【PHP数组key溢出】2021.6.1萌新赛 easy_web WriteUp

原创

Lxxx 于 2021-06-30 20:53:28 发布 113 收藏

分类专栏： 网络安全

本文链接：https://blog.csdn.net/qq_43661593/article/details/118369294

题目描述：

前景知识：

PHP数组key溢出：

> 通过PHP创建关联数组的时候，键值Key如果是数值型（可通过is_numeric()判断），则会在int有效范围内被自动转换为int型，如果超过int有效范围就会有问题，这就涉及到数组键值Key作为int型时的有效范围判断。

> PHP的int型数据取值范围，与操作系统相关，32位系统上为2的31次方，即-2147483648到2147483647，64位系统上为2的63次方，即-9223372036854775808到9223372036854775807。

这里给一段测试代码，测试环境如下

```
root@kali:~# php -v
PHP 7.4.15 (cli) (built: Feb 20 2021 09:45:56) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
    with Zend OPcache v7.4.15, Copyright (c), by Zend Technologies
```

首先测试一个普通情况，利用`array`函数创建一个数组

```
php > $arr = array( 1 => 'test1');
php > var_dump($arr[]=1);
int(1)
```

```
root@kali:~# php -a
Interactive mode enabled

php > $arr = array( 1 => 'test1');
php > var_dump($arr[]=1);
int(1)
```

这个时候往数组里插入一个值，然后使用`var_dump`一下，发现是可以正常返回的

但是，当我们的数组下标`key`足够大的时候，例如以下情况

```
php > $arr = array( 9223372036854775807 => 'test1' , 9223372036854775808 =>'test2');
php > var_dump($arr[]=1);
PHP Warning:  Cannot add element to the array as the next element is already occupied in php shell code on line 1
NULL
```

```
php > $arr = array( 9223372036854775807 => 'test1' , 9223372036854775808 => 'test2');
php > var_dump($arr[]=1);
PHP Warning:  Cannot add element to the array as the next element is already occupied in php shell code on line 1
NULL
```

可以看到，这个时候php报`warning`了，因为数组下标达到了`9223372036854775807`，这个时候想要再往里面插入元素，就会报错，`var_dump`之后返回一个`NULL`。

