

WORDCAMP BOLOGNA 2012

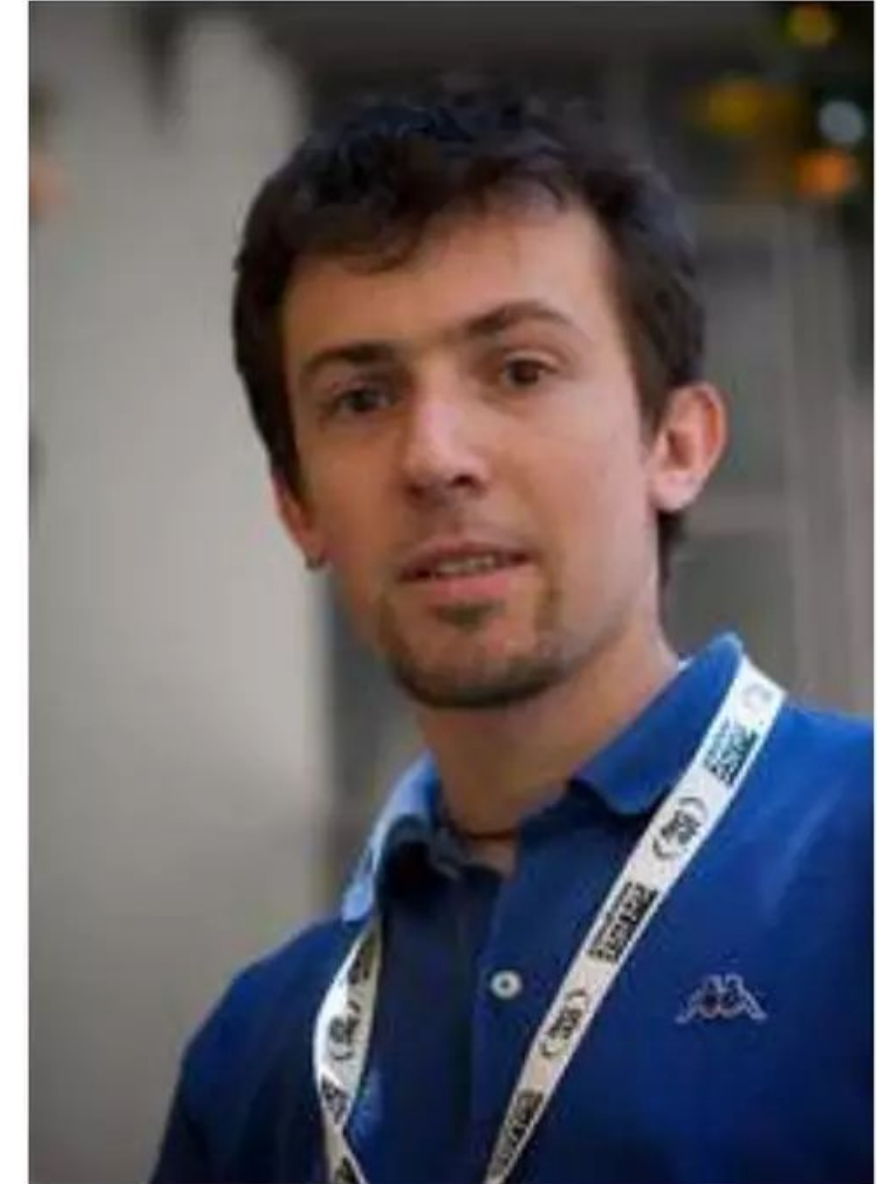


WordPress HARDENING (v3)



About me

- 37 years old
- Born in Turin (Italy)
- Co-Founder mavida.com
- ***WordPress Lover***



- <http://maurizio.mavida.com>
- <https://twitter.com/miziomon>
- <http://www.linkedin.com/in/mauriziopelizzone>

Why we need «hardening» ?





Technologies

[Content Management](#)
[Server-side Languages](#)
[Client-side Languages](#)
[JavaScript Libraries](#)
[Markup Languages](#)
[Character Encodings](#)
[Image File Formats](#)
[Site Elements](#)
[SSL Certificate Authorities](#)
[Social Widgets](#)
[Web Servers](#)
[Operating Systems](#)
[Content Delivery](#)
[Traffic Analysis Tools](#)
[Advertising Networks](#)
[Top Level Domains](#)
[Content Languages](#)

Trends

[Usage Trend](#)
[Market Share Trend](#)

Market

[Top Site Usage](#)
[Market Position](#)

[Technologies](#) > [Content Management](#)

Usage of content management systems for websites

This diagram shows the percentages of websites using various content management systems. See [technologies overview](#) for explanations on the methodologies used in the surveys. Our reports are updated daily.

