BUUCTF[ACTF2020 新生赛]Include

原创

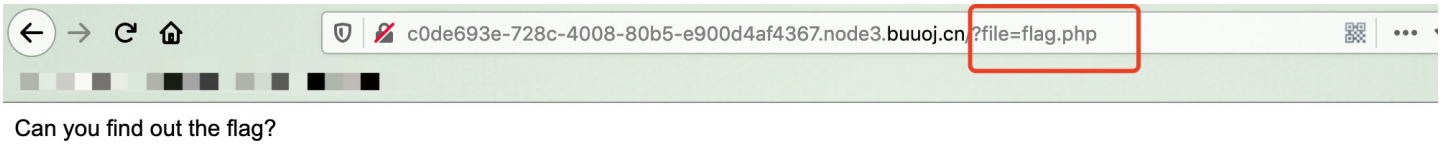
F10NAF11pp3d 于 2020-12-30 11:45:02 发布 56 收藏

分类专栏： BUUCTF

本文链接：https://blog.csdn.net/m0_46481239/article/details/111955468

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



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。

将得到的base64编码解码

得到flag