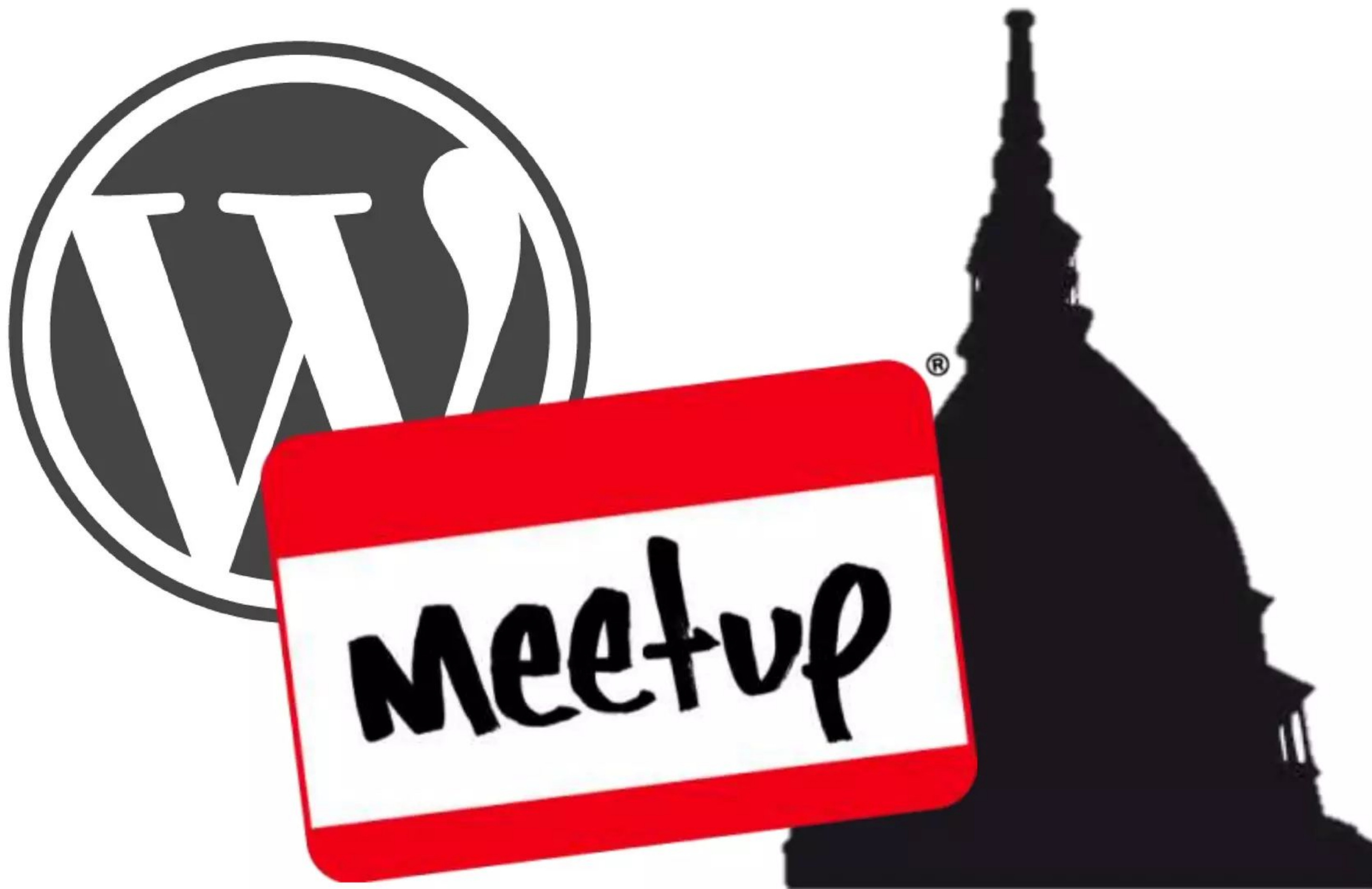




Torino, 10 Novembre 2015

WORDPRESS HARDENING

(LIGTH VERSION - v4)



About me

- Birth in Turin (Italy)
- Co-Founder @ mavida.com
- Solution architect
- ***WordPress proud user***
- *maurizio@mavida.com*
- *<http://www.mavida.com>*
- *<http://maurizio.mavida.com>*
- *<https://twitter.com/miziomon>*
- *<http://www.slideshare.net/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](#)
[Tag Managers](#)
[Top Level Domains](#)
[Content Languages](#)

Trends

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

Market

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

Breakdown

[Ranking](#)
[Server-side Languages](#)
[Client-side Languages](#)
[JavaScript Libraries](#)
[Markup Languages](#)
[Character Encodings](#)
[Image File Formats](#)
[Site Elements](#)

[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.