How to read the diagram:

68.5% of the websites use none of the content management systems that we monitor.

WordPress is used by 17.4% of all the websites, that is a content management system market share of 55.1%.

Request an extensive market report of specific content management systems.

[Learn more](#)



Technologies

Content Management Systems

Content management systems are web-based systems for creating and managing content on a website. Examples of content management systems include wikis, blogs, and bulletin boards.

E-commerce

E-commerce is the buying and selling of goods and services over the internet. We provide e-commerce solutions that help you surpass expectations.

Latest reports

Web technologies
5 November

Dangers



- 1. Info collection**
- 2. Password Brute force attack**
- 3. Exploit**
- 4. Human mistakes**
- 5. Server vulnerabilities**
- 6. Network vulnerabilities**
- 7. File Permissions**

- 1. Info collection**
- 2. Password Brute force attack**
- 3. Exploit**
- 4. Human mistakes**
- ~~5. Server vulnerabilities~~**
- ~~6. Network vulnerabilities~~**
- ~~7. File Permissions~~**

1. Info collection
2. Password Brute force attack
3. Exploit
- 4. Human mistakes**
- ~~5. Server vulnerabilities~~
- ~~6. Network vulnerabilities~~
- ~~7. File Permissions~~

Wpscan

WPScan is a black box WordPress vulnerability scanner.

[View the Project on GitHub](#)

Download
ZIP File

Download
TAR Ball

View On
GitHub

[Follow us on Twitter](#)

Have you found WPScan useful? Buy the developers a beer!

Donate

WPScan

INSTALL

WPScan comes pre-installed on the following Linux distributions:

- [BackBox Linux](#)
- [BackTrack Linux](#) (outdated WPScan installed, update needed)
- [Pentoo](#)
- [SamuraiWTF](#)

Prerequisites:

- Windows not supported
- Ruby => 1.9
- RubyGems
- Git

Installing on Debian/Ubuntu:

```
sudo apt-get install libcurl4-gnutls-dev libopenssl-ruby libxml2  
libxml2-dev libxslt1-dev
```

```
git clone https://github.com/wpscanteam/wpscan.git
```

```
cd wpscan
```

Some solutions



Delete readme.html



Version 3.4.2

Semantic Personal Publishing Platform

First Things First

Welcome. WordPress is a very special project to me. Every developer and contributor adds something unique to the mix, and together we create something beautiful that I'm proud to be a part of. Thousands of hours have gone into WordPress, and we're dedicated to making it better every day. Thank you for making it part of your world.

— Matt Mullenweg

Installation: Famous 5-minute install

1. Unzip the package in an empty directory and upload everything.
2. Open [wp-admin/install.php](#) in your browser. It will take you through the process to set up a `wp-config.php` file with your database connection details.

Prevent user enumeration (?author=n)

```
RewriteCond %{QUERY_STRING} (^|&)author=  
RewriteRule . http://%{SERVER_NAME}/? [L]
```

Hide wp_(login | admin | registrazione)

1. Block Access to login / admin
2. Prepare custom login url
3. Check key presence

```
RewriteRule ^login /wp-login.php?key=12345g&
```

```
RewriteCond %{HTTP_REFERER} !^wp-admin
```

```
...
```

```
RewriteCond %{QUERY_STRING} !^key=12345
```

```
RewriteRule ^app/wp-login\.php http://%{SERV
```

Deny php execution

```
Options All -Indexes
Order Allow,Deny
Deny from all
```

```
<Files ~ "\.(xls|doc|rtf|pdf|zip|rar|mp3|flv|swf|png|gif|jpg|js|css)$">
    Allow from all
</Files>
```

```
<Files permitted-filename.php>
    Allow from all
</Files>
```

Shrink plugins number

1. Remove inactive plugin
2. Remove useless plugin
3. Remove dangerous plugin
4. (Evaluate code integration)

DISALLOW PLUGIN INSTALL / UPDATE

```
/**  
 * edit your wp-config.php  
 */
```

```
define('DISALLOW_FILE_EDIT', true);  
define('DISALLOW_FILE_MODS', true);
```

Use **STRONG** password

Insecure Password

- giulia76
- password
- 123456
- qwerty
- matrix

Secure Password

- D7u8hI928FJYusx
- Z5BLI20T8by1524
- TLv7p64P63V5Hr1
- 6b83668I15qRP2I
- Um2d4Ejd9T1ExPr

<http://strongpasswordgenerator.com/>

CHANGE DIRECTORY STRUCTURE

Rename wp-content

```
/**  
 * edit your wp-config.php  
 */
```

```
define( 'WP_CONTENT_DIR', dirname( __FILE__ ) . '/public' );  
define( 'WP_CONTENT_URL', 'http://' . $_SERVER['HTTP_HOST'] . '/public' );
```

Change Upload Directory

Uploading Files

Store uploads in this folder

Default is `wp-content/uploads`

Full URL path to files

Configuring this is optional. By default, it should be blank.

