ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

ĐẶNG THỊ NGỌC TUYẾT

PHÂN TÍCH TỰ ĐỘNG CÁC WEBSITE ĐỂ PHÁT HIỆN LỖ HỔNG TIÊM NHIỄM SQL VÀ XSS

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Hà Nội - 2017

ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

ĐẶNG THỊ NGỌC TUYẾT

PHÂN TÍCH TỰ ĐỘNG CÁC WEBSITE ĐỂ PHÁT HIỆN LỖ HỔNG TIÊM NHIỄM SQL VÀ XSS

Ngành: Công nghệ thông tin

Chuyên ngành: Truyền dữ liệu và Mạng máy tính

Mã số:

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. NGUYỄN ĐẠI THỌ

Hà Nội - 2017

MỞ ĐẦU

Đặt vấn đề:

Hiện nay cùng với sự phát triển nhanh chóng của ứng dụng web thì vấn đề bảo mật ứng dụng web đang là lĩnh vực vô cùng nóng hổi nhằm đảm bảo an toàn cho tất cả người dùng. Ứng dụng web ngày nay dần trở thành mục tiêu tấn công phổ biến của tin tặc, các hình thức tấn công của các hacker cũng ngày càng tinh vi và phức tạp hơn. Trong các cuộc tấn công đó, lỗ hổng bị khai thác nhiều nhất là SQL Injection (chiếm 68% các cuộc tấn công lỗ hổng bảo mật web) và XSS (chiếm 61%).Trên Thế giới đã phát triển rất nhiều công cụ phát hiện và khai thác lỗ hổng bảo mật web như: Acunetix, SQLMap, Havij, BurpSuite, ZAP, XSSer, Nmap … Tuy nhiên, các phần mềm thường mất phí hoặc phiên bản miễn phí sẽ bị giới hạn nhiều tính năng, khó nâng cấp, bảo trì. Ngoài ra, các phần mềm chỉ thực hiện khai thác 01 lỗ hổng bảo mật chuyên biệt hoặc chỉ chú trọng phát hiện lỗ hổng bảo mật, chưa tập trung phần khai thác.

Mục tiêu nghiên cứu:

Luận văn lựa chọn đề tài nghiên cứu "*Phân tích tự động các Website để phát hiện lỗ hổng tiêm nhiễm SQL và XSS"* với mong muốn nghiên cứu cách thức khai thác lỗ hổng bảo mật website đồng thời xây dựng một công cụ hỗ trợ đắc lực trong quá trình kiểm tra lỗ hổng bảo mật đặc biệt có khả năng phát hiện và khai thác tốt lỗ hổng SQL Injection (SQLi) và XSS. Ngoài ra công cụ này còn bổ sung thêm một số tính năng như kiểm tra host tầng mạng, quét cổng, brute force tài khoản đăng nhập FTP và RDP, dò quét các file nhạy cảm, đường dẫn login của website... Công cụ này được xây dựng từ đầu nhằm mục đích có thể tùy ý xây dựng theo nhu cầu người dùng, nâng cấp phần mềm lúc cần thiết, đồng thời khắc phục những nhược điểm của các phần mềm scanner hiện thời, kiểm tra lỗ hổng bảo mật theo hình thức hộp đen, dễ dàng sử dụng.

Nội dung nghiên cứu:

- Nghiên cứu nguyên lý, cách thức hoạt động một số công cụ dò quét lỗ hổng bảo mật web hiện thời (SQL Map, Havij, Acunetix, Burp Suite...).
- Nghiên cứu phương pháp thu thập URL, trích xuất cấu trúc một website.
- Nghiên cứu phương pháp phát hiện lỗ hổng bảo mật SQLi, XSS.
- Nghiên cứu phương pháp khai thác lỗ hổng bảo mật SQLi, XSS.
- Nghiên cứu xử lý song song nhiều mục tiêu cùng lúc.
- Nghiên cứu phương pháp brute force tài khoản FTP, RDP.

Bố cục luận văn:

Chương I: Tổng quan về lỗ hổng bảo mật ứng dụng web, giới thiệu lỗ hổng SQLi và XSS

Giới thiệu tổng quan về các lỗ hổng bảo mật ứng dựng web, các hình thức tấn công lỗ hổng bảo mật SQLi, XSS và các phương pháp khai thác của từng loại tấn công, cách người quản trị, lập trình thực hiện để tránh bị hacker khai thác các lỗ hổng bảo mật trên.

Chương II: Khảo sát các phần mềm quét lỗ hổng ứng dụng web

Giới thiệu một số phần mềm mã nguồn mở, phần mềm thương mại dùng để dò quét các lỗ hổng bảo mật ứng dụng web tốt nhất hiện nay.

Chương III: Xây dựng phần mềm phân tích tự động Website phát hiện và khai thác lỗ hổng SQLi và XSS

Trình bày cách thức xây dựng công cụ tự động phát hiện và khai thác lỗ hổng SQLi và XSS. Từ các bước thực hiện bằng tay xây dựng mã nguồn tự động thực hiện khai thác, bypass các trường hợp cụ thể để có thể khai thác được những trang web có lỗ hổng bảo mật SQLi và XSS mà những phần mềm hiện tại không làm được.

Chương IV: Thử nghiệm và đánh giá kết quả

Thử nghiệm công cụ và đánh giá kết quả hoạt động chức năng thu thập dữ liệu, tự động phát hiện, khai thác lỗ hổng bảo mật SQLi và XSS; So sánh một cách tương đối với một số phần mềm khác.

CHƯƠNG I: TỔNG QUAN VỀ LỖ HỔNG BẢO MẬT WEB, GIỚI THIỆU LỖ HỔNG SQLI VÀ XSS

1.1. Lỗ hổng bảo mật ứng dụng web

Tổ chức OWASP đã thống kê 10 rủi ro an ninh cao nhất là: A1-Injection, A2-Broken Authentication and Session Management, A3-Cross-Site Scripting (XSS), A4-Insecure Direct Object References, A5-Security Misconfiguration, A6-Sensitive Data Exposure, A7-Missing Function Level Access Control; A8-Cross-Site Request Forgery (CSRF); A9-Using Known Vulnerable Components; A10-Unvalidated Redirects and Forwards.

1.2. Lỗ hổng bảo mật SQLi

1.2.1. Giới thiệu lỗ hổng SQLi

SQLi là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng trong việc kiểm tra dữ liệu nhập trong các ứng dụng web và các thông báo lỗi của hệ quản trị CSDL để tiêm các mã SQL vào dữ liệu đầu vào trước khi chuyển cho ứng dụng web xử lý và thi hành các câu lệnh SQL bất hợp pháp. Lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lí bằng các hệ quản trị CSDL như MySQL, SQL Server,Oracle, DB2, Sysbase. Công cụ dùng để tấn công là một trình duyệt web bất kì, chẳng hạn như Internet Explorer, Netscape, Lynx, Firefox,…

1.2.2. Phương pháp khai thác các loại SQLi

Nêu phương pháp khai thác SQLi với các dạng cơ sở dữ liệu MySQL, MS SQL Server, MS Access, PostgreSQL, Xpath SQL, Error based, Blind SQL, Bypass Filter.

