文件包含 [ACTF2020 新生赛]Include1（php://filter协议）

原创

一醉一休 已于 2022-02-23 17:01:01 修改 108 收藏
分类专栏： web 文章标签： web安全
于 2022-02-23 17:00:24 首次发布

简介

服务器解析执行php文件时能够通过包含函数加载另外一个文件中的php代码，当被包含的文件中存在木马时，也就意味着木马程序会在服务器上加载执行

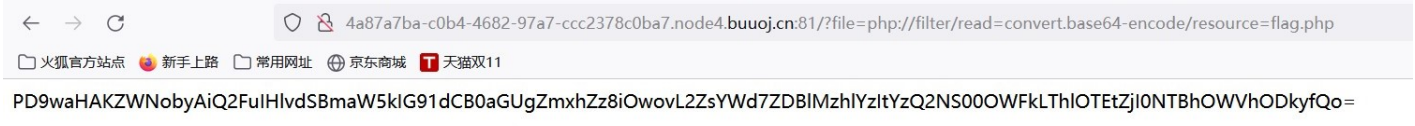
[ACTF2020 新生赛]Include1（php://filter协议）

1）一点开题目，没看到什么，点这个提示

2）只有这一句话

3）可以看到网址后面多了一个文件，也没有发现其他东西，可能是文件包含

4）文件包含直接读取的是文件，而不是文件源码，所以要想办法读取源码
`php://filter/read=convert.base64-encode/resource=xxx.php`（这个方法可以读取代码）



5）将文件源代码进行base64编码，然后网上小工具进行解码

Base64编码转换

```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZDBlMzhlYzItYzQ2NS00OWFkLThlOTEtZjI0NTBhOWVhODkyfQo=
```

清空 加密 解密 ☐解密为UTF-8字节流

```
<?php
echo "Can you find out the flag?";
//flag{d0e38ec2-c465-49ad-8e91-f2450a9ea892}
```


6）可以看到flag是被注释的

#对php://filter协议的理解

1）php://filter 是php中独有的一个协议，可以作为一个中间流来处理其他流，可以进行任意文件 的读取

1：是格式
2：是可选参数，有read和write，字面意思就是读和写
3：是过滤器。主要有四种：字符串过滤器，转换过滤器，压缩过滤器，加密过滤器。filter里可以 用一或多个过滤器（中间用|隔开），这也为解题提供了多种方法，灵活运用过滤器是解题的 关键。这里的过滤器是把文件flag.php里的代码转换（convert）为base64编码（encode）
4：是必选参数，后面写你要处理的文件名

2）read参数值可为
string.strip_tags： 将数据流中的所有html标签清除
string.toupper： 将数据流中的内容转换为大写
string.tolower： 将数据流中的内容转换为小写
convert.base64-encode： 将数据流中的内容转换为base64编码

convert.base64-decode： 与上面对应解码为典型的文件包含漏洞

我们可以通过构造含有漏洞的语句，查看想要看的代码： file=php://filter/read=convert.base64-encode/resource=index.php 。再将得到的base64码解码即可

3）read的应用

这会以字母全部大写的形式输出index.php文件内容，并且还会用rot13进行加密

file=php://filter/read=string.toupper |string.rot13/resource=index.php