BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG TP.HCM

KHOA: HỆ THỐNG THÔNG TIN VÀ VIỄN THÁM

ĐỒ ÁN MÔN HỌC

MÔN: AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN

NGHIÊN CỨU KĨ THUẬT ĐIỀU TRA PHÂN TÍCH TẤN CÔNG WEB (WEB FORENSIC)

Giảng viên hướng dẫn: **ThS. Phạm Trọng Huynh**

Sinh viên thực hiện: **Nguyễn Lê Quỳnh Anh** **MSSV: 0850080059**

Nguyễn Lam **MSSV: 0850080081**

Nguyễn Trường Thịnh **MSSV: 0850080105**

Lớp**:** **08_ĐH_CNPM**

Khoá**:** **08**

TP. Hồ Chí Minh, tháng 05 năm 2023

BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG TP.HCM

KHOA: HỆ THỐNG THÔNG TIN VÀ VIỄN THÁM

ĐỒ ÁN MÔN HỌC

MÔN: AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN

NGHIÊN CỨU KĨ THUẬT ĐIỀU TRA PHÂN TÍCH TẤN CÔNG WEB (WEB FORENSIC)

Giảng viên hướng dẫn: **ThS. Phạm Trọng Huynh**

Sinh viên thực hiện: **Nguyễn Lê Quỳnh Anh** **MSSV: 0850080059**

Nguyễn Lam **MSSV: 0850080081**

Nguyễn Trường Thịnh **MSSV: 0850080105**

Lớp**:** **08_ĐH_CNPM**

Khoá**:** **08**

TP. Hồ Chí Minh, tháng 05 năm 2023

LỜI MỞ ĐẦU

Với sự phát triển không ngừng của công nghệ 4.0, môi trường Internet ngày càng khẳng định vị trí của mình. Tuy nhiên, cùng với đó, các nguy cơ trên mạng cũng ngày càng tăng nhất là trong thời kì dịch bệnh diễn biến phức tạp, hệ thống làm việc và học tập trực tuyến đang được triển khai rộng rãi. Các cuộc tấn công mạng đang diễn ra từng ngày, từng giờ với số vụ và phương thức tấn công gia tăng với tốc độ đáng kinh ngạc, chỉ với một số kỹ thuật tấn công mạng, tin tặc có thể thâm nhập và đánh cắp dữ liệu quan trọng của công ty.

Chính vì vậy, việc nghiên cứu biện pháp ứng phó trước, trong và sau sự cố là đặc biệt quan trọng, nhóm chúng em đã chọn đề tài "Điều tra, phân tích tấn công Web (Web Forensic)". Trong phạm vi đề tài này, chúng ta cùng tìm hiểu về các biện pháp điều tra, phân tích tấn công lên ứng dụng web để có thể giảm thiểu đến mức thấp nhất những thiệt hại mà tin tặc để lại cũng như có các biện pháp ứng phó phù hợp trong tương lai.

Do vốn thời gian hạn chế nên đề tài còn nhiều sai sót, chúng em rất mong nhận được ý kiến góp ý từ thầy cô và các bạn.

Chúng em xin chân thành cảm ơn!

LỜI CẢM ƠN

Trong suốt quá trình học tập và hoàn thành đồ án này, chúng em đã nhận được rất nhiều sự hướng dẫn, giúp đỡ quý báu của các thầy cô giáo bộ môn, ban giám hiệu, gia đình và bạn bè.

Với lòng kính trọng và biết ơn sâu sắc chúng em xin được bày tỏ lời cảm ơn chân thành tới: Ban giám hiệu, Phòng đào tạo trường Đại học Tài Nguyên và Môi Trường đã tạo mọi điều kiện thuận lợi giúp đỡ chúng em trong quá trình học tập và hoàn thành đồ án này. Cảm ơn thầy Phạm Trọng Huynh, giảng viên bộ môn An toàn và bảo mật hệ thống thông tin và cũng là người thầy kính mến đã đã tận tình chỉ dạy những kiến thức bổ ích mà thầy đã mang đến cho chúng em, hết lòng giúp đỡ, dạy bảo, động viên chúng em trong suốt quá trình học tập và hoàn thành bài đồ án môn An toàn và bảo mật hệ thống thông tin.

Mặc dù chúng em đã có nhiều cố gắng cũng như nỗ lực bằng tất cả sự nhiệt tình và năng lực của mình để hoàn thiện bài tiểu luận, tuy nhiên vẫn khó tránh khỏi những thiếu sót, rất mong nhận được những đóng góp quý báu của thầy.

Một lần nữa chúng em xin chân thành cảm ơn, chúc thầy sức khỏe và thành đạt và mong thầy giữ mãi lửa nhiệt huyết trong công việc để những lứa học sinh sau có được những trải nghiệm tốt trong môn học.

Chúng em xin chân thành cảm ơn!

NHẬN XÉT

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Điểm

MỤC LỤC

DANH MỤC HÌNH

CHƯƠNG 1: TỔNG QUAN TÀI LIỆU

1.1. Tổng quan về đề tài:

1.1.1. Lý do chọn đề tài:

Ngày nay, với sự phát triển mạnh mẽ của Công nghệ Thông tin, việc sử dụng thông tin trên mạng Internet ngày càng được mở rộng và hiệu quả trên tất cả các ngành nghề, các lĩnh vực. Tuy nhiên, bên cạnh đó người sử dụng cũng phải đối mặt với những nguy cơ mất mát, rò rỉ thông tin, bị xâm hại các quyền riêng tư khi truy cập mạng. Đây là một trong những lý do khiến người sử dụng lo ngại, đặc biệt là các cơ quan nhà nước.

"Tấn công – Phòng thủ" trên mạng Internet là một trong những bài toán cần phải được đặt ra hàng đầu trong lĩnh vực An ninh Quốc phòng ngày nay. Vì vậy, em đã chọn đề tài: "ĐIỀU TRA, PHÂN TÍCH TẤN CÔNG WEB" cho đồ án môn học của mình.

1.1.2. Phạm vi nghiên cứu

Nghiên cứu điều tra phân tích tấn công web cho người dùng khi truy cập mạng.

1.1.3. Đối tượng

Tất cả mọi người truy cập vào Internet.

- **Kỹ thuật công nghệ:**

Các phương án phòng thủ: SQL Injection, Session Hiịacking, Cross Site Scripting (XSS)

1.1.4. Tính thực tiễn

Chiến tranh thông tin có quy mô rất lớn, nhằm vào nhiều lĩnh vực, khía cạnh, có phạm vi ảnh hưởng sâu rộng. Trong đề tài này, em tập trung phân tích các cách thức tấn công web. Nghiên cứu xây dựng thử nghiệm một công cụ trinh sát, tấn công và phòng thủ trên mạng.

1.1.5. Mục tiêu đề tài

- Tìm hiểu các kĩ thuật tấn công Web.
- Tìm hiểu điều tra số và điều tra tấn công Web.
- Tìm hiểu về kĩ thuật điều tra và phân tích phía người dùng.
- Tìm hiểu về kĩ thuật điều tra và phân tích phía máy chủ.
- Tìm hiểu về kĩ thuật phân tích tập nhật kí.
- Xây dựng công cụ phân tích tập nhật kí tự động để phát hiện tấn công.

CHƯƠNG 2: CƠ SỞ LÍ THUYẾT

2.1. TỔNG QUAN VỀ ĐIỀU TRA MẠNG VÀ THU THẬP CHỨNG CỨ

2.1.1. Khái niệm điều tra mạng

2.1.1.1. Khái niệm điều tra số

Điều tra số (đôi khi còn gọi là Khoa học điều tra số) là một nhánh của ngành Khoa học điều tra đề cập đến việc phục hồi và điều tra các tài liệu tìm thấy trong các thiết bị kỹ thuật số, thường có liên quan đến tội phạm máy tính. Thuật ngữ điều tra số ban đầu được sử dụng tương đương với điều tra máy tính nhưng sau đó được mở rộng để bao quát toàn bộ việc điều tra của tất cả các thiết bị có khả năng lưu trữ dữ liệu số. Điều tra số có thể được định nghĩa là việc sử dụng các phương pháp, công cụ kỹ thuật khoa học đã được chứng minh để bảo quản, thu thập, xác nhận, chứng thực, phân tích, giải thích, lập báo cáo và trình bày lại những thông tin thực tế từ các nguồn kỹ thuật số với mục đích tạo điều kiện hoặc thúc đẩy việc tái hiện lại các sự kiện nhằm tìm ra hành vi phạm tội hay hỗ trợ cho việc dự đoán các hoạt động trái phép gây gián đoạn quá trình làm việc của hệ thống.

Điều tra số gồm 3 giai đoạn: thu thập thông tin, phân tích, báo cáo.

2.1.1.2. Phân loại điều tra số

Điều tra số là một lĩnh vực liên quan đến việc phục hồi và điều tra các chứng cứ số được tìm thấy trong các thiết bị kỹ thuật số, được phân chia thành 3 loại là: điều tra máy tính, điều tra mạng và điều tra thiết bị di động. Trong đó, điều tra mạng (Network Forensics) tập trung vào việc chặn bắt, sao lưu và phân tích lưu lượng mạng nhằm phục vụ điều tra trong công tác phòng chống tội phạm mạng.

2.1.1.3. Điều tra mạng

Không giống các loại hình khác của điều tra số, điều tra mạng xử lý những thông tin dễ thay đổi và biến động, khó dự đoán. Lưu lượng mạng được truyền đi và sau đó bị mất, do đó việc điều tra được diễn ra rất linh hoạt, chủ động. Các điều tra viên chỉ có thể dựa vào thông tin từ các thiết bị an toàn như bộ lọc gói, tường lửa, hệ thống phát hiện xâm nhập đã được triển khai để dự đoán hành vi vi phạm. Các kỹ năng, kỹ thuật cần thiết cho việc điều tra mạng phức tạp và chuyên sâu, sử dụng thông tin được khai thác từ bộ nhớ đệm (cache) của web, proxy hay chặn bắt thụ động lưu lượng truy cập mạng và xác định các hành vi bất thường.

2.1.1.4. Các tấn công lên mạng máy tính

Bên cạnh những tiến bộ vượt bậc của công nghệ, các cuộc tân công mạng xuất hiện thường xuyên hơn, gây hậu quả càng ngày càng nghiêm trọng. Tấn công mạng là những hình thức xâm nhập trái phép vào một hệ thống máy tính, website, cơ sở dữ liệu, hạ tầng mạng, thiết bị của cá nhân hay tổ chức thông qua mạng internet với những mục đích bất hợp pháp.

- **Tấn công bằng mã độc**

Tấn công malware là hình thức phổ biến nhất. Malware bao gồm spyware (phần mềm gián điệp), ransomware (mã độc tống tiền), virus và worm (phần mềm độc hại có khả năng lây lan nhanh). Thông thường, tin tặc sẽ tấn công người dùng thông qua các lỗ hổng bảo mật, cũng có thể là dụ dỗ người dùng click vào một đường link hoặc email (phishing) để phần mềm độc hại tự động cài đặt vào máy tính. Một khi được cài đặt thành công, malware sẽ gây ra:

Ngăn cản người dùng truy cập vào một file hoặc folder quan trọng (ransomware).

- Cài đặt thêm những phần mềm độc hại khác**.**
- Lén lút theo dõi người dùng và đánh cắp dữ liệu (spyware).
- Làm hư hại phần mềm, phần cứng, làm gián đoạn hệ thống.