1.2.3. Phương pháp phòng chống SQLi

1.3. Lỗ hổng bảo mật XSS

1.3.1. Giới thiệu lỗ hổng bảo mật XSS

XSS (Cross Site Scripting) là một kiểu tấn công cho phép hacker chèn những đoạn script độc hại (thường là javascript hoặc HTML) vào website và sẽ được thực thi trong trình duyệt của người dùng nhằm đánh cắp những thông tin quan trọng như Cookie, mật khẩu... XSS không tấn công vào máy chủ của hệ thống mà chủ yếu tấn công trên máy client của người dùng. Đây là một trong những kỹ thuật tấn công phổ biến nhất của các ứng dụng web và ngày càng nguy hiểm.

1.3.2. Các dạng tấn công XSS

XSS được chia làm 3 dạng chính: Persistent XSS, Non-Persistent XSS, DOM-based XSS. Chi tiết các dạng như sau:

1.3.3. Cách thức phòng chống lỗ hổng XSS

CHƯƠNG II: KHẢO SÁT CÁC PHẦN MỀM QUÉT LỖ HỔNG ỨNG DỤNG WEB

2.1. Tổng quan công cụ quét lỗ hổng bảo mật

2.1.1. Giới thiệu công cụ quét lỗ hổng bảo mật

Công cụ quét lỗ hổng bảo mật (scanner) là công cụ phát hiện, khai thác, đánh giá lỗ hổng bảo mật của hệ thống thông tin bao gồm máy tính, hệ thống mạng, hệ điều hành và ứng dụng phần mềm. Các lỗ hổng đó có thể xuất phát từ nhà cung cấp, người quản trị mạng, người dùng.

2.1.2. Phương thức hoạt động của công cụ quét lỗ hổng bảo mật

Quá trình dò quét lỗ hổng gồm 03 giai đoạn: cấu hình, crawling, scanning. Cấu hình bao gồm xác định các URL của ứng dụng web và các tham số đầu vào; Crawling thu thập đường dẫn con, xác định cấu trúc của trang web; Scanning là quá trình giả lập các thao tác mà hacker có thể làm để tấn công ứng dụng web, sau đó phân tích lỗi phản hồi. Với mỗi giai đoạn, mỗi công cụ sử dụng các phương pháp khác nhau do đó kết quả cũng khác nhau.

2.1.3. Phân loại

Các công cụ scanner được phân làm 02 dạng chính: network-based và host-based.

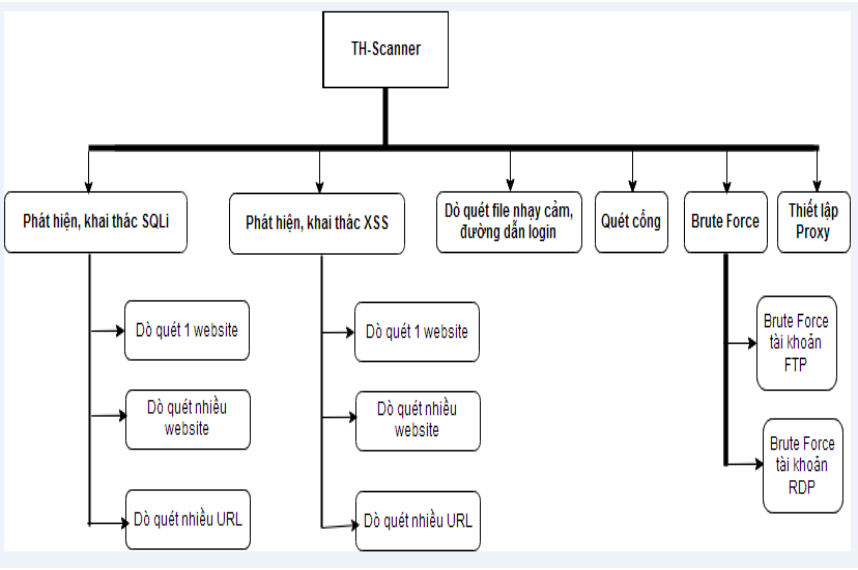
2.2 Giới thiệu một số công cụ dò quét lỗ hổng bảo mật web

Giới thiệu tính năng, đặc điểm một số công cụ dò quét lỗ hổng bảo mật web như: Acunetix Web Vulnerability Scanner, SQLMap, Burpsuite, Havij, ZAP, XSSer...

CHƯƠNG III. XÂY DỰNG PHẦN MỀM PHÂN TÍCH TỰ ĐỘNG WEBSITE, PHÁT HIỆN VÀ KHAI THÁC LỖ HỔNG BẢO MẬT SQLI VÀ XSS

Nhằm khắc phục những nhược điểm và tích hợp những tính năng của những phần mềm dò quét lỗ hổng bảo mật web hiện thời, đề tài chọn xây dựng công cụ tạm gọi tên là TH-Scanner.

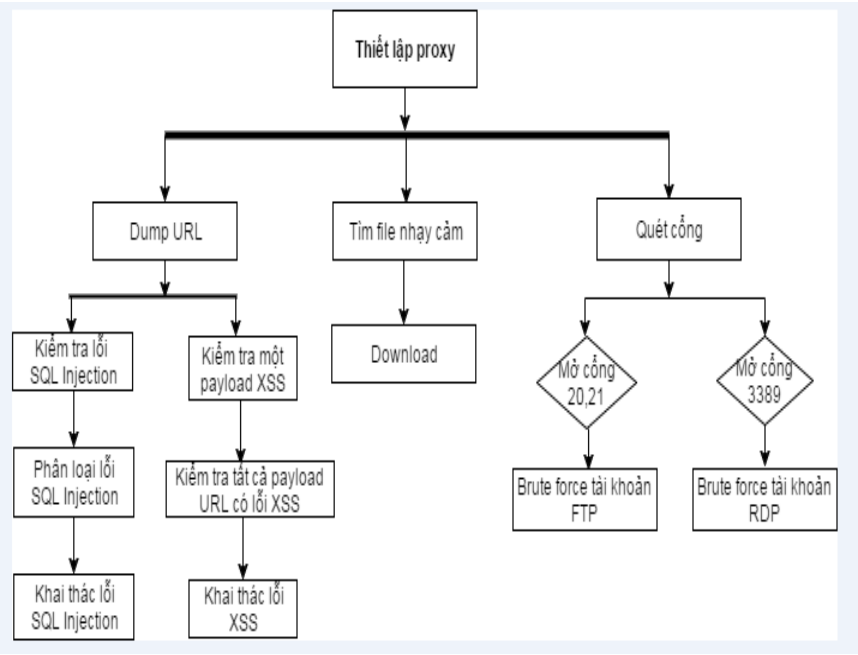
3.1. Sơ đồ phân rã chức năng:



Hình 1: Sơ đồ phân rã chức năng hệ thống

Phần mềm TH-Scanner gồm 05 mô-đun chính: phát hiện, khai thác SQLi; phát hiện, khai thác XSS; Mô-đun dò quét file nhạy cảm, đường dẫn login gồm các chức năng sau; quét cổng; brute-force tài khoản FTP và RDP.