☒ Organize my uploads into month- and year-based folders

Save Changes

Move WordPress Core

```
/**  
 * edit your wp-config.php  
 */  
define( 'WP_SITEURL', 'http://' . $_SERVER['SERVER_NAME'] . '/wordpress-core/');  
define( 'WP_HOME', 'http://' . $_SERVER['SERVER_NAME'] );
```

```
/**  
 * edit your index.php  
 */  
define('WP_USE_THEMES', true);  
require('./wordpress-core/wp-blog-header.php');
```

Structure Example

 assets	Cartella di file
 custom-upload-directory	Cartella di file
 wordpress-core	Cartella di file
 .htaccess	File HTACCESS
 index.php	File PHP
 wp-config.php	File PHP

 app	Cartella di file
 assets	Cartella di file
 files	Cartella di file
 .htaccess	File HTACCESS
 index.php	File PHP
 wp-config.php	File PHP

Codex References

- http://codex.wordpress.org/Hardening_WordPress
- http://codex.wordpress.org/Administration_Over_SSL
- http://codex.wordpress.org/Editing_wp-config.php

BLACKHOLE

You have fallen into a trap!

This site's [robots.txt](#) file explicitly forbids your presence at this location. The following Whois data will be reviewed carefully. If it is determined that you suck, you will be banned from this site. If you think this is a mistake, *now* is the time to [contact me](#).

Your IP Address is 93.50.19.249

```
WHOIS Lookup for 93.50.19.249  
Friday, June 15th 2012 @ 17:14:07
```

Your IP Address is 93.50.19.249

```
WHOIS Lookup for 93.50.19.249  
Friday, June 15th 2012 @ 17:14:07  
  
% This is the RIPE Database query service.  
% The objects are in RPSL format.  
%  
% The RIPE Database is subject to Terms and Conditions.  
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
```

RULES FOR BLACKHOLE

RewriteEngine On

RewriteBase /

RewriteRule ^(admin|wp-admin|wp-content)\$ blackhole/ [L]

RewriteRule ^(phpinfo|phpmyadmin)\$ blackhole/ [L]

BLACKHOLE PLUGIN

```
<?php
```

```
/*
```

```
Plugin Name: blackhole
```

```
Plugin URI: http://maurizio.mavida.com/
```

```
Description: blackhole
```

```
License: GPL
```

```
Version: 0.1
```

```
Author: Maurizio Pelizzone
```

```
Author URI: http://maurizio.mavida.com
```

```
*/
```

```
if (!is_admin()){
```

```
    include($_SERVER['DOCUMENT_ROOT'] . "/blackhole/blackhole.php");
```

```
}
```

FILE MONITOR

Plugin Directory

Username Password [Log in](#) (forgot?) or [Register](#)[Extend Home](#)[Plugins](#)[Developer Center](#)[Themes](#)[Mobile](#)[Ideas](#)[Kvetch!](#)

Search Plugins

[Search](#)Popular Tags [More »](#)[widget \(3137\)](#)[Post \(2074\)](#)[plugin \(1940\)](#)[admin \(1587\)](#)[posts \(1533\)](#)[sidebar \(1360\)](#)[comments \(1090\)](#)[twitter \(1062\)](#)[google \(1053\)](#)[images \(1021\)](#)[page \(971\)](#)[image \(892\)](#)

WordPress File Monitor

Monitor files under your WordPress installation for changes. When a change occurs, be notified via email.

[Download Version 2.3.3](#)[Description](#) [Installation](#) [Changelog](#) [Stats](#) [Support](#) [Developers](#)

Monitors your WordPress installation for added/deleted/changed files. When a change is detected an email alert can be sent to a specified address.

Features

- Monitors file system for added/deleted/changed files
- Sends email when a change is detected
- Multiple email formats for alerts
- Administration area alert to notify you of changes in case email is not received
- Ability to monitor files for changes based on file hash or timestamp
- Ability to exclude directories from scan (for instance if you use a cacheing system that stores its files within the monitored zone)
- Site URL included in notification email in case plugin is in use on multiple sites

Sorry for the delayed release for working with WordPress 3.0. *NOTE* I haven't tested the latest version with multi-site yet, only single site.