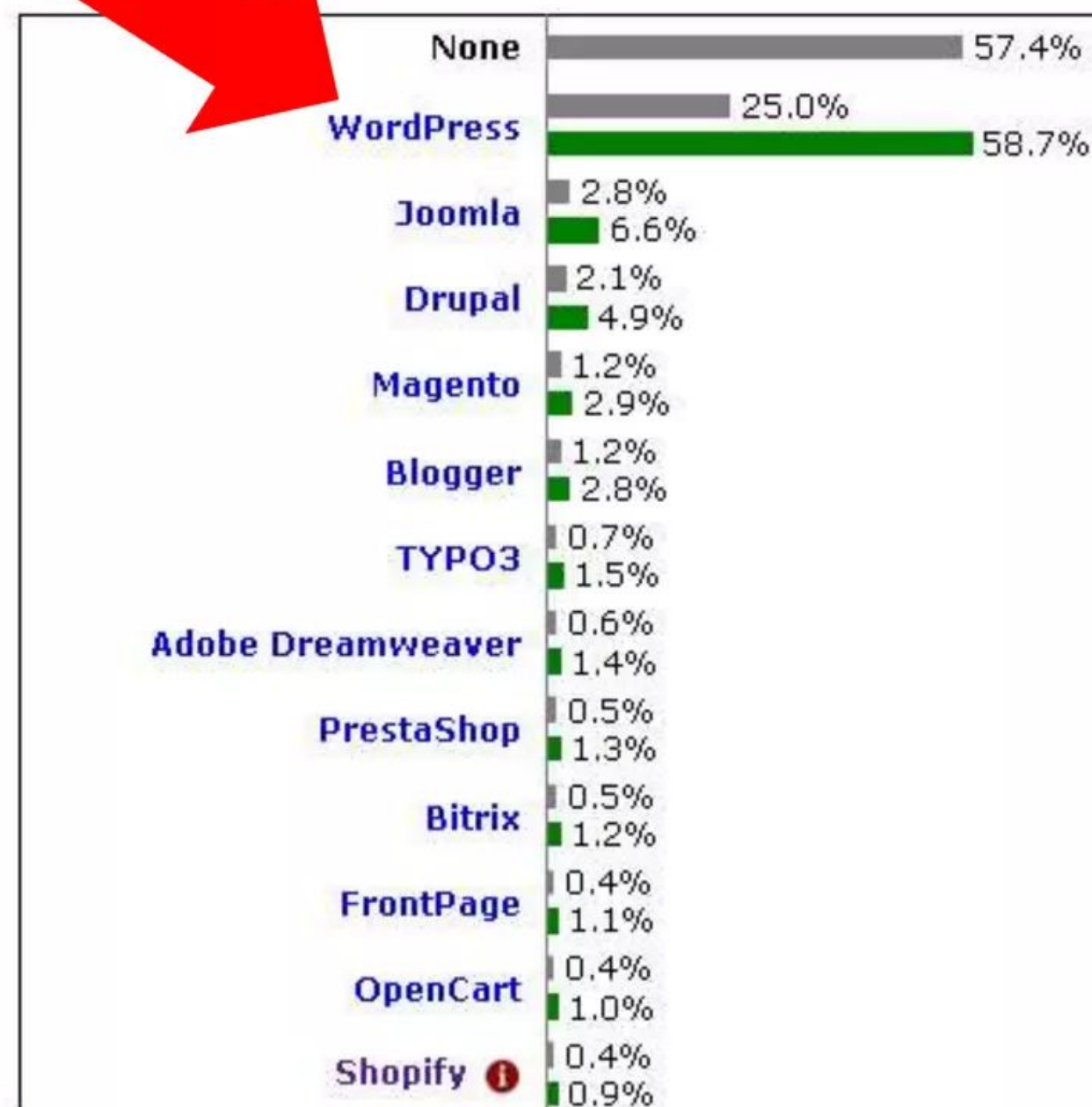
How to read the diagram:

57.4% of the websites use none of the content management systems that we monitor.

WordPress is used by 25.0% of all the websites, that is a content management system market share of 58.7%.

Request an extensive market report of specific content management systems.

[Learn more](#)



Technology Brief

Content Management Systems

Content management systems are web-based applications for creating and managing the content of a website. We include all such systems in this category, also systems that are often classified as wikis, blog engines or discussion boards.

Featured Products and Services

TemplateMonster

Premium [website templates](#), including themes for WordPress, Joomla, Drupal, Magento, Prestashop, and more.