- **Tấn công giả mạo**

Phishing là hình thức giả mạo thành một đơn vị/cá nhân uy tín để chiếm lòng tin của người dùng, thông thường qua email. Mục đích của tấn công Phishing thường là đánh cắp dữ liệu nhạy cảm như thông tin thẻ tín dụng, mật khẩu, đôi khi phishing là một hình thức để lừa người dùng cài đặt malware vào thiết bị (khi đó, phishing là một công đoạn trong cuộc tấn công malware).

- **Man–in–the–middle**

Tấn công trung gian (MitM), hay **tấn công nghe lén**, xảy ra khi kẻ tấn công xâm nhập vào một giao dịch/sự giao tiếp giữa 2 đối tượng. Khi đã chen vào giữa thành công, chúng có thể đánh cắp dữ liệu của giao dịch đó.

Loại tấn công này xảy ra khi:

- Nạn nhân truy cập vào một mạng Wifi công cộng không an toàn, kẻ tấn công có thể "chen vào giữa" thiết bị của nạn nhân và mạng Wifi đó. Vô tình, những thông tin nạn nhân gửi đi sẽ rơi vào tay kẻ tấn công.
- Khi phần mềm độc hại được cài đặt thành công vào thiết bị, một kẻ tấn công có thể dễ dàng xem và điều chỉnh dữ liệu của nạn nhân.

- **Từ chối dịch vụ**

DoS (Denial of Service) là hình thức tấn công mà tin tặc "đánh sập tạm thời" một hệ thống, máy chủ, hoặc mạng nội bộ. Để thực hiện được điều này, chúng thường tạo ra một lượng traffic/request khổng lồ ở cùng một thời điểm, khiến cho hệ thống bị quá tải, từ đó người dùng không thể truy cập vào dịch vụ trong khoảng thời gian mà cuộc tấn công DoS diễn ra.

Một hình thức biến thể của DoS là DDoS (Distributed Denial of Service): tin tặc sử dụng một mạng lưới các máy tính (botnet) để tấn công nạn nhân. Điều nguy hiểm là chính các máy tính thuộc mạng lưới botnet cũng không biết bản than đang bị lợi dụng để làm công cụ tấn công. Đọc thêm: Sự nguy hiểm của Tấn công DDoS.

- **Khai thác Zero – day**

Lỗ hổng Zero-day (0-day vulnerabilities) là các lỗ hổng bảo mật chưa được công bố, các nhà cung cấp phần mềm chưa biết tới, và dĩ nhiên, chưa có bản vá chính thức. Chính vì thế, việc khai thác những lỗ hổng "mới ra lò" này vô cùng nguy hiểm và khó lường, có thể gây hậu quả nặng nề lên người dùng và cho chính nhà phát hành sản phẩm.

- **Chiến thuật phòng chống**

Đối với cá nhân:

- Sử dụng mật khẩu mạnh.
- Hạn chế truy cập các điểm wifi công cộng.
- Không sử dụng các phần mềm crack.
- Cập nhật phần mềm, hệ điều hành mới nhất.
- Cẩn thận khi duyệt mail để tránh bị đánh lừa.
- Sử dụng phần mềm diệt virus.
- Không click vào các đường link không rõ nguồn gốc.

Đối với tổ chức, doanh nghiệp:

- Xây dựng chính sách bảo mật có các điều khoản rõ ràng.
- Lựa chọn phần mềm, đối tác một cách kỹ càng. Ưu tiên những bên có cam kết bảo mật và cam kết cập nhật thường xuyên.
- Không sử dụng các phần mềm crack.
- Sử dụng dịch vụ đám mây uy tín.
- Đánh giá bảo mật và xây dựng chiến lược an ninh tổng thể cho tổ chức.

2.1.2. Tổng quan về ứng dụng web

2.1.2.1. Khái niệm

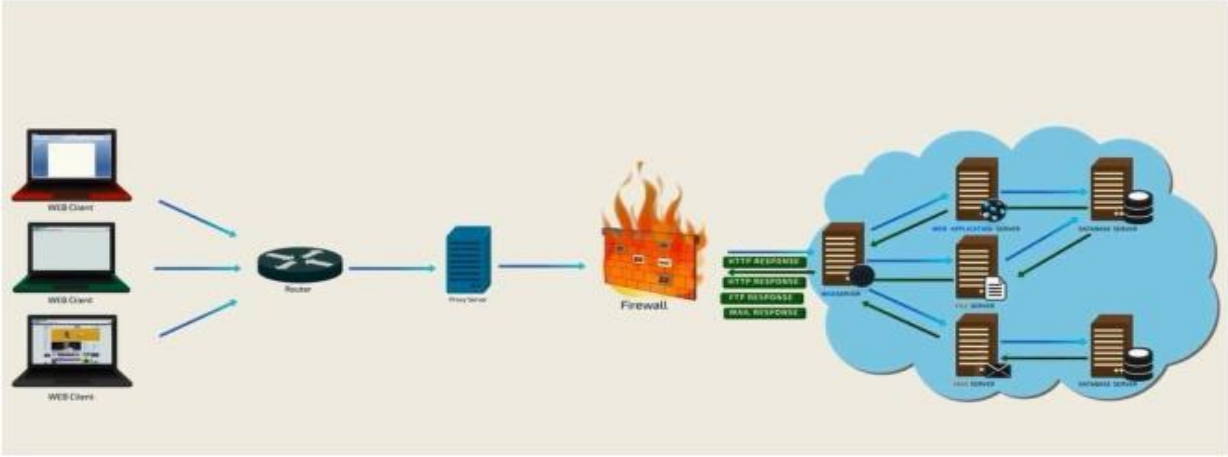
Ứng dụng web là một ứng dụng khách chủ sử dụng giao thức HTTP để tương tác với người dùng hay hệ thống khác.

Trình khách dành cho người dùng thường là một trình duyệt web như Internet Explorer, Firefox hay Google Chrome. Người dùng gửi và nhận các thông tin từ trình chủ thông qua việc tác dộng vào các trang Web. Các chương trình có thể là các trang trao dổi mua bán, các diễn đàn, giử nhận email...

Tốc độ phát triển các kỹ thuật xây dựng ứng dụng Web cũng phát triển rất nhanh. Trước đây những ứng dụng Web thường được xây dựng bằng CGI (Common Gateway Interface) được chạy trên các trình chủ Web và có thể kết nối vào các cơ sở dữ liệu đơn giản trên cùng một máy chủ. Ngày nay ứng dụng Web
được biết bằng Java (các ngôn ngữ tương tự) và chạy trên máy chủ phân tán, kết nối đến nhiều nguồn dữ liệu khác nhau.

2.1.2.2. Cấu trúc

Một ứng dụng web gồm các thành phần:



Hình 2. 1Cấu trúc ứng dụng Web

Trong đó:

- Máy khách sử dụng trình duyệt: IE, Firefox,…
- Máy chủ: Apache, IIS,…
- Cơ sở dữ liệu.
- Tường lửa.
- Proxy.

2.1.2.3. Hoạt động

Đầu tiên trình duyệt sẽ gửi một yêu cầu (request) đến trình chủ Web thông qua các phương thức cơ bản GET, POST,... của giao thức HTTP. Trình chủ lúc này có thể cho thực thi một chương trình được xây dựng từ nhiều ngôn ngữ như Perl, C/C++,.. hoặc trình chủ yêu cầu bộ diễn dịch thực thi các trang ASP, PHP, JSP,... theo yêu cầu của trình khách.

Tùy theo các tác vụ của chương trình được cài đặt mà nó xử lý, tính toán, kết nối đến cơ sở dữ liệu, lưu các thông tin do trình khách gửi đến... và từ đó trả về cho trình khách một luồn dữ liệu có định dạng theo giao thức HTTP, gồm hai phần:

- Header mô tả các thông tin về gói dữ liệu và các thuộc tính, trạng thái trao đổi giữa trình duyệt và máy chủ.
- Body là phần nội dung dữ liệu mà máy chủ gửi về máy trạm, nó có thể là một tập tin HTML, một hình ảnh, một đoạn phim hay một văn bản bất kỳ.

2.1.2.4. Các tấn công lên ứng dụng Web

Website là kênh cung cấp thông tin hiệu quả, nhanh chóng nhất nên thường xuyên là mục tiêu tấn công của tin tặc. Một trong những phương thức tấn công phổ biến nhất là khai thác các lỗi bảo mật liên quan đến ứng dụng web. Sau đây là một số cách thức tấn công thường được áp dụng nhất.

- **Tấn công Bruteforce**

Bruteforce là cách thức thử tất cả các khả năng có thể có để đoán các thông tin cá nhân đăng nhập: tài khoản, mật khẩu, số thẻ tín dụng…Nhiều hệ thống cho phép sử dụng mật khẩu hoặc thuật toán mã hóa yếu sẽ tạo điều kiện cho tin tặc sử dụng phương pháp tấn công này để đoán tài khoản và mật khẩu đăng nhập. Sau đó sử dụng các thông tin này để đăng nhập truy cập vào tài nguyên hệ thống. Biện pháp đối phó:

- Tăng cường độ mạnh cho mật khẩu (Độ dài ít nhất 6 ký tự, không chứa chuỗi username, chứa ít nhất 1 ký tự số, chứa ít nhất 1 ký tự đặc biệt, không cho phép thay đổi mật khẩu trùng lặp đã sử dụng, quản lý, điều khiển thông báo lỗi)
- Sử dụng cơ chế chứng thực (Basic hoặc Digest Authentication)
- Hạn chế số lần đăng nhập hoặc khóa tài khoản đăng nhập sai.
- Sử dụng module Mod_Dosevasive để xác định dấu hiệu của kiểu tấn công này.

- **Tấn công xác thực yếu**

Lỗi xác thự yếu sảy ra khi website cho phép truy cập các tài nguyên nhạy cảm mà không cần đủ quyền. Các trang của quản trị viên là ví dụ minh họa dễ thấy nhất. Nếu không có cơ chế kiểm soát truy cập phù hợp thì tin tặc hoàn toàn có thể vượt qua để có được quyền truy cập các trang này.

- **Tấn công cơ chế quản lý phiên**

Thông thường, khi một tài khoản thực hiện quá trình xác thực đối với server, server sử dụng các thông tin này tạo một sessionID duy nhất cho phép kết nối và duy trì kết nối. Nếu có thể đoán được sessionID thì việc chiếm phiên đăng nhập là hoàn toàn có thể. Các biện pháp đối phó:

- Sử dụng SSL trong quá trình truyền thông.
- Sử dụng cơ chế tạo sessionID ngẫu nhiên.
- Đặt giới hạn thời gian tồn tại cho sessionID.

- **XSS – Cross site scripting**

XSS là một trong những kỹ thuật tấn công phổ biến nhất hiện nay, đồng thời cũng là vấn đề bảo mật quan trọng đối với các nhà phát triển và người dùng web hiện nay. Bất kì một website nào cho phép người sử dụng đăng thông tin mà không có sự kiểm tra chặt chẽ các đoạn mã nguy hiểm thì đều có thể tiềm ẩn các lỗi XSS. Tin tặc tấn công bằng cách chèn vào các website động (ASP, PHP, CGI, JSP …) những thẻ HTML hay những đoạn mã script nguy hiểm có thể gây nguy hại cho những người sử dụng khác. Trong đó, những đoạn mã nguy hiểm được chèn vào hầu hết được viết bằng các Client-Site Script như JavaScript, JScript, DHTML và cũng có thể là cả các thẻ HTML Ví dụ: Sử dụng XSS chèn mã java script trực tiếp trên URL. Biện pháp đối phó:

- Lọc dữ liệu, chỉ cho phép các dữ liệu hợp lệ.
- Sử dụng Mod_Security để lọc một số dữ liệu tấn công XSS.

