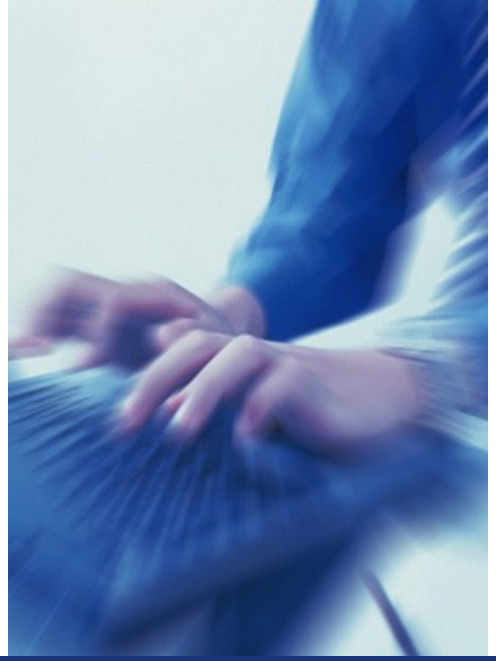
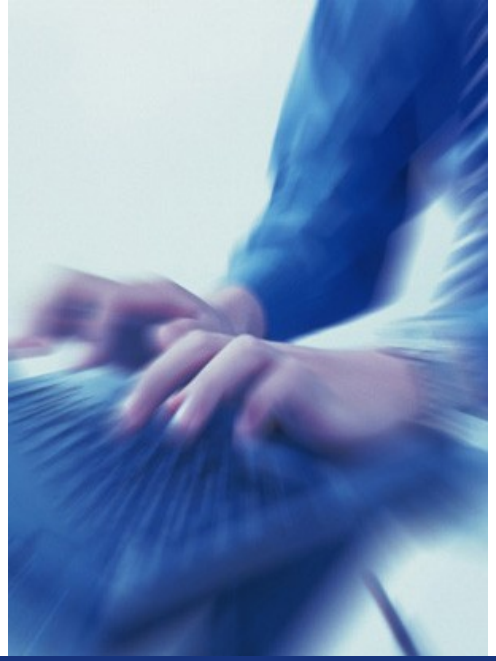


Lạc Tiên

PHÁT TRIỂN ỨNG DỤNG WEB APPLICATION SCANNING TỪ CORE SKIPFISH

(Dịch vụ rà soát và kiểm định bảo mật website)

www.webscan.com.vn



Lạc Tiên

Mentor: Trần Chí Cần
Developer: Lê Quốc Nhật Đông
Cộng đồng: HVA Online (Diễn đàn hacker Việt Nam)

www.webscan.com.vn

Nội dung

1. Đặt vấn đề
2. Tổng quan sản phẩm webscan
3. Phát triển nguồn mở sản phẩm
4. Demo sản phẩm

ĐẶT VẤN ĐỀ

- Phần lớn các cuộc tấn công mạng ở Việt Nam đều xuất phát từ nước ngoài
- Các lĩnh vực thường xuyên bị tấn công chủ yếu tập trung vào lĩnh vực tài chính ngân hàng, giao dịch trực tuyến, thương mại điện tử.
- Việt Nam bị xếp hạng cao trên thế giới về mức độ tấn công mã độc, lừa đảo trực tuyến.

ĐẶT VẤN ĐỀ

- Các tội phạm công nghệ cao thường xuyên thực hiện tấn công vượt qua hệ thống kiểm tra an ninh nhằm thay đổi các nội dung trên các trang điện tử, đánh cắp thông tin thẻ ứng dụng, tống tiền các nhà cung cấp dịch vụ
- Nhiều chuyên gia nhận định an ninh mạng trong năm 2012 vẫn là vấn đề nóng, khi các tin tặc có những thủ đoạn tinh vi nhắm vào các tổ chức, doanh nghiệp và thậm chí người dùng.

TỔNG QUAN DỰ ÁN WEBSCAN

- Tháng 3/2010, nhóm phát triển ứng dụng an ninh mạng của Google đã ra mắt Skipfish
- Skipfish hỗ trợ các tính năng cần có khi rà soát một trang web bất kì, nhận dạng các giá trị tùy biến trong form mẫu HTML.
- Chức năng chính của Skipfish là kiểm định cấu hình và các thông số kĩ thuật của website và các mô hình ứng dụng trực tuyến hiện đại ngày nay.

TỔNG QUAN DỰ ÁN WEBSCAN

- Tuy nhiên, Skipfish do Google phát triển còn tồn động khá nhiều vấn đề về sử dụng và triển khai.
- Bảng báo cáo lỗ hỏng của Skipfish còn sơ sài, thiếu đi tính chất tổng quan, không có giải pháp khắc phục lỗ hỏng, nhiều mô tả kĩ thuật đòi hỏi trình độ Security của người xem phải thông thạo (tương đương CISSP) mới hiểu được.
- Do đã ra mắt từ lâu và cộng đồng ít phát triển nên Skipfish chưa cập nhật các lỗ hỏng bảo mật mới nhất hiện nay.