3.2. Sơ đồ hoạt động



Hình 2: Sơ đồ hoạt động hệ thống

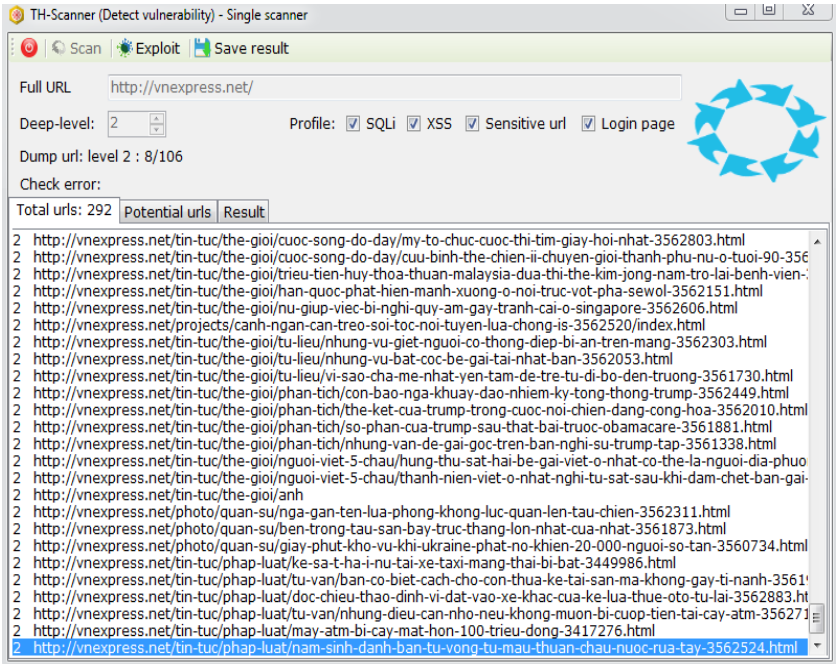
3.3. Các thuật toán chính:

Giới thiệu một số thuật toán như : dum URL, phát hiện lỗ hổng SQLi, phát hiện lỗ hổng XSS, khai thác lỗ hổng SQLi, khai thác lỗ hổng XSS, quét cổng, bruteforce tài khoản FTP

3.4. Xây dựng các mô-đun chức năng:

3.4.1. Mô-đun dump URL:

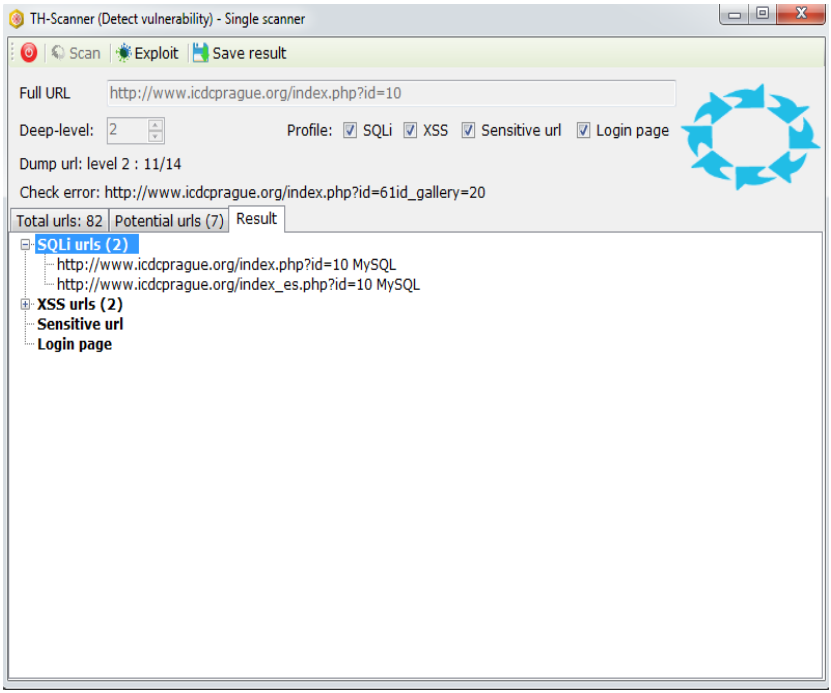
- Chức năng: Lấy tất cả các URL con của một URL cha theo số cấp quét định sẵn, lọc ra các URL tiềm năng có khả năng bị lỗi SQLi và XSS.



Hình 3: Giao diện mô-đun Dump URL

3.4.2. Mô-đun phát hiện lỗ hổng SQLi

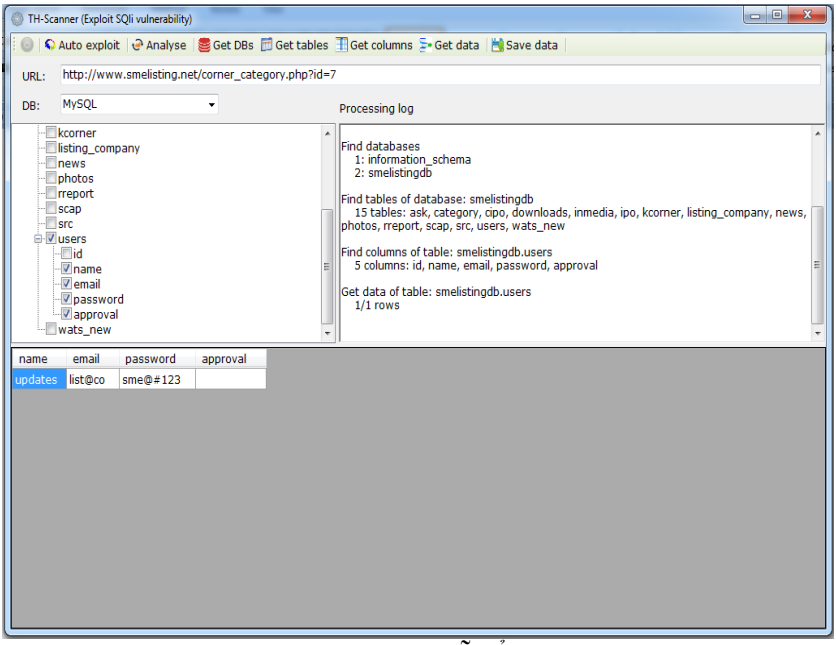
- Chức năng: Kiểm tra tất cả URL trong danh sách tiềm năng có lỗi SQLi hay không, nếu có thực hiện phân loại lỗi



Hình 4: Giao diện mô-đun phát hiện lỗ hổng SQLi

3.4.3. Mô-đun khai thác lỗ hổng SQLi

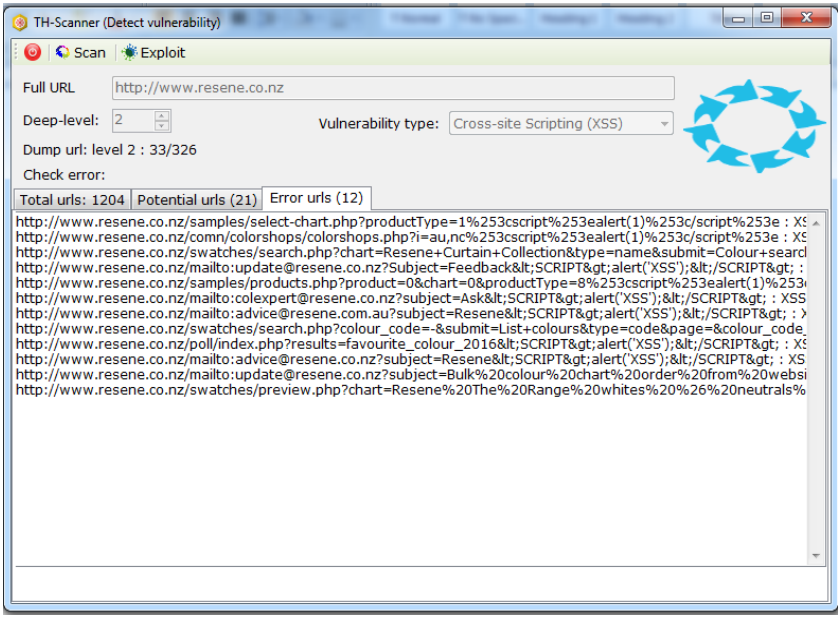
-Chức năng: Phân loại lỗi SQLi, xác định Database; Lấy tên CSDL; Lấy tên tất cả các bảng trong CSDL; Lấy tên tất cả các cột trong một bảng; Lấy toàn bộ thông tin của một bảng.