- **SQL Injection**

Tấn công SQL Injection được thực thi bằng cách chèn các câu truy vấn SQL vào dữ liệu tương tác giữa máy khách và trình ứng dụng. Quá trình khai thác lỗi SQL Injection thành công có thể giúp tin tặc lấy được các dữ liệu nhạy cảm trong cở sở dữ liệu, thay đổi cơ sở dữ liệu (Insert/Update/Delete), thực thi các hành động với quyền của người quản trị và cao hơn có thể điều khiển được hệ điều hành máy chủ Ví dụ: Xét đoạn mã truy vấn SQL sau:

SELECT * FROM Users WHERE Username=’$username’ AND Password=’$password’

Đây là một câu truy vấn thường hay được dùng trong các trình ứng dụng nhằm xác thực người dùng. Nếu câu truy vấn trả về một giá trị nói rằng thông tin về người dùng đang đăng nhập là đúng và được lưu trong cơ sở dữ liệu, thì người dùng được phép đăng nhập vào hệ thống, ngược lại thì không đăng nhập được. Người dùng nhập thông tin đó

vào các trường gọi là web form. Thay vì nhập đúng tên đăng nhập và mật khẩu, thử nhập vào các ký tự đặc biệt như:

$username = 1′ or ‘1’ = ‘1

$password = 1′ or ‘1’ = ‘1

Khi đó câu truy vấn sẽ là:

SELECT * FROM Users WHERE Username=’1′ OR ‘1’ = ‘1’ AND Password=’1′ OR ‘1’ = ‘1’

Giả sử rằng giá trị của các tham số được gửi tới máy chủ bằng phương thức GET, thì có một câu lệnh khai thác lỗi như sau:

‘%20or%20’1’%20=%20’1&password=1’%20or%20’1’%20=%20’1

Khi đó, truy vấn sẽ trả về một giá trị (hay một loạt các giá trị) vì điều kiện trên luôn luôn đúng (OR 1=1). Trong trường hợp này tin tặc sẽ đăng nhập được vào hệ thống mà không cần biết tên đăng nhập và mật khẩu. Trường hợp này sẽ rất nguy hiểm nếu dòng đầu tiên trong bảng “Users” là tài khoản của người quản trị (admin) vì tin tặc sẽ đăng nhập vào hệ thống bằng tài khoản đầu tiên trong bảng này. Biện pháp đối phó:

- Kiểm tra dữ liệu đầu vào.
- Sử dụng Mod_Security để lọc một số dữ liệu tấn công SQL injection.

➢ **Path Traveral**

Path Traversal hay còn được biết với một số tên khác như “dot-dot-slash”, “directory traversal”,”directory clumbing” và “backtracking” là hình thức tấn công truy cập đến những file và thư mục mà được lưu bên ngoài thư mục webroot. Hình thức tấn công này không cần sử dụng một công cụ nào mà chỉ đơn thuần thao tác các biến với ../ (dot-dot-slash) để truy cập đến file, thư mục, bao gồm cả source code, những file hệ thống, … Ví dụ:

GET/../../../../../some/file HTTP/1.0

GET /..%255c..%255c..%255csome/file HTTP/1.0

GET /..%u2216..%u2216some/file HTTP/1.0

Biện pháp đối phó: Sử dụng mod_security để lọc dữ liệu đầu vào.

2.2. KỸ THUẬT ĐIỀU TRA, PHÂN TÍCH TẤN CÔNG WEB

2.2.1. Kỹ thuật điều tra, phân tích phía người dùng

2.2.1.1. Điều tra, phân tích người dùng

Người dùng ứng dụng web là những khách hàng, người dùng mạng máy tính, quản trị viên hoặc các kẻ tấn công có nhu cầu kết nối tới trang web để thực hiện các hành động theo nhu cầu và mong muốn của bản thân.

Phân loại:

- Người dùng thông thường
- Kẻ tấn công

Chính vì vậy, điều tra và phân tích người dùng nhằm mục đích xác định người dùng là nạn ngân hay kẻ tấn công. Như đã biết có rất nhiều phương pháp tấn công phía client side ví dụ như: XSS, Phishing,… Nếu chúng ta không có những chứng cứ số hoặc không được tiếp cận các thiết bị truy cập website của người dùng, thì việc điều tra tấn công là rất khó khăn, vấn đề này rất cần thiết với người dùng hợp lệ và nạn nhân của các cuộc tấn công gián tiếp hoặc trực tiếp qua website.

Đối với kẻ tấn công, để xác nhận đúng một người có phải là kẻ tấn công hay không, ngoài chứng cứ, bằng chứng trên Server side, ta cũng cần các chứng cứ hay bằng chứng trực tiếp trên thiết bị truy cập website của người dùng nhằm đưa ra một quyết định vững chắc rằng họ vi phạm hoặc phạm tội.

Các kỹ thuật chính:

- Phân tích dữ liệu trên hệ điều hành.
- Phân tích dữ liệu trên trình duyệt.

Nội dung chuyên đề sẽ phân tích kỹ hơn về kỹ thuật phân tích dữ liệu trên trình duyệt.

2.2.1.2. Phân tích dữ liệu trên trình duyệt

Trình duyệt web là công cụ để thực hiện các hoạt động khác nhau trên Internet của người dùng, người dùng sử dụng trình duyệt cho nhiều chức năng như: tìm kiếm thông tin, truy cập vào tài khoản email, giao dịch thương mại điện tử, nhắn tin,... Trình duyệt cũng ghi lại nhiều dữ liệu liên quan đến hoạt động của người dùng, các thông tin như: URLs được truy cập bởi người dùng, cookie, tệp bộ nhớ cache, thời gian truy cập & thời gian sử dụng trình duyệt,...

Việc kiểm tra các bằng chứng nói trên là một trong các điểm chủ chốt của quá trình "Browser forensic". Các trình duyệt lưu trữ các tập tin quan trọng này ở nhiều phần khác nhau trên hệ điều hành, ngoài ra như ta đã thấy, có rất nhiều trình duyệt khác nhau, đồng nghĩa với nó đó chính là dữ liệu hoặc địa điểm lưu trữ các tập tin cũng khác nhau. Dưới đây là bảng tổng hợp các bản ghi Cache, các bản ghi. Lịch sử, Cookie registry và các tập tin đã tải xuống ở các trình duyệt nổi tiếng, để dễ dàng hơn trong quá trình truy vết và điều tra.

Web Browser	Operating System	File Path
Internet Explorer	Windows 95/98	C:\Temporary Internet Files\Content.ie5 C:\Cookies C:\History\History.ie5
	Windows 2000/XP	C:\Documents and Settings\%username%\Local Settings\Temporary Internet Files\Content.ie5 C:\Documents and Settings\%username%\Cookies C:\Documents and Settings\%username%\Local Settings\History\history.ie5
	Windows Vista, 7 and latest version	C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\ C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\
Firefox	Linux	/home/$USER/.mozilla/firefox/$PROFILE.default/places.sqlite
	MacOS-X	/Users/$USER/Library/Application Support/Firefox/Profiles/$PROFILE.default/places.sqlite
	Windows XP	C:\Documents and Settings\%username%\Application Data\Mozilla\Firefox\Profiles\%PROFILE%.default\places.sqlite
	Windows Vista,7 and latest version	C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles\%PROFILE%.default\places.sqlite
Safari	MacOS-X	/Users/$USER/Library/Safari/ /Users/$USER/Library/Caches/com.apple.Safari/
	Windows XP	C:\Documents and Settings\%username%\Application Data\Apple Computer\Safari\ C:\Documents and Settings\%username%\Local Settings\Application Data\Apple Computer\Safari\
	Windows 7	C:\Users\%username%\AppData\Roaming\Apple Computer\Safari\ C:\Users\%username%\AppData\Local\Apple Computer\Safari\
Opera	Linux	/home/$USER/.opera/
	MacOS-X	/Users/$USER/Library/Opera/
	Windows XP	C:\Documents and Settings\%username%\Application Data\Opera\Opera\
	Windows Vista, 7 and latest version	C:\Users\%username%\AppData\Roaming\Opera\Opera\
Google Chrome	Linux	/home/$USER/.config/google-chrome/Default/Preferences
	MacOS-X	/Users/$USER/Library/Application Support/Google/Chrome/Default/Preferences
	Windows XP	C:\Documents and Settings\%username%\Local Settings\Application Data\Google\Chrome\User Data\Default\Preferences
	Windows Vista, 7 and latest version	C:\Users\%username%\AppData\Local\Google\Chrome\User Data\Default\Preferences

Hình 2. 2. Tổng hợp bản ghi của một số trình duyệt nổi tiếng

Internet Explorer là trình duyệt web mà người dùng máy tính thường hay sử dụng, các hoạt động sẽ được lưu cho từng người dùng riêng tương ứng với thư mục người dùng của họ, dữ liệu được lưu trong Cookie, Cache, lịch sử và lịch sử tải xuống (tham khảo thêm ở hình 8). Ngoài ra dữ liệu cũng có thể được lưu trong tập tin cơ sở dữ liệu như index.dat hay container.dat và dữ liệu trong hai tập tin này được lưu dưới dạng nhị phân. Cũng lưu dữ liệu trong tập tin cơ sở dữ liệu dưới dạng nhị phân đó là trình duyệt Safari, tuy nhiên safari đặt tên tệp tin lưu trữ là history.plist, ở đây lưu trữ các thông tin như địa chỉ URLs, ngày tháng truy cập, lượng truy cập ở mỗi website. Firefox sử dụng định dạng

dữ liệu SQLite để lưu trữ các thông tin, chúng được đặt tên là places.sqlite. Opera thì lưu trữ các thông tin trên ở các tệp tin .dat khác nhau như: cookies4.dat, download.dat, global_history.dat. Google chrome cho phép lưu trữ dữ liệu trong tệp tùy chọn, tùy thuộc vào lựa chọn của người dùng.

Dưới đây là bảng cung cấp địa chỉ, nơi dùng để xóa các bản ghi của từng loại trình duyệt.

Web Browser	Delete Options Path
İnternet Explorer	Settings/ Internet Options/ / Deletes
Firefox	Settings /Privacy/History about:preferences#privacy
Google Chrome	Settings /History/Search Data chrome://settings/clearBrowserData
Safari	Settings / Privacy / Delete All Web Site Data Settings/History
Opera	Settings /History/Privacy and Security/Delete All Search Data opera://settings/clearBrowserData

Hình 2. 3. Địa chỉ xóa bản ghi dữ liệu của trình duyệt

2.2.2. Kỹ thuật điều tra, phân tích phía máy chủ

Hiện nay, có rất nhiều các thiết bị, công cụ hỗ trợ điều tra & phân tích tấn công một cách dễ dàng, ví dụ như các hệ thống: IDS/IPS, honey pot, honey net,... Tuy nhiên trong bài viết này sẽ đưa ra hai phương pháp chính hỗ trợ điều tra và phân tích tấn công web phía máy chủ, với trường hợp máy chủ Linux Apache & không hỗ trợ các hệ thống phát hiện xâm nhập hay phân tích dữ liệu hiện đại, chủ yếu dựa trên các công cụ mã nguồn mở miễn phí.

Hai phương pháp chính: Phân tích luồng dữ liệu và phân tích tập tin nhật ký.

