

WordPress Site Security & Backups

Better safe than sorry

WordPress Usage Statistics

- 73+ Million WordPress powered websites (2015)
- 18.9% of all websites are running WordPress
- 22 out of every 100 new domains in the US launches with WordPress
- Projected 300-500 Million WordPress sites by **2025**

What is CMS Security

- CMS security is a multifaceted hardening of your CMS site.
- This means guarding the CMS backend login page to keep crackers and automated cracking bots out.
- It means being able to identify when someone or something is trying to break into your site or compromise your CMS by inserting malicious files, and stopping them by dropping their connection and banning their IP address, essentially blocking them from future malicious intent.

How do the hackers do it?

- Hackers upload contaminated files via FTP or some kind of up-loaders.
 - To deal with contaminated file, we must first be able to identify the files.
 - Identification requires file scanning and verification processing that can verify the integrity of CMS site files.
 - When contaminated files are found, we have to have clean backup versions so we can revert back to them.
- Cracking of the login username and password.
 - In this case, the rule of right is to strengthen the password.
 - I also recommend that you implement security plugins and change the WordPress login process.
- Malicious access to the core files.
 - Caused by exploiting code vulnerabilities in Themes, Plugins and WP core files.
 - In this case its up to the site admin to keep up on plugin updates and WordPress core updates and implement updates ASAP.

Web Malware Stats

- 403 Million unique variants of malware in 2011 (Symantec)
 - 140% growth since 2010
- 81% increase in malicious web-based attacks between 2010-2011

WordPress – Vulnerable to Link Injection

Link Injection

- Hacker bots look for known exploits (SQL injection, folder permissions, etc.)
 - Exploits (weaknesses) allows them to insert spam files/link into **WordPress Themes, plugins, and core files**

How To Secure WordPress Sites

- Keep your site and systems up to date
 - Keep your Themes up to date
 - Keep your Plugins up to date
 - Keep your WordPress core up to date
- Salt your keys
- Delete WP Admin Account
- Harden file and folder permissions
- Harden passwords
- Restrict file access

WordPress Security

- Update your site and all its components
- Use Secret Keys – a secret key is a hashing salt that inserts random elements into your password, making it harder to hack
- Delete the Admin user account, after you create a new user with Administration privileges.
 - This is an old note. WP has not used the Admin account in a long time. (There used to be a user named “admin” created when you created a WP site)
- Restrict key File and folder permissions
 - Files set to 644
 - Folders set to 755

Move the wp-config.php file

- WordPress has the ability to move the wp-config.php file to one directory above the WordPress root.
- Moving it out of the root folder makes it nearly impossible for anyone (the hackers, crackers, and bots) to access it.

Lock down WP Login and WP Admin

- Add the code below to wp-config.php to force SSL (https) on login
 - Define('FORCE_SSL_LOGIN', true);
- Add code below to wp_config.php to force SSL (https) on all admin pages
 - Define('FORCE_SSL_ADMIN', true);

Lock Down WP Login and WP Admin

- Create an .htaccess file in your wp-admin directory
- Add the following code to it

```
AuthUserFile /dev/null
```

```
AuthGroupFile /dev/null
```

```
AuthType Basic
```

```
order denyAllow
```

```
deny from all
```

```
#IP address to Whitelist – may not be relevant
```

```
#Allow from 67.120.83.59
```

Keep Your Guard Up At All Times

- Keep your computer up to date
 - If your web host isn't keeping their servers and software up to date, get a better host
- Install Anti-virus on your client computers
- Use a firewall
- Backup your File System and Database (often)
- Have a disaster recovery plan & Practice using it
 - Practice your disaster recovery plan until you feel comfortable doing it.
 - Consider have yearly drills and keep the plan current, upgrading software and processes when necessary

Increase WordPress Login Password Security – Force Strong Password

“Weak passwords have always made WordPress blogs and websites an easy target for hackers and users will always use easy passwords unless there are policies which they have to adhere to.”

[Robert Abela](#) 2014

WordPress Allows Weak Passwords

- By default WordPress does not have any built in tools that allow you to enforce password policies.
- It only has a strength indicator, but that does not stop users from using weak passwords.
- Therefore the best way to ensure all your users use strong WordPress passwords is by configuring password policies with [WP Password Policy Manager](#) which all users have to adhere to.

WP Password Policy Manager

Home Upload Plugin

Updates

Search Results Featured Popular Recommended Favorites Keyword ▾ WP Pa:

35 i



WP Password Policy Manager

Configure WordPress password policies to ensure all WordPress users use strong passwords and improve the security of your WordPress.

By [wpkytten](#)

★★★★★ (14)
2,000+ Active Installs

Last Updated: 9 months ago
Untested with your version of WordPress



WP User Manager

WP User Manager is the best solution to manage your users from the front-end of your members.

By Alessandro

★★★★★ (71)
4,000+ Active Installs

Default WordPress Allows Weak Passwords

Share a little biographical information to fill out your profile. This may be shown publicly.

Profile Picture 

Account Management

New Password  Hide  Cancel

Very weak

Confirm Password Confirm use of weak password 

This allows users to add



WordPress with WP Password Policy Manager Prevents Passwords

The screenshot shows the WordPress Admin interface under the 'Users' section. On the left, a sidebar lists various menu items: Comments, Appearance, Plugins, Users (which is selected and highlighted in blue), All Users, Add New, Your Profile, Backup Guard, Tools, Settings, SuperCacher, and Collapse menu. The main content area is titled 'Account Management'. It features a 'Profile Picture' placeholder and a 'New Password' field containing the complex string 'NaxS@g8NX\$U2PB#&%WFc^hSD'. A green bar below the field indicates the password is 'Strong'. To the right of the field are 'Hide' and 'Cancel' buttons. Below the password field, a note says 'New password must' followed by a bulleted list of requirements: not be the same as your username, not be the same as the previous one, be at least 12 characters long, contain mixed case characters, contain numeric digits, and contain special characters. At the bottom, it says 'WordPress Password Policies by [WP Password Policy Manager](#)' and includes a blue 'Update User' button.

WordPress Password Policy Manager Settings

Password Expiration Policy

Examples: [5 days](#) [20 days](#) [6 hours](#) [3 weeks](#)

Leave blank to disable Password Expiry policy.

Password Length Policy

 characters

Leave blank to disable Password Length policy.

Mixed Case Policy

Password must contain a mix of uppercase and lowercase characters.

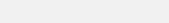
Numeric Digits Policy

Password must contain numeric digits ([0-9](#)).



Special Characters Policy

Password must contain special characters (eg: [.,!#\\$_+](#)).



Current Password Policy

When changing password on the profile page, the user must supply the current password.

Password History Policy

Remember old passwords

Leave blank to disable password history policy.

Users and Roles Exempt From Policies

 [Add](#)

Users and Roles in this list are free of all Password Policies.

Reset All Users' Passwords

[Reset All Passwords](#)

Use WP Cron



Only check this option if your site has many users.

WordPress Login Security

Login Lockdown is old and out of date

- Login Lockdown (offered by Some Web Hosts)
 - Login Lockdown may not be the best solution.
 - Its old and out of date.
 - Some web hosts offer [it still](#).
- The Login Lockdown Plugin is no longer supported, so please do not use it

The Login Lockdown Plugin Is Stale!