Hình 5: Giao diện mô-đun khai thác lỗ hổng SQLi

3.4.4. Mô-đun phát hiện lỗ hổng XSS

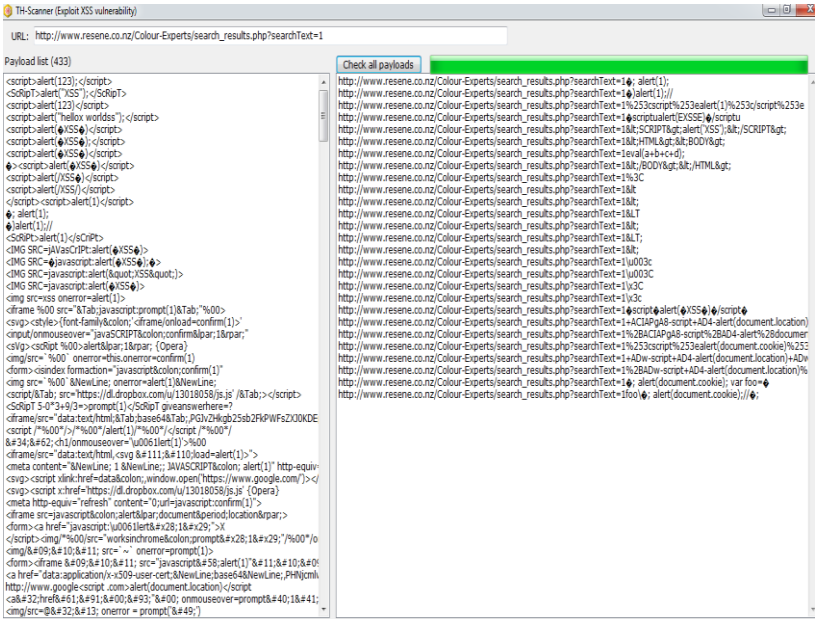
- Chức năng: Kiểm tra tất cả URL có lỗi XSS hay không.



Hình 6: Giao diện mô-đun phát hiện lỗ hổng XSS

3.4.5. Mô-đun khai thác lỗ hổng XSS

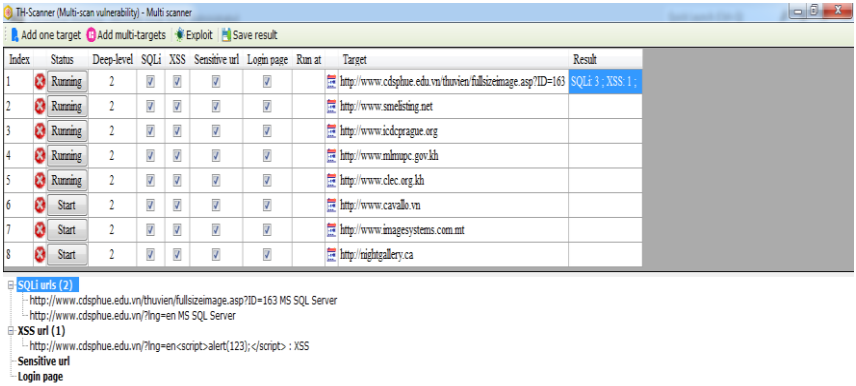
- Chức năng: Kiểm tra tất cả payload XSS mà URL có lỗi, thực hiện khai thác lỗ hổng XSS với từng payload.



Hình 7: Giao diện mô-đun khai thác lỗ hổng XSS

3.4.6. Mô-đun dò quét lỗ hổng nhiều website

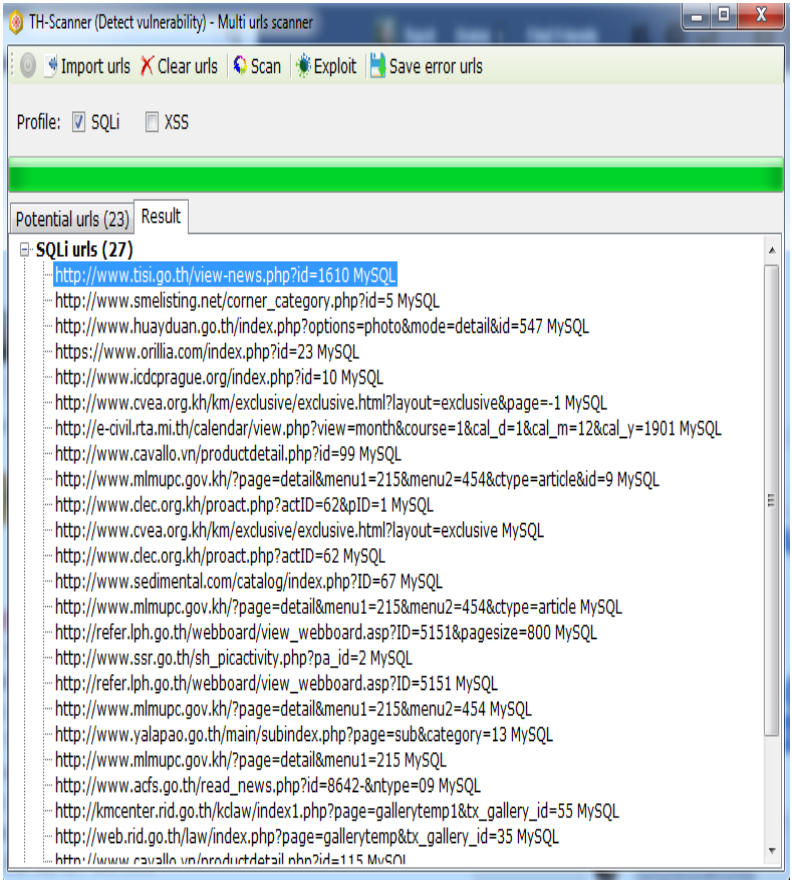
- Chức năng: Thực hiện đồng thời việc dumpURL, dò quét lỗ hổng và thực hiện khai thác với nhiều website cùng một lúc. Các lỗ hổng mô-đun thực hiện dò quét bao gồm: SQLi; XSS; Tìm các file nhạy cảm; Tìm đường dẫn login.



