攻防世界unserialize3题解

原创

shayebudon 于 2021-12-11 14:35:11 发布 2018 收藏
文章标签： web安全 安全

魔法函数，通常不需要我们手动调用，一般魔法函数是以__开头的，再碰到这几个魔法函数时就好好好想想能不能利用序列化与反序列化漏洞了：

__constuct()　在创建对象是自动调用

__destuct() 相当于c++中的析构最后会将对象销毁，所以在对象销毁时 被调用

__toString()　但一个对象被当成字符串使用时被调用

__sleep()　当对象被序列化之前使用

__wakeup() 将在被序列化后立即被调用 //咱们这道题就是利用的这个来利用序列化的

查看本题代码

看到了魔法函数_wakeup，在序列化后被调用

__wakeup()执行漏洞：一个字符串或对象被序列化后，如果其属性被修改，则不会执行__wakeup()函数，这也是一个绕过点。

将这个对象进行序列化传值，修改其属性这样就可以进行绕过__wakeup了

当被反序列化的字符串其中对应的对象的属性个数发生变化时，会导致反序列化失败而同时使得_wakeup()函数失效，就是问题的关键所在。正常结果应该为O:4:"xctf":1:{s:4:"flag";s:3:"111";}

改变字符串对应的对象个数属性

O:4:"xctf":2:{s:4:"flag";s:3:"111";} 绕过_wakeup

the answer is : cyberpeace{d2590faeda03ee383a7310de22c94102}