PHP hardening checklist: disable dangerous functions

Published: 2025-11-09 · Archived: 2026-04-06 00:48:21 UTC

A powerful language like PHP can give life and great functionality to your site but it can also destroy it. With this guide, we'll help you disable some of the most dangerous PHP functions out there. It will prevent most PHP shells from doing what they do best as well as protect you from poorly coded applications.

> We do this for our clients as part of our Server hardening package.

Updating PHP's configuration file

Find the location of your php.ini file

```
php


1php -i | grep php.ini
```

Open that file and look for `disable_functions` directive and replace it with the following line:

```
php


1disable_functions = exec,system,passthru,readfile,shell_exec,escapeshellarg,escapeshellcmd,proc_close,proc_oper
```

Now save the changes and restart Apache:

```
shell


1/etc/init.d/httpd restart
```

If you want to make sure that it's working, you can check with a php_info file or with

```
shell


1php -i | grep disable_functions
```

PHP Functions and Description

- **exec**: Execute an external program
- **system**: Execute an external program and display the output
- **passthru**: Execute an external program and display raw output
- **readfile**: Outputs a file
- **shell_exec**: Execute command via shell and return the complete output as a string
- **escapeshellarg**: Escape a string to be used as a shell argument
- **escapeshellcmd**: Escape shell metacharacters
- **proc_open**: Execute a command and open file pointers for input/output
- **proc_close**: Close a process opened by proc_open() and return the exit code of that process
- **ini_alter**: Alias of ini_set()
- **dl**: Loads a PHP extension at runtime
- **popen**: Opens process file pointer
- **parse_ini_file**: Parse a configuration file
- **show_source**: Alias of highlight_file()
- **curl_exec**: Perform a cURL session