Secure Premium Wordpress Hosting
[WP Engine](#)

[Present your product or service here](#)

Dangers

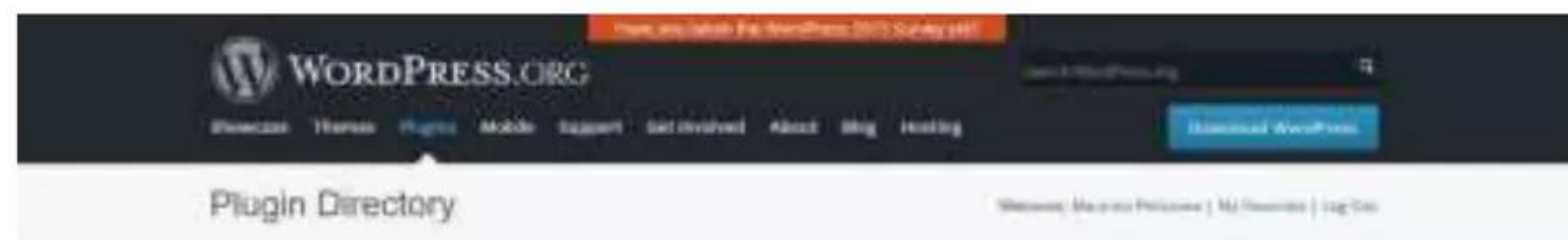


- 1. Social engineering**
- 2. Password Brute force attack**
- 3. Exploit**
- 4. Human mistakes**
- 5. Server vulnerabilities**
- 6. Network vulnerabilities**
- 7. File Permissions**

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

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

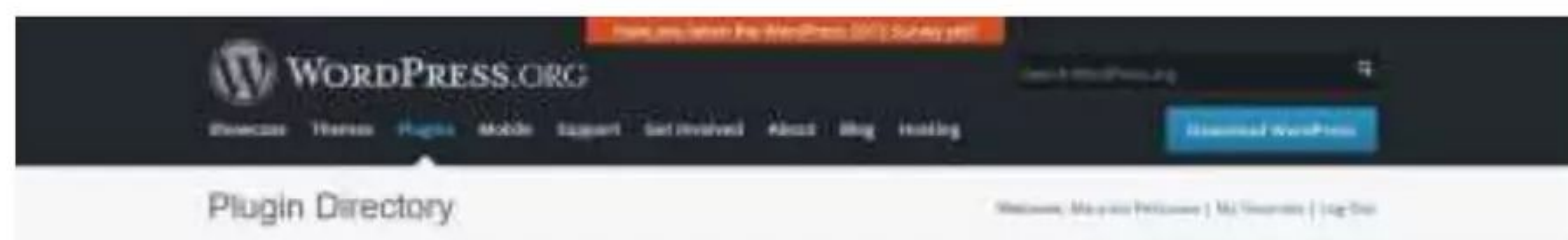
The solution



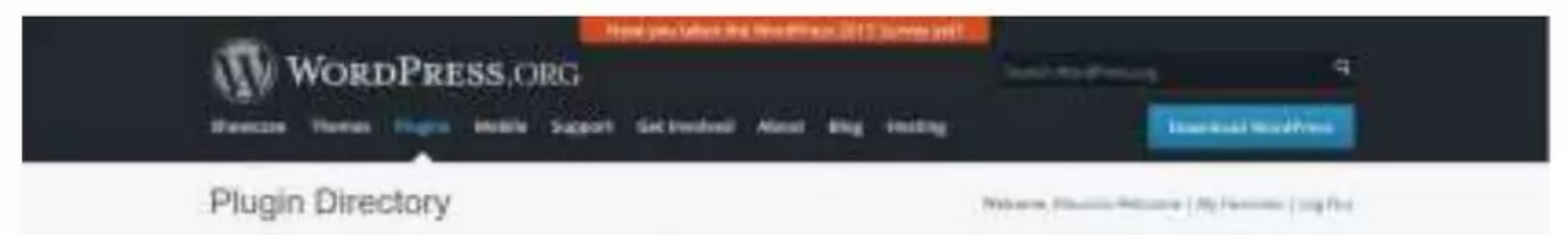
The backup plugin BackWPup Free can be used to back up your website, including files, database and more, to an external backup location via FTP, SFTP, WebDAV, or to a local directory. It is able to schedule backups and restore an installation. Please understand this free version is not a full backup solution. For more information, please visit our website.



Backup and restoration made easy. Complete backups; manual or scheduled (backing to ftp, Dropbox, Google Drive, Backspace, FTP, SFTP, email + others).
CraftPlus Backup and Restoration is a backup and restoration plugin for WordPress. It can backup your website to various locations and restore it back to its original state. It is a simple and easy-to-use plugin that can be used by anyone.



Duplicator, clone, backup, save and transfer an entire site from one location to another.
The Duplicator gives WordPress administrators the ability to migrate, copy or clone a site from one location to another. The plugin also serves as a simple backup utility. The Duplicator supports both manual and scheduled backup and restoration, if you need to move WordPress or backup WordPress this plugin can help simplify the process. For complete details visit www.duplicator.net.



VaultPress is a subscription service offering real-time backup, automated security scanning, and support from WordPress experts.
VaultPress is a real-time backup and security scanning service designed and built by Automattic, the same company that operates Jetpack by WordPress.com. The VaultPress plugin provides the required functionality to backup and synchronize every post, comment, media file, revision and database settings on our servers. Its best of all, you don't need to sign up for a VaultPress subscription.

