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

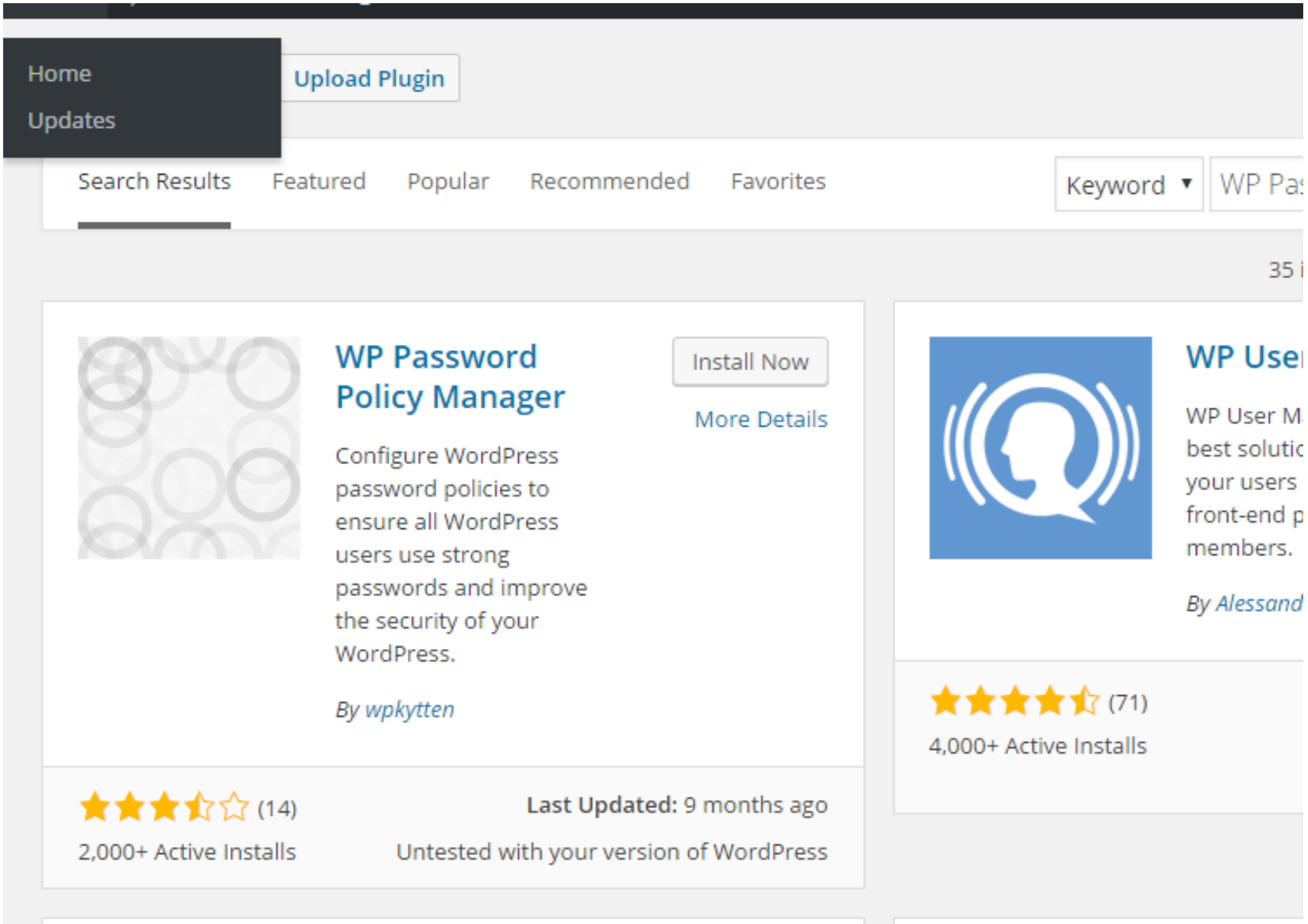
“Weak passwords have always made WordPress blogs and websites an easy target for hackers and users will always use easy passwords unless there are policies which they have to adhere to.”

Robert Abela 2014

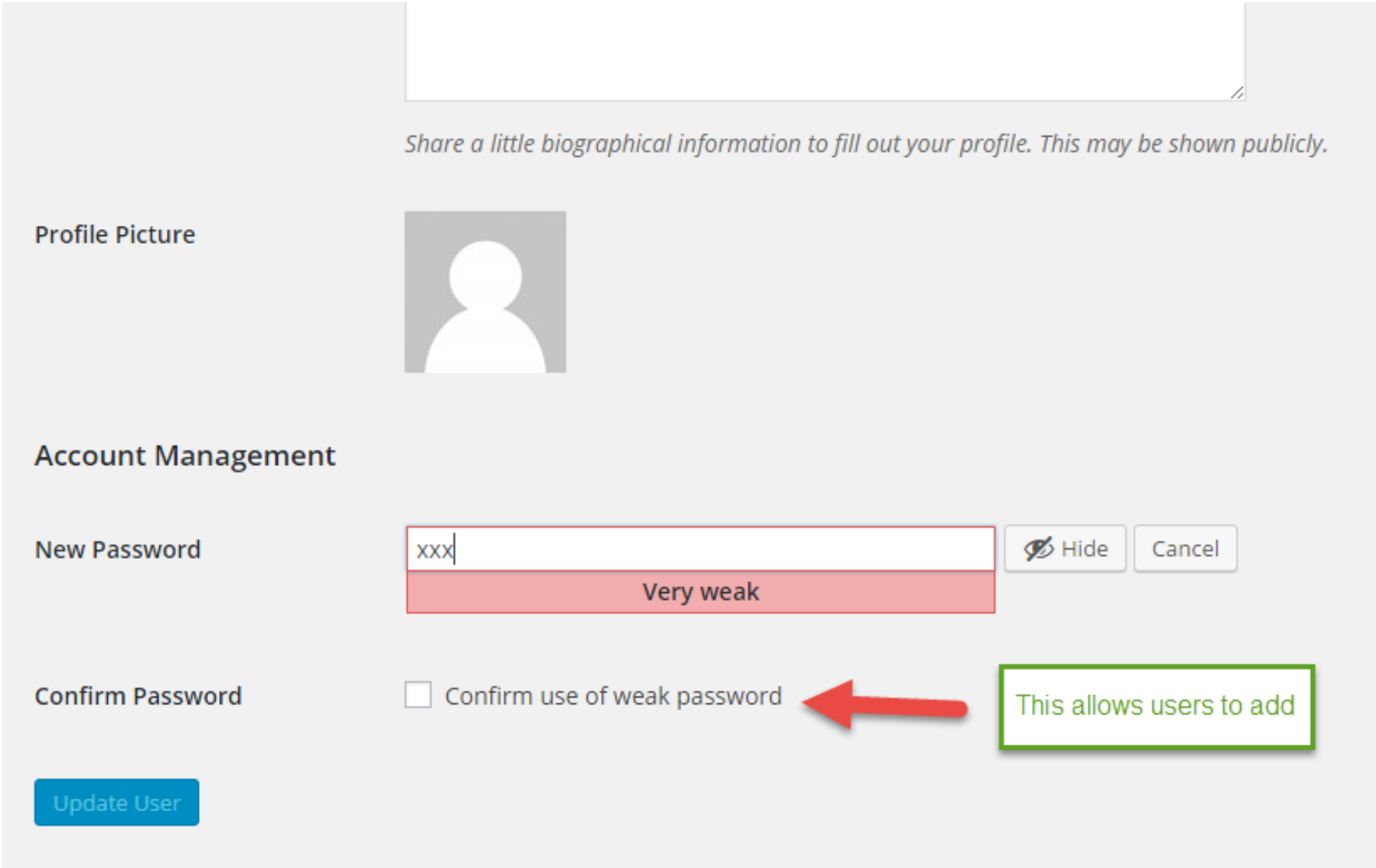
WordPress Allows Weak Passwords

- By default WordPress does not have any built in tools that allow you to enforce passwords 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 uses strong WordPress passwords is by configuring password policies with WP Password Policy Manager which all users have to adhere to.

