

# 攻防世界unserialize3

原创

[whisper\\_ZH](#) 于 2019-09-29 11:02:04 发布 1749 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/whisper\\_ZH/article/details/101676499](https://blog.csdn.net/whisper_ZH/article/details/101676499)

版权

## 本题学习知识点：

### PHP \_\_wakeup()函数漏洞

在程序执行前，serialize() 函数会首先检查是否存在一个魔术方法 \_\_sleep.如果存在，\_\_sleep()方法会先被调用，然后才执行串行化（序列化）操作。这个功能可以用于清理对象，并返回一个包含对象中所有变量名称的数组。如果该方法不返回任何内容，则NULL被序列化，导致一个E\_NOTICE错误。与之相反，unserialize()会检查是否存在一个\_\_wakeup方法。如果存在，则会先调用 \_\_wakeup方法，预先准备对象数据。但是这个wakeup()是可以被绕过的  
\_\_wakeup 触发于 unserialize() 调用之前,当反序列化时的字符串所对应的对象的数目被修改,\_\_wake 的函数就不会被调用.并且不会重建为对象,但是会触发其他的魔术方法比如\_\_destruct

[绕过方法及漏洞详细内容1](#)

[绕过方法及漏洞详细内容2](#)

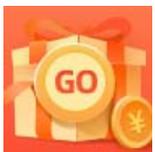
## 本题操作流程

点开题目明显看到是用code传参，利用wakeup函数漏洞进行操作



按本题知识先传入一个参数，成功触发了wakeup函数，拿到flag

the answer is : cyberpeace{



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)