Hình 8: Giao diện mô-đun dò quét lỗ hổng nhiều website

3.4.7. Mô-đun dò quét lỗ hổng nhiều URL

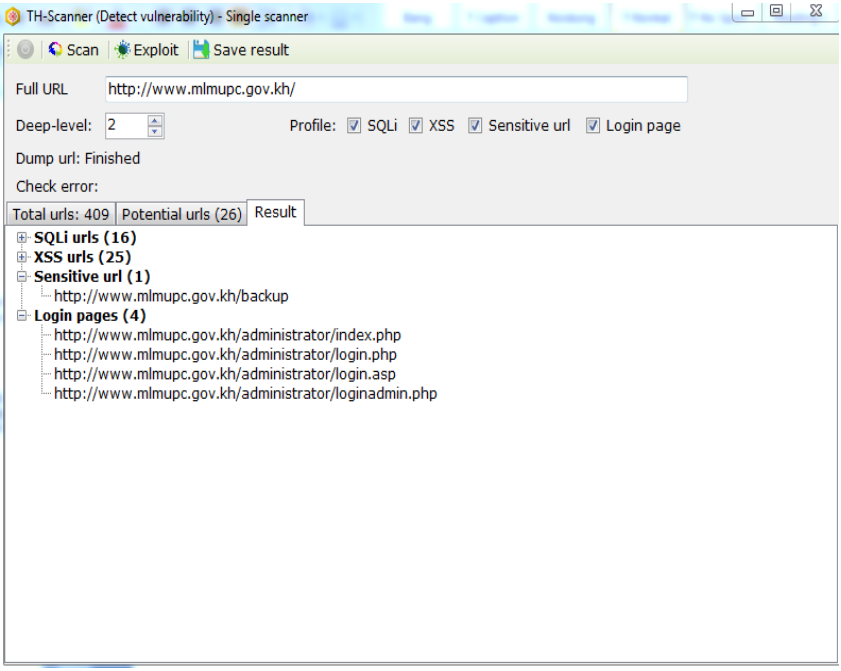
- Chức năng: Thực hiện đồng thời việc dò quét lỗ hổng, thực hiện khai thác lỗ hổng nhiều URL cùng một lúc. Các lỗ hổng mô-đun thực hiện dò quét bao gồm: SQLi và XSS



Hình 9: Giao diện mô-đun dò quét lỗ hổng nhiều URL

3.4.8. Mô-đun phát hiện file nhạy cảm

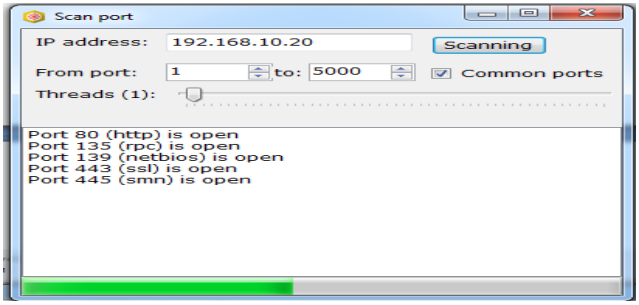
- Chức năng: Dò tìm các file nhạy cảm, có giá trị quan trọng nhưng do lỗi cấu hình người quản trị sơ hở để lộ.



Hình 10: Giao diện mô-đun phát hiện file nhạy cảm

3.4.9. Mô-đun quét cổng

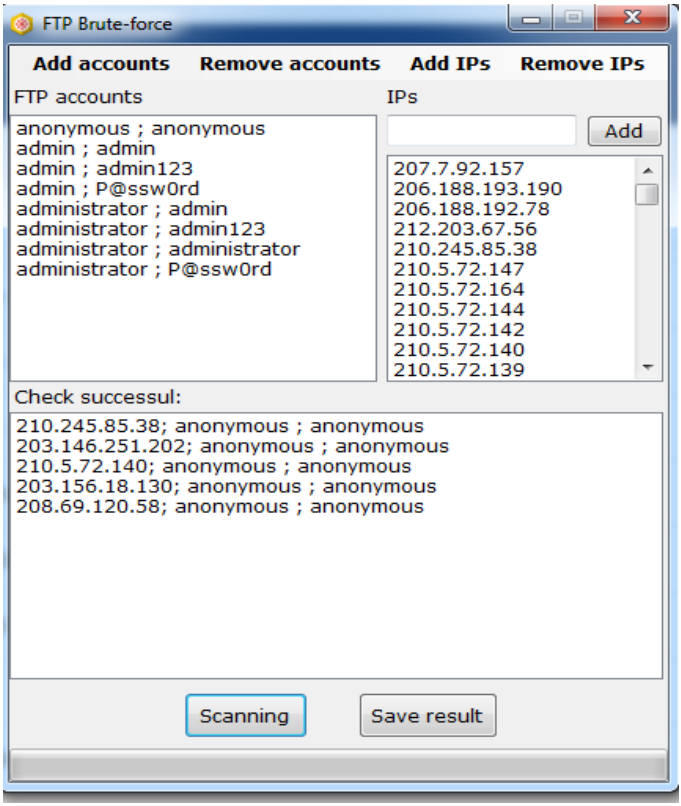
- Chức năng: Tìm tất cả cổng mở của một server.



Hình 11: Giao diện mô-đun quét cổng

3.4.10. Mô-đun brute force tài khoản đăng nhập dịch vụ FTP

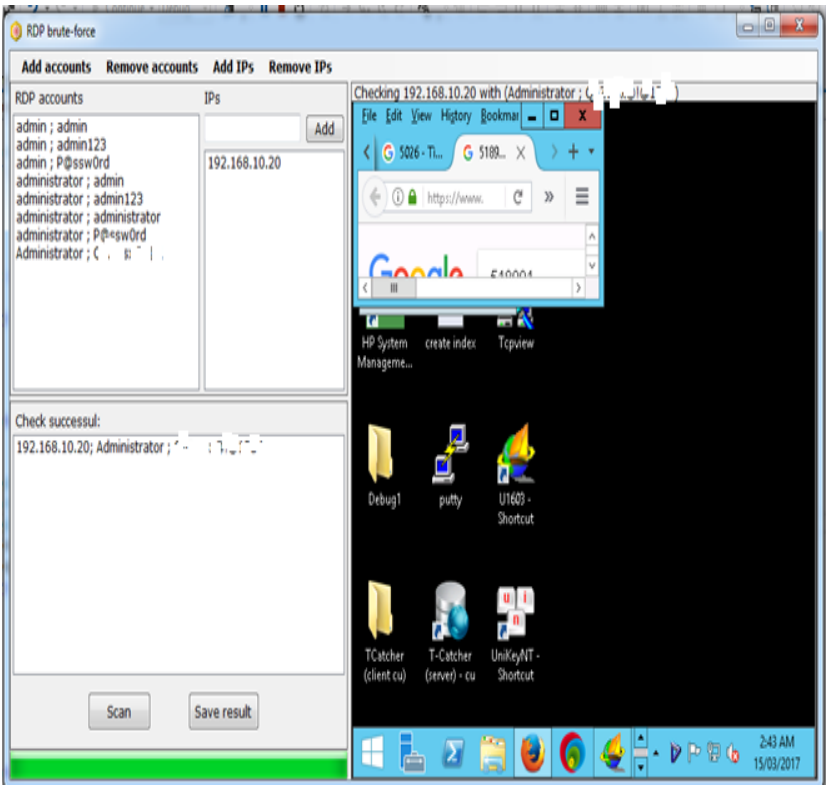
- Chức năng: Đoán tài khoản đăng nhập dịch vụ FTP của danh sách IP các server sử dụng từ điển các username và password thường sử dụng.



