[buuoj记录][ACTF2020 新生赛]Include

原创

Matrix_Ceasor 于 2020-06-25 12:04:38 发布 120 收藏

分类专栏： web 文章标签： php

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/qq_42250840/article/details/106956726

版权

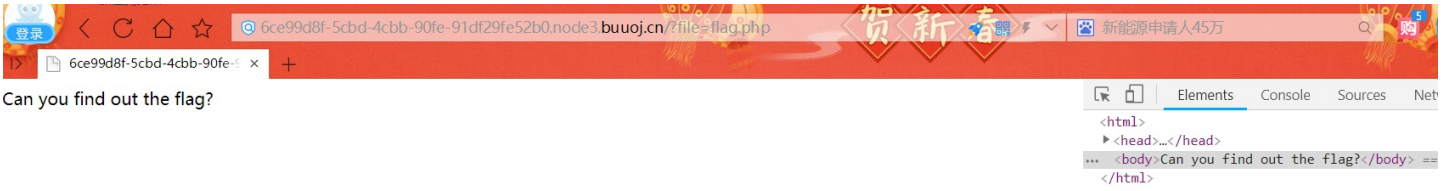
web 专栏收录该内容

16 篇文章 0 订阅

订阅专栏

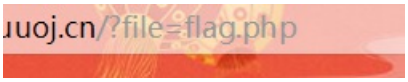
圈重点：*利用php://filter伪协议进行文件包含*

不多说，按照提示点进去



https://blog.csdn.net/qq_42250840

看到这，考虑"php://input"伪协议 + POST发送PHP代码

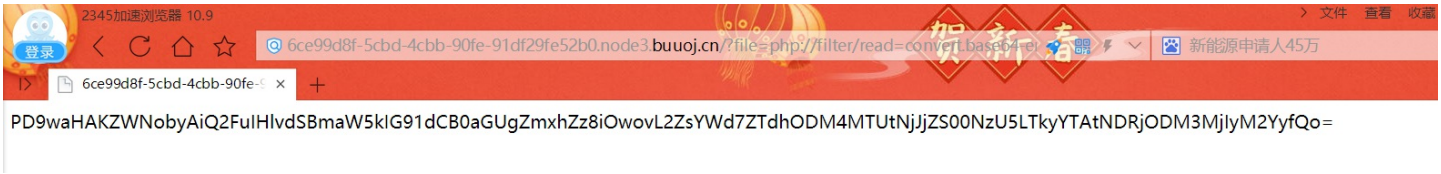


题目对php://input 进行了过滤

那就再试试 “php://filter"伪协议” 来进行包含

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

成功读取源码：



解码得到flag：

```php
<?php
echo "Can you find out the flag?";
//flag{c61c3a8a-71e9-4f6b-beb7-d1599f47ea7f}
```

本题考点：php://filter伪协议，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。