Please do not use it

The screenshot shows the WordPress.org Plugin Directory. The top navigation bar includes links for Showcase, Themes, Plugins, Mobile, Support, Get Involved, About, Blog, and Hosting, along with a 'Download WordPress' button. The main search bar is labeled 'Search WordPress.org'. On the left, there's a sidebar with links for Extending WordPress, Plugins (Developer Center), Themes, Mobile, Ideas, Kvetch!, and a search bar for 'Search Plugins' with a 'Popular Tags' section below it. The main content area shows the 'Login LockDown' plugin page. A yellow warning box at the top states: 'This plugin hasn't been updated in over 2 years. It may no longer be maintained or supported and may have compatibility issues when used with more recent versions of WordPress.' The plugin title 'Login LockDown' is displayed in large bold letters. Below the title, a description states: 'Limits the number of login attempts from a given IP range within a certain time period.' To the right of the description is a red 'Download Version v1.5' button. Below the description are tabs for Description, Installation, Stats, Support, Reviews, and Developers. The plugin's description text explains its function: '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. Administrators can release locked out IP ranges manually from the panel.' To the right of this text are several metadata fields: 'Requires: 2.5 or higher', 'Compatible up to: 2.8.4', 'Last Updated: 2009-9-17', and 'Downloads: 251,789'. At the bottom of the plugin page are sections for 'Ratings' and a 5-star rating icon.

WP Security Plugins

- Better WP Security
- BulletProof Security
- Login Security Solution
- Total Security
- Stealth Login Page
- WordFence
- SpamPot – adds a honeypot form field
- Spam Honey Pot - adds a honeypot form field

Better WP Security

WORDPRESS.ORG

Showcase Themes Plugins Mobile Support Get Involved About Blog Hosting

Search WordPress.org

Download WordPress

Plugin Directory

Username Password Log in (forgot?) or Register

Extending WordPress

Plugins

- Developer Center

Themes

Mobile

Ideas

Kvetch!

Search Plugins

Popular

Tags

More »

widget (3,827)

Post (2,420)

plugin (2,308)

admin (1,914)

posts (1,829)

sidebar (1,569)

The best way to secure WordPress

Better WP Security

The easiest, most effective way to secure WordPress. Improve the security of any WordPress site in seconds.

Download Version 3.5.6

Description Installation FAQ Screenshots Other Notes Changelog Stats Support Reviews Developers

#1 WORDPRESS SECURITY PLUGIN

Better WP Security takes the best WordPress security features and techniques and combines them in a single plugin thereby ensuring that as many security holes as possible are patched without having to worry about conflicting features or the possibility of missing anything on your site.

Requires: 3.6 or higher
Compatible up to: 3.6.1
Last Updated: 2013-8-24
Downloads: 1,124,303

BulletProof Security

WORDPRESS.ORG

Showcase Themes Plugins Mobile Support Get Involved About Blog Hosting

Search WordPress.org

Download WordPress

Plugin Directory

Username Password Log in (forgot?) or Register

Extending WordPress

Plugins

- Developer Center

Themes

Mobile

Ideas

Kvetch!

Search Plugins

Popular

Tags More »

widget (3,827)

Post (2,420)

plugin (2,308)

admin (1,914)

posts (1,829)

sidebar (1,569)

twitter (1,305)

google (1,304)

 **BULLETPROOF SECURITY**
XSS, RFI, CRLF, CSRF, Base64, Code Injection, SQL Injection ...
BulletProof Security **WEBSITE SECURITY**

WordPress Website Security Protection. Website security protection against: XSS, RFI, CRLF, CSRF, Base64, Code Injection and SQL Injection hacking...

[Download Version .49.2](#)

Description Installation FAQ Screenshots Other Notes Changelog Stats Support Reviews Developers

htaccess Core Website Security (Firewalls)

WordPress Website Security Protection: BulletProof Security protects your WordPress website against XSS, RFI, CRLF, CSRF, Base64, Code Injection and SQL Injection... hacking attempts. One-click .htaccess WordPress security protection. Protects wp-config.php, bb-config.php, php.ini, php5.ini, install.php and readme.html with .htaccess security protection. Security Logging. HTTP Error Logging. Login Security/Login Monitoring:

Requires: 3.0 or higher
Compatible up to: 3.6.1
Last Updated: 2013-9-17
Downloads: 844,222

Ratings

Login Security Solution

WORDPRESS.ORG

Showcase Themes Plugins Mobile Support Get Involved About Blog Hosting

Search WordPress.org

Download WordPress

Plugin Directory

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

Login Security Solution

Extending WordPress

Plugins [Developer Center](#)

Themes

Mobile

Ideas

Kvetch!

Search Plugins Search

Popular

Tags More »

widget (3,827)

Post (2,420)

plugin (2,308)

admin (1,914)

posts (1,829)

sidebar (1,569)

twitter (1,305)

google (1,304)

Security against brute force attacks by tracking IP, name, password; requiring very strong passwords. Idle timeout. Maintenance mode lockdown.

Download Version 0.42.0

Description Installation FAQ Other Notes Changelog Stats Support Reviews Developers

A simple way to lock down login security for multisite and regular WordPress installations.

- Blocks brute force and dictionary attacks without inconveniencing legitimate users or administrators
- Tracks IP addresses, usernames, and passwords
- Monitors logins made by form submissions, XML-RPC requests and auth cookies
- If a login failure uses data matching a past failure, the plugin slows down response times. The more failures, the longer the delay. This limits attackers ability to effectively probe your site, so they'll give up and go find an easier target.
- If an account seems breached, the "user" is immediately logged out and forced to use WordPress' password reset utility. This prevents any damage from being done and verifies the user's identity. But if the user is coming in from an IP address they have used in the past, an email is sent to the user making sure it was them logging in. All without intervention by an administrator.
- Can notify the administrator of attacks and breaches
- Supports IPv6

Requires: 3.3 or higher
Compatible up to: 3.6beta3
Last Updated: 2013-7-6
Downloads: 78,148

Ratings

4.7 out of 5 stars

5 stars	<div style="width: 80%; background-color: #f0ad4e;"></div>	41
4 stars	<div style="width: 10%; background-color: #f0ad4e;"></div>	3
3 stars	<div style="width: 5%; background-color: #f0ad4e;"></div>	1
2 stars	<div style="width: 5%; background-color: #f0ad4e;"></div>	1
1 stars	<div style="width: 5%; background-color: #f0ad4e;"></div>	1

Author

 Daniel Convisor

Stealth Login Page

WORDPRESS.ORG

Showcase Themes Plugins Mobile Support Get Involved About Blog Hosting

Search WordPress.org

Download WordPress

Plugin Directory

Username _____ Password _____ Log in (forgot?) or Register

Extending WordPress

Plugins

- Developer Center

Themes

Mobile

Ideas

Kvetch!

Search Plugins

Popular

Tags More »

widget (3,827)

Post (2,420)

plugin (2,308)

admin (1,914)

posts (1,829)

sidebar (1,569)

twitter (1,305)

google (1,304)

comments (1,289)

images (1,244)

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 authorization code. Those who do not enter this additional authorization will be automatically redirected to a customizable URL.