Tags: [files](#), [monitor](#), [plugin](#), [security](#)

Requires: 3.0 or higher

Compatible up to: 3.0.5

Last Updated: 2010-6-23

Downloads: 29,953

Average Rating

★★★★☆
(32 ratings)

Author



[mattwalters](#)

3 plugins

[Donate to this plugin »](#)

Support

Got something to say? Need help?

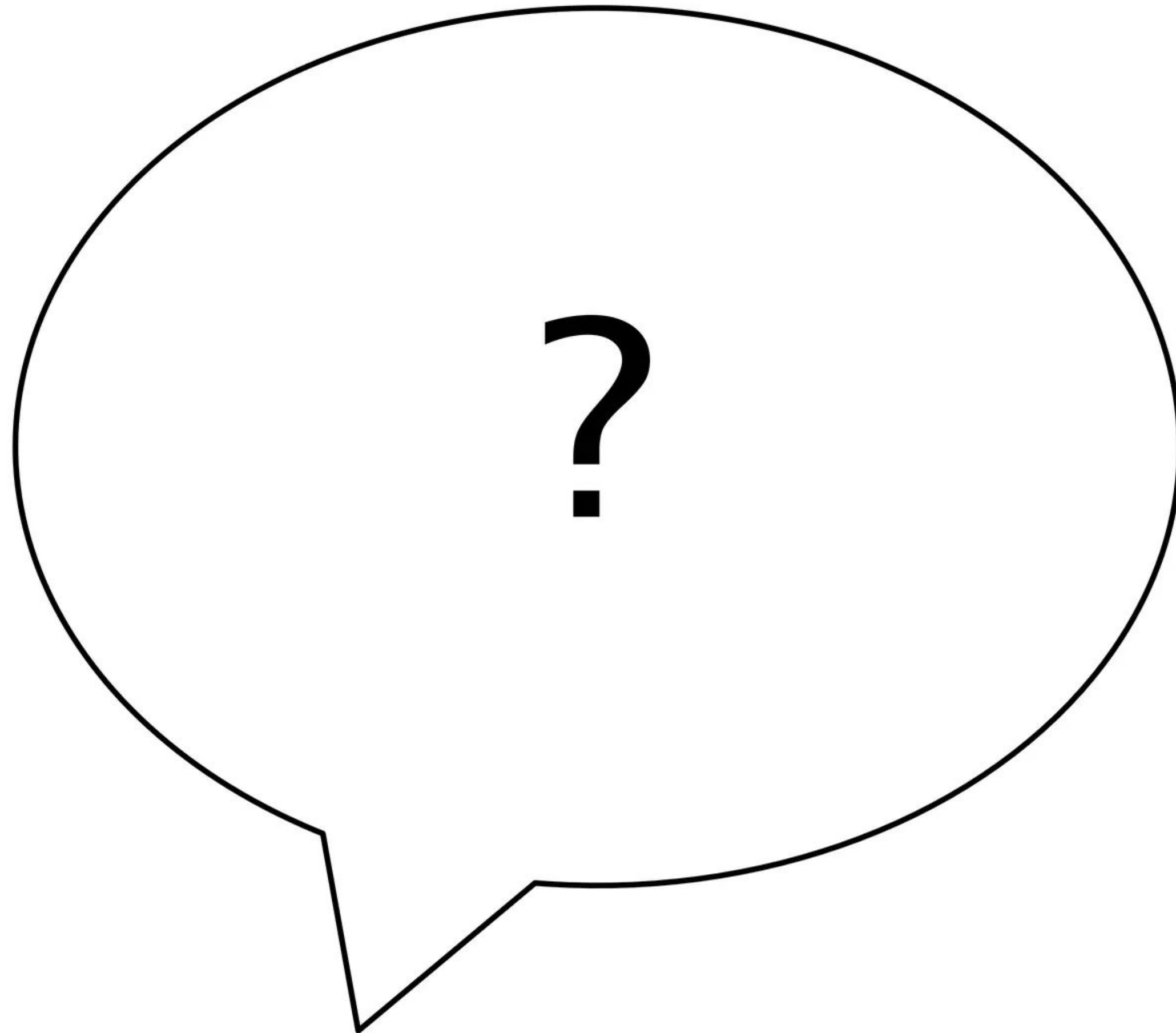
[View support forum](#)

Compatibility

WordPress

AVOID FTP





Thank you



Maurizio Pelizzone

@miziomon

maurizio@mavida.com

<http://maurizio.mavida.com>

