




buuctf include

原创

@DR  于 2021-01-13 14:58:51 发布  135  收藏 2

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/weixin_45711265/article/details/112565753

版权

Buuctf 的题：

include

首先考虑 "php://input" 伪协议 + POST 发送 PHP 代码 的经典套路,发现题目过滤了 php: //input 伪协议。

再考虑用 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。

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，解码得到 flag.