Checklist

Disallow access / delete readme.html



Version 4.3.1

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.
 1. If for some reason this doesn't work, don't worry. It doesn't work on all web hosts. Open up `wp-config-sample.php` with a text editor like WordPad or similar and fill in your database connection details.
 2. Save the file as `wp-config.php` and upload it.
 3. Open [wp-admin/install.php](#) in your browser.

```
<files readme.html>
```

```
Order allow,deny
```

```
Deny from all
```

```
</files>
```

ADVANCED USER

Check Admin Permission

The screenshot displays the WordPress 'Utenti' (Users) management interface. The sidebar on the left contains navigation links for various site components. The top bar shows the user 'Salve mavida' and options for screen settings and help. The main content area is titled 'Utenti' and includes a search bar and a table of users. The table has columns for 'Nome utente', 'Nome', 'E-mail', 'Ruolo', and 'Articoli'. The 'admin' user is listed with the role 'Nessuna' and 1 article. The 'mavida' user is listed with the role 'Amministratore' and 0 articles. A third user is listed with the role 'Amministratore' and 0 articles. The bottom of the page shows the WordPress version 4.3.1.

Utenti [Aggiungi nuovo](#)

Tutti (3) | [Amministratore](#) (2)

Azioni di Gruppo Cambia ruolo in... 3 elementi

☐	Nome utente	Nome	E-mail	Ruolo	Articoli
☐	admin		[REDACTED]	Nessuna	1
☐	mavida		[REDACTED]	Amministratore	0
☐			[REDACTED]	Amministratore	0

Azioni di Gruppo 3 elementi

Grazie per aver creato con [WordPress](#). Versione 4.3.1

Prevent WordPress users list

<http://www.yourwebsite.com/?author=1>

<http://www.yourwebsite.com/?author=2>

<http://www.yourwebsite.com/?author=3>

<http://www.yourwebsite.com/?author=4>

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

ADVANCED USER

Secure your wp_login.php

1. Hide
2. Capcha
3. Limit attempts
4. Restrict to your IP

Plugin Directory

Username Password [Log in](#) [\(forgot?\)](#) or [Register](#)

- Featured
- Popular
- Favorites
- Beta Testing

Developers

Search Plugins

Search

Popular Tags

- [widget](#) (5,550)
- [Post](#) (3,478)
- [plugin](#) (3,435)
- [admin](#) (2,930)
- [posts](#) (2,674)
- [sidebar](#) (2,131)
- [shortcode](#) (2,122)
- [google](#) (1,951)
- [twitter](#) (1,918)



Stealth Login Page

Protect your dashboard without editing the .htaccess file -- the FIRST one that completely blocks remote bot login requests.

[Download Version 4.0.0](#)

- Description
- Installation
- FAQ
- Screenshots
- Changelog
- Stats
- Support
- Reviews
- Developers

Protect your dashboard with a game-changing authorization code. The login form will never be the same again.

What it does

Without locking down access via IP address or file permissions, this plugin creates a secret login authorizaition code. Those who do not enter this additional authorization will be

Requires: 3.4.2 or higher
Compatible up to: 4.0.8
Last Updated: 11 months ago
Active Installs: 10,000+

Ratings

Plugin Directory

Username Password (forgot?) or Register

Featured
Popular
Favorites
Beta Testing

Developers

Search Plugins

Popular Tags

[widget](#) (5,550)

[Post](#) (3,478)

[plugin](#) (3,435)

[admin](#) (2,930)

[posts](#) (2,674)

[sidebar](#) (2,131)

[shortcode](#) (2,122)

[google](#) (1,951)

[twitter](#) (1,918)



Captcha on Login

Protect your blog from login brute force attacks adding a captcha on login page of your site

Download Version 2.1.2

[Description](#) [Installation](#) [FAQ](#) [Screenshots](#) [Other Notes](#) [Changelog](#) [Stats](#) [Support](#) [Reviews](#) [Developers](#)

Overview

Nowadays, it is common hackers trying to get access to your blog, so, it is very important you make some actions to prevent your blog from being hacked. A good way to turn the login system of your blog more secure is to use that plugin Captcha on Login. It will Protect your blog from login brute force attacks adding a captcha on login page. That

Requires: 3.0 or higher

Compatible up to: 4.2.5

Last Updated: 4 months ago

Active Installs: 10,000+

Ratings



Plugin Directory

Username Password [Log in](#) ([forgot?](#)) or [Register](#)

[Featured](#)
[Popular](#)
[Favorites](#)
[Beta Testing](#)

[Developers](#)

Search Plugins

Popular Tags

[widget](#) (5,550)

[Post](#) (3,478)

[plugin](#) (3,435)

[admin](#) (2,930)

[posts](#) (2,674)

[sidebar](#) (2,131)

[shortcode](#) (2,122)

[google](#) (1,951)

[twitter](#) (1,918)



Login LockDown

Limits the number of login attempts from a given IP range within a certain time period.