This is the first plugin that blocks external bot login requests - login requests must comply with the full login sequence or the request is rejected.

Requires: 3.4.2 or higher
Compatible up to: 3.6.1
Last Updated: 2013-7-30
Downloads: 24,656

Ratings

★★★★★ 4.5 out of 5 stars

5 stars [progress bar] 29
4 stars [progress bar] 1

Review 3 Security Plugins

- Login Security Solution
- Total Security
- Stealth Login Page

Login Security Solutions

- Tweaks the login process and adds notification of hack attempts
 - Keep in mind , this is just a warning sign.

Login Security Settings



Login Security Solution Settings

Login Failure Policies

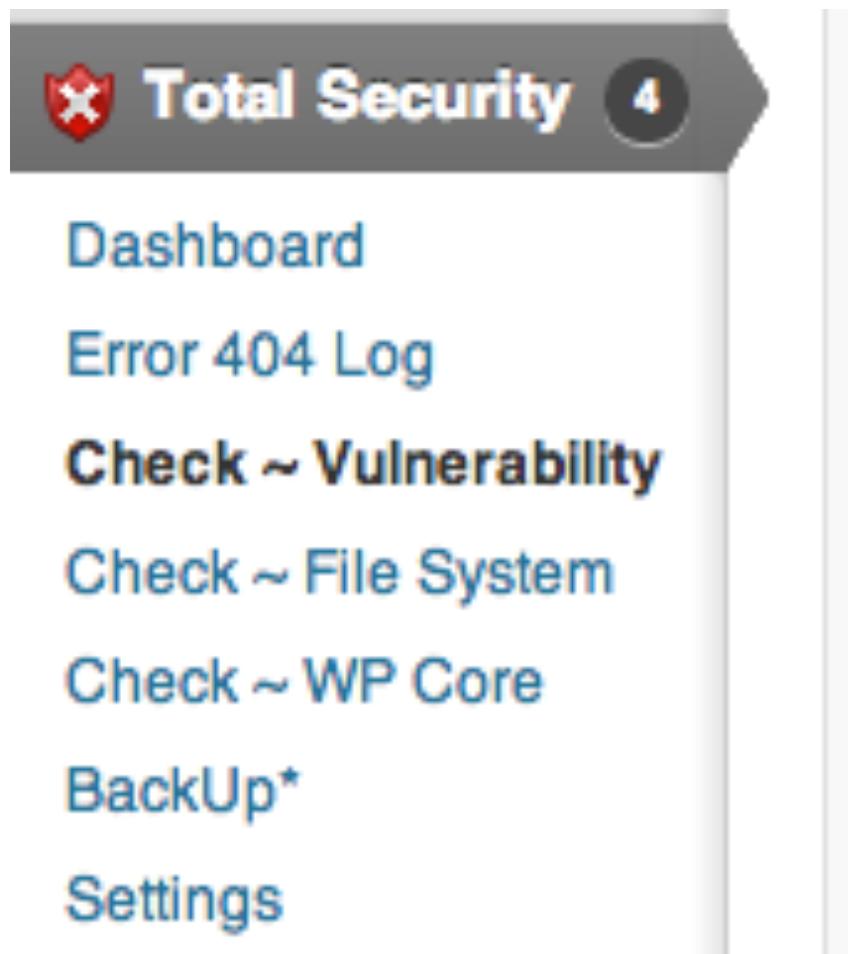
This plugin stores the IP address, username and password for each failed log in attempt. The data from future login failures are compared against the historical data. If any of the stored data matches, it will trigger a delay before the user can log in again. This is done by printing out the failure message. The goal is for the responses to take so long that the attackers give up and go find an easier target. The length of the delay is broken up into three tiers. The delay time within each tier increases in higher tiers. The delay time within each tier is randomized to complicate profiling by attackers.

Match Time	<input type="text" value="120"/>	How far back, in minutes, should login failures look for matching data? Default: 120.
Delay Tier 2	<input type="text" value="5"/>	How many matching login failures should it take to get into this (4 - 30 second) Delay Tier? Must be >= 2. Default: 5.
Delay Tier 3	<input type="text" value="10"/>	How many matching login failures should it take to get into this (25 - 60 second) Delay Tier? Must be > Delay Tier 2. Default: 10.
Notifications To	<input type="text"/>	
	The email address(es) the failure and breach notifications should be sent to. For multiple addresses, separate them with commas. If none is provided here, Default: .	
Failure Notification	<input type="text" value="50"/>	Notify the administrator after x matching login failures. 0 disables this feature. Default: 50.
Multiple Failure Notifications	Should multiple failure notifications be sent to the administrators?	
	<input checked="" type="radio"/> No, just notify them the first time that x matching login failures happen. <input type="radio"/> Yes, notify them upon every x matching login failures.	
Breach Notification	<input type="text" value="6"/>	Notify the administrator if a successful login uses data matching x login failures. 0 disables this feature. Default: 6.
Breach Email Confirm	<input type="text" value="6"/>	If a successful login uses data matching x login failures, immediately log the user out and require them to use WordPress' built-in password recovery feature. Default: 6.

Total Security

- As advertised, this is a total WordPress security dashboard solution
- You can run diagnostic vulnerability checks on the WP site, file system
 - Good first step security and vulnerability audit
- Has ability to create a hidden **wp-login** and **wp-admin page**
 - This is Safer than editing the “.htaccess” file by hand.

Good Visibility - Left Sidebar Toolbar



Dashboard



Total Security : Dashboard

You have not asked your users to change their passwords since the plugin was activated. Most users have weak passwords. This plugin's password policies prevent this from happening. Please improve security for everyone on the Internet by making all users pick new, strong, passwords.

Speaking of which, do YOU have a strong password? Make sure by changing yours too.

The following link leads to a user interface where you can either require all passwords to be reset or disable this notice.

[Change All Passwords](#)

Security Status

	Last run on	Medium Risk	High Risk	Overall Risk Rating
WP Core	September 28, 2013, 3:02 pm			
File System	September 28, 2013, 3:01 pm			
Vulnerability	September 28, 2013, 3:01 pm			

*Rerun the checks after changes in your configuration.

Additional Info

You can see all identified security problems of your website at one glance.

Each security problem comes with a detailed description and all the information needed so you can eliminate the problems and get secure.

Any red or orange dots? Follow the instructions and turn them into green dots!

[Phpinfo\(\)](#)

[Debug](#)

[Database Info](#)

All security checks are assigned one of the following risks:

No security risk has been identified.

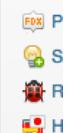
A medium security risk, resolve it as soon as possible.

The identified security issues have to be resolved immediately.

No security risk. (If possible, replace)

Error / Unable / Deactivated (No risk assessment)

Total



Do yo

Please
of this



Trans

Would
Contri
web ir
requir

Hide wp-login.php & wp-admin folder

Secure Hidden Login

Allows you to create custom URLs for user's login, logout and admin's login page, without editing any .htaccess files.

Those attempting to gain access to your login form will be automatically redirected to a customizable URL.

