php

□

- Downloads
- Documentation
- Get Involved
- Help

Search

Getting Started
- Introduction
- A simple tutorial

Language Reference
- Basic syntax
- Types
- Variables
- Constants
- Expressions
- Operators
- Control Structures
- Functions
- Classes and Objects
- Namespaces
- Exceptions
- Generators
- References Explained
- Predefined Variables
- Predefined Exceptions
- Predefined Interfaces and Classes
- Context options and parameters
- Supported Protocols and Wrappers

Security
- Introduction
- General considerations
- Installed as CGI binary
- Installed as an Apache module
- Filesystem Security
- Database Security
- Error Reporting
- Using Register Globals
- User Submitted Data
- Magic Quotes
- Hiding PHP
- Keeping Current

Features
- HTTP authentication with PHP
- Cookies
- Sessions
- Dealing with XForms
- Handling file uploads
- Using remote files

- Connection handling
- Persistent Database Connections
- Safe Mode
- Command line usage
- Garbage Collection
- DTrace Dynamic Tracing

Function Reference

- Affecting PHP's Behaviour
- Audio Formats Manipulation
- Authentication Services
- Command Line Specific Extensions
- Compression and Archive Extensions
- Credit Card Processing
- Cryptography Extensions
- Database Extensions
- Date and Time Related Extensions
- File System Related Extensions
- Human Language and Character Encoding Support
- Image Processing and Generation
- Mail Related Extensions
- Mathematical Extensions
- Non-Text MIME Output
- Process Control Extensions
- Other Basic Extensions
- Other Services
- Search Engine Extensions
- Server Specific Extensions
- Session Extensions
- Text Processing
- Variable and Type Related Extensions
- Web Services
- Windows Only Extensions
- XML Manipulation

Keyboard Shortcuts

| | |
|---|---|
| ? | This help |
| j | Next menu item |
| k | Previous menu item |
| g p | Previous man page |
| g n | Next man page |
| G | Scroll to bottom |
| g g | Scroll to top |
| g h | Goto homepage |
| g s | Goto search |

(current page)

/

Focus search box

PHP is a popular general-purpose scripting language that is especially suited to web development.

Fast, flexible and pragmatic, PHP powers everything from your blog to the most popular websites in the world.

### Download

- 5.6.8·Release Notes
- 5.5.24·Release Notes
- 5.4.40·Release Notes

16 Apr 2015

## PHP 5.4.40 Released

The PHP development team announces the immediate availability of PHP 5.4.40. 14 security-related bugs were fixed in this release, including CVE-2014-9709, CVE-2015-2301, CVE-2015-2783, CVE-2015-1352. All PHP 5.4 users are encouraged to upgrade to this version.

For source downloads of PHP 5.4.40 please visit our downloads page, Windows binaries can be found on windows.php.net/download/. The list of changes is recorded in the ChangeLog.

16 Apr 2015

## PHP 5.6.8 is available

The PHP development team announces the immediate availability of PHP 5.6.8. Several bugs have been fixed some of them beeing security related, like CVE-2015-1351 and CVE-2015-1352. All PHP 5.6 users are encouraged to upgrade to this version.

For source downloads of PHP 5.6.8 please visit our downloads page, Windows binaries can be found on windows.php.net/download/. The list of changes is recorded in the ChangeLog.

16 Apr 2015

## PHP 5.5.24 is available

The PHP development team announces the immediate availability of PHP 5.5.24. Several bugs have been fixed some of them beeing security related, like CVE-2015-1351 and CVE-2015-1352. All PHP 5.5 users are encouraged to upgrade to this version.

For source downloads of PHP 5.5.24 please visit our downloads page, Windows binaries can be found on windows.php.net/download/. The list of changes is recorded in the ChangeLog.

20 Mar 2015

## PHP 5.6.7 is available

The PHP development team announces the immediate availability of PHP 5.6.7. Several bugs have been fixed as well as CVE-2015-0231, CVE-2015-2305 and CVE-2015-2331. All PHP 5.6 users are encouraged to upgrade to this version.

For source downloads of PHP 5.6.7 please visit our downloads page, Windows binaries can be found on windows.php.net/download/. The list of changes is recorded in the ChangeLog.

20 Mar 2015

# PHP 5.5.23 is available

The PHP development team announces the immediate availability of PHP 5.5.23. Several bugs have been fixed as well as CVE-2015-0231, CVE-2015-2305 and CVE-2015-2331. All PHP 5.5 users are encouraged to upgrade to this version.

For source downloads of PHP 5.5.23 please visit our downloads page, Windows binaries can be found on windows.php.net/download/. The list of changes is recorded in the ChangeLog.