而这一点正是这道题最内层`if`语句的考点

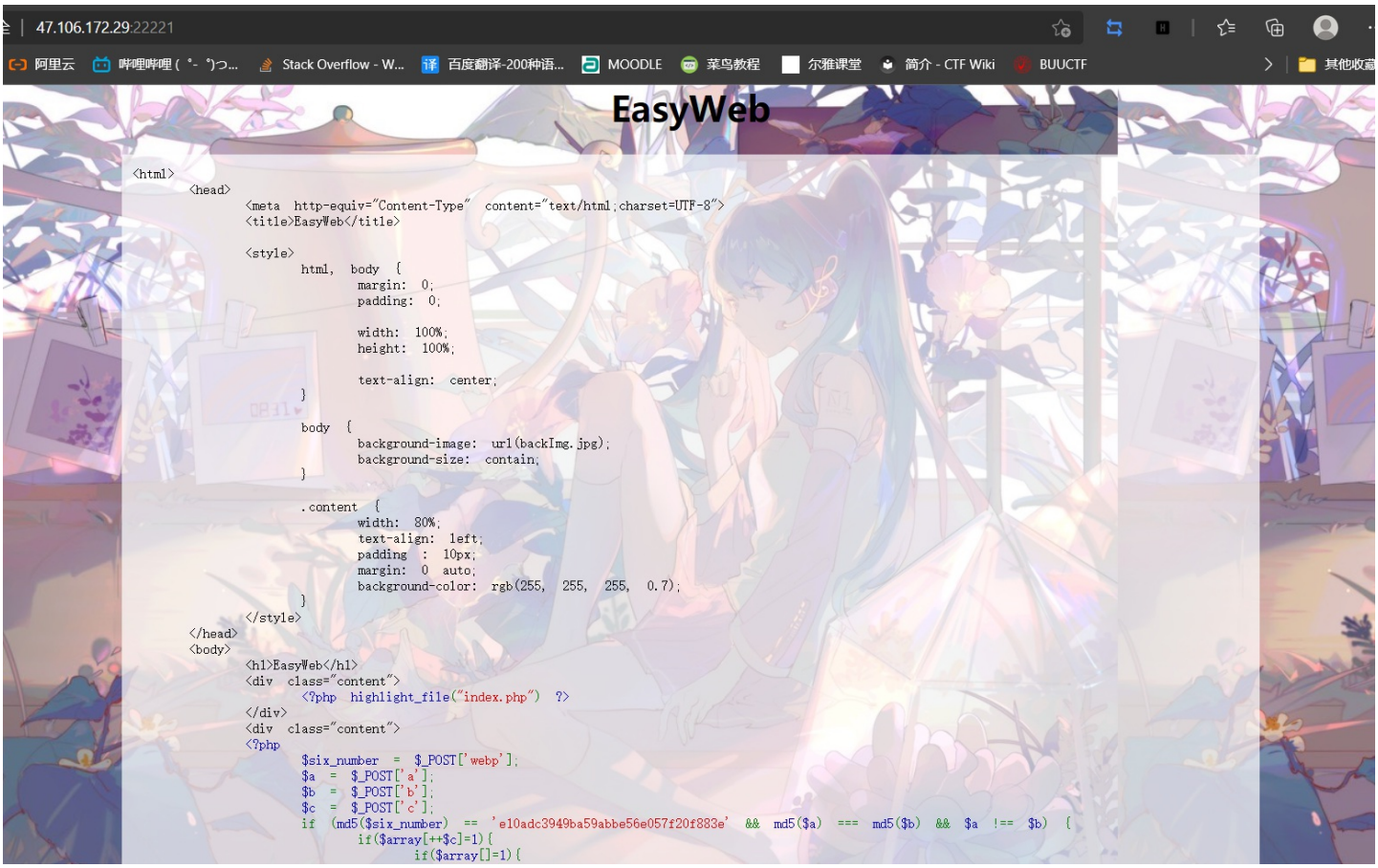
```
if($array[++$c]=1){
   if($array[]=1){
        echo "nonono";
   }
   else{
        require_once 'flag.php';
        echo $flag;
   }
}
```

这时候往里`c`传参`9223372036854775806`，要比上面提到的那个数字小`1`

因为题目是`++$c`，先加上1，变成`9223372036854775807`，然后执行最内层的`if`时，因为没有地方可以开数组了，就返回`NULL`，即`false`，这样一来就可以执行`else`里的语句

WriteUp:

打开题目，是一道`php+html`的代码审计：



代码如下：

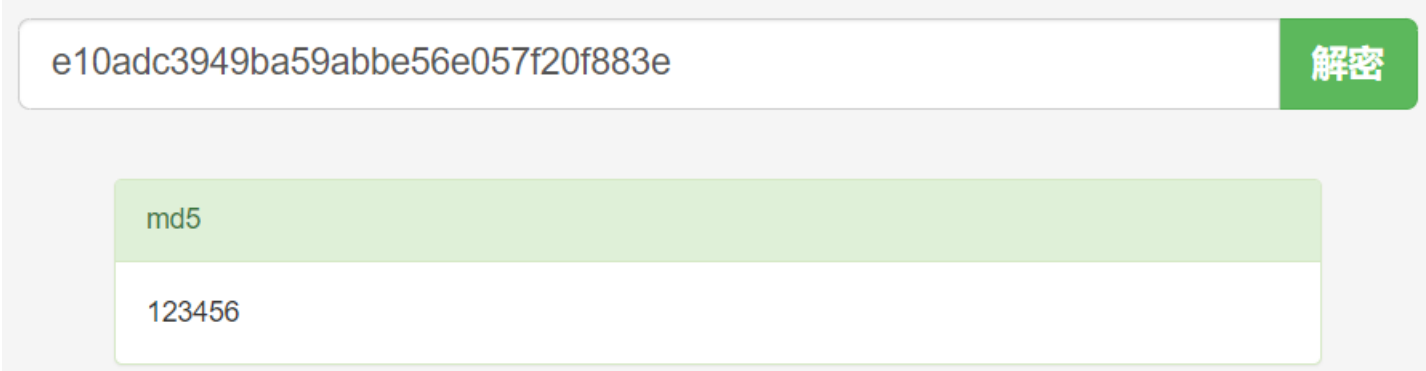
```
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html;charset=UTF-8">
        <title>EasyWeb</title>

        <style>
            html, body {
                margin: 0;
                padding: 0;

                width: 100%;
                height: 100%;

                text-align: center;
            }

            body {
                background-image: url(backImg.jpg);
                background-size: contain;
            }

            .content {
                width: 80%;
                text-align: left;
                padding : 10px;
                margin: 0 auto;
                background-color: rgb(255, 255, 255, 0.7);
            }
        </style>
    </head>
    <body>
        <h1>EasyWeb</h1>
        <div class="content">
            <?php highlight_file("index.php") ?>
        </div>
        <div class="content">
        <?php
            $six_number = $_POST['webp'];
            $a = $_POST['a'];
            $b = $_POST['b'];
            $c = $_POST['c'];
            if (md5($six_number) == 'e10adc3949ba59abbe56e057f20f883e' && md5($a) === md5($b) && $a !== $b) {
                if($array[++$c]=1){
                    if($array[]=1){
                        echo "nonono";
                    }
                    else{
                        require_once 'flag.php';
                        echo $flag;
                    }
                }
            }
        ?>
        </div>
    </body>
</html>
```

其中`php`部分的关键代码先拎出来

```php
<?php
    $six_number = $_POST['webp'];
    $a = $_POST['a'];
    $b = $_POST['b'];
    $c = $_POST['c'];
    if (md5($six_number) == 'e10adc3949ba59abbe56e057f20f883e' && md5($a) === md5($b) && $a !== $b) {
        if($array[++$c]=1){
            if($array[]=1){
                echo "nonono";
            }
            else{
                require_once 'flag.php';
                echo $flag;
            }
       }
    }
?>
```