TỔNG QUAN DỰ ÁN WEBSCAN

- Nhận thấy sự hạn chế của Skipfish, công ty Lạc Tiên và nhóm sinh viên CNTT của ĐH Hoa Sen quyết định sử dụng core Skipfish để phát triển một ứng dụng Web Application Scanner.
- Sử dụng ngôn ngữ lập trình là C/C++, Python, PHP, Java và Shell Script và triển khai trên máy chủ cài đặt Ubuntu Server 12.04.
- Được các thành viên chủ chốt bên cộng đồng hacker HVA hỗ trợ kĩ thuật và bên Lạc Tiên JSC hỗ trợ kinh phí triển khai.

TỔNG QUAN DỰ ÁN WEBSCAN

- Web Application Scanner (gọi tắt là webscan) dựa vào core Skipfish để xây dựng theo mô hình SaaS sử dụng công nghệ điện toán đám mây vào lĩnh vực phát hiện lỗ hổng bảo mật.
- Để tiến hành kiểm tra lỗ hổng website, người sử dụng không cần phải cài đặt bất kì phần mềm nào trên máy tính. Họ chỉ cần vào truy cập trang web **www.webscan.com.vn** để thực hiện quét.
- Hệ thống Webscan sẽ tương tác với website của người dùng, sử dụng các kĩ thuật detect và scanning rồi đưa ra bảng báo cáo tình trạng bảo mật website. Bảng báo cáo mô tả bằng tiếng Việt.

TỔNG QUAN DỰ ÁN WEBSCAN

- Ngoài ra, nhóm còn phát triển thêm tính năng rà soát lỗ hỏng HTTPS cho các website ngân hàng và webiste giao dịch trực tuyến, vốn không phải là tính năng của Skipfish.
- Khai thác lỗ hỏng HTTPS (giao thức SSL/TLS) vốn là cơn ác mộng đối với các website ngân hàng và giao dịch trực tuyến.

TỔNG QUAN DỰ ÁN WEBSCAN

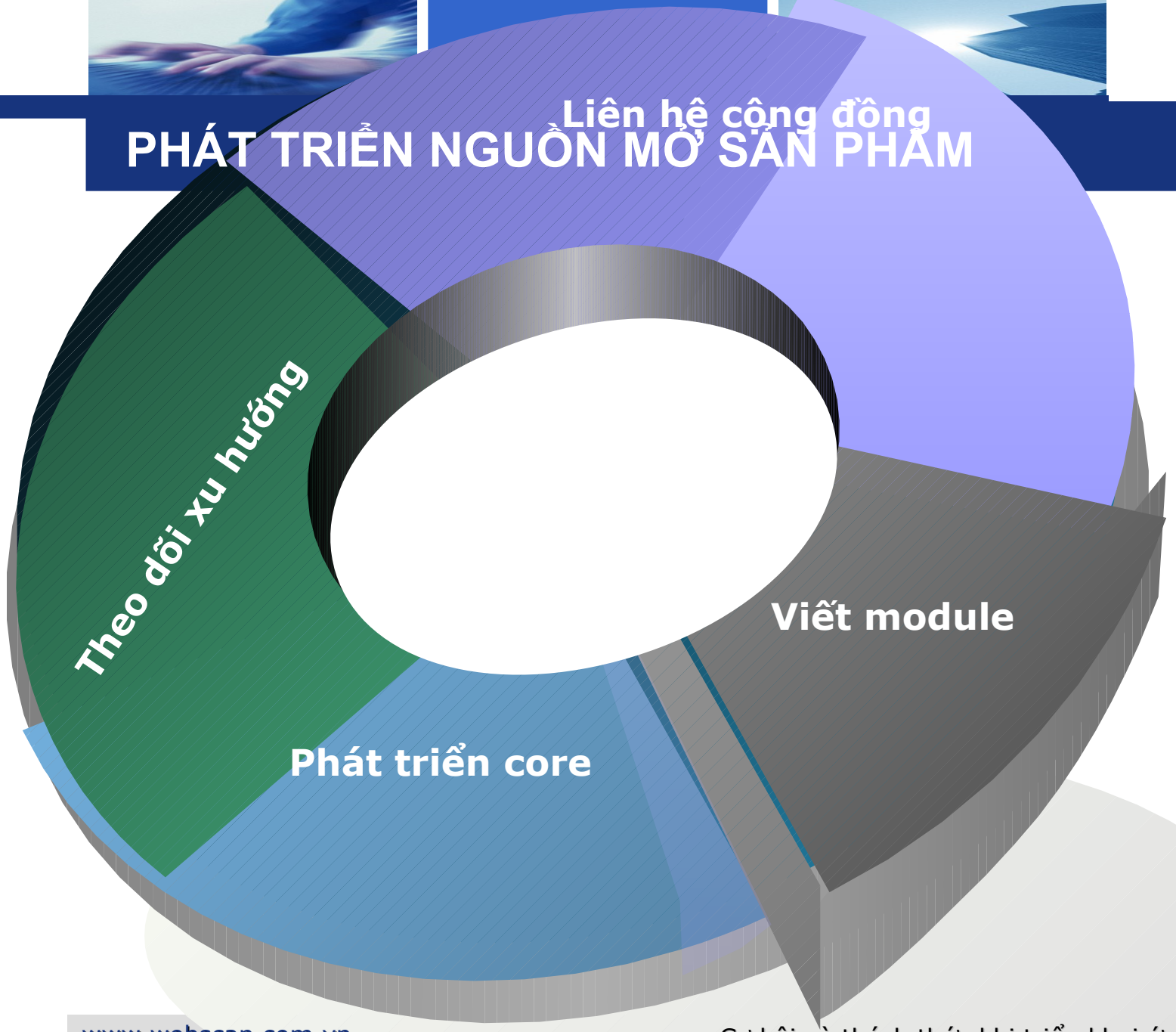
- Trong thời gian thử nghiệm sản phẩm, có khoảng 200 người sử dụng.
- Webscan (phiên bản 2.0) đã tiến hành kiểm tra gần 400 website thương mại điện tử và 150 website giao dịch trực tuyến.
- Trong 400 website thương mại điện tử đã phát hiện gần 9000 lỗ hỏng bảo mật, chủ yếu là lỗ hỏng SQL Injection và Cross Site Scripting.
- Trong 150 website giao dịch trực tuyến (sử dụng HTTPS) đã phát hiện gần 900 lỗ hỏng SSL/TLS, chủ yếu là kĩ thuật tấn công BEAST và SSL DoS.