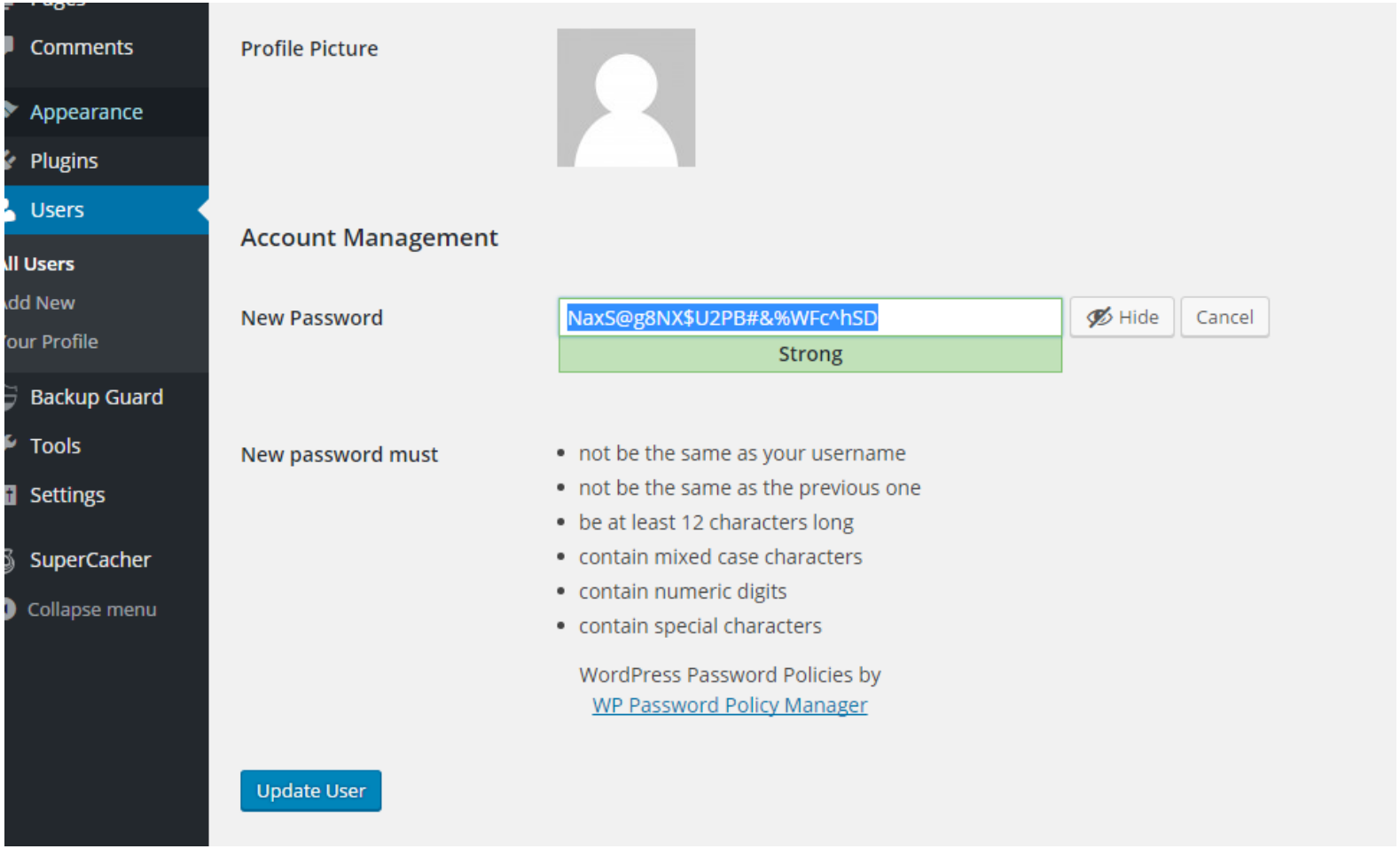
WP Password Policy Manager

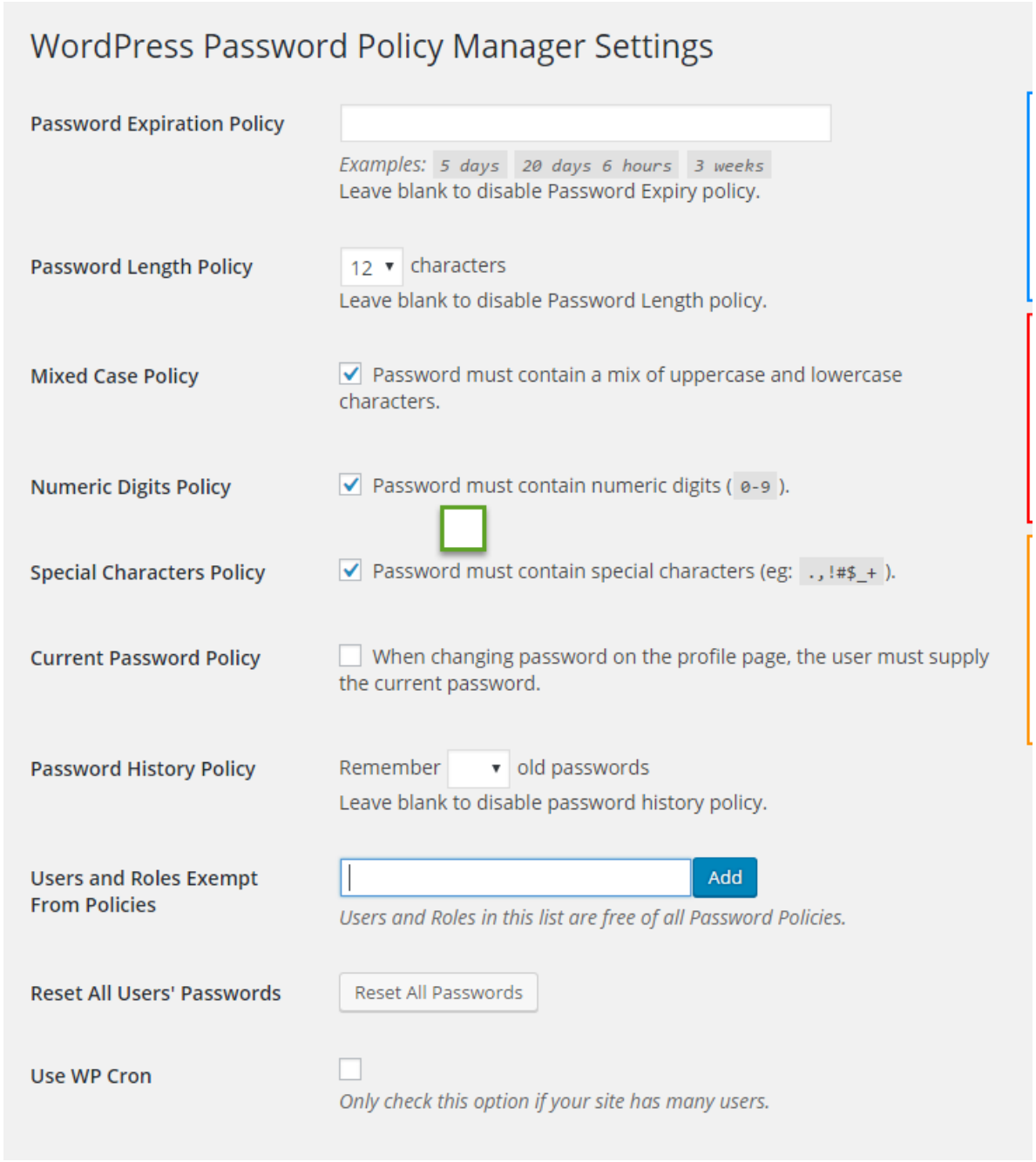


Default WordPress Allows Weak Passwords



WordPress with WP Password Policy Manager Prevents Passwords

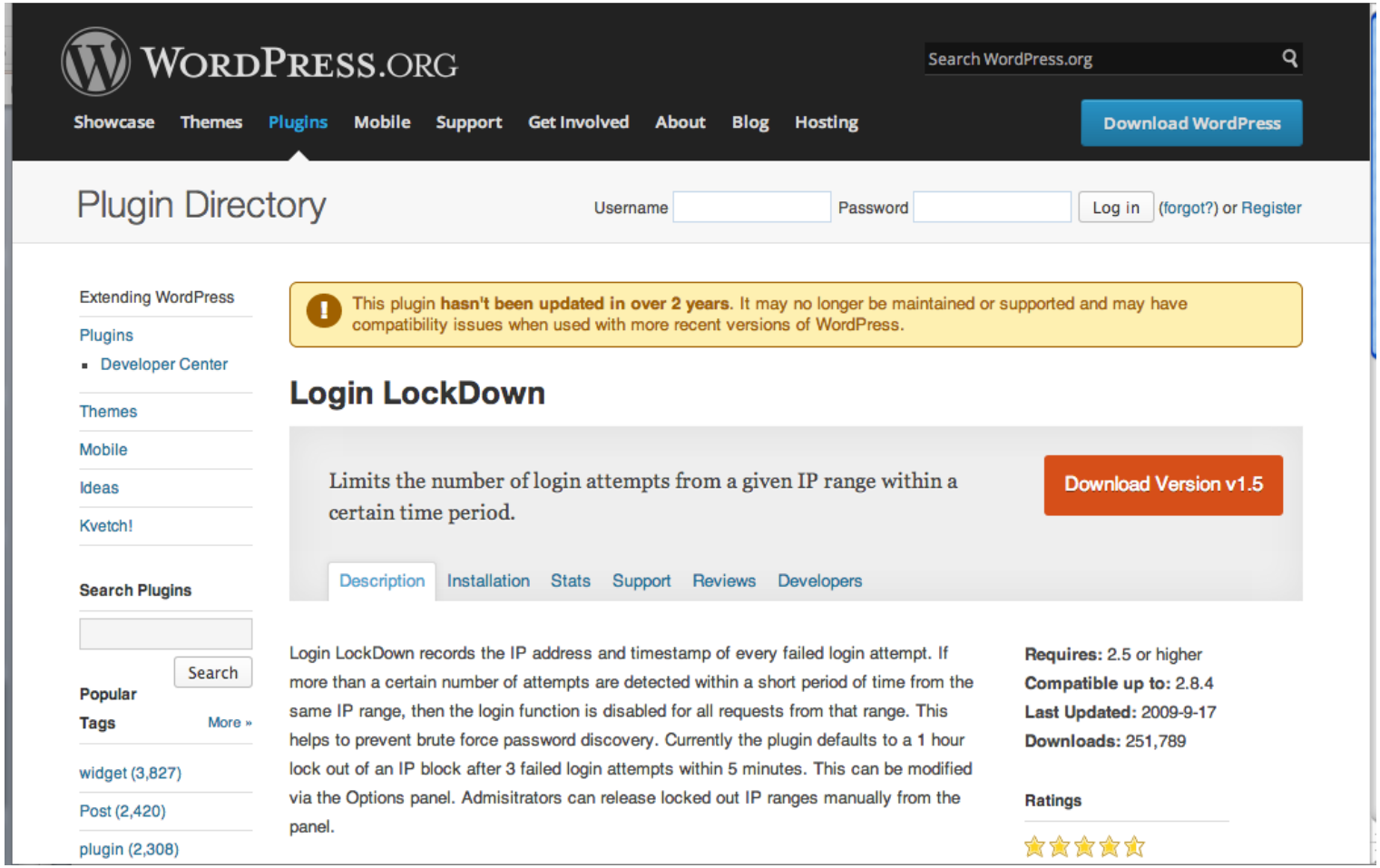



WordPress Password Policy Manager Settings
Password Expiration Policy
Examples: 5 days 20 days 6 hours 3 weeks
Leave blank to disable Password Expiry policy.
Password Length Policy
12 characters
Leave blank to disable Password Length policy.
Mixed Case Policy
Password must contain a mix of uppercase 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



WP Security Plugins

- Better WP Security
