PHP索引数组+unset使用不当导致的问题

blackwolf / 2018-07-14 09:34:37 / 浏览数 5526 安全技术 WEB安全 顶(1) 踩(0)

0x00前言

通常网站后台可以配置允许上传附件的文件类型，一般登录后台，添加php类型即可上传php文件getshell。但是，随着开发者安全意识的提高，开发者可能会在代码层面强

0x01问题详情

问题描述：

最近在审计某CMS代码过程中，发现后台限制文件上传类型的代码如下：

```
$ext_limit = $ext_limit != '' ? parse_attr($ext_limit) : '';
foreach (['php', 'html', 'htm', 'js'] as $vo) {
   unset($ext_limit[$vo]);
}
```

其目的是实现:获取配置中的允许上传文件类型$ext_limit并转换为数组，无论后台是否添加了php等类型文件，均强制从允许上传文件类型的数组中删除php,html,htm,js等

但是由于unset函数使用不当，导致其代码无法达到该目的。具体地，执行如下代码：

```
$ext_limit =  Array('gif','jpg','jpeg','bmp','png','php');
var_dump($ext_limit);
foreach (['php', 'html', 'htm', 'js'] as $vo) {
   unset($ext_limit[$vo]);
}
var_dump($ext_limit);
```

得到输出为如下，可以看到php并没有被删除

```
D:\wamp\www\test.php:15:
array (size=6)
 0 => string 'gif' (length=3)
 1 => string 'jpg' (length=3)
 2 => string 'jpeg' (length=4)
 3 => string 'bmp' (length=3)
 4 => string 'png' (length=3)
 5 => string 'php' (length=3)

D:\wamp\www\test.php:19:
array (size=6)
 0 => string 'gif' (length=3)
 1 => string 'jpg' (length=3)
 2 => string 'jpeg' (length=4)
 3 => string 'bmp' (length=3)
 4 => string 'png' (length=3)
 5 => string 'php' (length=3)
```

问题分析：

unset函数的使用说明可以参考php官网，简单理解就是：unset可以销毁掉一个变量；或者根据传入的key值，销毁数组类型中指定的键值对。
针对PHP
索引数组，调用unset时必须调用其对应的数字索引才能销毁指定的键值对。所以如果传入unset函数的参数不是索引，而是其值的情况（如此处unset('php')），无法销毁

0x03修复办法

修改以上存在缺陷的代码为如下,主要是枚举索引数组为key=>value的形式，根据value进行比较，满足条件时将对应的key传入unset函数，从而销毁删除。

```
$ext_limit =  Array('gif','jpg','jpeg','bmp','png','php');
var_dump($ext_limit);
foreach (['php', 'html', 'htm', 'js'] as $vo) {
   foreach($ext_limit as $key=>$value){
       if($value===$vo){
           unset($ext_limit[$key]);
       }
   }
}
```

```
var_dump($ext_limit);
```

输出结果如下(php对应的键值对已被删除)：

```
D:\wamp\www\test.php:15:
array (size=6)
 0 => string 'gif' (length=3)
 1 => string 'jpg' (length=3)
 2 => string 'jpeg' (length=4)
 3 => string 'bmp' (length=3)
 4 => string 'png' (length=3)
 5 => string 'php' (length=3)

D:\wamp\www\test.php:23:
array (size=5)
 0 => string 'gif' (length=3)
 1 => string 'jpg' (length=3)
 2 => string 'jpeg' (length=4)
 3 => string 'bmp' (length=3)
 4 => string 'png' (length=3)
```

0x04小结

使用索引数组时，如果要使用unset销毁删除指定的键值对，切记采用枚举索引数组为key=>value的形式，根据value进行比较，满足条件时将对应的key传入unset函数

ps:安全问题的分析与挖掘就是一个开发者与hacker攻防较量的过程，对抗的点就是哪一方考虑的更加周全。

上一篇：python的lxml库的xxe防御 下一篇：利用winrm.vbs绕过应用程序...

1. 5 条回复

大先知 2018-07-14 16:21:25

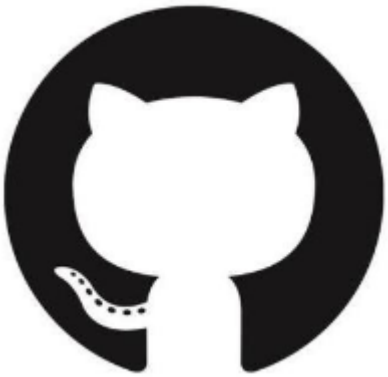
老哥，怎么不继续你的Struts2系列漏洞的分析了？之前的写的很好啊

0 回复Ta


blackwolf 2018-07-14 17:10:55

@大先知 大佬是不是回复错人了，我没有分享过struts2的文章哎！

0 回复Ta


chybeta 2018-07-14 21:45:45

@大先知 hhhh后续会继续更新的！

0 回复Ta


大先知 2018-07-15 16:59:45

@chybeta 坐等

0 回复Ta

大先知 2018-07-15 18:29:56

@blackwolf 眼花了。。我的锅

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