phương pháp lập trình an toàn và kỹ thuật kiểm thử. Chuyên gia CyStack tập trung vào các yêu cầu bảo mật sau:

- Yêu cầu về kiến trúc, thiết kế và mô hình hóa mối đe dọa
- Yêu cầu về quyền riêng tư và lưu trữ dữ liệu
- Yêu cầu về mã hóa
- Yêu cầu về quản lý phiên và xác thực
- Yêu cầu về kênh truyền dữ liệu
- Yêu cầu về tương tác trên nền tảng
- Yêu cầu về chất lượng code và cấu hình build
- Yêu cầu về khả năng phục hồi

Dịch vụ web và API

API (Giao diện lập trình ứng dụng) và web service là những thành phần quan trọng của công nghệ hiện đại và được sử dụng để cho phép việc liên lạc và trao đổi dữ liệu giữa các hệ thống và ứng dụng khác nhau. Việc đảm bảo tính bảo mật của API xử lý dữ liệu nhạy cảm và thường có thể tiếp xúc trực tiếp từ Internet nên dễ bị tấn công, vì vậy việc đảm bảo tính bảo mật của API là rất quan trọng.

Nhìn chung, kiểm thử cho API được thực hiện tương tự như cho các ứng dụng web và cũng tuân theo các tiêu chuẩn cơ bản đã đề cập trong phần trước. Bên cạnh đó, kiểm thử cho API cũng tuân theo một số hướng dẫn cụ thể:

- **OWASP API Security Top 10**: Đây là danh sách 10 rủi ro bảo mật API quan trọng nhất, được xây dựng bởi OWASP. Danh sách này cung cấp một điểm tiêu chuẩn để xác định các lỗ hổng và rủi ro phổ biến cho API.
- **REST API security guidelines**: REST là một kiến trúc phổ biến để xây dựng API. REST API security guidelines cung cấp các chủ đề để bảo mật API hiệu quả như kiểm tra cơ chế xác thực, phân quyền và kiểm lọc dữ liệu đầu vào.
- **Các tiêu chuẩn và quy định trong lĩnh vực cụ thể**: Một số lĩnh vực có các tiêu chuẩn hoặc quy định riêng áp dụng cho API, như PCI DSS cho các API xử lý dữ liệu thẻ tín dụng.
- **Yêu cầu bảo mật tùy chỉnh**: Ngoài các tiêu chuẩn chung, cũng có các yêu cầu bảo mật cụ thể cần áp dụng cho API trong từng dự án. Các yêu cầu này được xác định bởi nhà phát triển hoặc theo các quy định của ngành.

Ứng dụng desktop

Ứng dụng desktop là các chương trình phần mềm chạy trên máy tính và được sử dụng cho nhiều mục đích khác nhau cho công việc, giao tiếp và giải trí. Việc đảm bảo rằng các ứng dụng này an toàn là điều quan trọng để bảo vệ dữ liệu nhạy cảm, ngăn chặn các cuộc tấn công và duy trì độ tin cậy của hệ thống.

Kiểm thử các ứng dụng desktop liên quan đến quan đến việc tuân theo các hướng dẫn kiểm thử bảo mật tương tự như ứng dụng di động. Để xác định các lỗ hổng trong các ứng dụng desktop, đội ngũ CyStack sử dụng OWASP Top 10 Desktop Application Security Risks như Injection, Broken Authentication & Session Management, Hardcoded Secrets in files, Missing Code-Signing, và Verification for File Integrity, Usage of Outdated Softwares, hoặc Usage of Obsolete Components/Services of Windows/3rd Party vendors.

Cơ sở hạ tầng

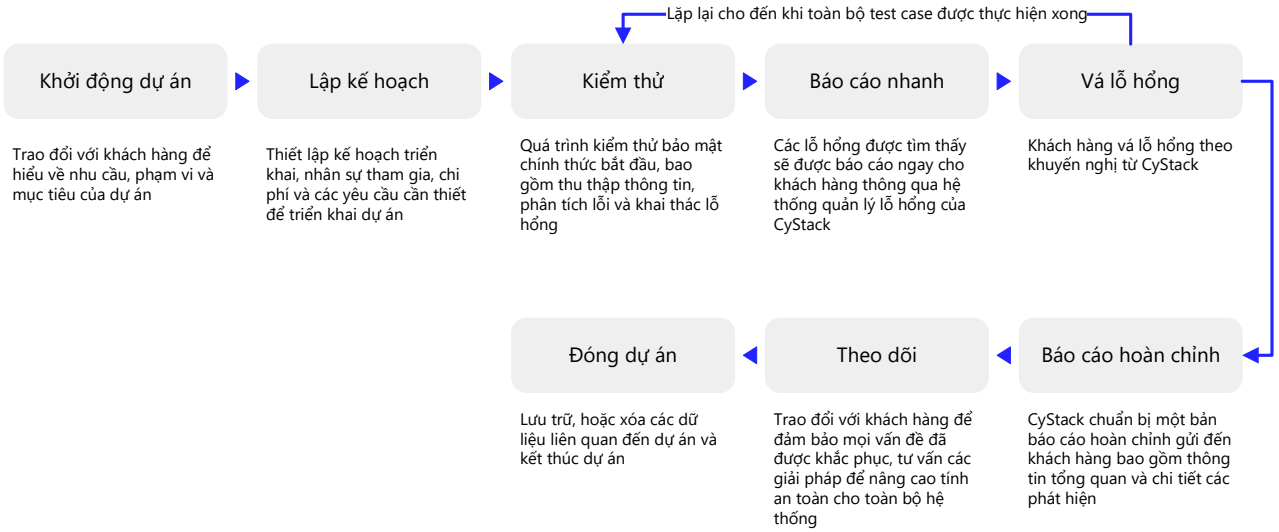
Hạ tầng mạng là một yếu tố quan trọng đối với mọi ứng dụng khi ứng dụng được triển khai. Trong hạ tầng mạng có lưu trữ dữ liệu nhạy cảm và cấu hình của ứng dụng nên thường là mục tiêu của tin tặc, vì vậy việc kiểm thử bảo mật cho hạ tầng rất quan trọng. Các lỗi bảo mật hoặc tấn công vào hạ tầng của doanh nghiệp có thể dẫn đến mất dữ liệu, ngừng trệ dịch vụ và những hậu quả khác.

Giải pháp Pentest của CyStack giúp khách hàng đánh giá tính bảo mật của toàn bộ cơ sở hạ tầng, bao gồm hạ tầng đám mây, máy chủ và mạng nội bộ.

Ứng dụng đặc thù

Các phần mềm đặc thù được các doanh nghiệp thiết kế và sử dụng cho các mục đích kinh doanh riêng có thể tồn tại nhiều vấn đề bảo mật nguy hiểm. Giải pháp pentest của CyStack giúp phát hiện các lỗ hổng bảo mật và những điểm yếu trong ứng dụng bao gồm việc lộ lọt dữ liệu nhạy cảm, quá trình giao tiếp không an toàn giữa client-server. CyStack cũng cung cấp Whitebox Testing để phân tích và xác định các lỗ hổng trong các hệ thống công nghệ thông tin quan trọng được các doanh nghiệp lớn sử dụng cho hoạt động kinh doanh hoặc được cung cấp dưới dạng dịch vụ cho khách hàng. Cách tiếp cận toàn diện này kết hợp phân tích tĩnh và động của từng thành phần trong hệ thống để đảm bảo không bỏ sót các lỗ hổng bảo mật trong quá trình kiểm thử.

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