- BullitProof 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

BulletProof Security

Login Security Solution

Stealth Login Page

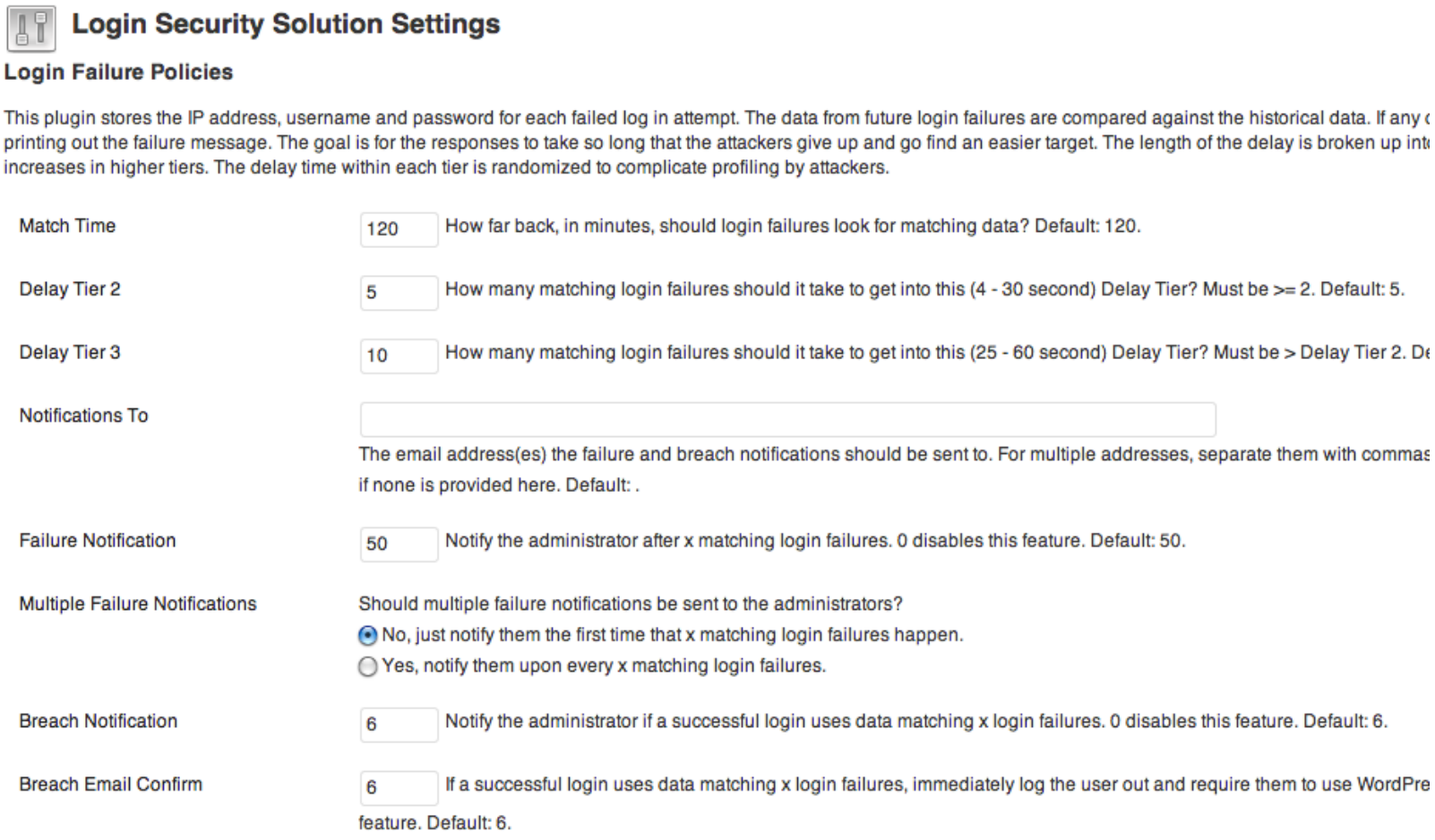
Review 3 Security Plugins

- 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

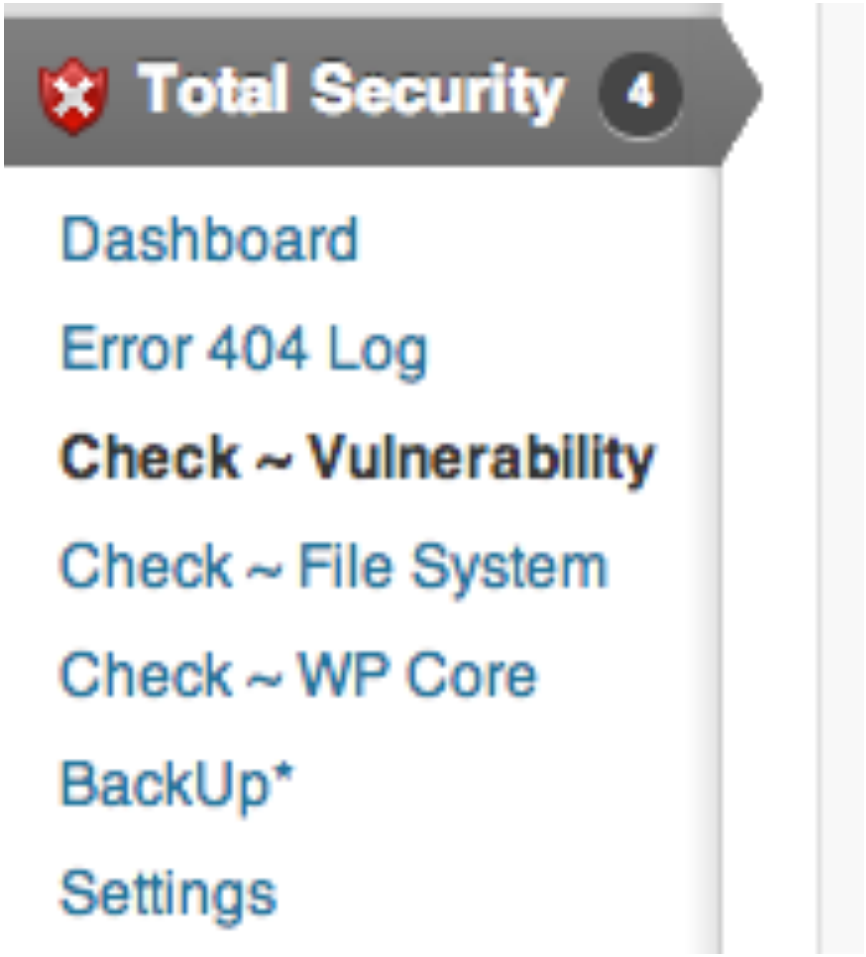
This plugin stores the IP address, username and password for each failed log in attempt. The data from future login failures are compared against the historical data. If any c
printing out the failure message. The goal is for the responses to take so long that the attackers give up and go find an easier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