Hide "wp-login.php" and "wp-admin" folder

1234

Secret key

URL to redirect unauthorized attempts

Leave blank for 404 page

Tip: add eg. /intrusion-detection/ for log in Error 404 Log, or "/" for home.

Vulnerability Scan

Securing Hidden Login

Secure Hidden Login

Allows you to create custom URLs for user's login, logout and admin's login page, without editing any .htaccess files.

Login url: `./wp-login.php?login_key=████████`
You need to remember new address to login!

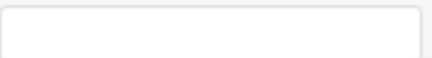
Those attempting to gain access to your login form will be automatically redirected to a customizable URL.

Hide "wp-login.php" and "wp-admin" folder



Secret key

URL to redirect unauthorized attempts



Leave blank for 404 page

Tip: add eg. /intrusion-detection/ for log in Error 404 Log, or "/" for home

Vulnerability Scan

Total Security Vulnerability Check Details

W	Test the strength of WordPress database password.	<input checked="" type="checkbox"/>
W	Check if security keys and salts have proper values.	<input checked="" type="checkbox"/>
W	Check if table prefix is the default one "wp_".	Yes <input checked="" type="checkbox"/>
W	Check if general debug mode is enabled.	<input checked="" type="checkbox"/>
W	Check if WordPress installation address is the same as the site address.	Yes <input type="checkbox"/>
W	Check if <i>uploads</i> folder is browsable by browsers.	<input checked="" type="checkbox"/>
W	Check if "anyone can register" option is enabled.	<input checked="" type="checkbox"/>
W	Check if plugins/themes file editor is enabled.	Enabled <input checked="" type="checkbox"/>
W	Check if user with username "admin" exists.	<input checked="" type="checkbox"/>
W	Test if user with "ID=1" is administrator.	Yes <input checked="" type="checkbox"/>
W	Check admin password strength with a <i>600</i> most commonly used	<input checked="" type="checkbox"/>
W	Check if "Secure Hidden Login" is enabled	Disabled <input checked="" type="checkbox"/>

Stealth Login Page Plugin

- Without locking down access via IP address or file permissions, this plugin creates a secret login authorization code.
 - Those who do not enter this additional authorization will be automatically redirected to a customizable URL.
- **This was the first plugin to block external bot login requests**
 - login requests must comply with the full login sequence or the request is rejected.
- **Helps prevent brute-force attacks, and bot-nets**
 - Just like socks help prevent blisters

Setting Stealth Login Page Options

Stealth Login Page Options

You have not asked your users to change their passwords since the plugin was activated. Most users have weak passwords. This plugin's purpose is to help you improve security for everyone on the Internet by making all users pick new, strong, passwords.

Speaking of which, do YOU have a strong password? Make sure by changing yours too.

The following link leads to a user interface where you can either require all passwords to be reset or disable this notice.

[Change All Passwords](#)

Enable/Disable Stealth Login Page

Enable Stealth Mode

Enter an authorization code below. Think of it as another password or a PIN. Without a proper entry from the login form, the login form will redirect.

Enter an authorization code

Unsuccessful attempts to gain access to your dashboard will be automatically redirected to a customizable URL. Enter that URL below.

URL to redirect unauthorized attempts to http://cnn.com

Email authorization code to admin

[Save Settings](#)

Your authorization code is:

Stealth Login Adds an extra Authorization code to the login process



Site Checking Software

SUCURI

<http://Sucuri.net>

- Free Website Malware Scanner: <http://sitecheck.sucuri.net/scanner/>
- Website monitoring
- Hack cleanup services
- Sucuri Security Plugin
 - Free to clients
 - Web Application Firewall
 - Integrity Monitoring
 - Auditing
 - Hardening



<http://Sucuri.net>

Sucuri SiteCheck – Not bad!

The screenshot shows the Sucuri SiteCheck homepage. At the top, there's a navigation bar with links for HOME, TOUR, PRICING, BLOG, GLOBAL, and CONTACT. The main title "Sucuri SiteCheck" is prominently displayed. Below it, a section titled "Free Website Malware Scanner" features a text input field for entering a URL and a large green "SCAN WEBSITE" button. A disclaimer below the input field states: "Disclaimer: Sucuri SiteCheck is a free & remote scanner. Although we do our best to provide the best results, 100% accuracy is not realistic, and not guaranteed." To the right, there's a sidebar titled "Sucuri Plans" with a "POPULAR" plan highlighted. This plan includes "POWERFUL SCANNING", "5 WEBSITES", and a price of "\$189.99 Yearly". It also lists included features: "Malware Cleanup (No False Positives)", "Website Integrity Monitoring", "Email & Twitter Alerts", "Manual Website Scan", and "Blacklist Removal". A large green "GET CLEAN" button is at the bottom of the plan summary.

Sucuri SiteCheck

Free Website Malware Scanner

Enter a URL (ex. sucuri.net) and the Sucuri SiteCheck scanner will check the website for known malware, blacklisting status, website errors, and out-of-date software.

Scan Website **SCAN WEBSITE**

Disclaimer: Sucuri SiteCheck is a free & remote scanner. Although we do our best to provide the best results, 100% accuracy is not realistic, and not guaranteed.

Protect Your Interwebs!

Tour of Sucuri Security

SUCURI
PROTECT YOUR INTERWEBS

INFECTED WITH PHARMA HACK?

We have extensive experience working with the Pharma Hack, short for Pharmaceutical Hack. Let us clear this annoying SPAM from your site.

GET CLEAN

Sucuri Plans

POPULAR

POWERFUL SCANNING

5 WEBSITES

\$189.99 Yearly

INCLUDES

- Malware Cleanup (No False Positives)
- Website Integrity Monitoring
- Email & Twitter Alerts
- Manual Website Scan
- Blacklist Removal

Lets Run A Site Scan

FREE WEBSITE SCANS BY SUCURI SITECHECK



**VISIT OUR [COVERAGE & PRICING](#) PAGE FOR
DETAILS ON HOW SUCURI CAN HELP YOU.**



Scan Results

Sucuri
PROTECT YOUR INTERNET

HOME TOUR PRICING BLOG

Sucuri SiteCheck

Free Website Malware Scanner

Sitecheck Results **Website details** **Blacklisting status**

 web site: mikehchase54.net/wpsecurity
status: **Verified Clean**
web trust: **Not Blacklisted**

*This site was just scanned a few minutes ago.

Security report (No threats found):

 Blacklisted:	No
 Malware:	No
 Malicious javascript:	No
 Malicious iFrames:	No
 Drive-By Downloads:	No
 Anomaly detection:	No
 IE-only attacks:	No
 Suspicious redirections:	No

Scan Result Details



web site:

mikehchase54.net/wpsecurity

status:

Verified Clean

web trust:

Not Blacklisted

**This site was just scanned a few minutes ago.*

Security report (*No threats found*):

- Blacklisted:** No
- Malware:** No
- Malicious javascript:** No
- Malicious iFrames:** No
- Drive-By Downloads:** No
- Anomaly detection:** No
- IE-only attacks:** No
- Suspicious redirections:** No
- Spam:** No

Very important note about site scanning tools (USE CAUTION!!!)

