漏洞影响版本

PHP5 < 5.6.25 PHP7 < 7.0.10

漏洞原理

`__wakeup`触发于`unserilize()`调用之前，但是如果被反序列话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`失效。

参考链接

https://www.cnblogs.com/zy-king-karl/p/11436872.html 本人参考这位师傅的博客而写。

漏洞验证

验证条件

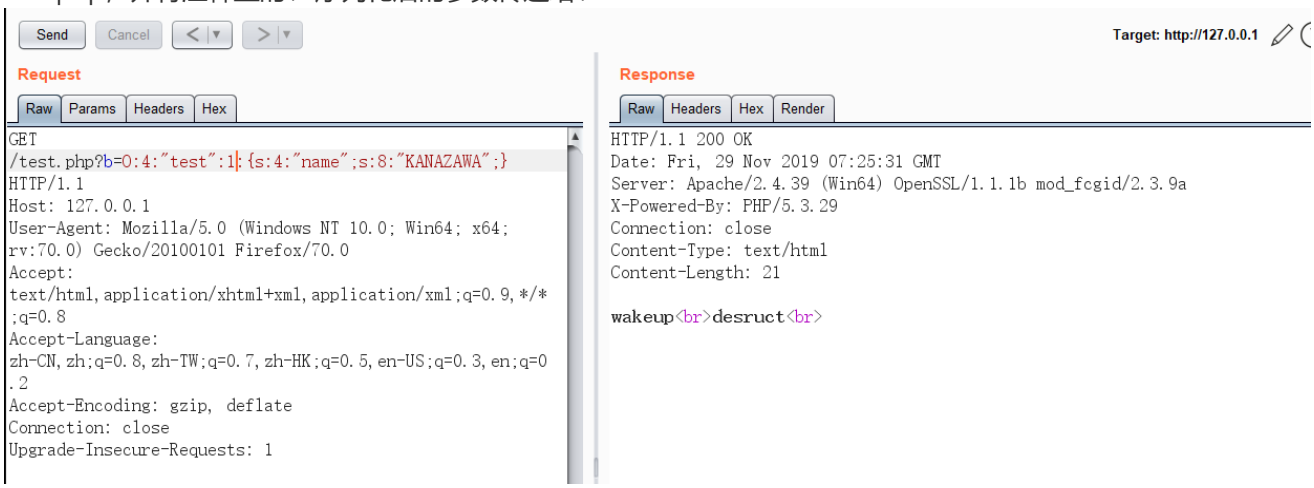
PHP5 < 5.6.25 PHP7 < 7.0.10

验证过程

编写一个测试脚本 test.php

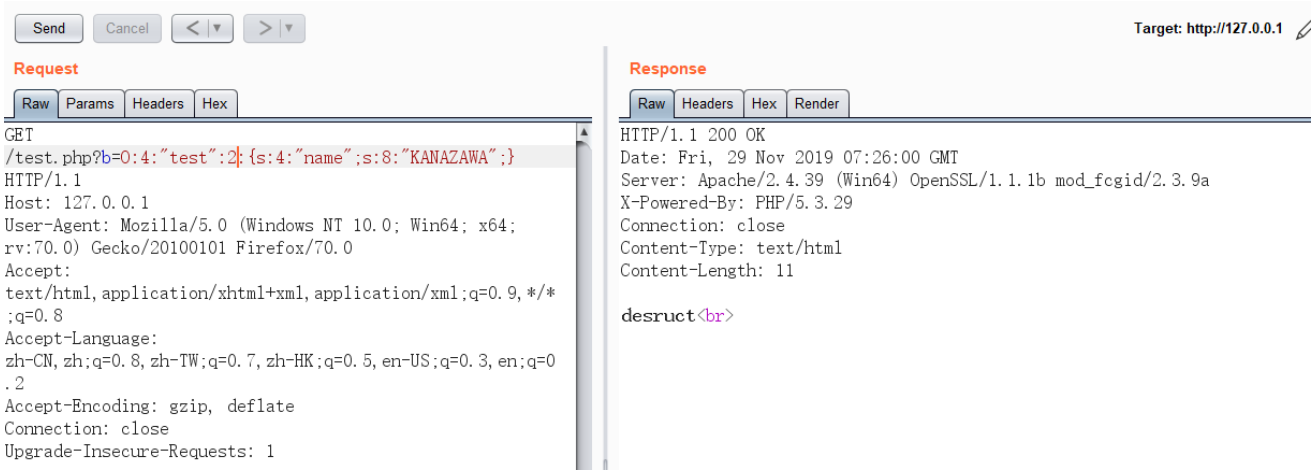
```php
<?php

class test{
    public $name = "KANAZAWA";
    public function __wakeup(){
        echo "wakeup<br>";
    }
    public function __destruct(){
        echo "desruct<br>";
    }
}

/*$a = new test();
$a = serialize($a);
echo $a;
$a = O:4:"test":1:{s:4:"name";s:8:"KANAZAWA";}*/

$b = $_GET['b'];
@$un_b = unserialize($b);
echo $un_b->name."<br>";

?>
```