Match Time	120	How far back, in minutes, should login failures look for matching data? Default: 120.
Delay Tier 2	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	10	How many matching login failures should it take to get into this (25 - 60 second) Delay Tier? Must be > Delay Tier 2. De
Notifications To		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	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? (•) No, just notify them the first time that x matching login failures happen. ( ) Yes, notify them upon every x matching login failures.
Breach Notification	6	Notify the administrator if a successful login uses data matching x login failures. 0 disables this feature. Default: 6.
Breach Email Confirm	6	If a successful login uses data matching x login failures, immediately log the user out and require them to use WordPre feature. Default: 6.

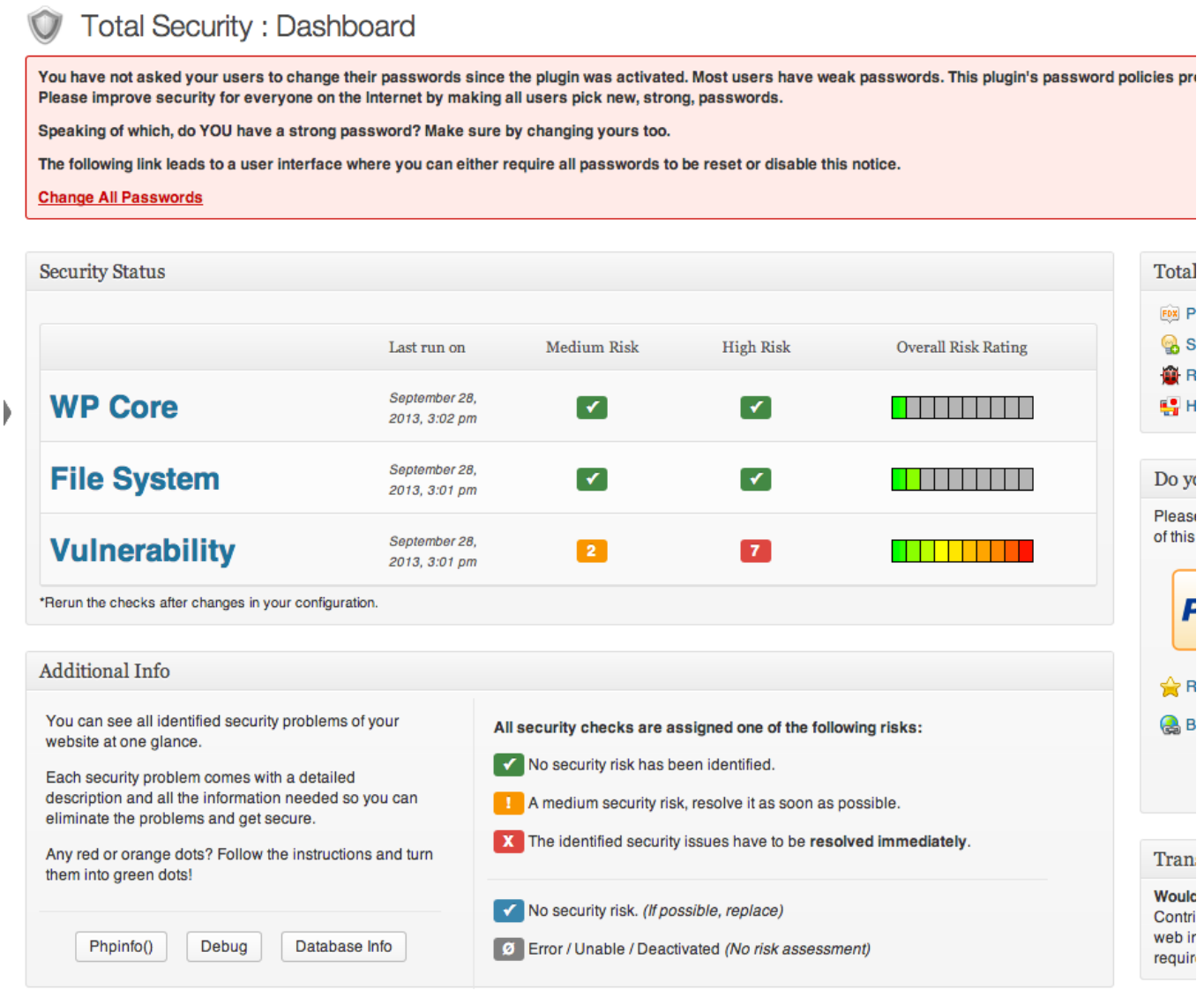
Total Security

- 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.