Phương pháp	Điểm mạnh	Điểm yếu
Phân tích luồng dữ liệu	Có thể phân tích tất cả các thông tin	Dữ liệu cần phải được chặn bắt**.** Dữ liệu có thể cần được lắp ráp, chống phân mảnh, chuẩn hóa (Các gói tin IP, IP fragments,...). Rất khỏ để chặn bắt và giải mã dữ liệu trên đường chuyền đã mã hóa (Encrypted traffic, High Traffic load,...
Phân tích tập tin nhật kí	Dữ liệu có sẵn trong các tập tin	Các tập tin nhật ký thường chỉ chứa một phần nhỏ của toàn bộ dữ liệu (ví dụ: thiếu các tham số trong gói POST HTTP)

2.2.2.1. Phân tích luồng dữ liệu

Luồng dữ liệu (RFC3679) là một chuỗi các gói tin được gửi từ một nguồn cụ thể tới một đích hoặc nhiều đích, trong đó nguồn gán nhãn cho chuỗi các gói tin này là một luồng riêng.

Một số dấu hiệu cần chú ý:

- Địa chỉ IP nguồn, đích.

- Cổng
- Giao thức và cờ hiệu
- Hướng luồng dữ liệu
- Khối lượng dữ liệu được truyền

Quan hệ giữa các địa chỉ IP:

- One to many: Spam, Scan port trên 1 dải mạng,...
- Many to one: DDOS attack, máy chủ syslog,...
- Many to many: Đồng bộ dữ liệu, phát tán virus,...
- One to one: Tấn công có mục tiêu, truyền tin,...

Phân tích luồng dữ liệu thực hiện việc thanh tra một chuỗi các gói tin có liên quan đến nhau nhằm xác định các hành vi nghi ngờ, trích xuất dữ liệu hay phân tích các giao thức trong luồng.

Một số công cụ nổi tiếng sử dụng trong quá trình phân tích luồng dữ liệu: Wireshark, Tshark, TCP dump, …

2.2.2.2. Phân tích nhật ký

Các web server chuẩn như Apache và IIS tạo thông điệp ghi nhật ký theo một chuẩn chung (CLF – common log format). Tệp nhật ký CLF chứa các dòng thông điệp cho mỗi một gói HTTP request, cấu tạo như sau:

Host Ident Authuser Date Request Status Bytes

Trong đó:

- Host: Tên miền đầy đủ của client hoặc IP.
- Ident: Nếu chỉ thị IdentityCheck được kích hoạt và client chạy identd, thì đây là thông tin nhận dạng được client báo cáo.

- Authuser: Nếu URL yêu cầu xác thực HTTP thì tên người dùng là giá trị của mã thông báo này.
- Date: Ngày và giờ yêu cầu.
- Request: Dòng yêu cầu của client, được đặt trong dấu ngoặc kép (“”).
- Status: Mã trạng thái (gồm ba chữ số).
- Bytes: số bytes trong đối tượng trả về cho client, ngoại trừ các HTTP header.

Mỗi yêu cầu có thể chứa các các dữ liệu bổ sung như đường liên kết hoặc chuỗi ký tự của người dùng.

Nếu mã thông báo không có giá trị, thì mã thông báo được biểu thị bằng một dấu gạch ngang (-).

Ví dụ:

192.168.40.131 - - [08/May/2018:08:43:52 -0400] "GET /dvwa/login.php HTTP/1.1" 200 1289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0"

Lợi ích lớn nhất của tập tin nhật ký là tính sẵn có tương đối đơn giản và phân tích nội dung của chúng. Máy chủ web như Apache mặc định phải cho phép ghi nhật ký. Các ứng dụng thường thực hiện ghi nhật ký để đảm bảo truy xuất nguồn gốc của các hành động của chúng. Trong khi lưu lượng mạng đầy đủ cung cấp các thông tin bổ sung, chi phí mua lại và xử lý của nó thường lớn hơn lợi ích của nó. Việc thu thập lưu lượng mạng yêu cầu: trong suốt với gói tin và thường là phần cứng bổ sung. Quan sát lưu lượng có thể đạt được với hubs, các cổng SPAN, vòi hoặc thiết bị nội tuyến. Mọi thiết bị đều phải mua, cài đặt và được hỗ trợ. Một khi dữ liệu đã được thu thập thì sẽ được phân tích ngay lập tức. Hiện tại, lưu lượng truy cập mạng được thu thập có cùng dạng với tệp nhật ký và sẵn sàng để được phân tích. Cuối cùng, các tệp nhật ký cung cấp khả năng dễ dàng và dễ xử lý để theo dõi bảo mật.

2.2.3. Một số công cụ hỗ trợ điều tra mạng và điều tra tấn công web

Hỗ trợ cho quá trình điều tra là các công cụ phục vụ cho công tác điều tra, có khả năng chặn bắt, sao lưu, trích xuất, khôi phục và phân tích các dữ liệu mạng. Những công cụ này có thể giúp điều tra viên xác định thời gian, cách thức, nội dung mà dữ liệu được truyền đi hay nhận về, cung cấp lượng chứng cứ số nhanh chóng, chính xác, tạo thuận lợi cho việc điều tra.

2.2.3.1. Wireshark

WireShark có một bề dày lịch sử, Gerald Combs là người đầu tiên phát triển phần mềm này. Phiên bản đầu tiên được gọi là Ethereal được phát hành năm 1998. Tám năm sau kể từ khi phiên bản đầu tiên ra đời, Combs từ bỏ công việc hiện tại để theo đuổi một cơ hội nghề nghiệp khác. Thật không may, tại thời điểm đó, ông không thể đạt được thoả thuận với công ty đã thuê ông về việc bản quyền của thương hiệu Ethereal. Thay vào đó, Combs và phần còn lại của đội phát triển đã xây dựng một thương hiệu mới cho sản phẩm "Ethereal" vào năm 2006, dự án tên là WireShark.

WireShark đã phát triển mạnh mẽ và đến nay, nhóm phát triển cho đến nay đã lên tới 500 cộng tác viên. Sản phẩm đã tồn tại dưới cái tên Ethereal không được phát triển thêm.

Lợi ích Wireshark đem lại đã giúp cho nó trở nên phổ biến như hiện nay. Nó có thể đáp ứng nhu cầu của cả các nhà phân tích chuyên nghiệp lẫn nghiệp dư và nó đưa ra nhiều tính năng để thu hút mỗi đối tượng khác nhau.

2.2.3.2. Snort

Snort là một hệ thống phát hiện xâm nhập mạng (NIDS) mã nguồn mở miễn phí. NIDS là một kiểu của hệ thống phát hiện xâm nhập (IDS), được sử dụng để giám sát dữ liệu di chuyển trên mạng. Cũng có thể các hệ thống phát hiện xâm nhập Host-based, được cài đặt trên một Host cụ thể và chỉ để phát hiện các sự tấn công nhắm đến Host đó. Mặc

dù tất cả các phương pháp phát hiện xâm nhập vẫn còn mới nhưng Snort được đánh giá là hệ thống tốt nhất hiện nay.

Snort chủ yếu là một IDS dựa trên luật, tuy nhiên các Input plug-in cũng tồn tại để phát hiện sự bất thường trong các Header của giao thức. Snort sử dụng các luật được lưu trữ trong các File Text, có thể được chỉnh sửa bởi người quản trị. Các luật thuộc về mỗi loại được lưu trong các File khác nhau. File cấu hình chính của Snort là snort.conf. Snort đọc những luật này vào lúc khởi tạo và xây dựng cấu trúc dữ liệu cung cấp nhằm phân tích các dữ liệu thu được. Tìm ra các dấu hiệu và sử dụng chúng trong các luật là một vấn đề đòi hỏi sự tinh tế, vì càng sử dụng nhiều luật thì năng lực xử lý càng được đòi hỏi để thu thập dữ liệu trong thực tế. Snort có một tập hợp các luật được định nghĩa trước để phát hiện các hành động xâm nhập và chúng ta cũng có thể thêm vào các luật của chính mình. Cũng có thể xóa một vài luật đã được tạo trước để tránh việc báo động sai.

2.2.3.3. Foremost

Foremost là một chương trình điều khiển (console) dùng để khôi phục tệp tin dựa vào tiêu đề, phụ đề và các cấu trúc dữ liệu bên trong. Quá trình này thường được gọi là chạm khắc dữ liệu (data carving). Foremost có thể làm việc trên các tệp tin ảnh, chẳng hạn được tạo ra bởi dd, Safeback, Encase,... hoặc trực tiếp từ trên ổ cứng. Tiêu đề và phụ đề có thể được xác định bởi một tệp tin cấu hình hoặc có thể sử dụng một switch dòng lệnh dựa trên dạng tệp tin tích hợp. Các dạng tích hợp này sẽ tra cứu cấu trúc dữ liệu của định dạng tệp tin được cung cấp được nhằm đảm bảo việc phục hồi sẽ nhanh và đáng tin cậy hơn.

2.2.3.4. NetworkMiner

NetworkMiner là một công cụ phân tích điều tra mạng (Network Forensics Analysis Tool – NFAT) cho Windows. NetworkMiner có thể được sử dụng như một công cụ chặn bắt gói tin thụ động nhằm nhận biết các hệ điều hành, các phiên làm việc, tên host, các port mở... mà không cần đặt bất cứ luồng dữ liệu nào lên mạng.

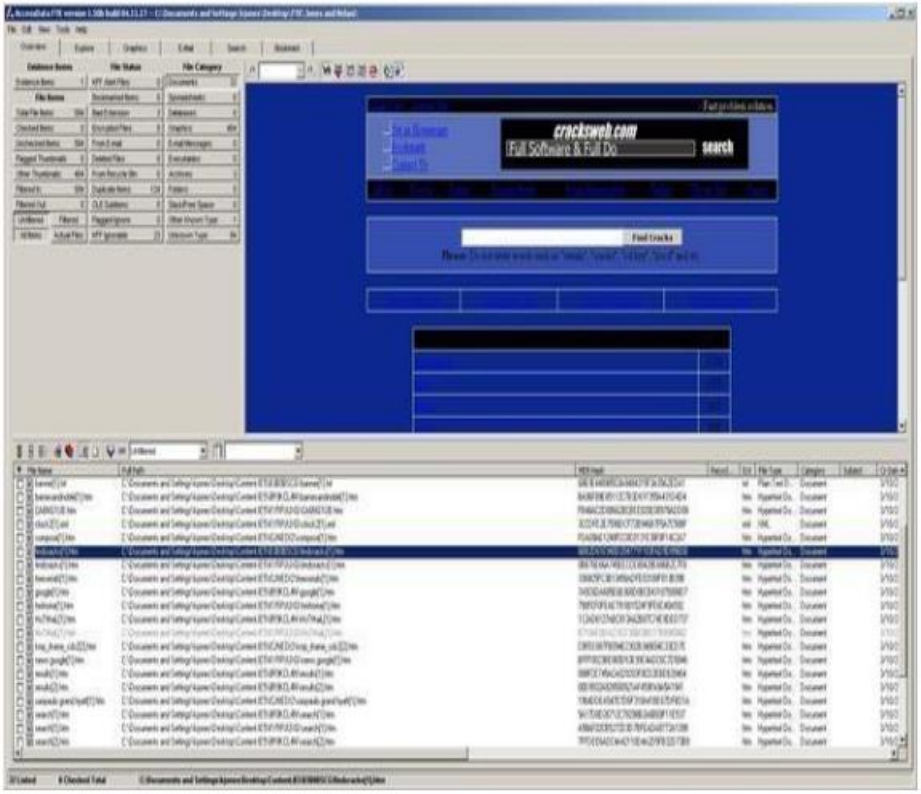
NetworkMiner cũng có thể phân tích các tệp tin .pcap trong trường hợp ngoại tuyến và tái tạo các tập tin truyền tải, cấu trúc thư mục hay chứng chỉ từ tệp tin .pcap. Mục đích của NetworkMiner là thu thập dữ liệu (chẳng hạn như chứng cứ pháp lý) về các host trên mạng chứ không phải thu thập dữ liệu về lưu lượng truy cập, là quan tâm đến trung tâm máy chủ (nhóm các thông tin trên từng máy) chứ không phải là trung tâm gói tin (thông tin về danh sách các gói tin, khung nhìn...). NetworkMiner cũng rất tiện dụng khi phân tích mã độc như C&C (command & control – ra lệnh và điều khiển) kiểm soát lưu lượng truy cập từ mạng lưới botnet.

