PHP执行系统命令函数实例讲解

作者：有故事的人 来源：范文网 www.wtabcd.cn/fanwen/

本文原地址：https://www.wtabcd.cn/fanwen/zuowen/bd7a71adb4d9bde99195e770a31b7237.html

命令注入

命令注入（command injection），对一些函数的参数没有做过滤或过滤不严导致的，可以执行系统或者应用指令（cmd命令或者bash命令）的一种注入攻击手段。

常见的执行系统命令的函数有

system()passthru()exec()shell_exec()popen()proc_open(教资面试报名费)pcntl_exec()

system()函数

string system (string $command [, int &$return_var])

$com六年级下册第一单元作文mand为执行的命令，&return_var可选，用来存放命令执行后的状态码

system()函数执行有回显，将执行结果输出到页面上

passthru()函数

void passthru (string $command [, int &$return_var])

和system函数类似，$command英语作文模版为执行的命令，&return_var可选，用来存放命令执行后的状态码

执行有回显，将执行结果输出到页面上

exec()函数

string exec (string $command [, array &$output [, int &$return_var]])

$command是要执行的命令

$output是获得执行命令输出的每一行字符串，$return_var用来保存命令执行的状态码（检测成功

或失败）

exec()函数执行无回显，默认返回最后一行结果

shell_exec()函数

string shell_exec(string &command)

&command是要执行的命令

shell_exec()函数默认无回显，通过echo可将执行结果输出到页面

反引号`

shell_exec() 函数实际上仅是反撇号 (`) 操作符的变体，当禁用shell_exec时，`也不可执行

在php中称之为执行运算符，php 将尝试将反引号中的内容作为 shell
命令来执行，并将其输出信息返回

popen()函数

resource popen (string $command , string $mode)

函数需要两个参数，一个是执行的命令command，另外一个是指针文件的连接模式mode，有r和w代表读和写。

函数不会直接返回执行结果，而是返回一个文件指针，但是命令已经执行。

popen()打开一个指向进程的管道，该进程由派生给定的command命令执行而产生。

返回一个和fopen()所返回的相同的文件指针，只不过它是单向的（只能用于读或写）并且必须用pclose()来关闭。

此指针可以用于fgets()，fgetss()和fwrite()

proc_open()函数

resource proc_open (string $cmd ,array $descriptorspec ,array &$pipes [, string $cwd [, array $env [, array $other_options]]])

与popen函数类似，但是可以提供双向管道

pcntl_exec()函数

void pcntl_exec (string $path [, array $args [, array $envs]]刷票软件 360)

path是可执行二进制文件路径或一个在文件第一行指定了 一个可执行文件路径标头的脚本
args是一个要传递给程序的参数的字符串数组。

pcntl是linux下的一个扩展，需要额外安装，可以支持 php 的多线程操作。

pcntl_exec函数的作用开学考是在当前进程空间执行指定程序，版本要求：php > 4.2.0

对这些危险函数，可以在php.ini中禁用，进行安全加固

到此这篇关于php执行系统命令函数实例讲解的文章就介绍到这了,更多相关php执行系统命令函数内容请搜索www.887551.com以前的文章或继续浏览下面的相关文章希望大家以后多多支持www.887551.com！