[Download Version v1.6.1](#)

[Description](#) [Installation](#) [Changelog](#) [Stats](#) [Support](#) [Reviews](#) [Developers](#)

Login LockDown records the IP address and timestamp of every failed login attempt. If more than a certain number of attempts are detected within a short period of time from the same IP range, then the login function is disabled for all requests from that range. This helps to prevent brute force password discovery. Currently the plugin defaults to a 1 hour lock out of an IP block after 3 failed login attempts within 5 minutes. This can be modified via the Options panel. Adminsitrators can release locked out IP ranges manually from the

Requires: 3.6 or higher
Compatible up to: 4.0.8
Last Updated: 1 year ago
Active Installs: 200,000+

Ratings

Directory dei plugin

Nome utente Password (dimenticata?) o [Registrati](#)

[In primo piano](#)

[Popolari](#)

[Preferiti](#)

[Test delle versioni](#)

[Beta](#)

[Sviluppatori](#)

Cerca plugin

Tag più popolari

[widget](#) (5.550)

[Post](#) (3.478)

[plugin](#) (3.435)

[admin](#) (2.930)

[posts](#) (2.674)

[sidebar](#) (2.131)

[shortcode](#) (2.122)

[google](#) (1.951)



Login IP & Country Restriction

This plugin hooks in the authenticate filter. By default, the plugin is set to allow all access and you can configure the plugin to allow the login on

[Scarica la Versione 3.1](#)

[Descrizione](#)

[Installazione](#)

[FAQ](#)

[Schermate](#)

[Altre note](#)

[Registro delle modifiche](#)

[Statistiche](#)

[Supporto](#)

This plugin hooks in the authenticate filter. By default, the plugin is set to allow all access and you can configure the plugin to allow the login only from some specified IPs or the specified countries. PLEASE MAKE SURE THAT YOU CONFIGURE THE PLUGIN TO ALLOW YOUR OWN ACCESS. If you set a restriction by IP, then you have to add your own IP (if you are using the plugin in a local setup the IP is 127.0.0.1 or ::1, this is added in your list by default). If you set a restriction by country, then you have to select from the list of

Richiede: not tested o superiore

Compatibile fino a: wp 4.3.1

Ultimo aggiornamento: 2 settimane fa

Installazioni attive: 500+

Deny access to xmlrpc.php

Have you taken the WordPress 2015 Survey yet?

 **WORDPRESS.ORG**

Search WordPress.org

Download WordPress

Showcase Themes Plugins Mobile **Support** Get Involved About Blog Hosting

Codex

Codex tools: Log in



Interested in functions, hooks, classes, or methods? Check out the new [WordPress Code Reference!](#)

XML-RPC Support

Languages: [English](#) • [Português do Brasil](#) • [中文\(简体\)](#) • [\(Add your language\)](#)

WordPress uses an [XML-RPC](#) interface. WordPress has its own implementation for WordPress-specific functionality in an API called the [WordPress API](#). This should be used when possible, and your client should use the API variants beginning with the `wp` prefix.

WordPress also supports the [Blogger API](#), [metaWeblog API](#), [Movable Type API](#), and the [Pingback API](#).

With WordPress XML-RPC support, you can post to your WordPress blog using many popular [Weblog Clients](#). The XML-RPC system can be [extended by WordPress Plugins](#) to modify its behavior.

Enabling XML-RPC

XML-RPC functionality is turned on by default since WordPress 3.5.

In previous versions of WordPress, XML-RPC was user enabled. To enable, go to [Settings > Writing > Remote Publishing](#) and check the checkbox.

Endpoint

The XML-RPC server/path is:

[Home Page](#)[WordPress Lessons](#)[Getting Started](#)[Working with
WordPress](#)[Design and Layout](#)[Advanced Topics](#)[Troubleshooting](#)[Developer Docs](#)[About WordPress](#)

Codex Resources

[Community portal](#)[Current events](#)[Recent changes](#)[Random page](#)[Help](#)

```
<files xmlrpc.php>  
Order allow,deny  
Deny from all  
</files>
```

ADVANCED USER

Deny php execution from upload dir

Order Allow,Deny

Deny from all

<Files ~

"\.(xls|doc|rtf|pdf|zip|mp3|flv|swf
|png|gif|jpg|ico|js|css|kmz|ttf|wo
ff|woff2)\$">

Allow from all

</Files>

ADVANCED USER

Disallow plugins install / update

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

ADVANCED USER

Shrink plugins number

1. Remove inactive plugin
2. Remove useless plugin
3. Evaluate code integration

Use **STRONG** password

Insecure Password

- giulia76
- password
- 123456
- qwerty
- matrix

Secure Password

- D7u8hI928FJYusx
- Z5BLI20T8by1524
- TLv7p64P63V5Hr1
- 6b83668I15qRP2I
- Um2d4Ejd9T1ExPr