2.2.3.5. Net Analysis

NetAnalysis là một công cụ được cấp phép do công ty Digital Detective phát triển để điều tra số các trình duyệt web, hỗ trợ Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari và Opera bowsers. Nó cho phép kiểm tra lịch sử Internet, bộ nhớ cache, cookie và các thành phần khác. công cụ này cho phép thu thập nhanh bằng chứng theo hành vi của người dùng. Phần mềm này cũng có các công cụ phân tích hiệu quả để giải mã và hiểu dữ liệu. Đồng thời, nó có khả năng sử dụng các truy vấn SQL để xác định bằng chứng liên quan. Ngoài ra nó có thể được sử dụng để phục hồi các thành phần trình duyệt web đã xóa.

2.2.3.6. FTK

FTK là một trong những công cụ được phát triển để phân tích toàn bộ hệ thống. Nó cho phép phân tích dữ liệu trình duyệt web với tính năng, đặc điểm. Lịch sử trình duyệt web được ảo hóa chi tiết. Internet Explorer, Firefox, Chrome, Safari và Opera là trình duyệt được hỗ trợ. Ngoài ra, dữ liệu trình duyệt web đã xóa có thể được phục hồi bởi FTK. Phần mềm này cũng có tính năng báo cáo kết quả phân tích.



Hình 2. 4. Giao diện FTK

2.2.3.7. Browser History Examiner

Browser Hisotry Examiner là một công cụ được cấp phép phát triển bởi Foxton Forensics Company, có chức năng trích xuất và phân tích lịch sử web. Nó hỗ trợ các trình duyệt web Chrome, Firefox, Internet Explorer và Edge. Và nó có thể phân tích nhiều loại dữ liệu dưới dạng tải xuống, dữ liệu bộ nhớ cache và tệp URL đã truy cập.

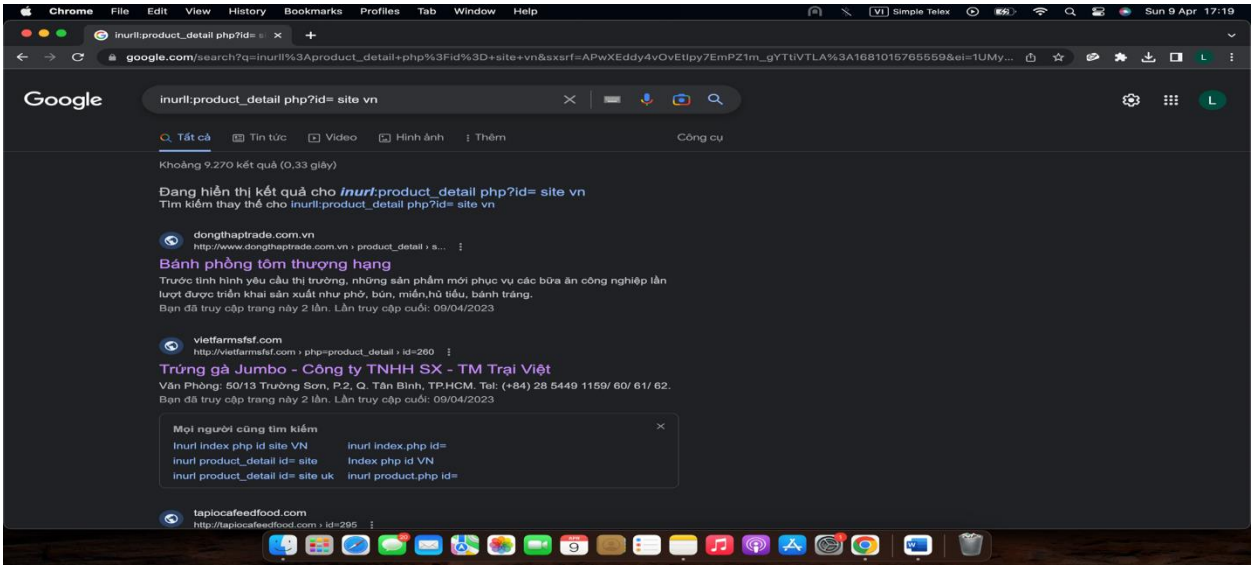
2.2.3.8. Encase

Encase là một công cụ phân tích được phát triển để kiểm tra toàn bộ hệ thống. Nó cho phép kiểm tra trình duyệt web, dữ liệu với các tính năng của trình duyệt. Với sự trợ giúp của một tập lệnh đơn giản, tất cả các lịch sử trình duyệt, cookie và tệp bộ nhớ cache được sao chép vào một tệp bằng cách sử dụng phần mềm của bên thứ ba.. Nó cũng cho phép phục hồi các thành phần internet đã bị xóa. Dữ liệu thu được có thể được phân tích bằng cách lọc theo các thông số từ và thời gian chính.

CHƯƠNG 3: CÀI ĐẶT VÀ THỰC NGHIỆM, ĐIỀU TRA TẤN CÔNG

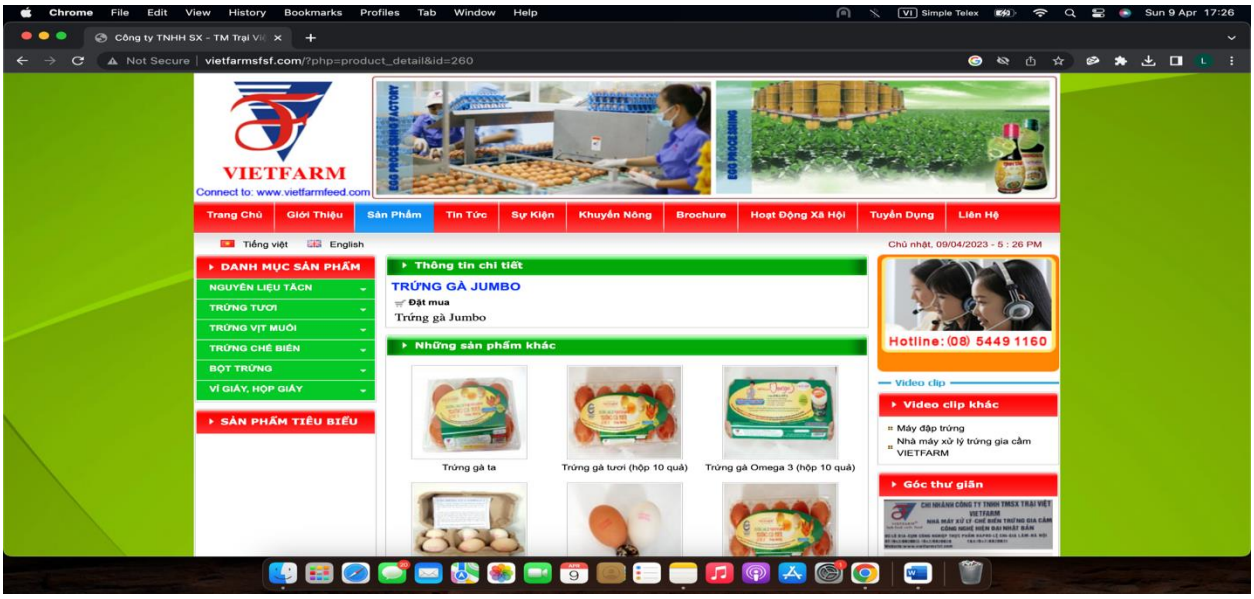
3.1. Tấn công SQL Injection bằng HackBar

Bước 1: Tìm website bị lỗi bằng lệnh "inurll:product_detail php?id= site vn"



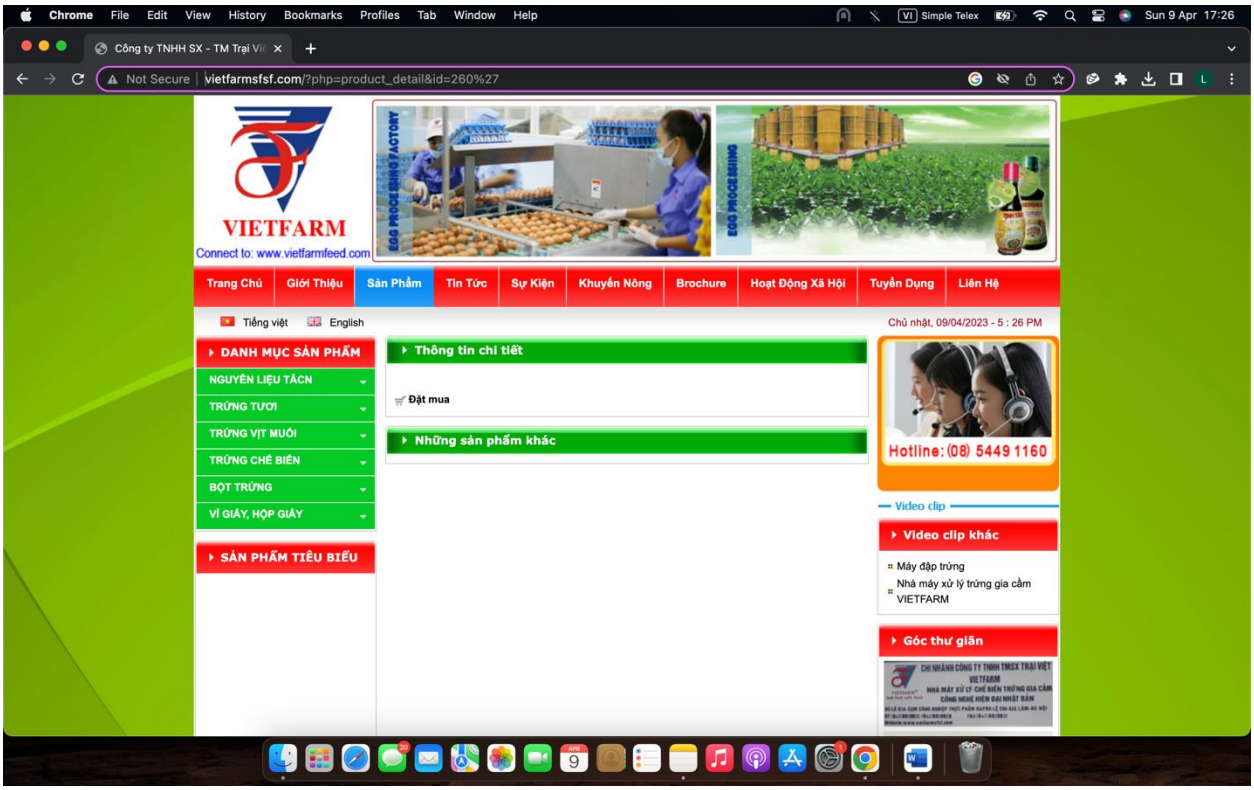
Hình 3. 1. Hình ảnh bước 1

Bước 2: Kiểm tra website có lỗi để khai thác không bằng cách thêm '