- ONLY RUN WEBSITE SCAN TOOLS on websites you are personally responsible for or you are the web site administrator for the site being scanned
 - Scan companies track who runs the scans
 - Excessive scanning can appear to be a denial of service (DOS) attack
 - You do not want to be brought up on charges a denial of service attack

[Twitter](#) [Facebook](#) [Share](#)



Charges in Distributed Denial of Service Attack Against Santa Cruz County Website

Defendants Alleged to Be Part of "People's Liberation Front," Hacking Group Associated with "Anonymous"

U.S. Attorney's Office
September 22, 2011

Northern District of California
(415) 436-7200

IP Address Blocking

- IP address blocking prevents connection between a server or website and certain IP addresses or ranges of addresses.
- IP address blocking effectively bans undesired connections from hosts using affected addresses to a website, mail server, or other Internet server.
- IP address blocking is commonly used to protect against brute force attacks.
- Both companies and schools offering remote user access use programs such as **DenyHosts** or **Fail2ban** for protection from unauthorized access while allowing permitted remote access.
- **IP Address blocking is also used for censorship.**

IP Address Blocking on repeated invalid login attempts – Using a WP Plugin

- This is referred to as bad behavior IP block and ban.
 - If someone reputably tried to hack into your system the plugin bans the IP address for a period of time.
 - The number of invalid login attempts can be configured.
 - Ban can be changed from a period of time (hours) to a permanent ban

WordPress IP Blocking Plugins

- Shield (formerly Simple Firewall)
- All In One WP Security & Firewall
- Ninja-Firewall (WP-Edition)
- IP Geo Block – For Xenophobic site owners and site owners who do not want to be global players or do not want a global presence.
 - If this is you, this plugin may be perfect for you!

Shield (formerly Simple Firewall)

Description Installation Changelog FAQ Reviews

Shield is the most powerful [WordPress protection system](#) available. Designed for maximum compatibility with your WordPress sites, it provides a super simple approach for both beginner and advanced users. NO more nasty site lockouts! Experience the difference that a great security plugin makes, alongside common-sense security design. You'll never look back!

Do you want to secure your WordPress site, without getting overwhelmed?

Stand out from the herd - what makes ours different?

- No restriction on security features - it's all there.
- Easy-To-Setup Interface.
- It won't break your website - you'll never get that horrible, pit-of-your-stomach feeling you get with other security plugins when your website doesn't load anymore.
- Plugin Self Security Protection - the *only* WordPress Security Plugin that protects against tampering.
- Exclusive membership to a private security group where you can learn more about WordPress security.

Awesome Features

- Blocks malicious URLs and requests
- Blocks **ALL** automated spambot comments.
- Hide your WordPress Admin and Login page.
- Prevents brute force attacks on your login and any attempted automatic bot logins.
- Verify user identity with email-based Two-Factor Authentication
- Monitor login activity and restrict username sharing, with User Sessions Management
- Review admin activity with a detailed Audit Trail Log
- Turn on and turn off WordPress Automatic Updates separately for plugins, themes and Core
- Easy to use kill switch to temporarily turn off all Firewall Features without disabling the plugin or even logging into WordPress.

Plugin Admin Access Protection

The **only** WordPress security plugin with a WordPress-independent security key to protect itself. [more info](#)

Shield Dashboard

My WordPress Demo Site 1 0 + New Purge SG Cache Howdy, mchase

Dashboard Jetpack Posts Media Pages Comments Appearance Plugins Users Tools Settings Shield

Dashboard - Overview of the plugin settings

Notice - The Shield plugin does not automatically turn on certain features when you install. [Click to read about any important updates from the plugin home page.](#) [Dismiss this notice](#)

Global Options General Options Third Party Services

Global Plugin Security Options

Enable Features Global Plugin On/Off Switch
Uncheck this option to disable all Shield features.

Save All Settings

The screenshot shows the WordPress dashboard with the 'Shield' plugin active. The left sidebar has a dark theme with white text. The 'Shield' menu item is highlighted with a blue background. The main content area is titled 'Dashboard - Overview of the plugin settings'. It features a notice about feature activation. Below the notice is a row of ten icons representing different security features: Dashboard (green gear), Security Admin (orange shield), Firewall (green wall), Login Protection (orange key), User Management (green people), Comments SPAM (orange speech bubbles), Automatic Updates (green circular arrow), Hack Protection (orange X), Lockdown (green padlock), IP Manager (orange location pin), Audit Trail (orange eye), and Premium Support (green telephone). A navigation bar at the bottom includes 'Global Options', 'General Options' (which is selected and highlighted in blue), and 'Third Party Services'. The 'General Options' section is titled 'Global Plugin Security Options' and contains a 'Enable Features' section with a checked checkbox for 'Global Plugin On/Off Switch' and a note to uncheck it to disable all features. A large blue 'Save All Settings' button is at the bottom.

All-in-one WP Security Plugin

- **COMPREHENSIVE, EASY TO USE, STABLE AND WELL SUPPORTED WORDPRESS SECURITY PLUGIN**
- WordPress itself is a very secure platform. This plugin adds extra security and firewall to your site by enforcing good security practices.
- The All In One WordPress Security plugin will take your website security to a whole new level.
- This plugin is designed and written by experts and is easy to use and understand.

All-in-one WP Security Plugin

- It reduces security risk by **checking for vulnerabilities**, and by **implementing and enforcing the latest recommended WordPress security practices and techniques**.
- All In One WP Security also uses an unprecedented security points grading system to measure how well you are protecting your site based on the security features you have activated.
- **The All In One WordPress Security plugin doesn't slow down your site and it is 100% free.**

All-in-one WP Security Dashboard

My WordPress Demo Site 1 0 New Purge SG Cache Howdy, mchase

Dashboard Jetpack Posts Media Pages Comments Appearance Plugins Users Tools Settings WP Security

Would you like All In One WP Security & Firewall to re-insert the security rules in your .htaccess file which were cleared when you deactivated the plugin? [Yes](#) [No](#)

Dashboard System Info Locked IP Addresses Permanent Block List AIOWPS Logs

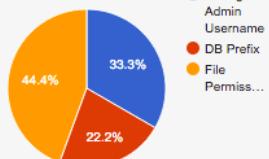
For information, updates and documentation, please visit the [AIO WP Security & Firewall Plugin Page](#)
[Follow us](#) on Twitter, Google+ or via Email to stay up to date about the new security features of this plugin.

Security Strength Meter



Total Achievable Points: 470
Current Score of Your Site: 45

Security Points Breakdown



Category	Percentage
Change Admin Username	33.3%
DB Prefix	22.2%
File Permiss...	44.4%

Get To Know The Developers

Wanna know more about the developers behind this plugin?

