

【ACTF2020】新生赛]Include

原创

Dddddddddd. 于 2021-08-02 01:07:08 发布 74 收藏

文章标签: [unctf](#)

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/DddddXxxxx/article/details/119307494>

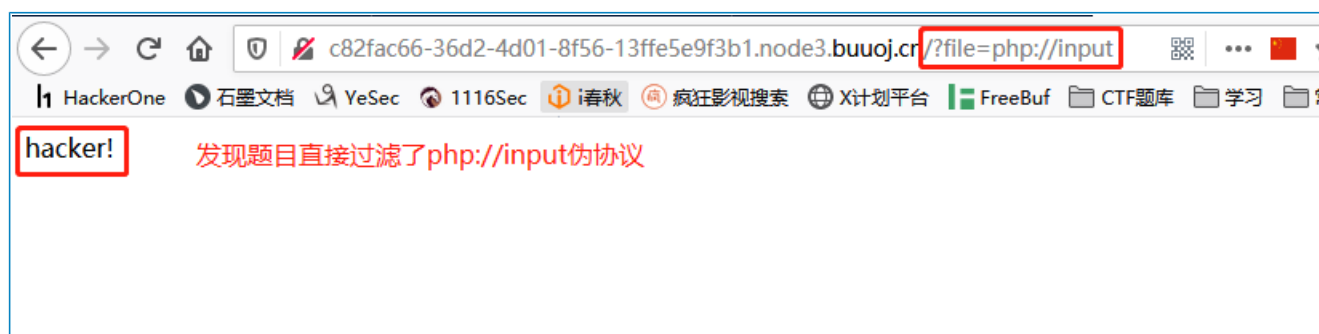
版权

本题主要考查了利用php://filter伪协议进行文件包含

进入题目根据Tip进入正题, 可以看到URL中存在文件包含(题目名也很直接)



首先考虑 "php://input"伪协议 + POST发送PHP代码 的经典套路

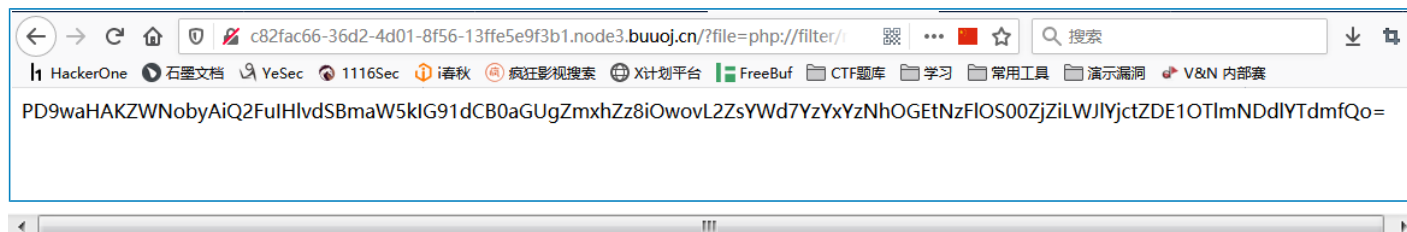


重新考虑之后使用 "php://filter"伪协议" 来进行包含。当它与包含函数结合时, php://filter流会被当作php文件执行。所以我们一般对其进行编码, 阻止其不执行。从而导致任意文件读取。

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

这里需要注意的是使用php://filter伪协议进行文件包含时, 需要加上read=convert.base64-encode来对文件内容进行编码

发送请求得到base64编码后的flag.php文件源码:



解码之, 得到Flag