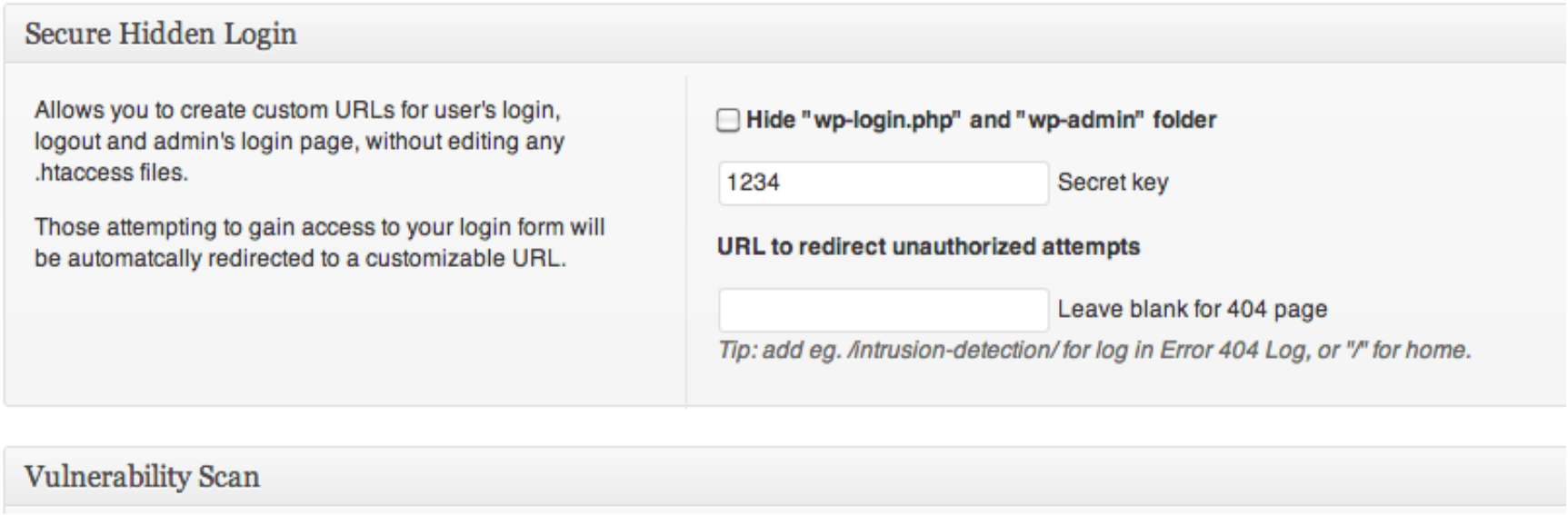
Good Visibility - Left Sidebar Toolbar



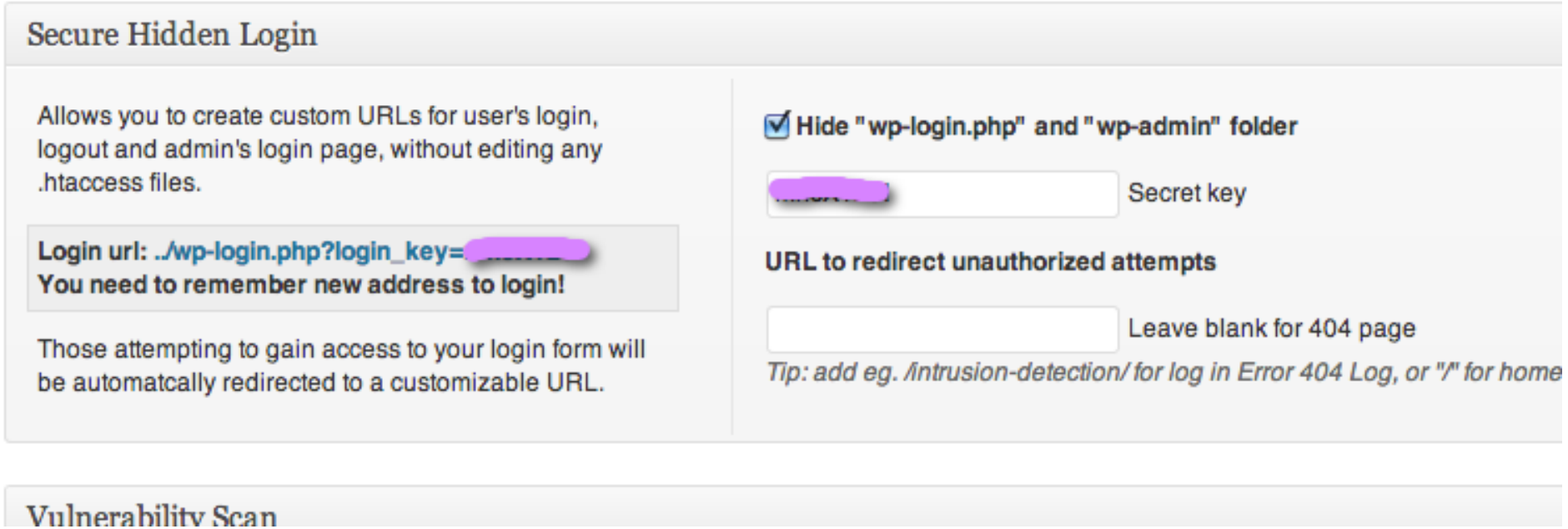
Dashboard


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 pr
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
2
7
*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)

Hide wp-login.php & wp-admin folder



Securing Hidden Login



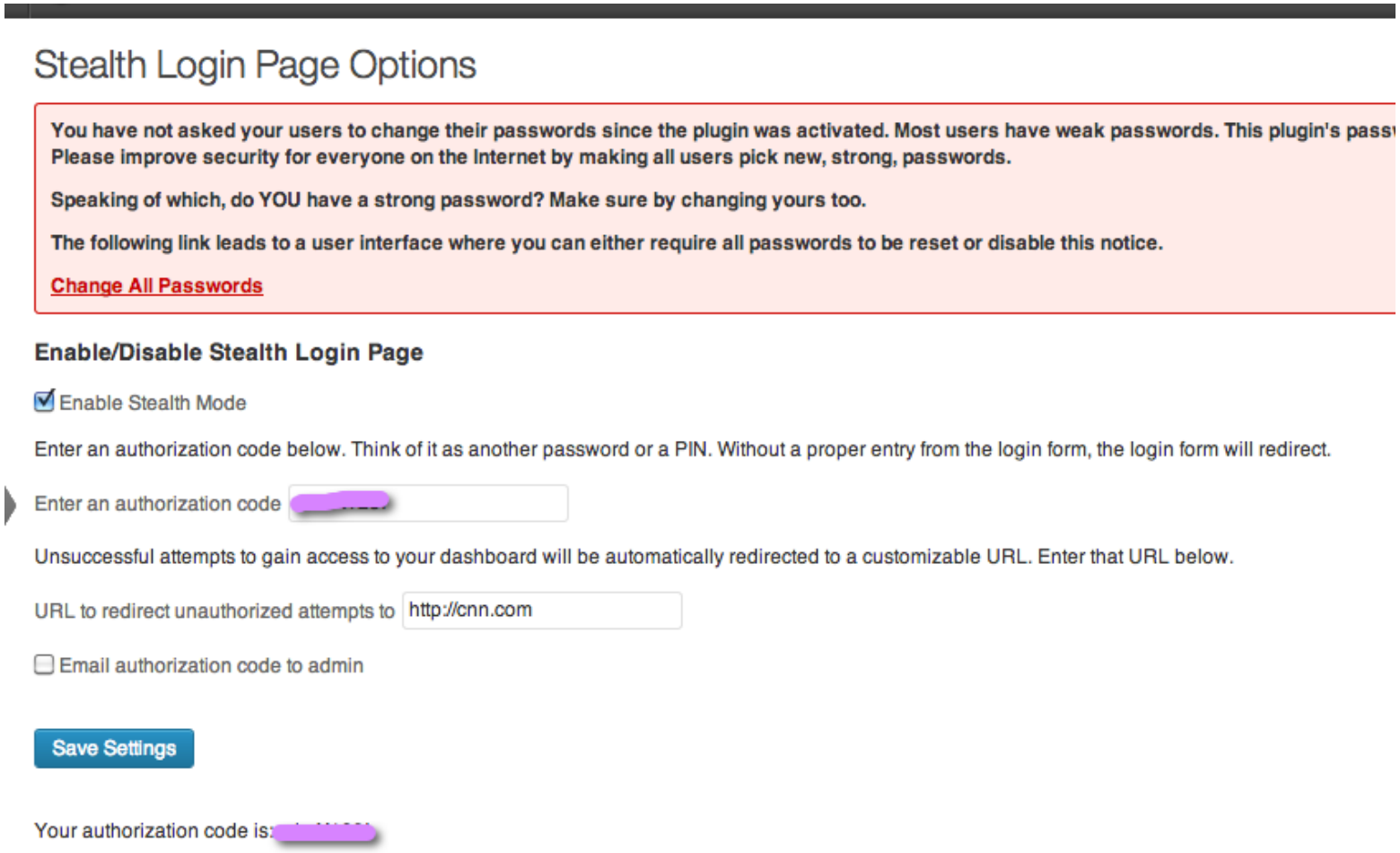
Total Security Vulnerability Check Details

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

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 Adds an extra Authorization code to the login process

