Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Home > Faq > Apache

PHP.INI settings: Disable exec, shell_exec, system, popen and Other Functions To Improve Security

Posted by Vivek Gite <vivek@nixcraft.com>

Q. I run a small Apache based webserver for my personal use and it is shared with friends and family. However, most script kiddie try to exploit php application such as wordpress using exec() , passthru() , shell_exec() , system() etc functions. How do I disable these functions to improve my php script security? [1]

A. PHP has a lot of functions which can be used to crack your server if not used properly. You can set list of functions in php.ini using disable_functions directive. This directive allows you to disable certain functions for security reasons. It takes on a comma-delimited list of function names. disable_functions is not affected by Safe Mode. This directive must be set in php.ini For example, you cannot set this in httpd.conf.

Open php.ini file:

```
# vi /etc/php.ini
```

Find disable_functions and set new list as follows:

```
disable_functions
=exec,passthru,shell_exec,system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini_file,
```

Save and close the file. Restart httpd:

```
# service httpd restart
```

Further readings:

1. php.ini directives [2]
2. PHP Security [3]

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/linux-unix-apache-lighttpd-phpini-disable-functions/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/faq/category/php/**
[2] php.ini directives: **http://www.php.net/manual/en/ini.php**
[3] PHP Security: **http://www.php.net/manual/en/security.php**