PHÁT TRIỂN NGUỒN MỞ CHO SẢN PHẨM

PHÁT TRIỂN NGUỒN MỞ CHO SẢN PHẨM

Source Code	Triển khai lên máy chủ và public ra cộng đồng bằng kho mã nguồn SourceForge
Cơ sở dữ liệu lỗ hỏng	Đóng vai trò cực kì quan trọng trong việc đánh giá chất lượng của một sản phẩm bảo mật, mang tính phát triển lâu dài.
Hợp tác với cộng đồng	Đây là sản phẩm security nên việc hợp tác với cộng đồng chuyên về security (điển hình là HVA) phải được đưa lên hàng đầu và có kế hoạch lâu dài.

PHÁT TRIỂN NGUỒN MỞ SẢN PHẨM



PHÁT TRIỂN NGUỒN MỞ CHO SẢN PHẨM

THẾ MẠNH

1. Đội ngũ phát triển
2. Công ty Lạc Tiên hỗ trợ
3. Cộng đồng HVA hợp tác.

CƠ HỘI

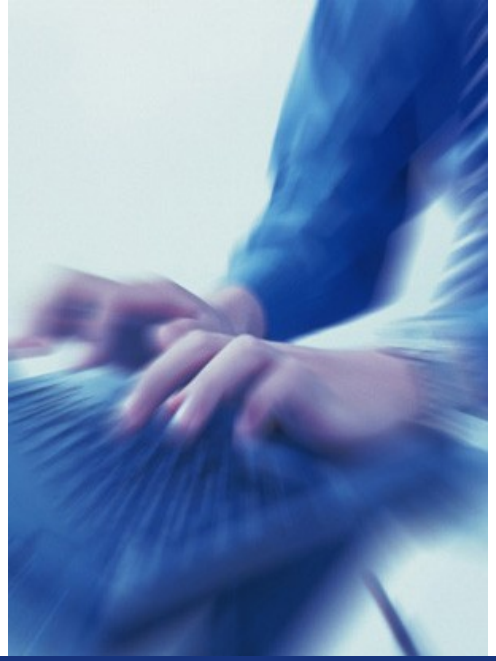
1. Quảng bá sản phẩm và kiến thức cho cộng đồng.
2. Nhu cầu về an toàn thông tin quốc gia đang rất cần những sản phẩm bảo mật do chính người Việt làm ra.
3. Vấn đề nguồn mở được khuyến khích phát triển.

THÁCH THỨC

Ngày càng có nhiều kĩ thuật tấn công mới được công bố, nên việc cập nhật CSDL phải lưu ư.

RỦI RO

1. Vấn đề về nhân lực
2. Vấn đề kinh phí triển khai



Lạc Tiên

www.webscan.com.vn

Thank You !

Link demo Project: http://www.webscan.com.vn