[WPSolutions](#)
[Tips and Tricks HQ](#)

Spread the Word

We are working hard to make your WordPress site more secure. Please support us, here is how:

[Follow us on Google+](#)
[Post to Twitter](#)
[Give us a Good Rating](#)

Critical Feature Status

IP Geo Block with Zero Day Exploit Protection

- There are some cases of a site being infected.
 - The first one is the case that contaminated files are uploaded via FTP or some kind of up-loaders. In this case, scanning and verifying integrity of files in your site is useful to detect the infection.
 - The second one is cracking of the login username and password. In this case, the rule of right is to strengthen the password.
 - The third one is caused by malicious access to the core files.
 - The major issue in this case is that a plugin or theme in your site can potentially has some vulnerability such as XSS, CSRF, SQLi, LFI and so on.
 - For example, if a plugin has vulnerability of Local File Inclusion (LFI), the attackers can easily download the wp-config.php without knowing the username and password by simply hitting wp-admin/admin-ajax.php?action=show&file=..../wp-config.php on their browser.
- For these cases, the protection based on the **IP address is not a perfect solution for everyone.**
- But for some site owners or some certain cases such as 'zero-day attack', combination with WP-ZEP can still reduce the risk of infection against the specific attacks.
- That's why this plugin is here.

IP Geo Block Dashboard

The screenshot shows the WordPress dashboard with the 'IP Geo Block' plugin active. The left sidebar has a 'Settings' tab selected. The main content area displays validation rule settings, including fields for matching rules, country codes, and extra IP addresses.

IP Geo Block: Downloading geolocation databases was successfully done.

Validation rule settings

Your IP address / Country: 69.243.146.71 / US (Cache) [Scan your country code](#)

Matching rule: White list

Country code for matching rule (ISO 3166-1 alpha-2): US (comma separated)

White list of extra IP addresses prior to country code (CIDR): (comma separated)

Black list of extra IP addresses prior to country code (CIDR): (comma separated)

\$_SERVER keys to retrieve extra IP addresses: (comma separated)

Response code (RFC 2616): 403 Forbidden

Max number of failed login attempts per IP address: 5

Country Codes – For Blocking Countries

	Not used: not used in ISO 3166-1 in deference to intergovernmental intellectual property organisation names.
	Unassigned: free for assignment by the ISO 3166/MA only.

Officially assigned code elements [edit]

The following is a complete list of the 249 current officially assigned ISO 3166-1 alpha-2 codes, with the following columns:

- **Code** — ISO 3166-1 alpha-2 code
- **Country name** — English short country name officially used by the ISO 3166 Maintenance Agency (ISO 3166/MA)^[15]
- **Year** — Year when alpha-2 code was first officially assigned (1974, first edition of ISO 3166)
- **ccTLD** — Corresponding [country code top-level domain](#) (note that some are inactive); exceptions where another ccTLD is assigned for the country are shown in parentheses
- **ISO 3166-2** — Corresponding [ISO 3166-2](#) codes
- **Notes** — Any unofficial notes

Code	Country name	Year	ccTLD	ISO 3166-2	Notes
AD	Andorra	1974	.ad	ISO 3166-2:AD	
AE	United Arab Emirates	1974	.ae	ISO 3166-2:AE	
AF	Afghanistan	1974	.af	ISO 3166-2:AF	
AG	Antigua and Barbuda	1974	.ag	ISO 3166-2:AG	
AI	Anguilla	1983	.ai	ISO 3166-2:AI	AI previously represented French Afar and Issas
AL	Albania	1974	.al	ISO 3166-2:AL	
AM	Armenia	1992	.am	ISO 3166-2:AM	
AO	Angola	1974	.ao	ISO 3166-2:AO	
AQ	Antarctica	1974	.aq	ISO 3166-2:AQ	Covers the territories south of 60° south latitude Code taken from name in French: <i>Antarctique</i>
AR	Argentina	1974	.ar	ISO 3166-2:AR	
AS	American Samoa	1974	.as	ISO 3166-2:AS	
AT	Austria	1974	.at	ISO 3166-2:AT	
AU	Australia	1974	.au	ISO 3166-2:AU	Includes the Ashmore and Cartier Islands and the Coral Sea Islands
AW	Aruba	1986	.aw	ISO 3166-2:AW	
...

Additional Web Resources

- **Security Related Articles**
 - http://codex.wordpress.org/Hardening_WordPress
 - <http://blog.sucuri.net/2012/04/lockdown-wordpress-a-security-webinar-with-dre-armeda.html>
 - <http://blog.sucuri.net/2012/04/ask-sucuri-how-to-stop-the-hacker-and-ensure-your-site-is-locked.html>
 - <http://blog.sucuri.net/2012/04/ask-sucuri-what-should-i-know-when-engaging-a-web-malware-company.html>
- **Clean a Hacked Site**
 - http://codex.wordpress.org/FAQ_My_site_was_hacked
 - <http://www.marketingtechblog.com/wordpress-hacked/>
- **Support Forums**
 - Hacked: <http://wordpress.org/tags/hacked>
 - Malware: <http://wordpress.org/tags/malware>

Wordfence & Wordfence Assistant

My WP Backup Test Site 1 0 New Purge SG Cache Howdy, mchase Help ▾

Visit Site Add Plugins Upload Plugin

Search Results Featured Popular Recommended Favorites Keyword ▾ WordFence

43 items « < 1 of 2 > »

 **Wordfence Security** [Install Now](#) [More Details](#)
The Wordfence WordPress security plugin provides free enterprise-class WordPress security, protecting your website from hacks and malware.
By Wordfence
★★★★★ (2,707) 1+ Million Active Installs Last Updated: 2 days ago ✓ Compatible with your version of WordPress

 **Wordfence Assistant** [Install Now](#) [More Details](#)
Wordfence Assistant provides data management utilities for Wordfence users.
By Mark Maunder
★★★★★ (3) 3,000+ Active Installs Last Updated: 2 days ago ✓ Compatible with your version of WordPress

Wordfence – Free version is limited

- Its worth installing just for the security scan
- Its complicated to learn and use
- Be patient and take your time and always install the additional assistant plugin – so you can get in if and when you lock yourself out of the site

Wordfence Assistant

Why does this additional plugin exist?

- In rare cases, Wordfence users can accidentally lock themselves out of their system.
- Wordfence provides a built-in user-friendly system to regain access to your website which allows site administrators to send themselves an unlock email which contains a link that unlocks their website.
- Because Wordfence has become so popular, we see edge cases where systems administrators no longer have access to their old email address or the email unlock does not work for another reason.
- To help unlock sites with that problem, we've provided this plugin which you can install after you've removed Wordfence from your system.
- You can use this plugin to modify the Wordfence data in your database and disable the Wordfence firewall so that if you reinstall Wordfence the firewall won't lock you out again.
- You can also use this plugin to delete all Wordfence data.

WordFence Scan

To make your site as secure as possible, take a moment to optimize the Wordfence Web Application Firewall: [Click here to configure.](#) [Dismiss](#)
If you cannot complete the setup process, [click here for help.](#)

Wordfence Scan

You have not set an administrator email address to receive alerts for Wordfence. Please [click here to go to the Wordfence Options Page](#) and set an email address where you will receive security alerts from this site.

[Use My Email Address](#) [Dismiss](#)

[Learn more about scanning](#)

[Start a Wordfence Scan](#)

[Click to kill the current scan.](#)

[Read our scanning documentation.](#) You can also [start the tour again](#), [subscribe to get WordPress Security Alerts and Product News](#) or [visit our support website help](#). Love Wordfence? You can help by doing two simple things: [Go to WordPress.org now and give this plugin a 5★ rating](#). Blog about Wordfence and link to the [plugin page](#) or [www.wordfence.com](#). Spreading the word helps us keep the best features free.