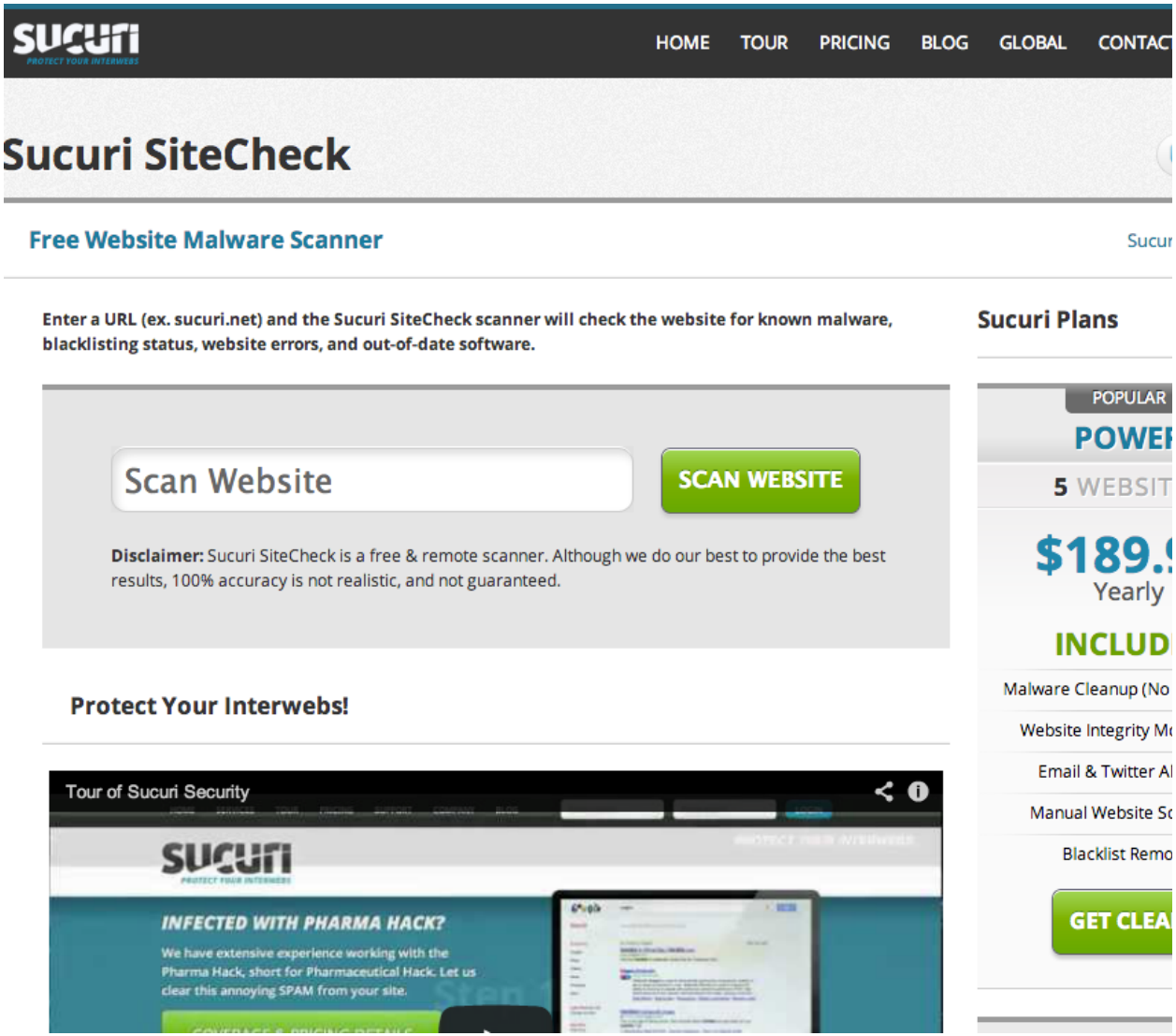
Site Checking Software

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

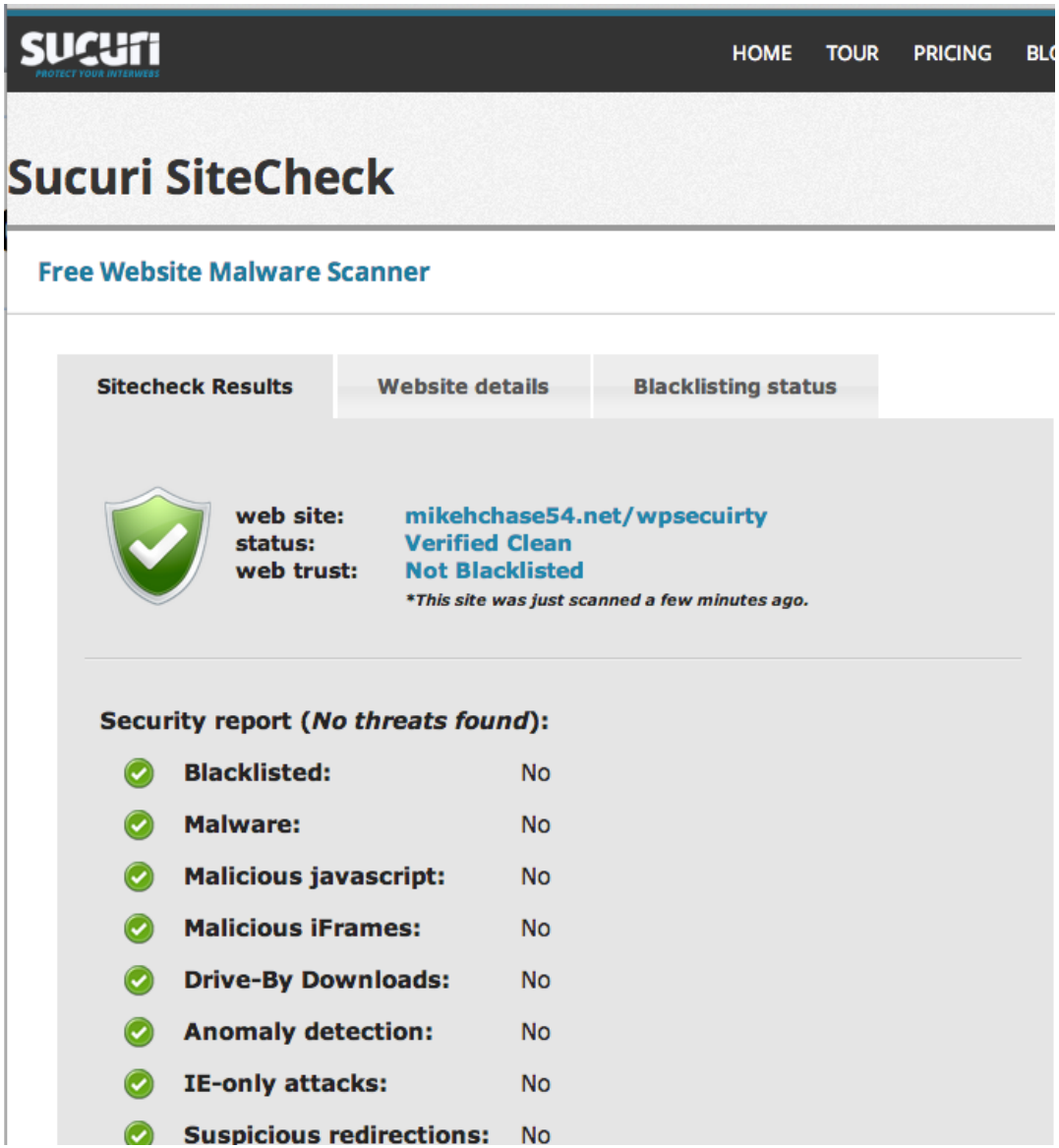
http://Sucuri.net

Sucuri SiteCheck – Not bad!



Lets Run A Site Scan

Scan Results



Scan Result Details

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

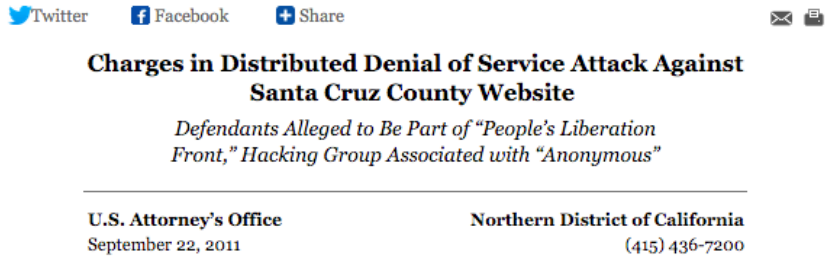
**This site was just scanned a few minutes ago.*

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 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 — **Northern District of California**
September 22, 2011 — (415) 436-7200

IP Address Blocking

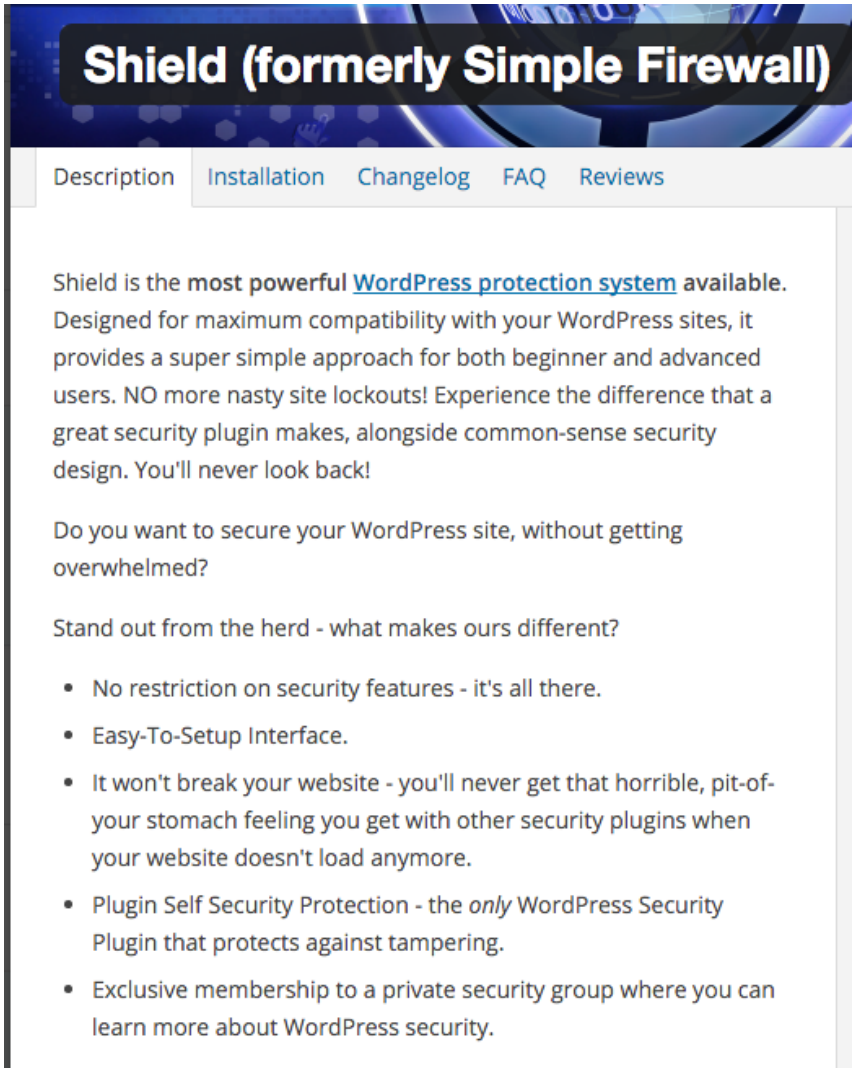
- IP address blocking prevents connection between a server or website and certain IP addresses or ranges of addresses.
- IP address blocking effectively bans undesired connections from hosts using affected addresses to a website, mail server, or other Internet server.
- IP address blocking is commonly 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!