访问test.php，并将注释里的$a序列化后的参数传递给$b



可以发现发序列化前先调用的是**_wakeup**方法，再调用**_destruct**。

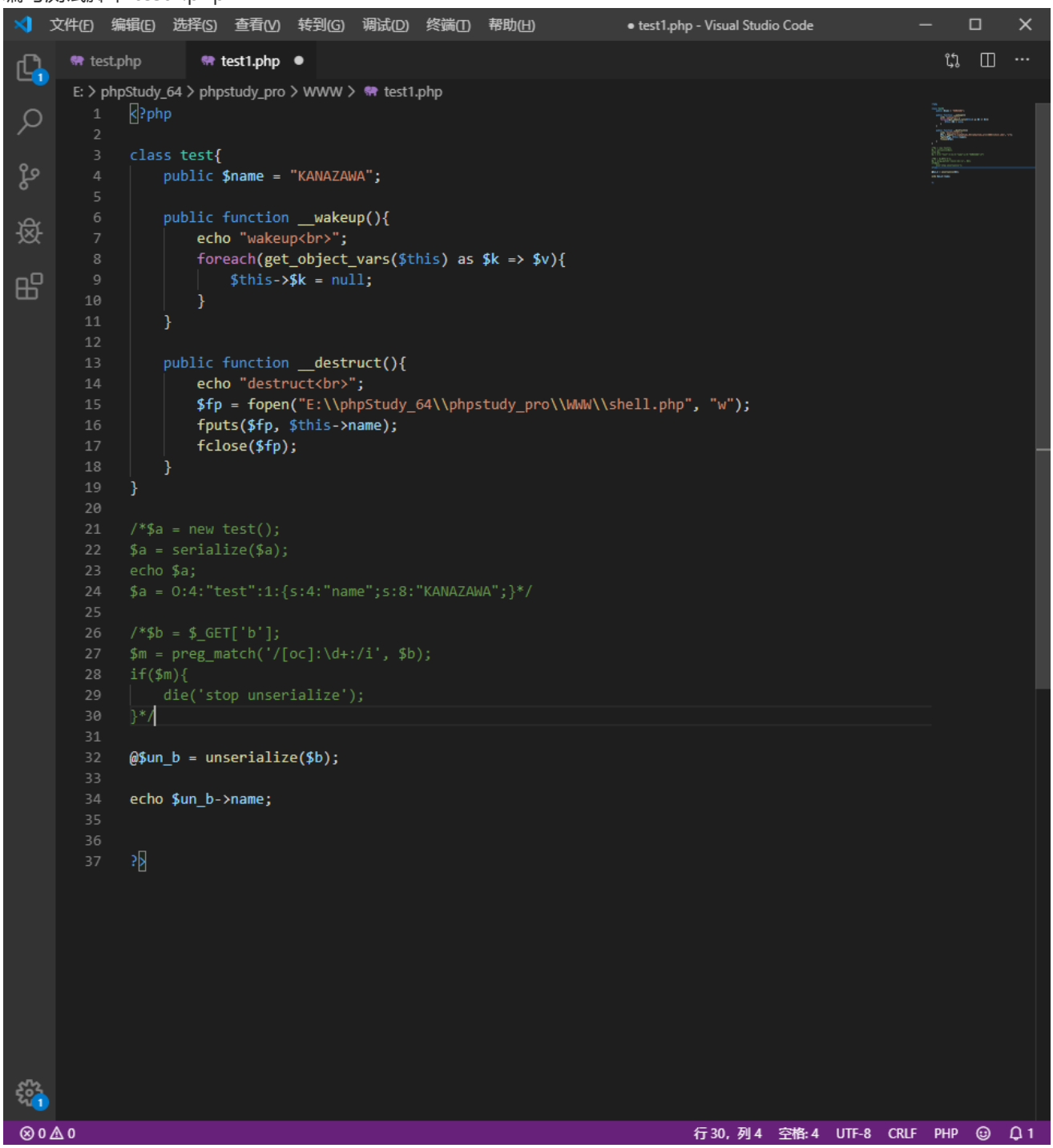
现将传入的序列化数据的对象变量个数由1更改为2，看看执行结果。



可发现页面只执行了**_destruct**方法。

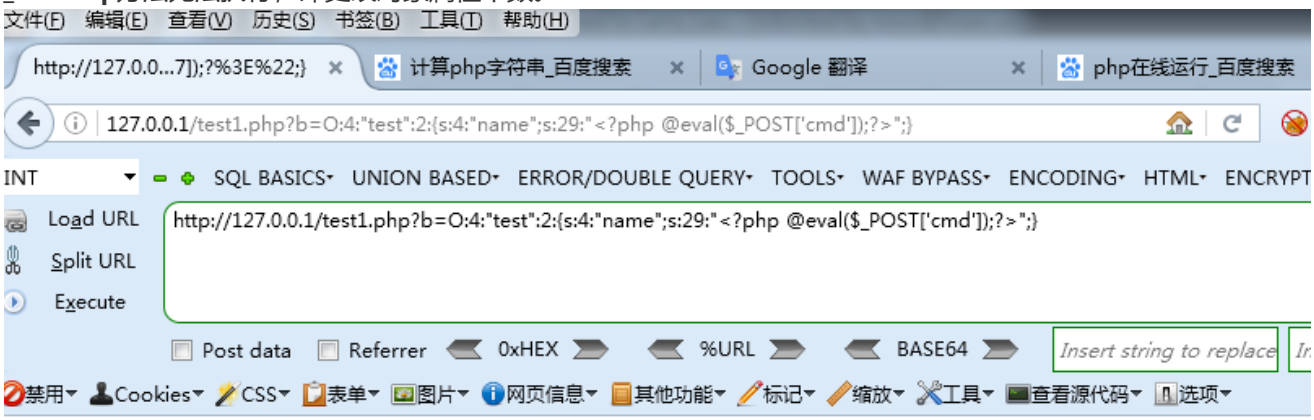
漏洞利用

编写测试脚本 test1.php



可以发现**'/[oc]:\d+:/i'**，它是过滤输入的object类型，但是我们可以进行绕过**o:4->o:+4**,这样就可以完成绕过。

