

BÀI TẬP CTF

Bảo mật web và ứng dụng – NT213.M21.ANTN

Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

Sinh viên thực hiện: *19520199 – Lê Tôn Nhân*

Challenge 3: Local File Inclusion - Wrappers (level medium)

Link challenge: <https://www.root-me.org/en/Challenges/Web-Server/Local-File-Inclusion-Wrappers>

- Thử thách yêu cầu ta lấy flag

Local File Inclusion - Wrappers

40 Points 

Abbreviated LFI

Author

sambecks, 2 March 2016

Level ?

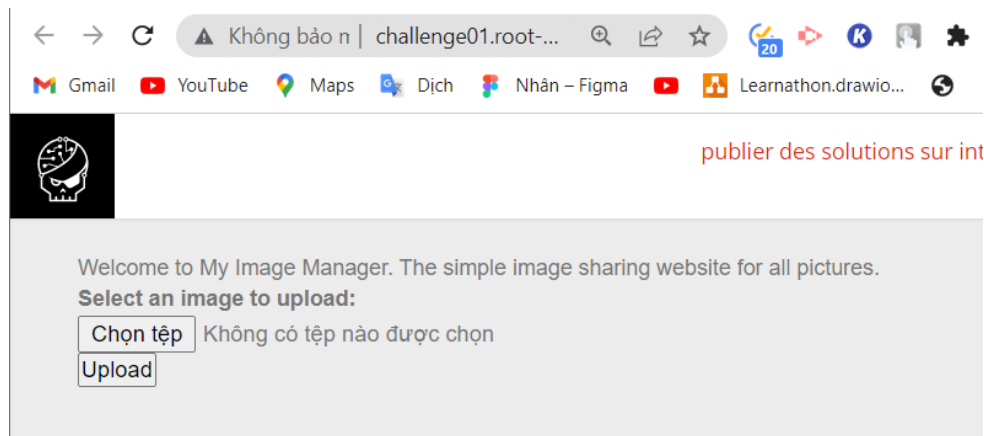


Statement

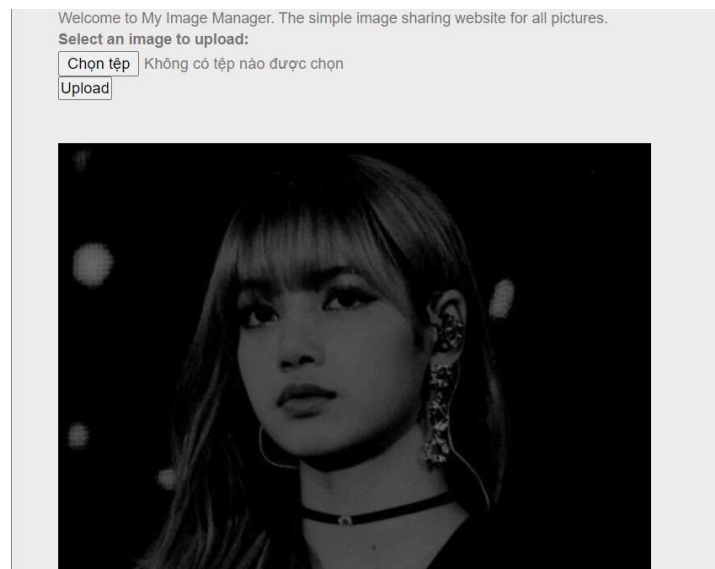
Retrieve the flag.

[Start the challenge](#)

- Truy cập vào challenge ta có trang web như bên dưới



- Trang web cho phép ta upload file ảnh
- Thử upload 1 file ảnh



- Ảnh của ta được hiển thị lên màn hình sau khi click vào upload
- Thử tìm kiếm các thử liên quan đến wrapper lfi ta tìm được giải pháp sau ([web-application-penetration-testing-local-file-inclusion-lfi-testing](#))

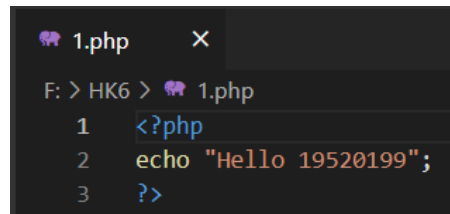
PHP ZIP Wrapper LFI

The zip wrapper processes uploaded .zip files server side allowing a penetration tester to upload a zip file using a vulnerable file upload function and leverage 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

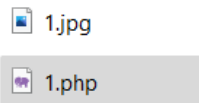
If the file upload function does not allow zip files to be uploaded, attempts can be made to bypass the file upload function (see: OWASP file upload testing document).

