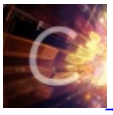
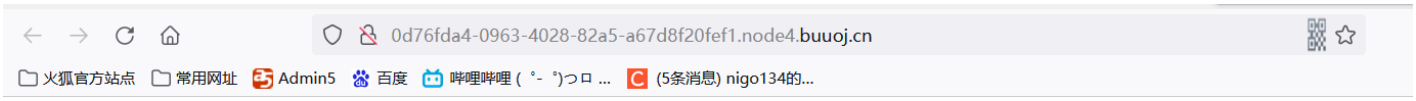
NO.5 [ACTF2020 新生赛]Include

原创

nigo134 于 2021-07-19 16:08:28 发布 12 收藏
分类专栏： 文件操作 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/nigo134/article/details/118899180
版权


文件操作 同时被 2 个专栏收录
1 篇文章 0 订阅
订阅专栏


BUUCTF
57 篇文章 0 订阅
订阅专栏



tips

https://blog.csdn.net/nigo134

知识点

?file=flag.php 猜测文件包含漏洞

php://filter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。

php://filter 伪协议文件包含读取源代码，加上read=convert.base64-encode，用base64编码输出，不然会直接当做php代码执行，看不到源代码内容。

php://input 伪协议 + POST发送PHP代码 （不行）

payload:

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

base64解密后得到flag