buuctf include

原创

@DR 于 2021-01-13 14:58:51 发布 135 收藏 2

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.