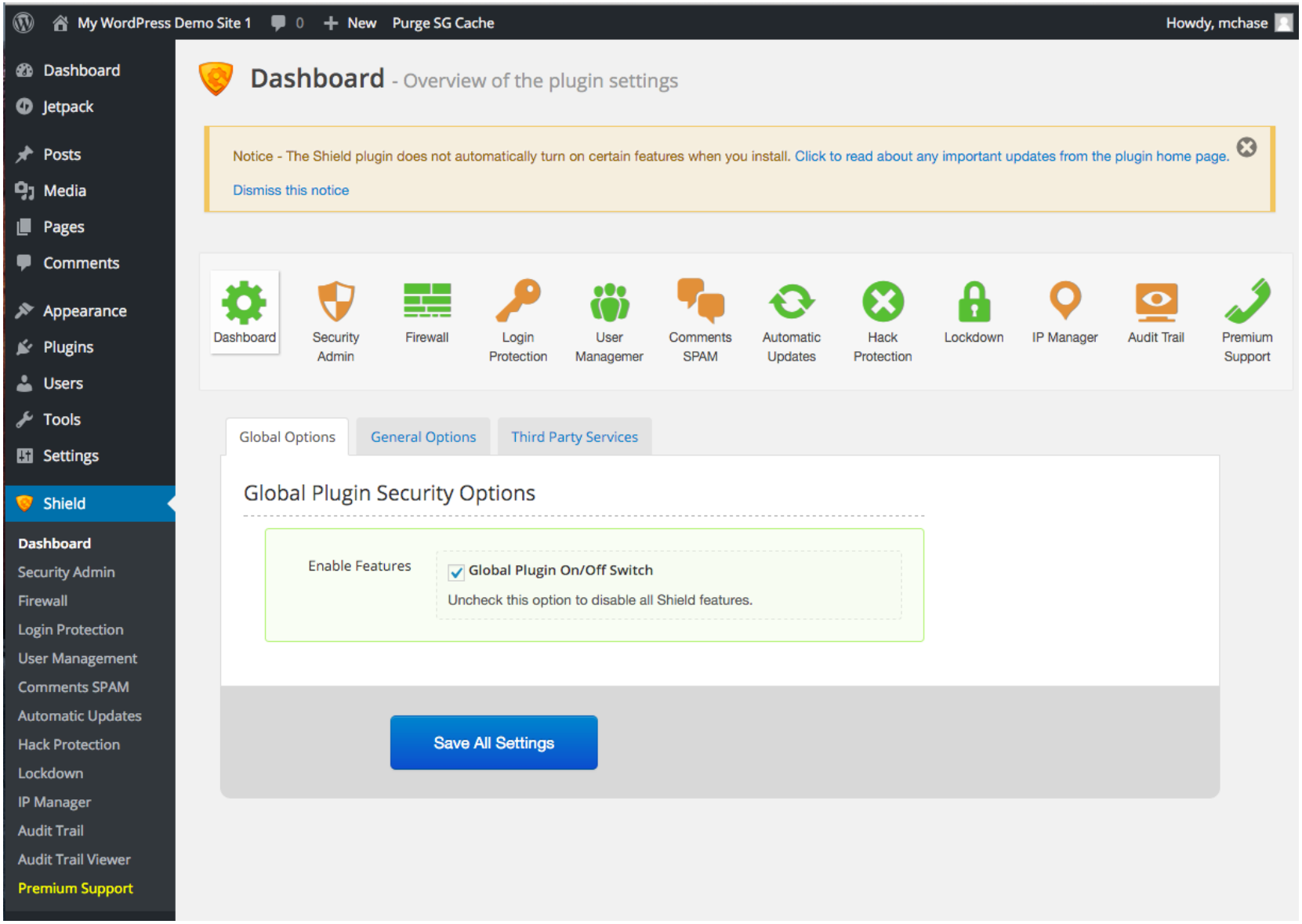
Awesome Features

- 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 sharin, 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