Scan Summary

[Jun 22 23:02:21] Scanning comments for URL's in Google's Safe Browsing List	Secure.
[Jun 22 23:02:21] Scanning for weak passwords	Secure.
[Jun 22 23:02:21] Scanning DNS for unauthorized changes	Secure.
[Jun 22 23:02:21] Scanning to check available disk space	Secure.
[Jun 22 23:02:21] Scanning for old themes, plugins and core files	Problems found.
[Jun 22 23:02:22] Scanning for admin users not created through WordPress	Secure.
[Jun 22 23:02:22] Scan complete. You have 15 new issues to fix. See below.	Scan Complete.

You are running the Wordfence Community Scan signatures

WordFence – Issue alters

you have fixed all the issues below, you can [click here to mark all new issues as fixed](#). You can also [ignore all new issues](#) which will exclude all issues listed below from future scans.

[Bulk operation»»](#)

SEVERITY	ISSUE
	<p>Your WordPress version is out of date</p> <p>Current WordPress Version: 4.5.2 New WordPress Version: 4.5.3 Severity: Critical Status: New</p> <p>WordPress version 4.5.3 is now available. Please upgrade immediately to get the latest security updates from WordPress. Click here to update now.</p> <p>Resolve: I have fixed this issue Ignore this issue</p>
	<p>The Plugin "Akismet" needs an upgrade.</p> <p>Plugin Name: Akismet Plugin Website: http://akismet.com/ Current Plugin Version: 3.1.10 New Plugin Version: 3.1.11 Severity: Critical</p>

Spam Honey Pot

Add Plugins [Upload Plugin](#)

You have not set an administrator email address to receive alerts for Wordfence. Please [click here to go to the Wordfence Options Page](#) and set an email address where you will receive security alerts from this site.

[Use My Email Address](#) [Dismiss](#)

Search Results Featured Popular Recommended Favorites Keyword (x)

109 items < < 1 of 4 > >

 Spam Honey Pot Adds a hidden text field to the comment form to trap spam bots. <i>By Matthew Turland</i>  (3) 2,000+ Active Installs Last Updated: 1 year ago Untested with your version of WordPress	 PWH Honey Pot This plugin adds an email honey pot address to catch spammers and email harvesters. <i>By InfoBahn</i>  (0) 100+ Active Installs Last Updated: 3 months ago Untested with your version of WordPress
 AVH First Defense Against Spam The AVH First Defense Against Spam plugin gives you the ability to block spammers before any content is served. <i>By Peter van der Does</i>  (14) 10,000+ Active Installs Last Updated: 1 year ago Untested with your version of WordPress	 Spam Oborona YandexCleanWeb The fight against spam in comments by free service Yandex .NET Web <i>By Djon</i>  (2) 0+ Active Installs Last Updated: 2 years ago Untested with your version of WordPress

SpamPot

Add Plugins [Upload Plugin](#)

You have not set an administrator email address to receive alerts for Wordfence. Please [click here to go to the Wordfence Options Page](#) and set an email address where you will receive security alerts from this site.

[Use My Email Address](#) [Dismiss](#)

Search Results Featured Popular Recommended Favorites Keyword ▾ [SpamPot](#)

2 it



SpamPot

Installed

Adds a honeypot form field on the registration and login pages to trap spammers.

By Keith Drakard

5 stars (0)

20+ Active Installs

Last Updated: 2 months ago

✓ Compatible with your version of WordPress

SpamPot On WP Site

The screenshot shows the WordPress admin dashboard with the 'Plugins' menu item selected, indicated by a blue background and the number '12' in a red circle. The main content area displays a list of installed plugins. The 'SpamPot' plugin is visible, showing its description, version (0.32), author (Keith Drakard), and links to activate, edit, or delete it. A mouse cursor is hovering over the 'Delete' link. Below the 'SpamPot' entry, there is a note about a new version available.

Plugin	Description	Version	Author	Action Links
SG CachePress	Through the settings of this plugin you can manage how your Wordpress interacts with NGINX and Memcached.	2.3.4	By SiteGround	View details
SpamPot	There is a new version of SG CachePress available. View version 2.3.8 details or update now .	0.32	By Keith Drakard	Activate Edit Delete
The Events Calendar	The Events Calendar is a carefully crafted, extensible plugin that lets you easily share your events. Beautiful. Solid. Awesome.	4.1.3	By Modern Tribe, Inc.	View details Support View All Add-Ons
Ultimate Hover Effects	Ultimate Hover Effects is simple modern. yet stylish hover effects for image captions. Eve catching image			

WordPress Site Backups

- Its important to make and store site backups during site development
- It's embarrassing to kill your site the day before its due, while **adding that last plugin**, and not having a way to recover a working version.
- WordPress offers many different plugins for site backups and disaster recovery
- Your web host also offers a backup and restore service (usually its an extra cost)

About Plugin Backups

- Backup and restore plugins that run from [within](#) the WordPress admin dashboard are not the best solution
 - If you kill your site and can not login, so what if you have a backup, you can not login to restore the site
 - You will end up deleting the site, re-creating it, installing the backup plugin, and then use the last backup to restore the site. This takes a lot of time and energy

Additional Plugin Backup Issues

- Most free backup plugins only backup to the Web Host server.
- All our Service learning sites are on a shared web host. If you use one of these backup plugins, you will use up our **free** space and **shut us down**.
- If you use a backup plugin, use one like ALL IN ONE MIGRATION, which copies the backup to your desktop computer, not the Web Host server file system.

WordPress Backup Plugins

- **UpdraftPlus Backup and Restoration**
- **WP-DB-Backup**
- **Duplicator**
- **BackUpWordPress**
- **WordPress Backup to Dropbox**
- **All In One Migration**

- Do not use Revisor – communication with GIT shuts our SiteGround down

UpdraftPlus Backup and Restoration

- UpdraftPlus Backup and Restoration is one of the most popular free backup plugins available for WordPress.
 - With more than half a million installs and an extraordinarily favorable 4.9 (out of a possible five) star rating, it should definitely make your shortlist.
- You can use Updraft to back up your files to the cloud via Amazon S3, as well as other popular online file storage solutions including Google Drive, Dropbox, Rackspace Cloud.
 - You can also backup your files to the server of your choice with an FTP transfer. (DO NOT BACKUP TO SITEGROUND, please)
- UpdraftPlus is also offered as a premium version.
 - Premium gives you a gigabyte of backup storage on the
 - Updraft Vault, additional backup options (including Microsoft OneDrive, SCP, WebDAV, and OpenStack Swift), secure FTP, the ability to clone databases, automatic backup when updating WordPress themes, and the ability to send backups to remote destinations.
 - The premium version costs between \$70 and \$145, depending on the number of sites.

WP-DB-Backup

Database only backup, not Files

- Very little is written about WP-DB-Backup on its plugin page. However, its lack of a thorough marketing message apparently hasn't diminished its popularity.
 - The plugin has been downloaded more than half a million times and enjoys a 4.6 star rating.
- WP-DB-Backup, as the name implies, **backs up your database, not your files**. If you want your files backed up as well, you'll need to look for an alternative solution.