- Thực hiện làm theo các thủ thuật ở trên
 - o Tạo 1 file shell có extension là .php (đặt tên ngắn nhất có thể vì dài sẽ bị path name too long)
 - o Nén file thành zip. Vì ta cần up zip lên để sau đó giải nén ra file shell (Trong linux sử dụng command: `zip <shell name> <name zip>`)
 - o Trang web chỉ cho phép ta upload file JPG nên ta sẽ đổi đuôi file .zip thành .jpg (cái extension không quan trọng vì các byte header của file sẽ cho OS biết định dạng chính xác của file)
 - o Sau đó up lên và tìm đường dẫn đến file đó thông qua payload:
`?page=zip://<pathToZipFile>%23<shellFileName>`
 - o Ta không cần thêm đuôi .php vào cuối cùng (vì server sẽ mặc định đuôi file đó là .php, nếu ta nhập vào thì sẽ bị Attack Detect)
- Tạo file php với nội dung như bên dưới

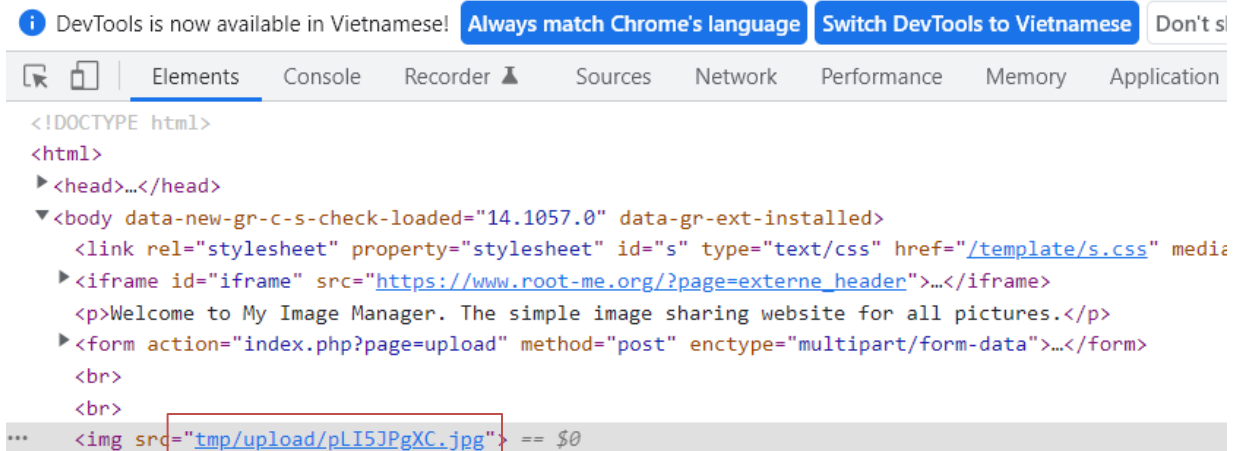


```
1 <?php
2 echo "Hello 19520199";
3 ?>
```

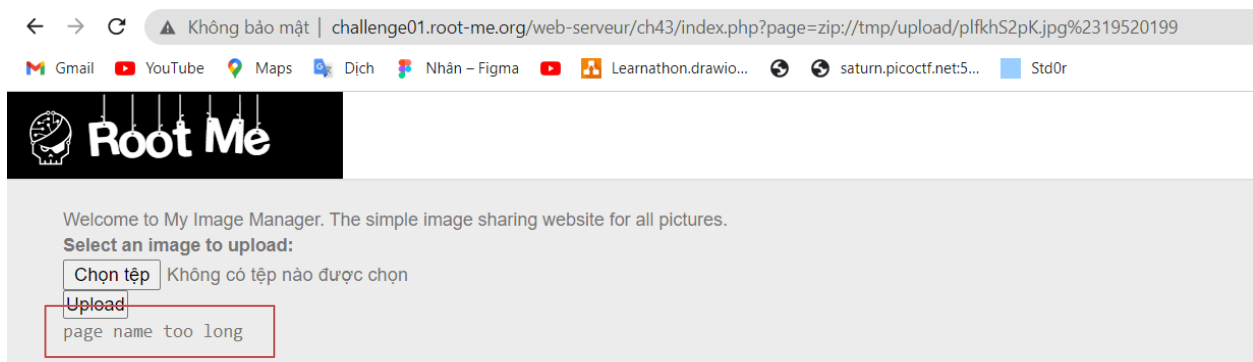
- Sau đó ta tiến hành zip và đổi tên thành jpg