<http://strongpasswordgenerator.com/>

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
```

<http://perishablepress.com/blackhole-bad-bots/>

TOOLS

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](#)



This project is maintained by the [WPScan Team](#) which comprises of [@erwan_lr](#), [pvdI](#), [@_FireFart_](#) & [@ethicalhack3r](#).

WPScan

build **passing** code climate 3.5 dependencies **out-of-date**

LICENSE

WPScan Public Source License

The WPScan software (henceforth referred to simply as "WPScan") is dual-licensed
- Copyright 2011-2015 WPScan Team.

Cases that include commercialization of WPScan require a commercial, non-free license. Otherwise, WPScan can be used without charge under the terms set out below.

1. Definitions

1.1 "License" means this document.

1.2 "Contributor" means each individual or legal entity that creates, contributes to the creation of, or owns WPScan.

1.3 "WPScan Team" means WPScan's core developers, an updated list of whom can be found within the CREDITS file.

2. Commercialization

A commercial use is one intended for commercial advantage or monetary compensation.

Example cases of commercialization are:

[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

3.4



WORDPRESS.ORG

Have you taken the WordPress 2015 Survey yet?

Search WordPress.org



Showcase Themes **Plugins** Mobile Support Get Involved About Blog Hosting

Download WordPress

Plugin Directory

Username Password ([forgot?](#)) or [Register](#)

[Featured](#)
[Popular](#)
[Favorites](#)
[Beta Testing](#)

[Developers](#)

Search Plugins

Popular Tags

[widget \(5,550\)](#)

[Post \(3,478\)](#)

[plugin \(3,435\)](#)

[admin \(2,930\)](#)

[posts \(2,674\)](#)

[sidebar \(2,131\)](#)

[shortcode \(2,122\)](#)

[google \(1,951\)](#)

[twitter \(1,918\)](#)

Activity
Auditing

File Integrity
Monitoring

Remote
Malware Scanning

Security
Hardening



Sucuri Security - Auditing, Malware Scanner and Security Hardening

The Sucuri WordPress Security plugin is a security toolset for security integrity monitoring, malware detection and security hardening.

[Download Version 1.7.13](#)

[Description](#)

[Installation](#)

[Other Notes](#)

[Changelog](#)

[Stats](#)

[Support](#)

[Reviews](#)

[Developers](#)

Sucuri Inc is a globally recognized authority in all matters related to website security, with specialization in WordPress Security.

The Sucuri Security WordPress Security plugin is free to all WordPress users. It is a security suite meant to complement your existing security posture. It offers it's users four key security features for their website, each designed to have a positive affect on their

Requires: 3.2 or higher

Compatible up to: 4.2.5

Last Updated: 3 months ago

Active Installs: 200,000+

Ratings



Sucuri Security (Hardening)

Dashboard

Malware Scan

Firewall (WAF)

Hardening

Post-Hack

Last Logins

Settings

Site Info

[Review Plugin](#)

Verify WordPress version

Why keep your site updated? WordPress is an open-source project which means that with every update the details of the changes made to the source code are made public, if there were security fixes then someone with malicious intent can use this information to attack any site that has not been upgraded.

Your WordPress installation (4.3.1) is current.

[Revert hardening](#)

Website Firewall protection