Hình 12: Giao diện mô-đun brute force FTP

3.4.11. Mô-đun brute force tài khoản đăng nhập dịch vụ RDP

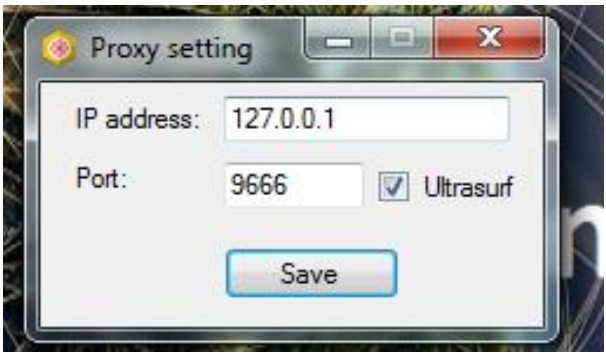
- Chức năng: Đoán tài khoản đăng nhập dịch vụ RDP của danh sách IP các server sử dụng từ điển các username và password thường sử dụng.



Hình 13: Giao diện mô-đun brute force RDP

3.4.12. Mô-đun thiết lập Proxy

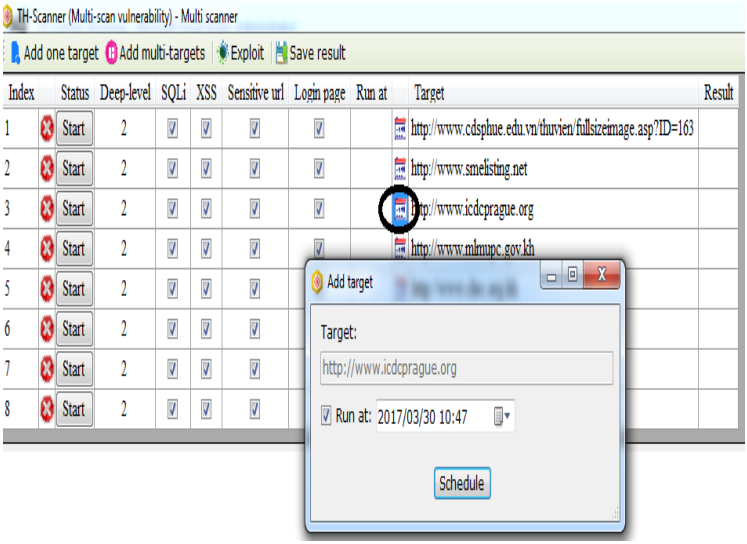
- Chức năng: Thiết lập Proxy, sử dụng UltraSurf, kiểm tra kết nối.



Hình 14: Giao diện mô-đun thiết lập Proxy

3.4.13. Mô-đun lập lịch

- Chức năng: Lập lịch chương trình tự động quét URL, phát hiện và khai thác lỗ hổng, sau đó lưu kết quả vào file text tránh tình trạng thực hiện dò quét lỗ hổng một mục tiêu nhiều lần. Sử dụng control timer, 30s sẽ kiểm tra một lần những mục tiêu nào có lập lịch và thời gian lập lịch bằng thời gian hiện tại thì chương trình tự động kích hoạt chức năng dò quét lỗ hổng.



Hình 15: Giao diện mô-đun lập lịch

CHƯƠNG IV. THỬ NGHIỆM VÀ ĐÁNH GIÁ KẾT QUẢ

4.1. Thử nghiệm công cụ TH_Scanner

4.1.1. Thử nghiệm phát hiện và khai thác lỗ hổng SQLi

Công cụ có thể phát hiện và khai thác lỗ hổng SQLi với các dạng SQLi với CSDL MySQL, SQL Server, Error Based, Blind SQL. Thực hiện bypass việc lọc các ký tự, chặn các hàm do người lập trình thiết lập: bypass lỗi 403, 404, 406, 500, thực hiện một số bypass nâng cao.

4.1.2. Thử nghiệm phát hiện và khai thác lỗ hổng XSS

TH_Scanner có thể phát hiện và khai thác lỗ hổng XSS với 433 payload. Ngoài thực hiện việc hiển thị các thông điệp, phần mềm còn thực hiện chèn các link độc hại,

lấy cookie, session, key logger, bypass việc lọc các ký tự meta data do người lập trình thiết lập.

4.1.3. Thử nghiệm khai thác các lỗ hổng bảo mật khác

- Phát hiện file dữ liệu nhạy cảm của website: Có khả năng quét và phát hiện 31 loại file dữ liệu nhạy cảm gồm: pub.zip, pub.rar, public_html.zip, public_html.rar, html.zip, html.rar, backup …

- Tiến hành xử lý song song nhiều mục tiêu, thực hiện crawler, phát hiện và khai thác đồng thời 02 lỗ hổng SQLi và XSS. Qua thử nghiệm với máy tính cấu hình sử dụng bộ xử lý Intel Core i5-6200U CPU, RAM 8GB có thể thực hiện đồng thời 53 mục tiêu, TH_Scanner chạy hơn 200 threads chiếm 6% CPU.

4.1.4. Nhận xét

TH_Scanner có thể phát hiện và khai thác tốt với các lỗ hổng SQLi dạng MySQL, SQL Server, một số dạng bypass cơ bản và nâng cao, có thể khai thác những website có độ bảo mật trung bình của cơ quan chính phủ, tổ chức giáo dục, tuy nhiên vẫn chưa khai thác được hết với tất cả các dạng CSDL, chưa bypass nhiều dạng lọc nâng cao do người lập trình cấu hình.

Với lỗ hổng XSS, có khả năng phát hiện tốt URL có lỗ hổng XSS và khai thác một số payload với XSS. Với một số URL thực hiện lọc ký tự metadata nâng cao chưa thực hiện bypass tốt.

Với chức năng brute force tài khoản đăng nhập FTP và RDP bộ từ điển đoán mật khẩu còn ít do đó mới chỉ thực hiện brute force được với một số mật khẩu đơn giản.

4.2. So sánh với các công cụ Scanner khác

4.2.1. So sánh tính năng:

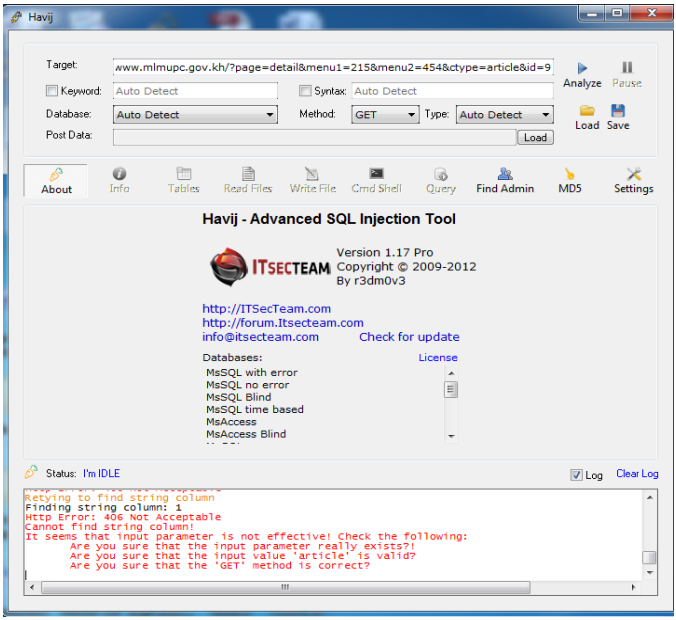
Tính năng	Crawler	Phát hiện, khai thác SQLi	Phát hiện, khai thác XSS	Lập lịch chạy nhiều website cùng lúc	Brute force FTP	Brute force RDP	Quét cổng	Thiết lập Proxy	Đánh chặn	Tự động nhận diện và nhập thông tin vào webform
TH_Scanner	Có	Có	Có	Có	Có	Có	Có	Có	Không	Không
Acunetix	Có	Có	Có	Có	Không	Không	Có	Có	Không	Có
SQLMap	Không	Có	Không	Không	Không	Không	Có	Không	Không	Có
BurpSuite	Có	Có	Có	Có	Không	Không	Có	Có	Có	Có
Havij	Không	Có	Không	Không	Không	Không	Không	Không	Không	Không
XSSer	Có	Không	Có	Không	Không	Không	Có	Có	Không	Không

