php代码审计ctf隐藏了目录,CTF中PHP代码审计小tips-7

转载

yao lifu 于 2021-03-16 15:05:00 发布 62 收藏
文章标签： php代码审计ctf隐藏了目录
阅读次数

MiniProject_PHP_Code_audit-7 Writeup

整体逻辑：

xctf中的一道题目

考点：

接收参数中不能出现某一字符，file_get_contents()使用可以 php:// 伪协议绕过。

file_get_contents — 将整个文件读入一个字符串 file_get_contents() 函数是用于将文件的内容读入到一个字符串中的首选方法。如果操作系统支持，还会使用内存映射技术来增强性能。 但是接收参数中不能出现某一字符，file_get_contents()使用可以 php:// 伪协议绕过 。

php://input可以读取没有处理过的POST数据。相较于$HTTP_RAW_POST_DATA而言，它给内存带来的压力较小，并且不需要特 殊的php.ini设置。php://input不能用于enctype=multipart/form-data

Coentent-Type仅在取值为application/x-www-data-urlencoded和multipart/form-data两种情况下，PHP才会将http请求数据包中相应的数据填入全局变量$_POST

测试代码：class Read{

public $file = 'php://filter/read=convert.base64-encode/resource=f1aG.php';

}

$file = new Read;

echo serialize($file);

结果为序列化字符串【如图】：

Writeup：

借鉴大佬的思路，

这个题目考察的是php封装协议和lfi【图一为index.php，图二为class.php】

这个题目首先要突破的是：if(isset($user)&&(file_get_contents($user,'r')===”the user is admin”)) 如何让file_get_contents($user,'r')===”the user is admin”呢？ 答案是用php的封装协议php://input，因为php：//input可以得到原始的post数据【图三】：

然后我到了：include($file); //class.php 这一步 这个很明显是暗示你去读取class.php 如何读呢？这里用到php的另一个封装协议：php://filter 利用这个协议就可以读取任意文件了 利用方法：php://filter/convert.base64-encode/resource=index.php 这里把读取到的index.php的内容转换为base64的格式【图四】

但是class.php把我们引入到另一个地方，就是利用反序列化来读取flag文件 于是我们构造反序列化的参数【反序列化后续再讲】： http://localhost/ctf/index.php?user=php://input&file=class.php&pass=O:4:"Read":1:{s:4:"file";s:57:"php://filter/read=convert.base64-encode/resource=f1aG.php";} 这里也是利用php://filter来读取flag文件【图五，图六】

参考链接：