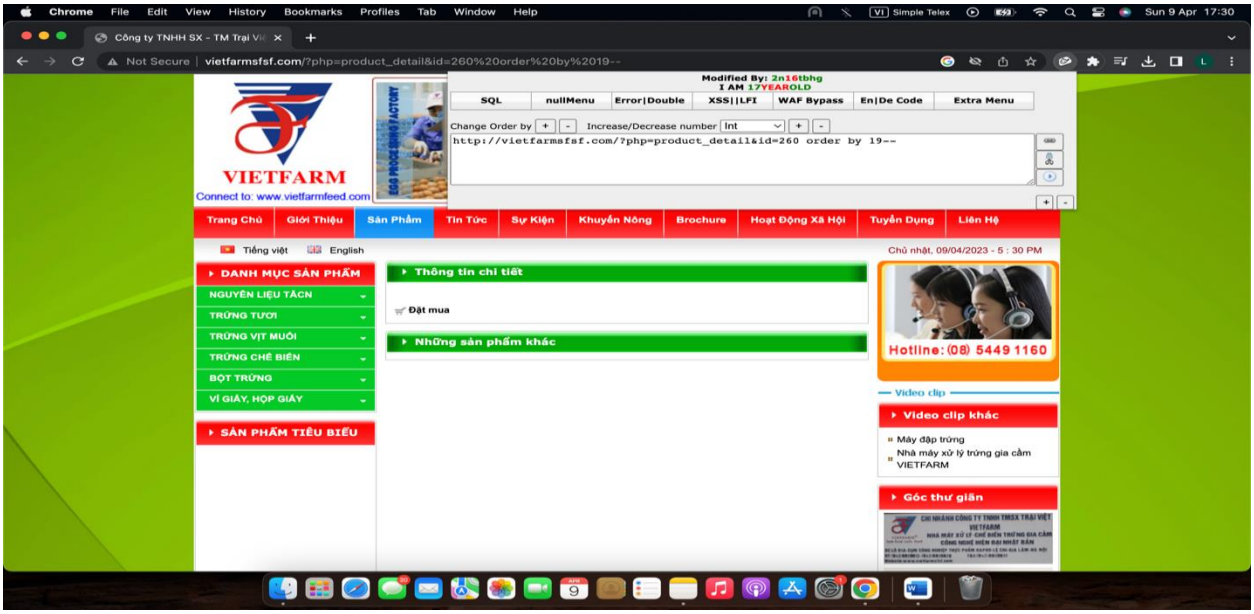
Hình 3. 2. Hình ảnh bước 2 (1)

Nếu không có lỗi sẽ không có gì thay đổi còn nếu có sẽ như sau:



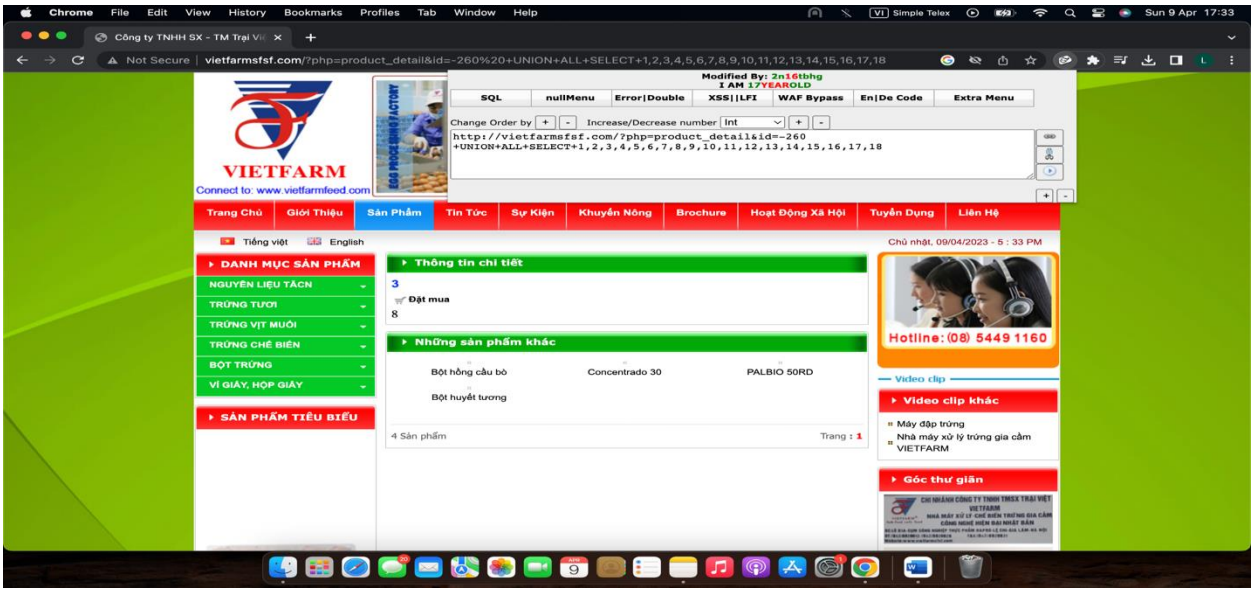
Hình 3. 3. Hình ảnh bước 2 (2)

Bước 3: Tìm tổng số cột ở đây số 19 không còn gì có nghĩa chỉ có 18 cột



Hình 3. 4. Hình ảnh bước 3

Bước 4: Tìm cột bị lỗi bằng lệnh union select và thêm - trước id

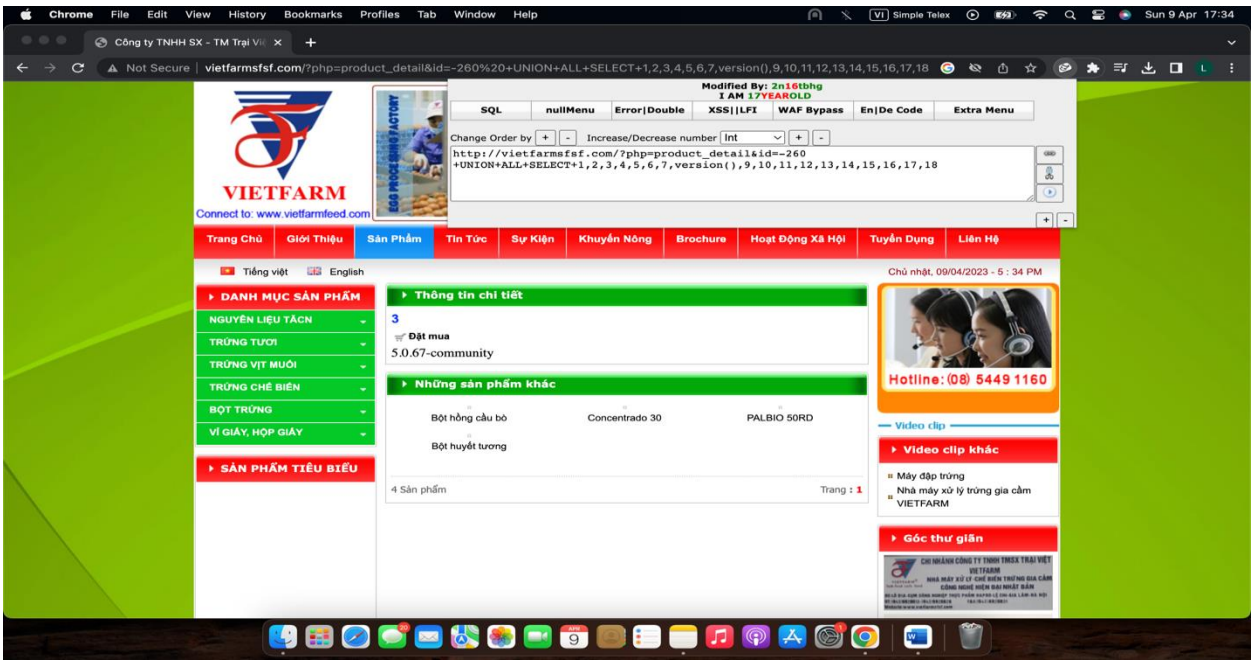


Hình 3. 5. Hình ảnh bước 4 (1)

Ở đây sẽ thấy lỗi ở cột 8 và ta sẽ khai thác ở lỗ hỏng này:

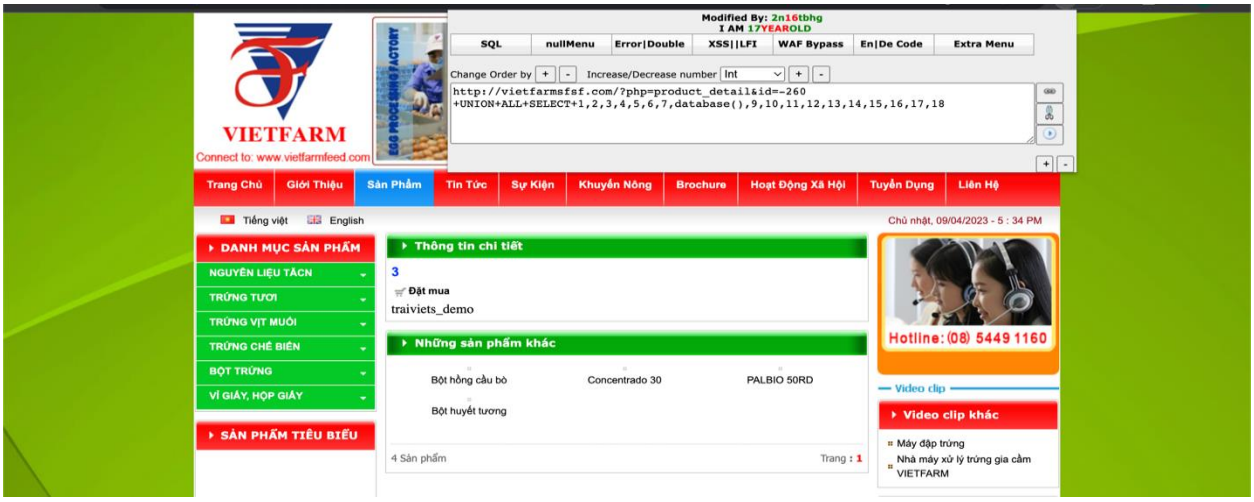
Ví dụ:

- **Version:**



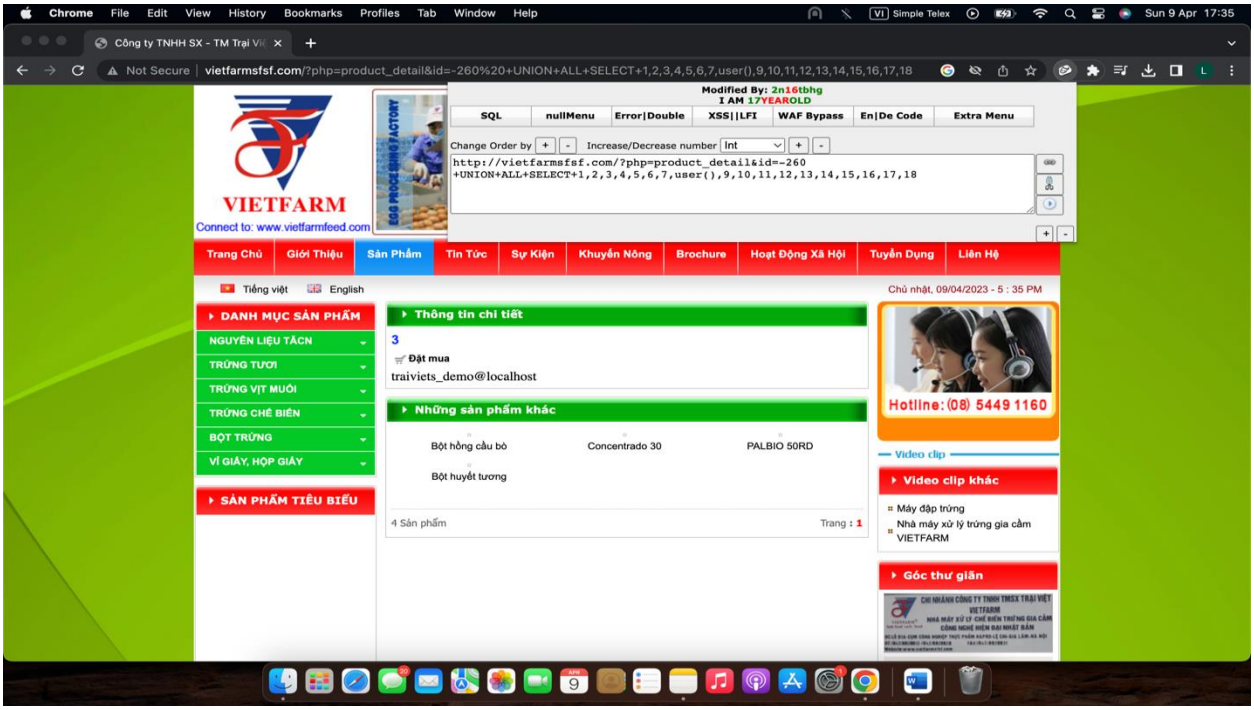
Hình 3. 6. Hình ảnh bước 4 (2)

- **Database:**



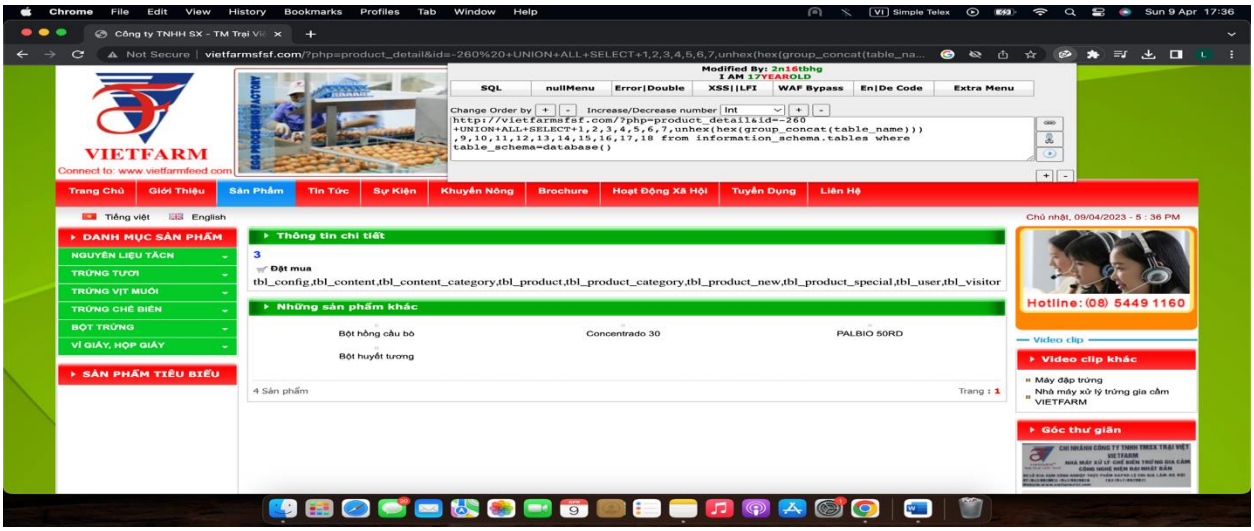
HHình 3. 7. Hình ảnh bước 4 (3)

➢ **Về User:**



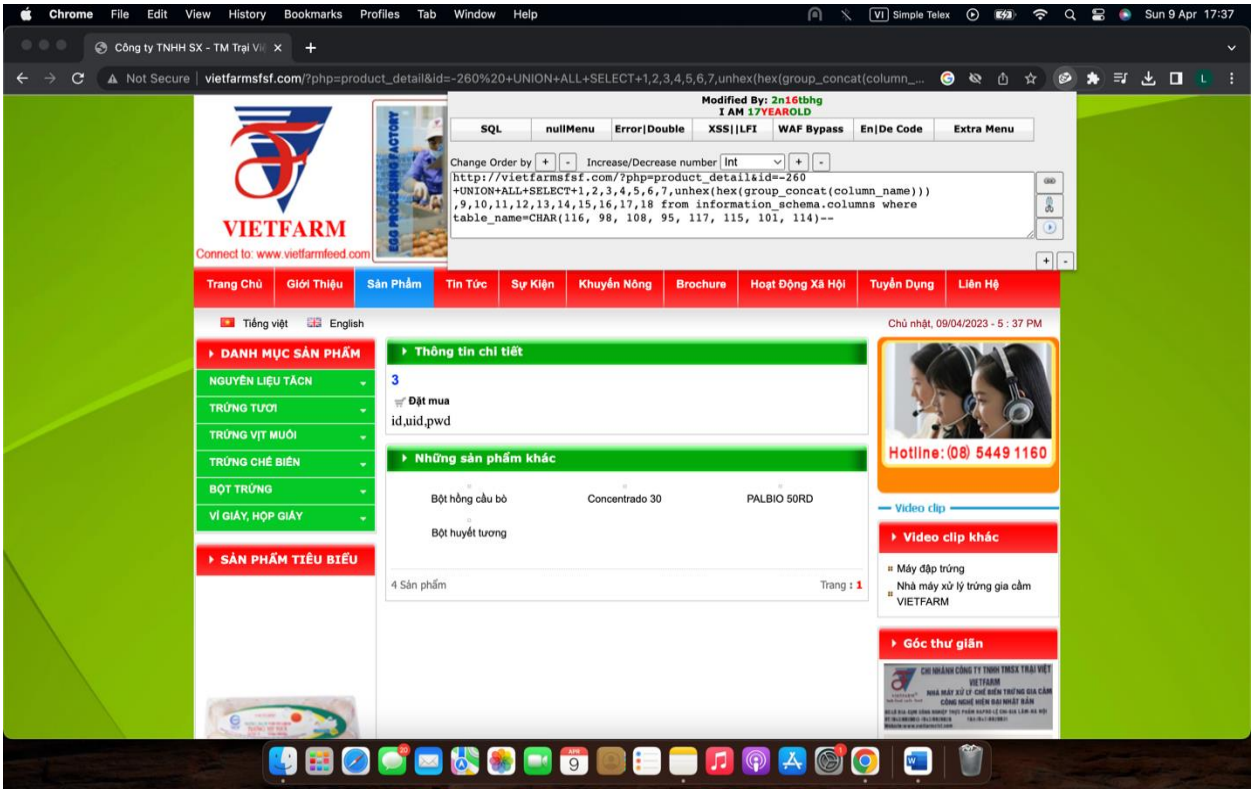
Hình 3. 8. Hình ảnh bước 4 (4)

Bước 5: Liệt kê các bảng trong database



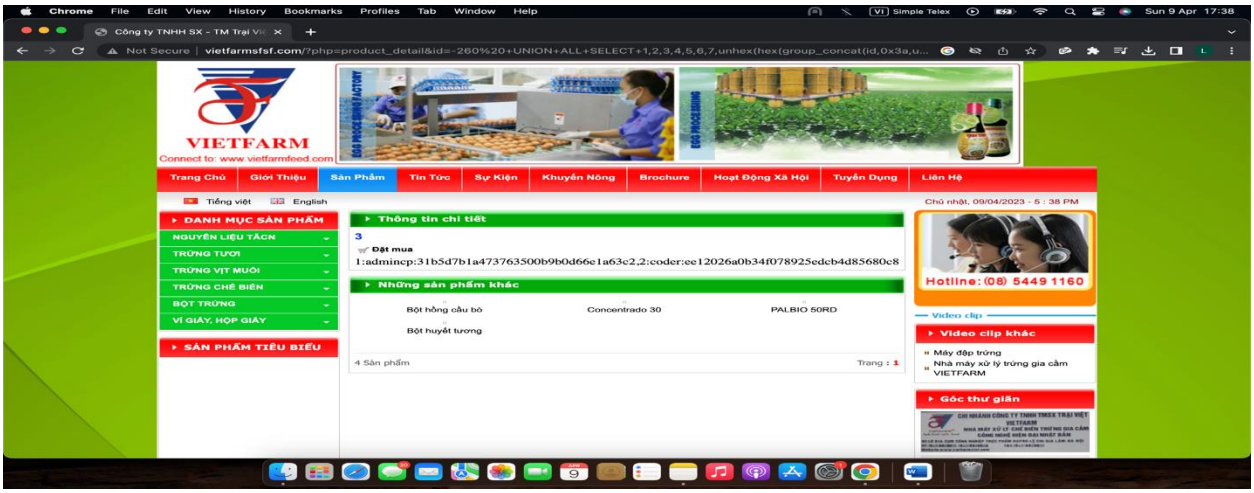
Hình 3. 9. Hình ảnh bước 5

Bước 6: Liệt kê các cột trong bảng tbl_user



Hình 3. 10. Hình ảnh bước 6

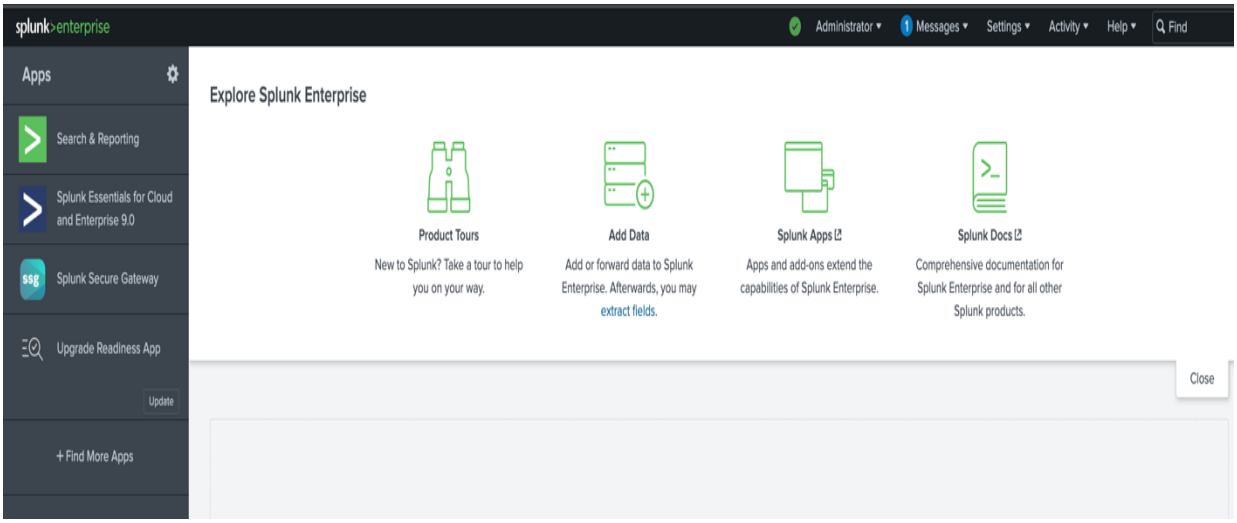
Bước 7: xem thông tin trong bảng tbt_user(id,uid,pwd)