19 Mar 2015

# PHP 5.4.39 Released

The PHP development team announces the immediate availability of PHP 5.4.39. Six security-related bugs were fixed in this release, including CVE-2015-0231, CVE-2015-2305 and CVE-2015-2331. All PHP 5.4 users are encouraged to upgrade to this version.

For source downloads of PHP 5.4.39 please visit our downloads page, Windows binaries can be found on windows.php.net/download/. The list of changes is recorded in the ChangeLog.

20 Nov 2013

# Our modern web theme goes live!

The PHP web team are delighted to announce the launch of the new web theme that has been in beta for many months. Lots of hard work has gone into this release and we will be continually improving things over time now that we have migrated away from the legacy theme.

From an aesthetics point of view the general color scheme of the website has been lightened from the older dark purple. Lots of borders and links use a similar purple color to attain consistency. Fonts are smoother, and colors, contrast and highlighting have significantly improved; especially on function reference pages. Code examples should now be much more readable.

The theme is marked up using HTML5 and is generally much more modern. We are using Google Fonts and Bootstrap for our theme base.

To provide valuable feedback, you can use the 'Feedback' widget on the side of the page (not visible on smartphones) and to report bugs, you can make use of the bugs.php.net tracker. Despite our extensive multi-device/multi-browser testing, we may have missed something. So, if you spot any issues please do get in touch.

Special thanks to the guys who helped make this happen, you know who you are!

24 Oct 2013

# A further update on php.net

We are continuing to work through the repercussions of the php.net malware issue described in a news post earlier today. As part of this, the php.net systems team have audited every server operated by php.net, and have found that two servers were compromised: the server which hosted the www.php.net, static.php.net and git.php.net domains, and was previously suspected based on the JavaScript malware, and the server hosting bugs.php.net. The method by which these servers were compromised is unknown at this time.

All affected services have been migrated off those servers. We have verified that our Git repository was not compromised, and it remains in read only mode as services are brought back up in full.

As it's possible that the attackers may have accessed the private key of the php.net SSL certificate, we have revoked it immediately. We are in the process of getting a new certificate, and expect to restore access to php.net sites that require SSL (including bugs.php.net and wiki.php.net) in the next few hours.

To summarise, the situation right now is that:

- JavaScript malware was served to a small percentage of php.net users from the 22nd to the 24th of October 2013.
- Neither the source tarball downloads nor the Git repository were modified or compromised.
- Two php.net servers were compromised, and have been removed from service. All services have been migrated to new, secure servers.
- SSL access to php.net Web sites is temporarily unavailable until a new SSL certificate is issued and installed on the servers that need it.

Over the next few days, we will be taking further action:

- php.net users will have their passwords reset. Note that users of PHP are unaffected by this: this is solely for people committing code to projects hosted on svn.php.net or git.php.net.

We will provide a full post mortem in due course, most likely next week. You can also get updates from the official php.net Twitter: @official_php.

24 Oct 2013

# A quick update on the status of php.net

On 24 Oct 2013 06:15:39 +0000 Google started saying www.php.net was hosting malware. The Google Webmaster Tools were initially quite delayed in showing the reason why and when they did it looked a lot like a false positive because we had some minified/obfuscated javascript being dynamically injected into userprefs.js. This looked suspicious to us as well, but it was actually written to do exactly that so we were quite certain it was a false positive, but we kept digging.

It turned out that by combing through the access logs for static.php.net it was periodically serving up userprefs.js with the wrong content length and then reverting back to the right size after a few minutes. This is due to an rsync cron job. So the file was being modified locally and reverted. Google's crawler caught one of these small windows where the wrong file was being served, but of course, when we looked at it manually it looked fine. So more confusion.

We are still investigating how someone caused that file to be changed, but in the meantime we have migrated www/static to new clean servers. The highest priority is obviously the source code integrity and after a quick:

```
git fsck --no-reflog --full --strict
```

on all our repos plus manually checking the md5sums of the PHP distribution files we see no evidence that the PHP code has been compromised. We have a mirror of our git repos on github.com and we will manually check git commits as well and have a full post-mortem on the intrusion when we have a clearer picture of what happened.

Older News Entries

Upgrading to PHP 5.6

Upcoming conferences

- PHP Tour Luxembourg
- Italian phpDay 2015
- SOLIDay 2015
- International PHP Conference Spring 2015

User Group Events

Special Thanks

Social media

- @official_php

- Copyright © 2001-2015 The PHP Group
- My PHP.net
- Contact
- Other PHP.net sites
- Mirror sites
- Privacy policy