Hình 16: So sánh TH_Scanner và các công cụ Scanner khác

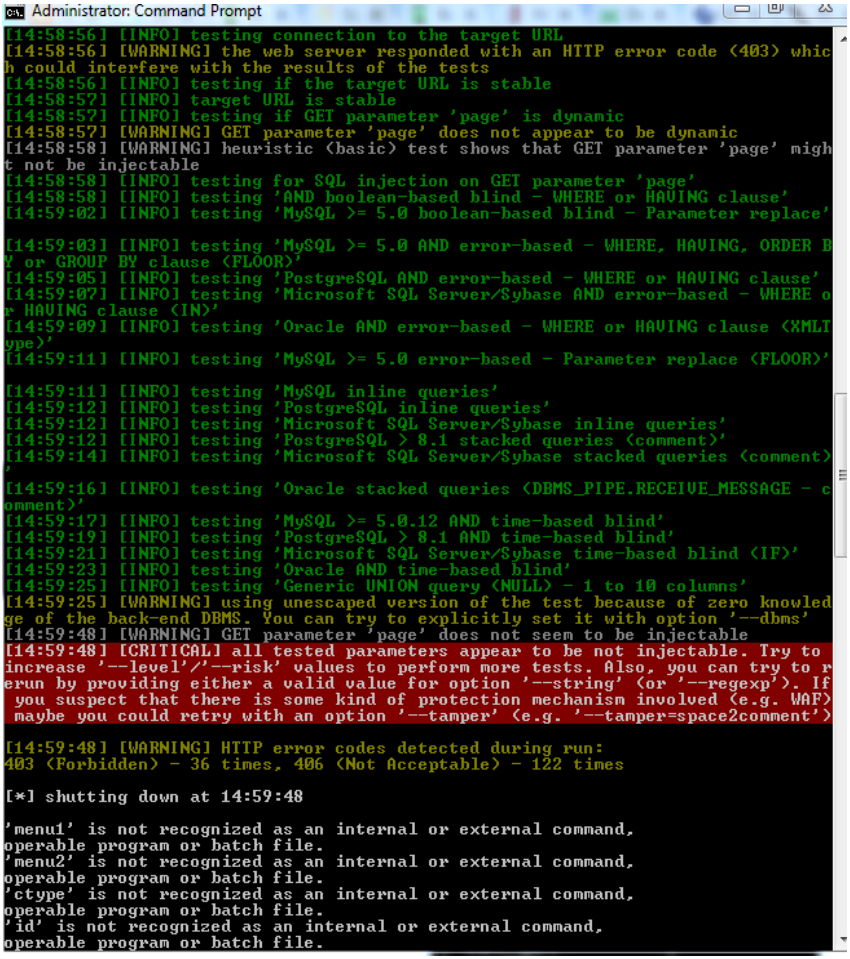
4.2.2. So sánh hiệu quả:

** Danh sách một số website mà TH_Scanner có thể phát hiện và khai thác thành công trong khi những phần mềm Scanner khác không làm được.*

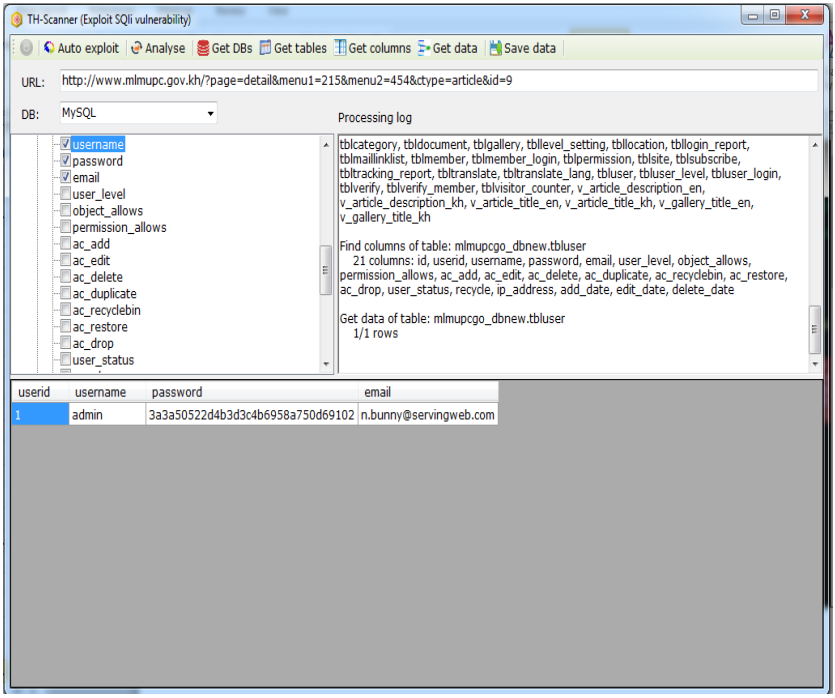
Với URL:
http://www.mlmupc.gov.kh/?page=detail&menu1=215&menu2=454&ctype=article&id=9