Hình 3. 11. Hình ảnh bước 7

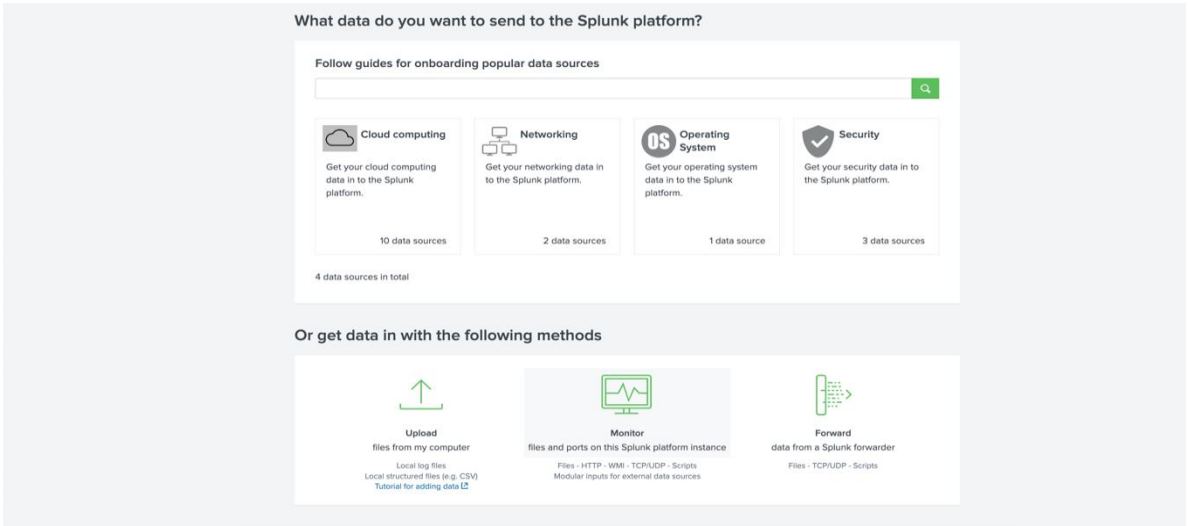
3.2. Phân tích tập nhật kí tấn công

Bước 1: nhấn add data



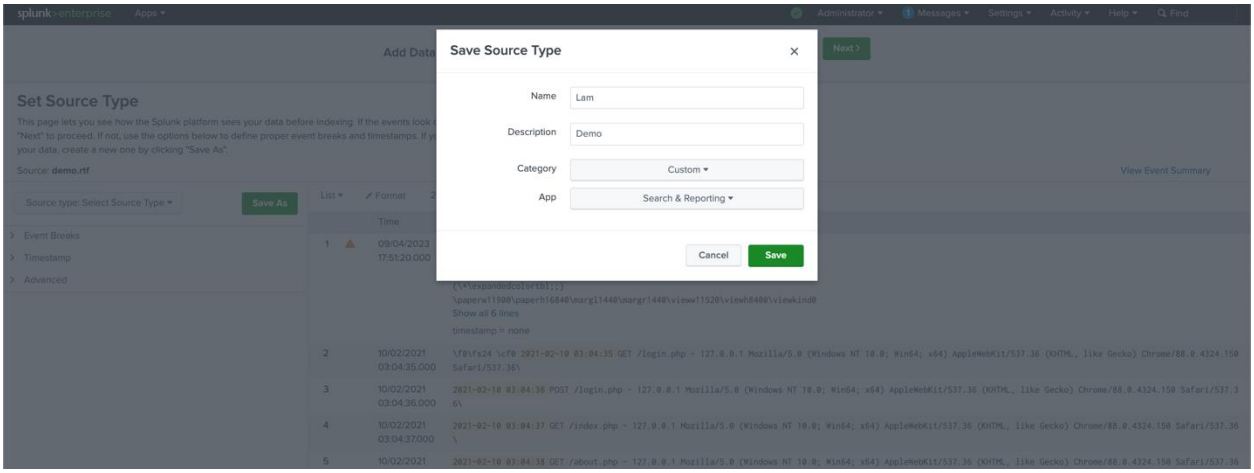
Hình 3. 12. Hình ảnh bước 1

Bước 2: Upload file



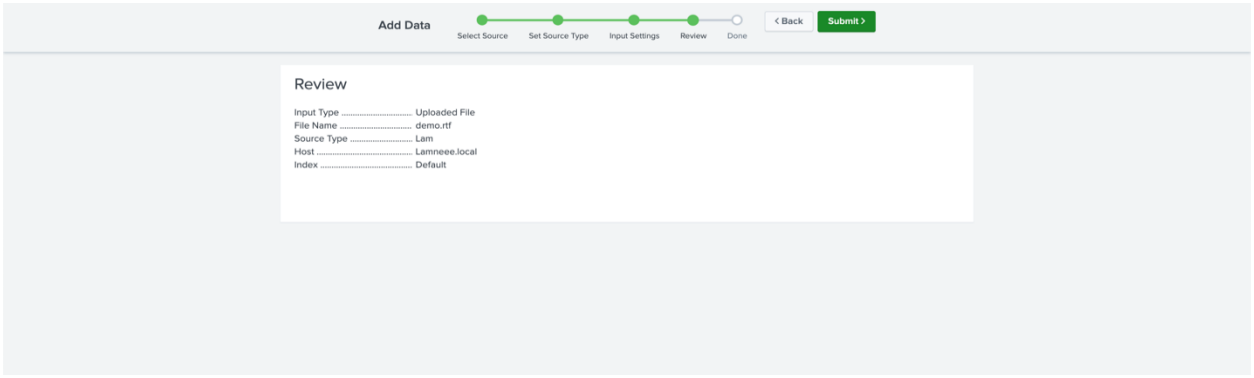
Hình 3. 13. Hình ảnh bước 2

Bước 3: Lưu thông tin cơ bản



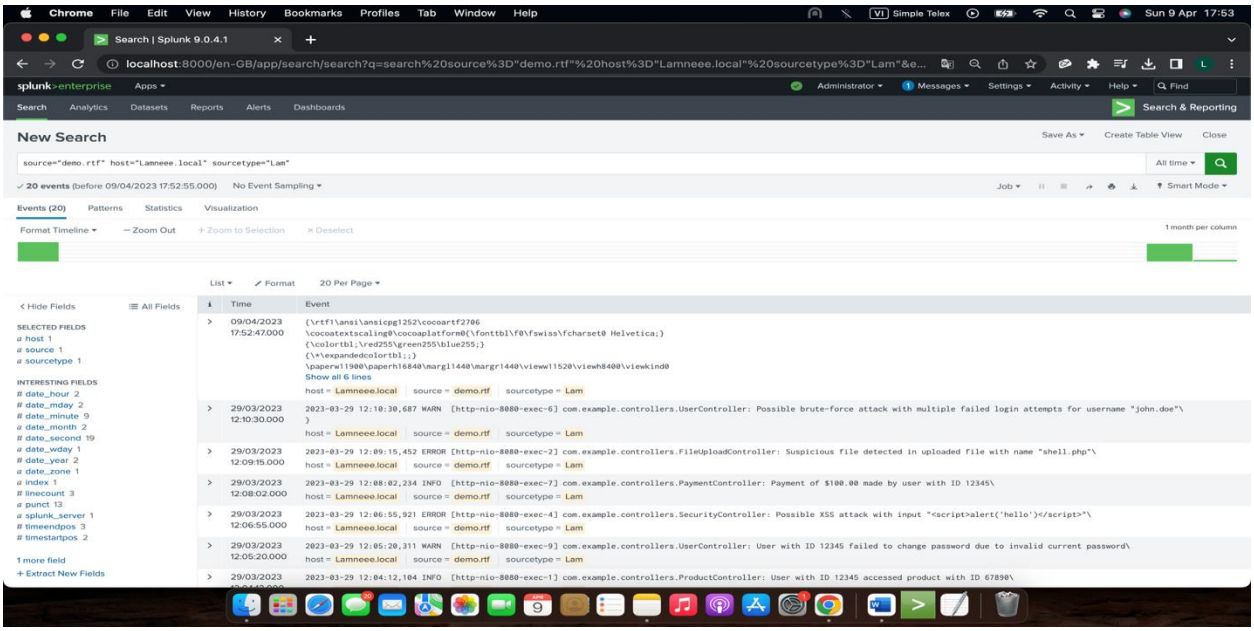
Hình 3. 14. Hình ảnh bước 3

Bước 4: Kiểm tra lại



Hình 3. 15. Hình ảnh bước 4

Bước 5: Kết quả



Hình 3. 16. Hình ảnh bước 5

CHƯƠNG 4: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

4.1. Kết quả:

Trong quá trình học tập và làm đồ án môn học với sự hướng dẫn tận tình của thầy giáo ThS. Phạm Trọng Huynh, đồ án môn học của em đã được hoàn thành đúng thời hạn và đạt được những kết quả như sau:

- Tìm hiểu các kĩ thuật tấn công Web.
- Tìm hiểu điều tra số và điều tra tấn công Web.
- Tìm hiểu về kĩ thuật điều tra và phân tích phía người dùng.
- Tìm hiểu về kĩ thuật điều tra và phân tích phía máy chủ.
- Tìm hiểu về kĩ thuật phân tích tập nhật kí.
- Xây dựng công cụ phân tích tập nhật kí tự động để phát hiện tấn công.

4.2. Hướng phát triển

- Hiểu được các phương pháp tấn công, phòng thủ cơ bản qua mạng máy tính hay website sẽ làm cho các lập trình viên phái triển các ứng dụng với tính bảo mặt, an toàn cho sản phẩm cao hơn.

- Tấn công, phòng thủ mạng hiện tại chỉ được quan tâm với số nhiều bởi các chuyên gia, các trung tâm bảo mật, các doanh nghiệp, chính phủ. Và vì thế nó rất hữu ích và hiệu quả cao khi được đưa vào các lớp, các khóa học của sinh viên.

CÁC TÀI LIỆU THAM KHẢO

Tài liệu:

[1] Bảo mật trên mạng, Bí quyết và giải pháp, NXB Thống kê, 3/2000

[2] Báo CAND số ra ngày 19/9/2016.

[3] COHE07Cohen, F., Managing network security- part 14: 50 ways to defeat Your intrusion detection system, Network Security,December 1997,pp.11-14.

[4] Dương Thanh Tuấn, Tìm hiểu kỹ thuật phòng thủ mạng, 2014.

[5] Hacking Exposed - Linux cna Brian Hatch - James Lee - George Kurtz.

[6] Hacking Exposed - Windows 2000 cna Joel Scambray - Stuart McClure.

[7] Một số hình thức tấn công mạng phổ biến, Bkav security

[8] Nguyễn Anh Tuấn, Các vấn đề về an ninh mạng, 2008 Network

[9] Security Secrets & Solution cna Joel Scambray - Stuart McClure

[10] Thái Hồng Nhị, An toàn thông tin mạng máy tính, truyền tin số và truyền dữ liệu, NXB Khoa học và kỹ thuật.

[11] Tài liệu kèm phần mềm FreeS/WAN (http:// www.freeswan.org)

[12] http://www.bkav.com.vn

[13] http://www.hackerVN.net

[14] http://packetstorm.secuify.com

15] http://www.warez.com/archive/serialnumbers