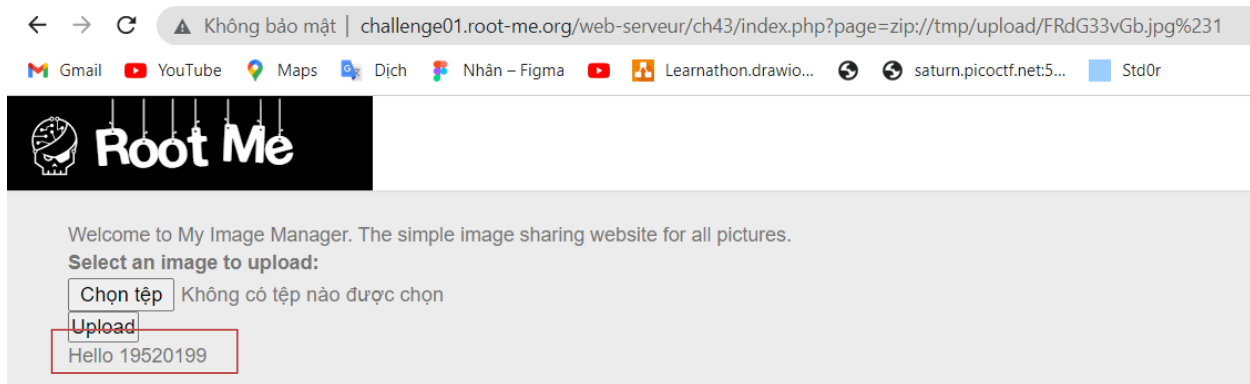
- Upload file này lên và kiểm tra mã nguồn



- Ta tìm được đường dẫn tới file là tmp/upload/pLI5JPgXC.jpg
- Sử dụng payload ?page=zip://<pathToZipFile>%23<shellFileName> và kiểm tra kết quả
- Trường hợp với tên file là 19520199 ta nhận được kết quả name quá dài



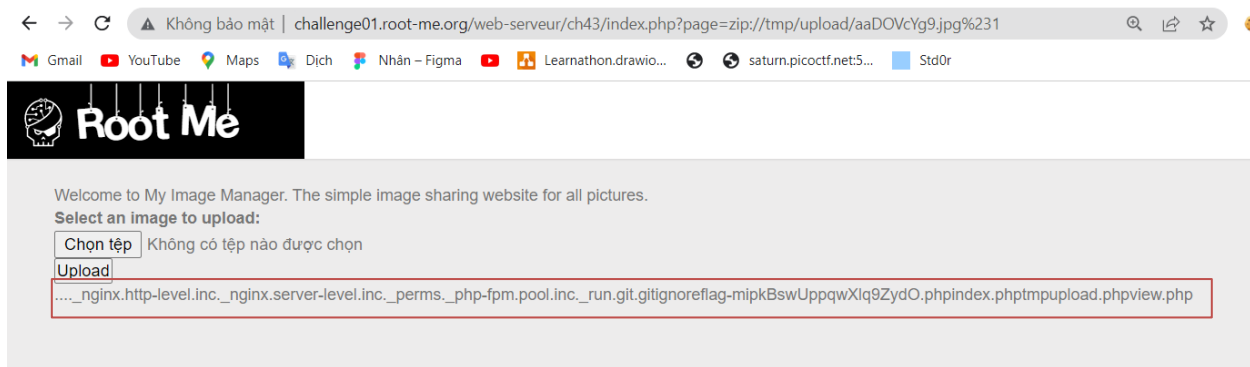
- Trường hợp với tên file là 1 ta thực thi code thành công



- Ta đã thực thi thành công đoạn code của mình. Vậy mục tiêu của ta là tìm flag từ một file nào đó
- Sử dụng đoạn code sau để scan tất cả các file có thể có

```
1.php X
F: > HK6 > 1.php
1 <?php
2 $scan = scandir('.'); foreach($scan as $file){echo $file;}
3 ?>
```

- Ta tìm được các file như bên dưới



- Ta thấy được 1 file có tên là **flag-mipkBswUppqwXlq9ZydO.php**
- Thay đổi code của ta thành đọc nội dung của file flag vừa tìm được

```
1.php X
F: > HK6 > 1.php
1 <?php
2 $data = file_get_contents("flag-mipkBswUppqwXlq9ZydO.php"); echo $data;
3 ?>
```

- Upload file và kết quả ta tìm được flag nằm trong phần comment, khi xem mã nguồn



- Ta thu được flag là **lf1-Wr4pp3r_Ph4R_pwn3d**
- Nộp flag vừa tìm được và ta vượt qua thử thách thành công

Local File Inclusion - Wrappers

40 Points 🌩️

Abbreviated LFI

Author

sambecks, 2 March 2016

Level ①



Statement

Retrieve the flag.

Start the challenge

6 related ressource(s)

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

Validation

Well done, you won 40 Points

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

FLAG: lf1-Wr4pp3r_Ph4R_pwn3d