Duplicator

- Duplicator is a backup solution that not only backs up your data, but also duplicates your entire WordPress site.
- This is a powerful backup solution. Maybe that's why the plugin has been installed more than half a million times and currently enjoys a 4.9 star rating.
- This plugin gives you the opportunity to migrate, copy, or clone your entire site from one location to another, which is a great solution if you're looking for complete redundancy in the event that you need a failover option if your primary site goes down.
- **Just make sure you do not store the backup file on the SiteGround server.**

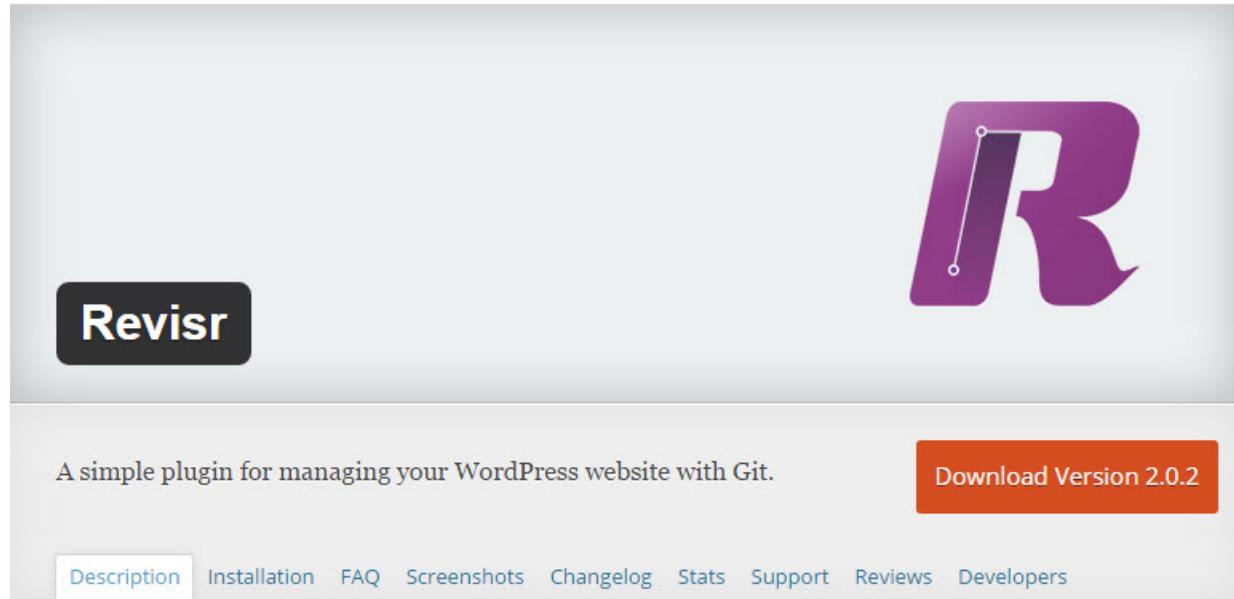
BackUpWordPress

- The appropriately named BackUpWordPress is another excellent option if you're looking for a free WordPress backup system.
 - It's been installed more than 200,000 times, and enjoys a 4.7 (out of a possible 5) star rating.
- This plugin requires PHP version 5.3.2 or later.
 - It's not too likely that your WordPress installation is using an old version of PHP, but you'll want to ensure that your version is compliant with this plugin before you install it.
- BackUpWordPress **will back up your entire site, including your files and your database, at a schedule that suits your needs.**
 - It requires no setup and works on low memory
 - **This is an excellent advantage if you're operating on a shared host environment.**
- The plugin also gives you the option to use zip and mysqldump for faster backups. That can be a significant benefit if time is of the essence.
- The plugin offers numerous extensions for various cloud storage services, such as **Dropbox and Google Drive.**
 - **You can also purchase a bundle option that will enable you to back up your files to multiple locations. This additional option is highly recommended.**

WordPress Backup to Dropbox

- You won't be surprised to learn that WordPress Backup to Dropbox is a backup solution that works with Dropbox. It's also a popular solution with more than 100,000 installations.
- With this backup, you'll obviously need a Dropbox account for your backup. That will cost money if your backup is more than 2Gb. Setup is easy – you just authorize the plugin with Dropbox. Once that's completed, your backups are fully automated.
- This plugin requires PHP version 5.2.16 or higher with cURL support. Check with your host administrators to check you have the required versions installed.
- The tool also claims to have premium options available for people who need additional functionality, and also offers support for multiple languages.
-

DO NOT USE – Revisr for any DePaul Web Hosted WP Sites



A screenshot of the Revisr plugin page on WordPress.org. The page features a large purple 'R' logo with a line through it. A black button on the left says 'Revisr'. Below the logo, a sub-headline reads 'A simple plugin for managing your WordPress website with Git.' To the right is an orange 'Download Version 2.0.2' button. Below the headline are navigation links: Description (highlighted), Installation, FAQ, Screenshots, Changelog, Stats, Support, Reviews, and Developers. The main content area describes the plugin's purpose and lists its features. On the right, there are details like required version (3.9.2 or higher), compatibility up to 4.4.4, last updated 7 months ago, and active installs over 2,000+. Below that is a 'Ratings' section showing a 4.8 out of 5 stars rating with 19 reviews for 5 stars, 1 review for 4 stars, and 0 reviews for 3 stars.

Revisr works with GIT. Using this plugin will shut us down on SiteGround. It uses a tremendous amount of communication between the website and GIT and uses up our bandwidth allocation and SiteGround turns us off.

Do Use – All In One Migration for WP Site Backups (covered in Migration Lecture)

The screenshot shows the WordPress.org Plugin Directory. At the top, there's a navigation bar with links to Showcase, Themes, Plugins, Mobile, Support, Get Involved, About, Blog, and Hosting, along with a "Download WordPress" button. Below the navigation is a search bar and a login form. The main area is titled "Plugin Directory" and features a sidebar with links to Featured, Popular, Favorites, Beta Testing, Developers, and a search bar for "Search Plugins". Under "Popular Tags", there are links for "widget (5,926)", "Post (3,671)", "plugin (3,617)", "admin (3,136)", "posts (2,807)", "shortcode (2,399)", "sidebar (2,226)", "google (2,104)", and "twitter (2,052)". The main content area displays the "All-in-One WP Migration" plugin. It has a large banner with the text "The Complete Wordpress Migration" and "Focus on creating engaging websites. We take care of moving your website to any server." Below the banner, a large button says "All-in-One WP Migration". A description below the button states: "All-in-One WP Migration is the only tool that you will ever need to migrate a WordPress site." To the right of this text is a "Download Version 5.43" button. Below the download button is a row of tabs: Description (which is active), Installation, Screenshots, Changelog, Stats, Support, Reviews, and Developers. The "Description" tab contains text about the plugin's functionality, mentioning it allows exporting databases, media files, plugins, and themes, and applying find/replace operations. To the right of this text are several compatibility details: Requires: 3.3 or higher, Compatible up to: 4.5.3, Last Updated: 1 week ago, and Active Installs: 200,000+. At the bottom of the plugin page, there's a "Ratings" section.