

# [ACTF2020 新生赛]Include 1 -WP

原创

秋水want揽星河 于 2022-03-10 19:02:43 发布 3494 收藏

分类专栏: [笔记](#) 文章标签: [php](#) [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/m0\\_52314120/article/details/123408317](https://blog.csdn.net/m0_52314120/article/details/123408317)

版权

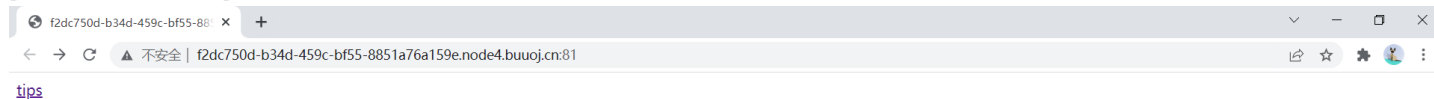


[笔记](#) 专栏收录该内容

6 篇文章 0 订阅

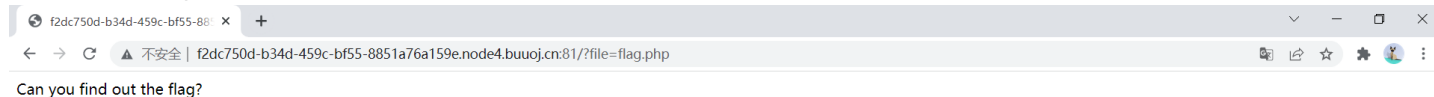
订阅专栏

[ACTF2020 新生赛]Include



CSDN @秋水want揽星河

进入页面后的Tips进入正题

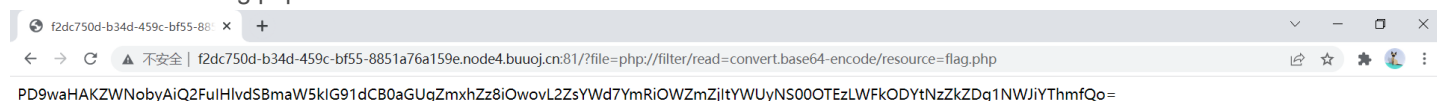


观察URL发现关键字，猜测为文件包含

使用PHP伪协议测试代码，使用php://input的协议，发现过滤器。

则考虑php://filter——设计用于数据流打开时的筛选过滤应用。对于一体式的文件函数非常有用

编码后构造Payload：`http://f29b525f-b020-42cf-9117-b500de373d55.node4.buuoj.cn:81/?file=php://filter/read=convert.base64-encode/resource=flag.php`



解码后得到flag

另附自用帖集合帖用以伪协议学习：

<https://segmentfault.com/a/1190000018991087>