PHP執行外部程式因 selinux 限制 apache exec 而無法執行

作者是 Administrator
週一, 16 四月 2018 14:31 - 最近更新 週一, 16 四月 2018 14:42

以下說明轉自 http://emn178.pixnet.net/blog/post/72463845-php%E5%9F%B7%E8%A1%8C%E5%A4%96%E9%83%A8%E7%A8%8B%E5%BC%8F

How to execute an external program in PHP

說明 PHP如何執行外部程式，以及可能造成無法成功執行的原因，包含 SELinux、 php.ini設定 、 Sudoer、 環境變數路徑和參數問題 。

在 php中可以使用shell_exec(), exec(), system()等函式執行外部程式，但是要注意有些設定可能會限制而無法執行，這裡以 Linux系統為主要討論，要注意的地方如下：

1. SELinux

這是加強系統安全的模組，但沒有特別去設定的話時常會無法讓程式正常運作，而且在 php端沒有任何訊息，例如執行 shell_exec("ls")，沒有任何訊息 。 不過如果被 SELinux封鎖的話，在 /var/log/messages裡面會有類似以下的訊息：

你可以輸入以下指令來查詢目前針對 httpd的設定

?

```
# /usr/sbin/getsebool -a | grep httpd
```

例如會輸出

```
 allow_httpd_anon_write -- off  allow_httpd_mod_auth_pam -- off
allow_httpd_sys_script_anon_write -- off  httpd_builtin_scripting -- on
httpd_can_network_connect -- off  httpd_can_network_connect_db -- off
httpd_can_network_relay -- off  httpd_disable_trans -- off  httpd_enable_cgi -- on
httpd_enable_ftp_server -- off  httpd_enable_homedirs -- on  httpd_rotatelogs_disable_trans --
off  httpd_ssi_exec --off  httpd_suexec_disable_trans -- off  httpd_tty_comm -- off  httpd_unified
-- on
```

你可以依據需求更改，根據網路上找到的資料，httpd_ssi_exec為 on可以解決掉這問題，輸入

```
# setsebool -P httpd_ssi_exec 1
```

停用 **SELinux**

除此之外，你也可以直接關閉 SELinux，修改 SELinux設定檔，不同系統可能會不同位置，以我用到的 CentOS為 /etc/selinux/config，有的系統在
/etc/sysconfig/selinux

```
# vi /etc/selinux/config
```

將 SELINUX的值改成 disabled

```
SELINUX=disabled
```

然後還要的要重開機，

暫時停用

或者也可以暫時的停用啟用 SELinux，不同系統有不同方式，Fedora和 Red Hat setenforce開關

停用

?
```
# setenforce 0
```

啟用

?
```
# setenforce 1
```

有些則用以下方是

停用

?
```
echo 0 >/selinux/enforce
```

啟用

?
```
echo 1 >/selinux/enforce
```

2. php.ini

safe_mode

另外 php.ini的safe_mode如果被啟用的話，shell_exec()就無法使用，而 exec()則只能執行在safe_mode_exec_dir下的檔案

disable_functions

有些版本的 php.ini會預設將 shell_exec()等函式放到這下面，顧名思義在這之下的函式就無法使用，確認 shell_exec()等沒有被設定在這項目之下

3. Sudoer

網頁的執行身分通常是 apache，你可以在 php中使用以下方式查看

?

```
<?php
```

所以 php當然只能執行 apache有權限執行的指令，如同 Linux一般系統帳號的權限設定一樣，要使用 sudoer設定 apache允許執行的指令，你可以使用以下指令來編輯

?

```
# visudo
```

或

?

```
# vi /etc/sudoers
```

apache沒有密碼同時避免輸入密碼的過程，使NOPASSWD的屬性，例如我們給 root權限來測試如下

?

```
apache  ALL=(ALL)     NOPASSWD: /sbin/ifconfig
```

由於 apache沒有 tty，註解requiretty設定

?

```
#requiretty
```

最後再 php中可使用 sudo取得權限，例如

?

```
<?php
```

4. 環境變數

由於 php執行外部程式的環境變數不太一樣，所以有時候必須要使用絕對路徑才能正確執行程式 。

5. escapeshellarg

如果呼叫的程式會帶入動態的參數，應該要使escapeshellarg()函式來檢驗，尤其是參數會由使用者輸入的內容來決定的時候，例如

PHP執行外部程式因 selinux 限制 apache exec 而無法執行

作者是 Administrator
週一, 16 四月 2018 14:31 - 最近更新 週一, 16 四月 2018 14:42

? 1 2 3 <?php

6. 其他

有些程式雖然在 ssh執行的時候是正常有輸出訊息，但是在 php執行外部程式就是沒有，例如直接輸入 /usr/bin/java會有使用說明，但 php端看不到，不過直接執行 jar程式還是可以正常運作，應該是 shell_exec()只回傳 stdout的資料， stderr看不到，要讓 shell_exec()都看的到可以在指令後 2>上 '
&1 1> /dev/null
'，例如

? 1 2 3 <?php

文章標籤