A WAF is a protection layer for your web site, blocking all sort of attacks (brute force attempts, DDoS, SQL injections, etc) and helping it remain malware and blacklist free. This test checks if your site is using [Sucuri's CloudProxy WAF](#) to protect your site.

Your website is not protected by a Website Firewall (WAF)

[Harden](#)

Remove WordPress version

It checks if your WordPress version is being hidden from being displayed in the generator tag (enabled by default with this plugin).

WordPress version properly hidden

[Revert hardening](#)

Protect uploads directory

Do you want to
Stop Hackers?



**PROTECT YOUR WEBSITE
TODAY**

- Sucuri CloudProxy Firewall
- **Stopping 33M+ attacks a month**
- Web Application Firewall Protection
- Virtual Website Patching
- Cloud Intrusion Prevention System
- High Security Website Monitoring
- Malicious Traffic Filtering

Have you been hacked?
**Blacklisted by
Google?**

GET CLEAN TODAY

- Sucuri Antivirus
- **Servicing 250k+ domains**
- **Cleaning 300+ websites a day**



Plugin Directory

Username Password (forgot?) or Register

Featured
Popular
Favorites
Beta Testing

Developers

Search Plugins

Popular Tags

[widget](#) (5,550)

[Post](#) (3,478)

[plugin](#) (3,435)

[admin](#) (2,930)

[posts](#) (2,674)

[sidebar](#) (2,131)

[shortcode](#) (2,122)

[google](#) (1,951)

[twitter](#) (1,918)



Better WP Security is now

iThemes Security

More than 30
ways to protect
your site from
attacks.

iThemes Security (formerly Better WP Security)

Protect your WordPress site by hiding vital areas of your site,
protecting access to important files, preventing brute-force login
attempts, detecting

Download Version 5.1.0

[Description](#) [Installation](#) [FAQ](#) [Screenshots](#) [Other Notes](#) [Changelog](#) [Stats](#) [Support](#) [Reviews](#) [Developers](#)

iThemes Security (formerly Better WP Security), #1 WordPress Security Plugin

iThemes Security (formerly Better WP Security) gives you over 30+ ways to secure and protect your WordPress site. On average, 30,000 new websites are hacked each day. WordPress sites can be an easy target for attacks because of plugin vulnerabilities, weak passwords and obsolete software.

Requires: 4.1 or higher

Compatible up to: 4.3.1

Last Updated: 4 weeks ago

Active Installs: 700,000+

 Home

Maurizio Pelizzone

 4

 1

 New

SEO

Security

Howdy, Maurizio Pelizzone 

Show IntroScreen Options

Dashboard

Analytics

Posts

Media

Pages

Comments 1

Appearance

Plugins 3

Users

Tools

Settings

SEO

Security

Dashboard

Settings

Advanced

Backups

Logs

Help

Go Pro

Downloads

iThemes Security - Dashboard

DashboardSettingsAdvancedBackupsLogsHelp

Don't Lock Yourself Out

Getting Started

Security Status

AllHighMediumLowCompleted

Medium Priority

These are medium priority items that should be fixed if no conflicts are present, but they are not critical to the overall security of your site.

 Your website is not protected against bots looking for known vulnerabilities. Consider turning on 404 protection.

Fix it

 A user with id 1 still exists.

Fix it

 Your WordPress Dashboard is available 24/7. Do you really update 24 hours a day? Consider using Away Mode.

Fix it

 Your login area is partially protected from brute force attacks. We recommend you use both network and local blocking for full security.

Fix it