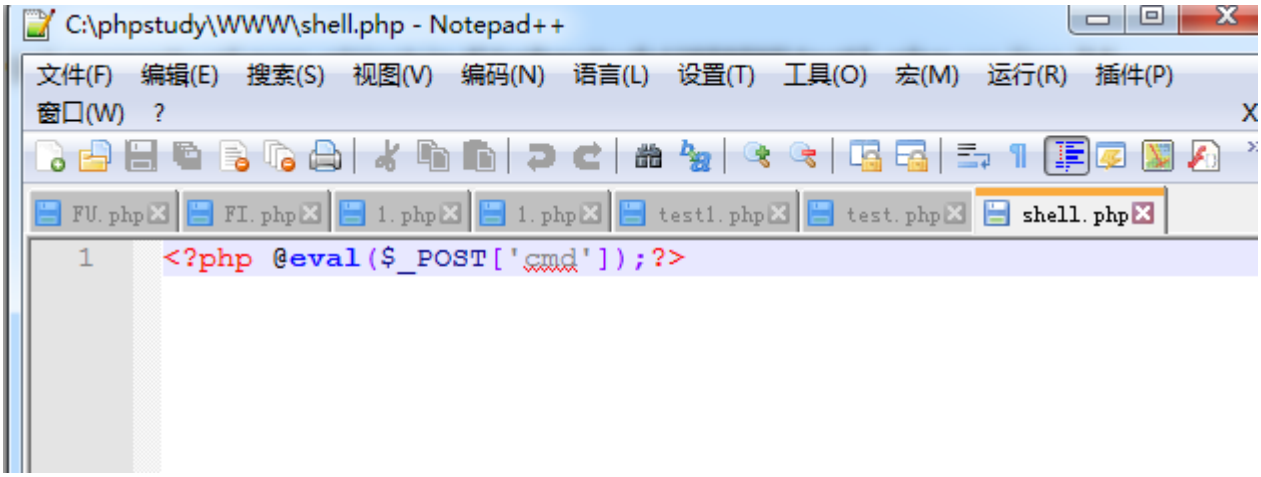
在进一步审计，发现**_wakeup**方法中清除了对象属性，使得**_destruct**方法中写入文件内容会为空，所以我们得让**_wakeup**方法无法执行，即更改对象属性个数。



destruct

Notice: Trying to get property of non-object in **C:\phpstudy\WWW\test1.php** on line **34**

写入成功



防御方式

升级php版本