

# BUU-[ACTF2020 新生赛]Include 1

原创

[一只会飞的猪-FlaggingPig1](#)  于 2021-02-04 22:23:24 发布  118  收藏

分类专栏: [自学 ctfhub题目](#)

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/weixin\\_47346400/article/details/113665637](https://blog.csdn.net/weixin_47346400/article/details/113665637)

版权



[自学](#) 同时被 2 个专栏收录

34 篇文章 0 订阅

订阅专栏



[ctfhub题目](#)

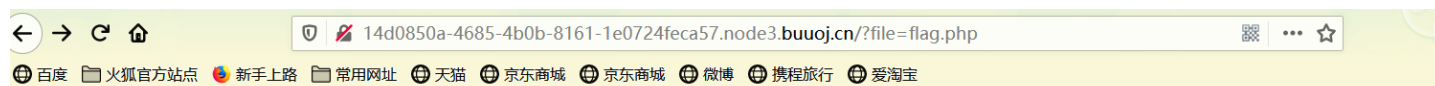
11 篇文章 0 订阅

订阅专栏

[ACTF2020 新生赛]Include

打开靶机发现一个超链接，点击之后出现一段话

“Can you find out the flag?”

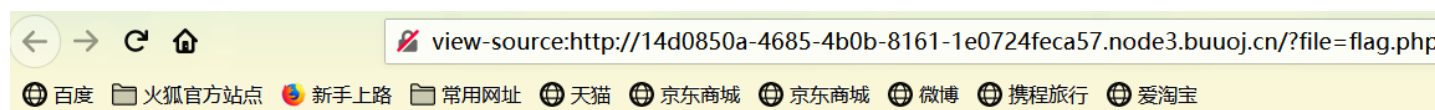


Can you find out the flag?



解题思路:

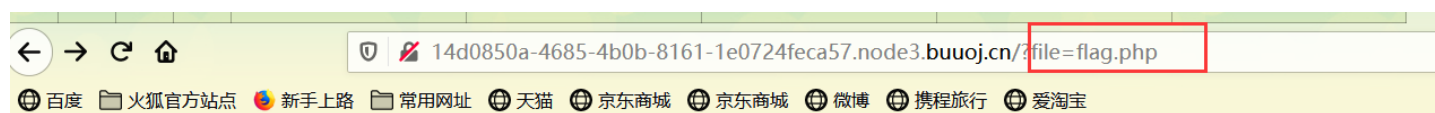
①查看源码注入，无果，



- 1 `<meta charset="utf8">`
- 2 Can you find out the flag?

②抓包，无果

③仔细看url，发现有flag.php



Can you find out the flag?

判断此题为PHP伪协议题目

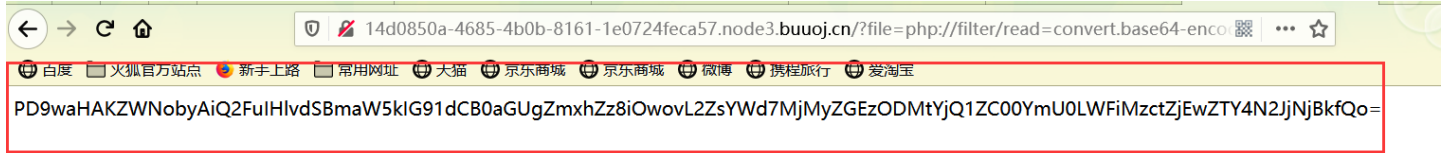
构建payload

## php://filter 伪协议

该伪协议读取源代码并进行base64编码输出，不然会直接当做php代码执行就看不到源代码内容了。

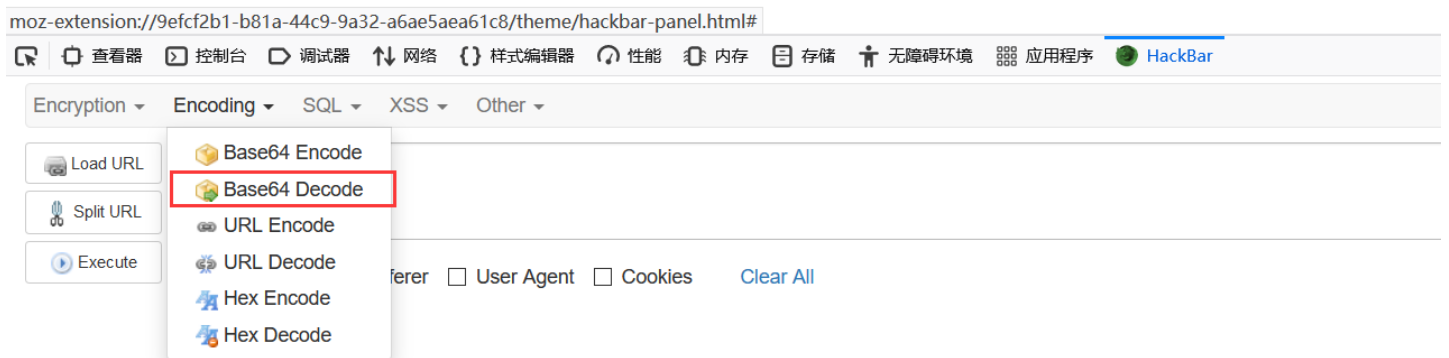
```
php://filter/read=convert.base64-encode/resource=XXX.php
```

得到base64编码的flag.php,进行解码:



[https://blog.csdn.net/weixin\\_47346400](https://blog.csdn.net/weixin_47346400)

在这使用firefox中的hackbar



[https://blog.csdn.net/weixin\\_47346400](https://blog.csdn.net/weixin_47346400)

成功得到flag



[https://blog.csdn.net/weixin\\_47346400](https://blog.csdn.net/weixin_47346400)

over



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)