可以看到，该`php`代码中，要求我们POST传递4个参数：`webp`，`a`，`b`，`c`

先看第一层`if`语句，首先一个变量`md5`加密后为`e10adc3949ba59abbe56e057f20f883e`



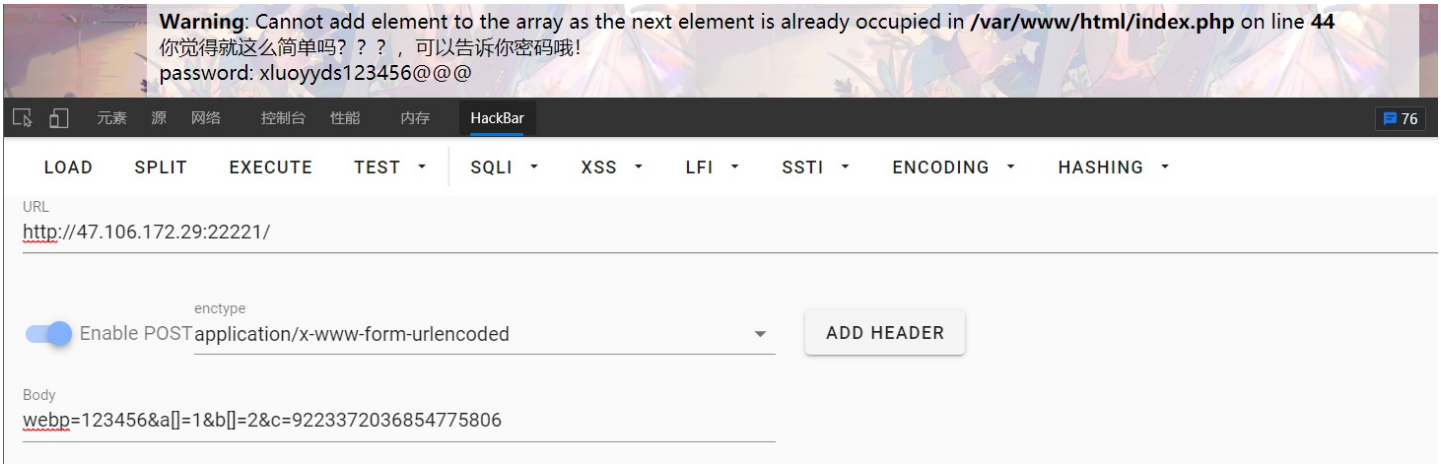
所以对`webp`传参`123456`

再看`$a`和`$b`，是常见的`md5`绕过，可以用数组绕过，也可以用`0e\d+`的形式绕过

因此对`a`传`a[]=1`，对`b`传`b[]=2`

根据前景知识，对`c`参数传`9223372036854775806`即可绕过最内层if语句

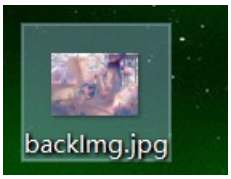
整一个传参如下：



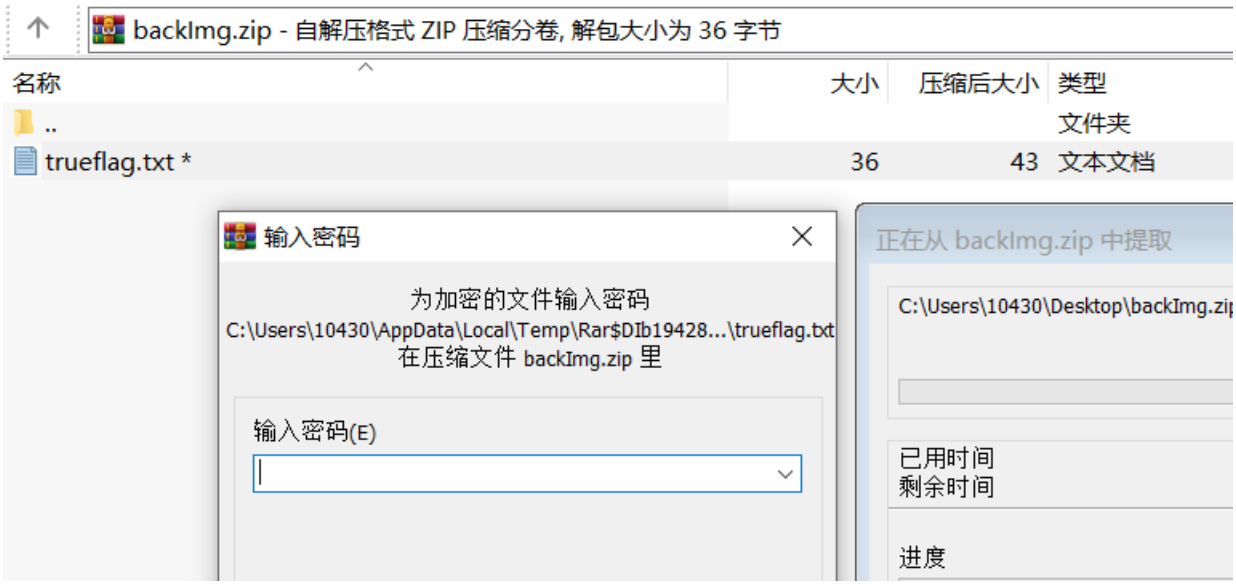
然而题目并没有直接给我们`flag`，只是给了一个密码：`xluoyyds123456@@@`

结合题目给的`hint`，说是背景图片上可能有我们想要的东西

于是我们下载图片，给了一个密码，猜测是一个压缩包



将`.jpg`后缀改成`.zip`后缀



可以看到，压缩包可以正常被打开

输入网页中给的密码`xluoyyds123456@@@`

得到`flag`：`newsctf{this_1s_veryveryveryeasyweb}`

我愿称之为套神，web+misc杂交的鼻祖