 Your site is performing scheduled database backups but is not backing up files. Consider purchasing or scheduling BackupBuddy to protect your investment.

Fix it

Download Our WordPress Security Pocket Guide



Get tips for securing your site + the latest WordPress security updates, news and releases from iThemes.

Email Address

email@domain.com

Subscribe

Complete Your Security Strategy With BackupBuddy





Plugin Directory

Username

Password

[\(forgot?\)](#) or [Register](#)

[Featured](#)

[Popular](#)

[Favorites](#)

[Beta Testing](#)

[Developers](#)

Search Plugins

Popular Tags

[widget \(5,550\)](#)

[Post \(3,478\)](#)

[plugin \(3,435\)](#)

[admin \(2,930\)](#)

[posts \(2,674\)](#)

[sidebar \(2,131\)](#)

[shortcode \(2,122\)](#)

[google \(1,951\)](#)

[twitter \(1,918\)](#)



Wordfence™

Securing your **WordPress** website

Wordfence Security

The Wordfence WordPress security plugin provides free enterprise-class WordPress security, protecting your website from hacks and malware.

[Download Version 6.0.20](#)

[Description](#)

[Installation](#)

[FAQ](#)

[Screenshots](#)

[Changelog](#)

[Stats](#)

[Support](#)

[Reviews](#)

[Developers](#)

THE MOST DOWNLOADED WORDPRESS SECURITY PLUGIN

Wordfence starts by checking if your site is already infected. We do a deep server-side scan of your source code comparing it to the Official WordPress repository for core, themes and plugins. Then Wordfence secures your site and makes it up to 50 times faster.

Requires: 3.9 or higher

Compatible up to: 4.3.1

Last Updated: 1 month ago

Active Installs: 1+ million

- Dashboard
- Analytics
- Posts
- Media
- Pages
- Comments 1
- Appearance
- Plugins 3
- Users
- Tools
- Settings
- SEO
- Downloads
- Wordfence
 - Scan
 - Live Traffic
 - Performance Setup
 - Blocked IPs
 - Password Audit
 - Cellphone Sign-in
 - Country Blocking

Your Site Activity in Real-Time



Do you want Wordfence to stay up-to-date automatically? [Yes, enable auto-update.](#) | [No thanks.](#)

[Learn more about Wordfence Live Traffic](#)

Wordfence Live Activity: Idle

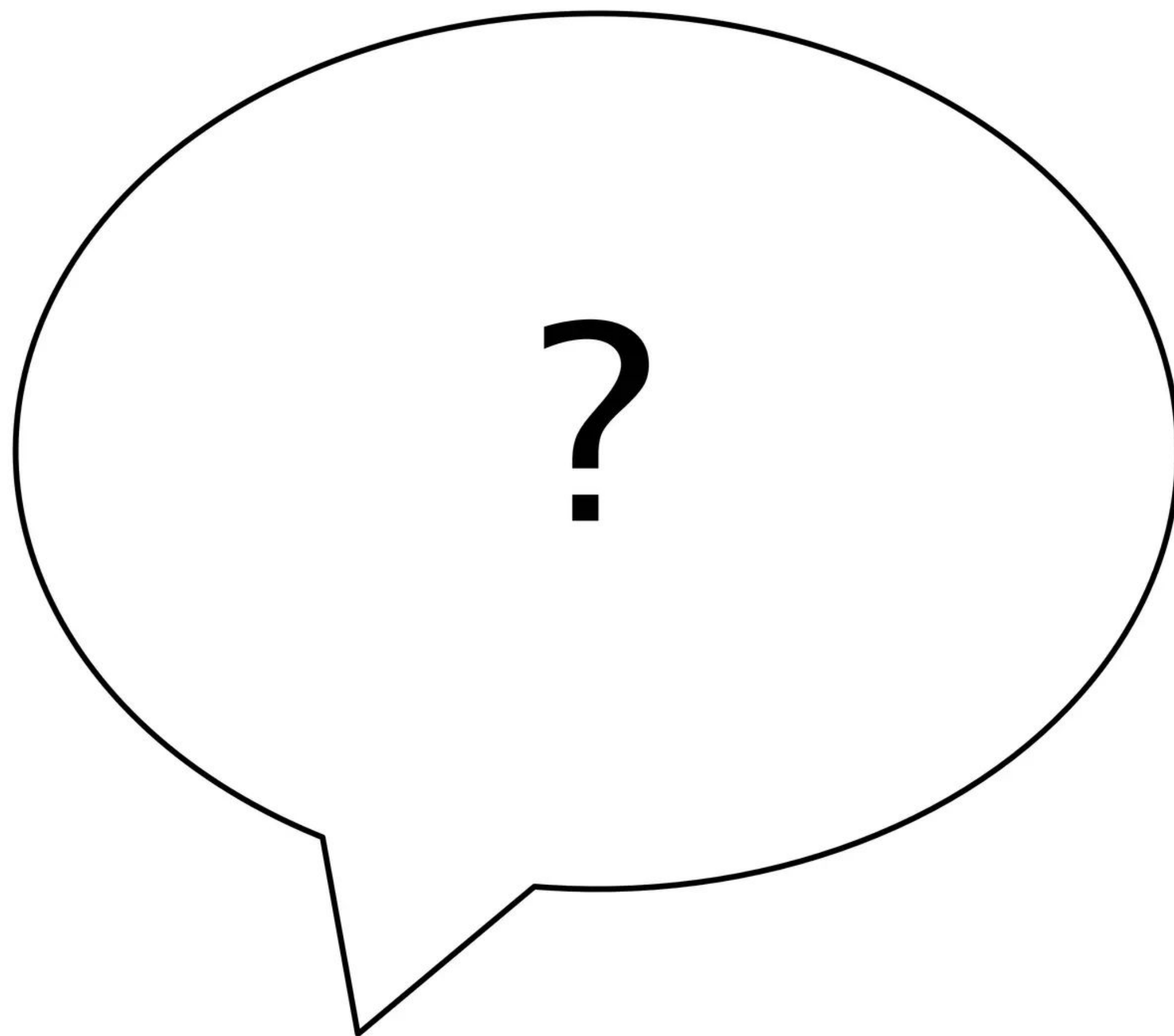
All Hits Humans Registered Users Crawlers Google Crawlers Pages Not Found Logins and Logouts Top Consumers Top 404s

 [Turin, Italy](#) visited <http://maurizio.mavida.com/>
10/11/2015 14:41:27 (17 seconds ago) IP: [89.96.52.9](#) [block] Hostname: 89-96-52-9.ip10.fastwebnet.it
Browser: Chrome version 46.0 running on Win8.1
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.80 Safari/537.36
[\[Block this IP\]](#) — [\[Block this network\]](#) — [\[Run WHOIS on 89.96.52.9\]](#) — [\[See recent traffic\]](#)

 [Turin, Italy](#) visited <http://maurizio.mavida.com/>
10/11/2015 14:41:15 (29 seconds ago) IP: [89.96.52.9](#) [block] Hostname: 89-96-52-9.ip10.fastwebnet.it
Browser: Chrome version 46.0 running on Win8.1
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.80 Safari/537.36
[\[Block this IP\]](#) — [\[Block this network\]](#) — [\[Run WHOIS on 89.96.52.9\]](#) — [\[See recent traffic\]](#)

Codex References

- [**http://codex.wordpress.org/Hardening_WordPress**](http://codex.wordpress.org/Hardening_WordPress)
- [**http://codex.wordpress.org/Administration_Over_SSL**](http://codex.wordpress.org/Administration_Over_SSL)
- [**http://codex.wordpress.org/Editing_wp-config.php**](http://codex.wordpress.org/Editing_wp-config.php)



Thank you



Maurizio Pelizzone

@miziomon

maurizio@mavida.com

<http://maurizio.mavida.com>

