[ACTF2020 新生赛]Include

原创

-眼里有星河- 已于 2022-04-22 17:26:57 修改 954 收藏
分类专栏： 题目wp 文章标签： php web安全 网络
于 2022-04-22 17:25:10 首次发布

打开有个链接tips，再点进去发现一句话

```
Can you find out the flag?
```

而且后面传入一个参数是file=flag.php

```
http://39f0e8ed-769a-4b4b-84d3-52367874da03.node4.buuoj.cn:81/?file=flag.php
```

而且题目名字是include，所以这肯定是一个文件包含漏洞的题

接下来我们学习一下伪协议

> php:// 访问各个输入/输出流（I/O streams），在CTF中经常使用的
> 是php://filter和php://input，php://filter用于**读取源码**，php://input用于**执行php代码**。

下面是常见伪协议的作用

协议	作用
php://input	可以访问请求的原始数据的只读流，在POST请求中访问POST的data部分，在enctype="multipart/form-data" 的时候php://input 是无效的。
php://output	只写的数据流，允许以 print 和 echo 一样的方式写入到输出缓冲区。
php://fd	(>=5.3.6)允许直接访问指定的文件描述符。例如 php://fd/3 引用了文件描述符 3。
php://memory php://temp	(>=5.1.0)一个类似文件包装器的数据流，允许读写临时数据。两者的唯一区别是 php://memory 总是把数据储存在内存中，而 php://temp 会在内存量达到预定义的限制后（默认是 2MB）存入临时文件中。临时文件位置的决定和 sys_get_temp_dir() 的方式一致。
php://filter	(>=5.0.0)一种元封装器，设计用于数据流打开时的筛选过滤应用。对于一体式（all-in-one）的文件函数非常有用，类似 readfile()、file() 和 file_get_contents()，在数据流内容读取之前没有机会应用其他过滤器。

php://filter参数详解

该协议的参数会在该协议路径上进行传递，多个参数都可以在一个路径上传递。具体参考如下：

php://filter 参数	描述	
resource=<要过滤的数据流>	必须项。它指定了你要筛选过滤的数据流。	
read=<读链的过滤器>	可选项。可以设定一个或多个过滤器名称，以管道符（*\	*）分隔。
write=<写链的过滤器>	可选项。可以设定一个或多个过滤器名称，以管道符（\	）分隔。
<; 两个链的过滤器>	任何没有以 *read=* 或 *write=* 作前缀的筛选器列表会视情况应用于读或写链。	

想了解更多或者想了解其他伪协议请参考PHP伪协议总结 - SegmentFault 思否

构造payload

```
?file=php://filter/read=convert.base64-encode/resource=flag.php
```

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZTNkNDI1OTUtZjdiYy00YTA5LWE0M2MtYzdhN2ViNmFhM2UzfQo=

得到的base64字符串再decode一下就得到flag

```
<?php
echo "Can you find out the flag?";
//flag{e3d42595-f7bc-4a09-a43c-c7a7eb6aa3e3}
```