Hình 17: Sử dụng công cụ Havij



Hình 18: Sử dụng công cụ SQL Map



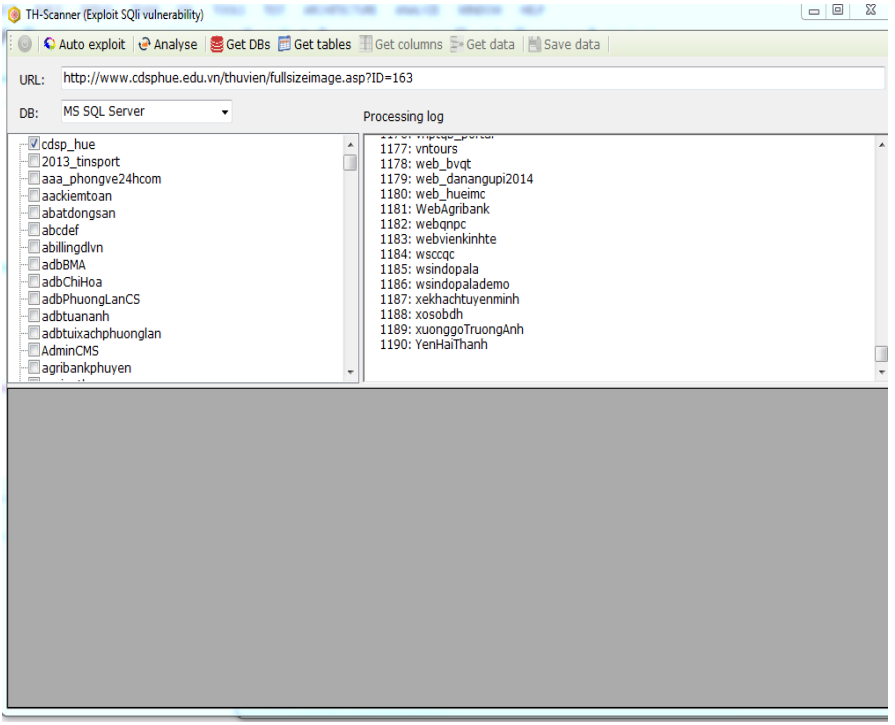
Hình 19: Sử dụng TH_Scanner

** TH_Scanner có thể lấy được toàn bộ tên các CSDL với SQL Server:*

Sử dụng câu lệnh:

```
http://ww.site.com/index.php?id=1 and 1=convert(int,(SELECT top 1 substring((STUFF((SELECT name as temp FROM Sys.Databases FOR XML PATH('')),1,0,'')),-100,4000) as csdl FROM Sys.Databases ))--+
```

Với website http://www.cdsphue.edu.vn/ có thể lấy được toàn bộ 1190 CSDL đặt trên server.



Hình 20: TH_Scanner lấy được toàn bộ CSDL trên server

4.2.3. Nhận xét:

Về tính năng, TH_Scanner bổ sung thêm một số tính năng mà các công cụ Scanner khác ít có như: Khai thác đồng thời cả lỗi SQLi, XSS; lập lịch chạy nhiều website cùng lúc, Brute Force FTP, Brute Fore RDP. Tuy nhiên, TH_Scannner còn thiếu nhiều tính năng so với các phần mềm khác như: tự động nhận diện và nhập thông tin vào webform, khai thác Google Hacking Database, thực hiện lệnh, truy cập file hệ thống, giải mã mật khẩu tài khoản, cài mã độc, tải dữ liệu về server hoặc gửi dữ liệu về email…

Về tính hiệu quả, TH_Scanner có thể khai thác một số website có mức độ bảo mật trung bình, bypass một số hàm lọc do người lập trình thiết lập, tuy nhiên còn nhiều website mà TH_Scanner không phát hiện và khai thác được trong khi các phần mềm Scanner khác làm được.

KẾT LUẬN

Qua một thời gian nghiên cứu, được sự giúp đỡ tận tình của giáo viên hướng dẫn, các đồng nghiệp, gia đình, đến nay đề tài "*Phân tích tự động các Website để phát hiện lỗ hổng tiêm nhiễm SQL và XSS*" cơ bản đã đạt được các mục tiêu đề ra:

+ Nghiên cứu các lỗ hổng bảo mật ứng dụng web, phương pháp khai thác lỗ hổng bảo mật SQLi, XSS với từng loại cơ sở dữ liệu, cách thức bypass việc lọc các ký tự đầu vào do người lập trình thiết lập.

+ Xây dựng công cụ có các chức năng: crawler, phát hiện và khai thác lỗ hổng bảo mật SQLi và XSS, dò quét các file nhạy cảm, đường dẫn đăng nhập, brute force tài khoản đăng nhập FTP và RDP.

+ Tiến hành xử lý song song, lập lịch có thể thực hiện dò quét nhiều mục tiêu đồng thời trên cả 05 chức năng là: crawler, dò quét SQLi, XSS, tìm file nhạy cảm, đường dẫn đăng nhập.

+ Công cụ này có khả năng phát hiện và khai thác tốt một số mục tiêu mà các phần mềm scanner hiện tại không thực hiện được.

Hướng phát triển:

Trong thời gian tới, tiếp tục hoàn thiện các chức năng hệ thống như: nghiên cứu bổ sung thêm các giải pháp bypass nâng cao trong khai thác lỗ hổng SQLi; giải pháp bypass ký tự metadata trong khai thác XSS, xây dựng bộ từ điển tương đối đầy đủ brute force tài khoản FTP, RDP; thử nghiệm với nhiều website đầu vào để có thể khai thác nhiều dạng SQLi và XSS nhất. Ngoài ra, bổ sung thêm một số tính năng mới như crack mật khẩu, cài mã độc lên server, truy

cập file hệ thống…, phát triển công cụ thành hệ thống kiểm tra lỗ hổng bảo mật web tương đối hoàn thiện.

TÀI LIỆU THAM KHẢO

A. Tài liệu Tiếng Việt:

[1] Lê Đình Duy (2013), Tấn công kiểu SQL injection-Tác hại và phòng tránh, Khoa CNTT-Trường ĐH Khoa Học Tự Nhiên TP.HCM.

[2] Võ Đỗ Thắng (2013), Tấn công và phòng thủ cho ứng dụng Web, Trung tâm An ninh mạng Athena

B. Tài liệu Tiếng Anh:

[3] Lwin Khin Shar, Hee Beng Kuan Tan (2012), Mining Input Sanitization Patterns for Predicting SQL Injection and Cross Site Scripting Vulnerabilities.

[4] Dennis Appelt, Cu Duy Nguyen, Lionel C. Briand, Nadia Alshahwan (2014), Automated Testing for SQL Injection Vulnerabilities: An Input Mutation Approach.

[5] Hossain Shahriar, Mohammad Zulkernine (2008), MUSIC: Mutation-based SQL Injection Vulnerability Checking

[6] Hanqing Wu, Liz Zhao (2015), Web Security: A WhiteHat Perspective. Auerbach Publications.

[7] Dafydd Stuttard (2011), Marcus Pinto, the Web Applicaion Hacker's Handbook: Finding and Exloiting Security Flaws, Second Edition.

[8] Michael Martin, Monica S. Lam (2011), Automatic Generation of XSS and SQL Injection Attacks with Goal-Directed Model Checking.

[9] Adam Kiezun, Philip J. Guo, Karthick Jayaraman, Michael D. Ernst (2009), Automatic Creation of SQL Injection and Cross-Site Scripting Attacks.

[10] Stefan Kals, Engin Kirda, Christopher Kruegel, and Nenad Jovanovic (2006), SecuBat: A Web Vulnerability Scanner.

C. Trang web

[11] https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)#Detection_Techniques

[12] http://gh0stsec.blogspot.com/2016/02/attack-sql-injection-part-1.html

[13]https://securityforall.wordpress.com/2012/05/30/sql-injection-tutorials-huong-dan-day-du-ve-sql-injection/

[14] https://www.owasp.org/index.php/SQL_Injection_Bypassing_WAF

[15]https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)

[16] http://securityidiots.com/Web-Pentest/SQL-Injection

[17] http://ctf.ist-vnisa.org.vn/web/top-10-owasp.html

[18] https://www.slideshare.net/sbc-vn/scb-2013-owasp-top-10-2013

[19] https://www.slideshare.net/sbc-vn/tnh-hnh-antt-vit-nam-l-cng-ph-cmc-infosec

[20] https://www.infosec.gov.hk/english/technical/files/vulnerability.pdf

[21] http://antoanthongtin.vn/Detail.aspx?NewsID=8770130c-2615-4621-a534-e877bb81d4ad&CatID=838ca04c-c317-484d-a461-00b464748b71.