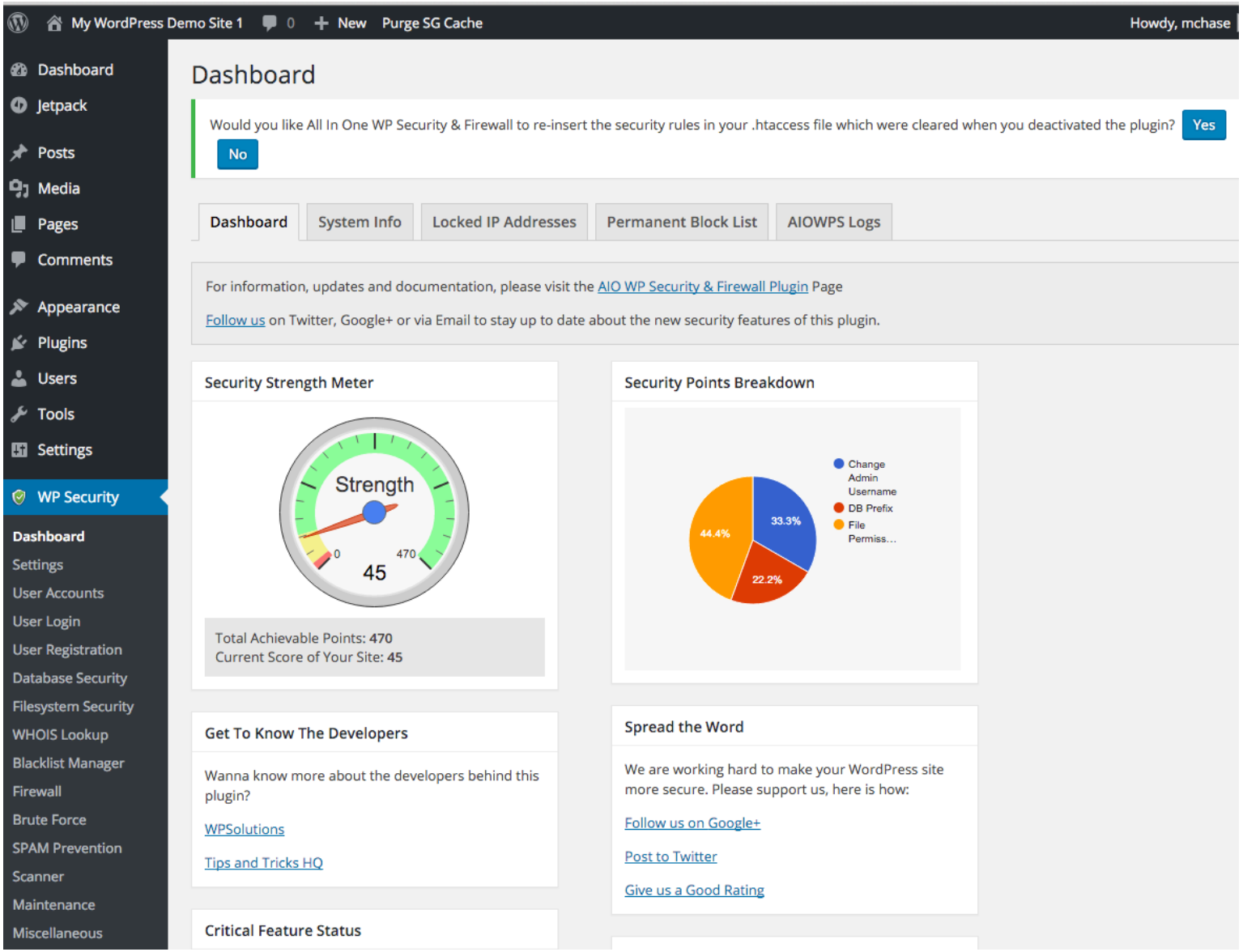
All-in-one WP Security Plugin

- 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.**

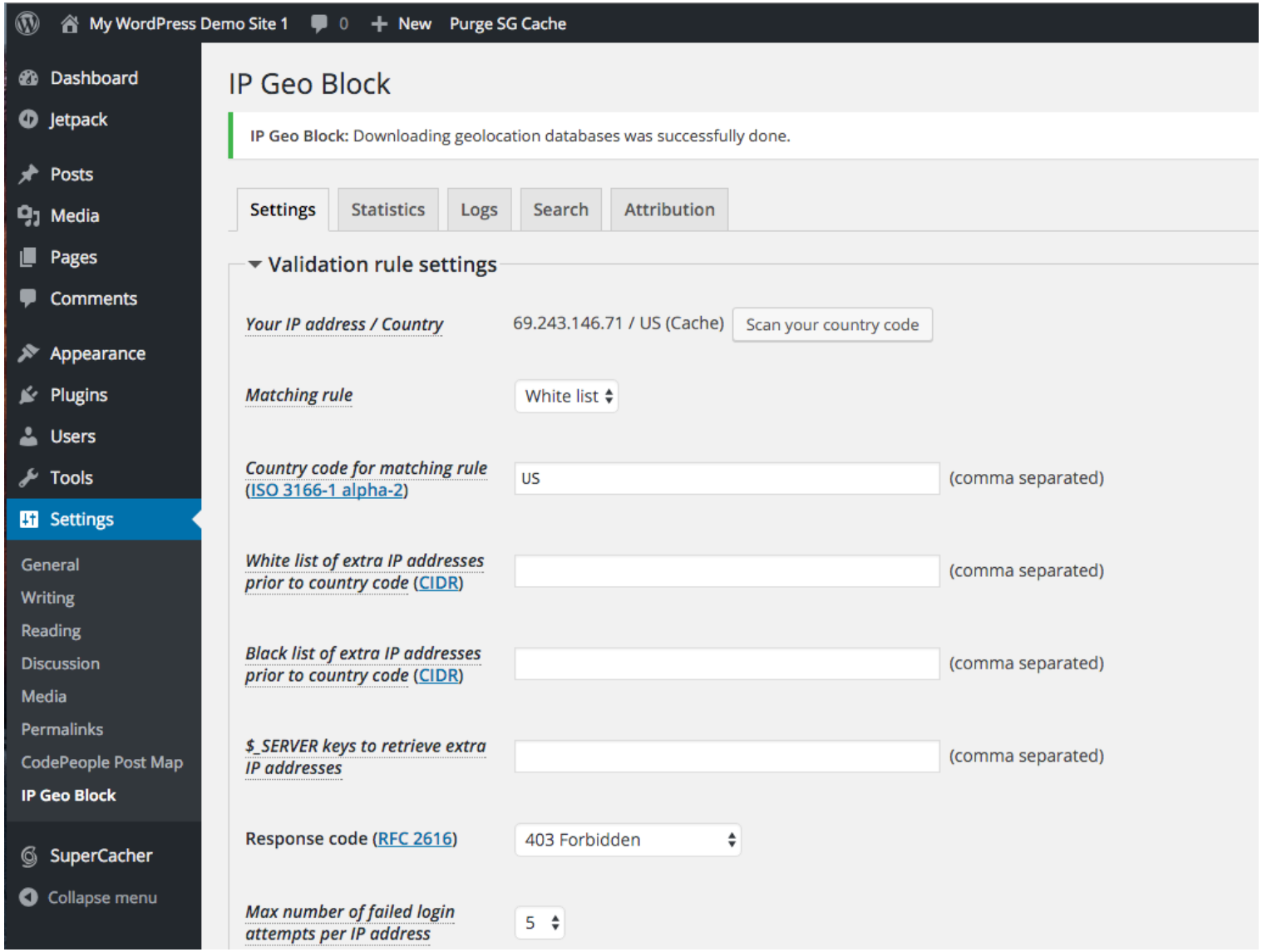
All-in-one WP Security Dashboard



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



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:

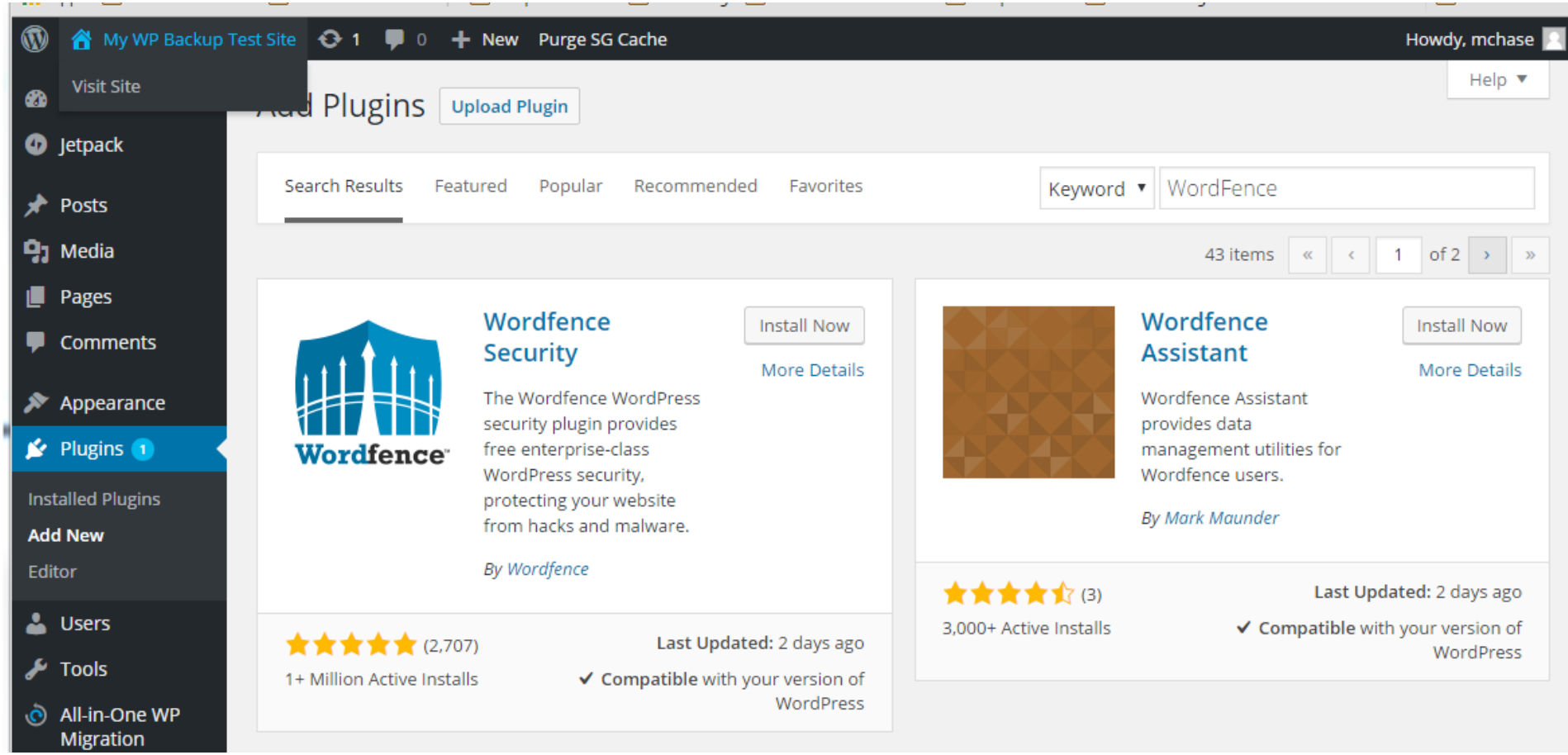
- **Code** — ISO 3166-1 alpha-2 code
- **Country name** — English short country name officially used by the ISO 3166 Maintenance Agency (ISO 3166/MA)[15]
- **Year** — Year when alpha-2 code was first officially assigned (1974, first edition of ISO 3166)
- **ccTLD** — Corresponding country code top-level 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: *Antarctique*
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



Wordfence – Free version is limited

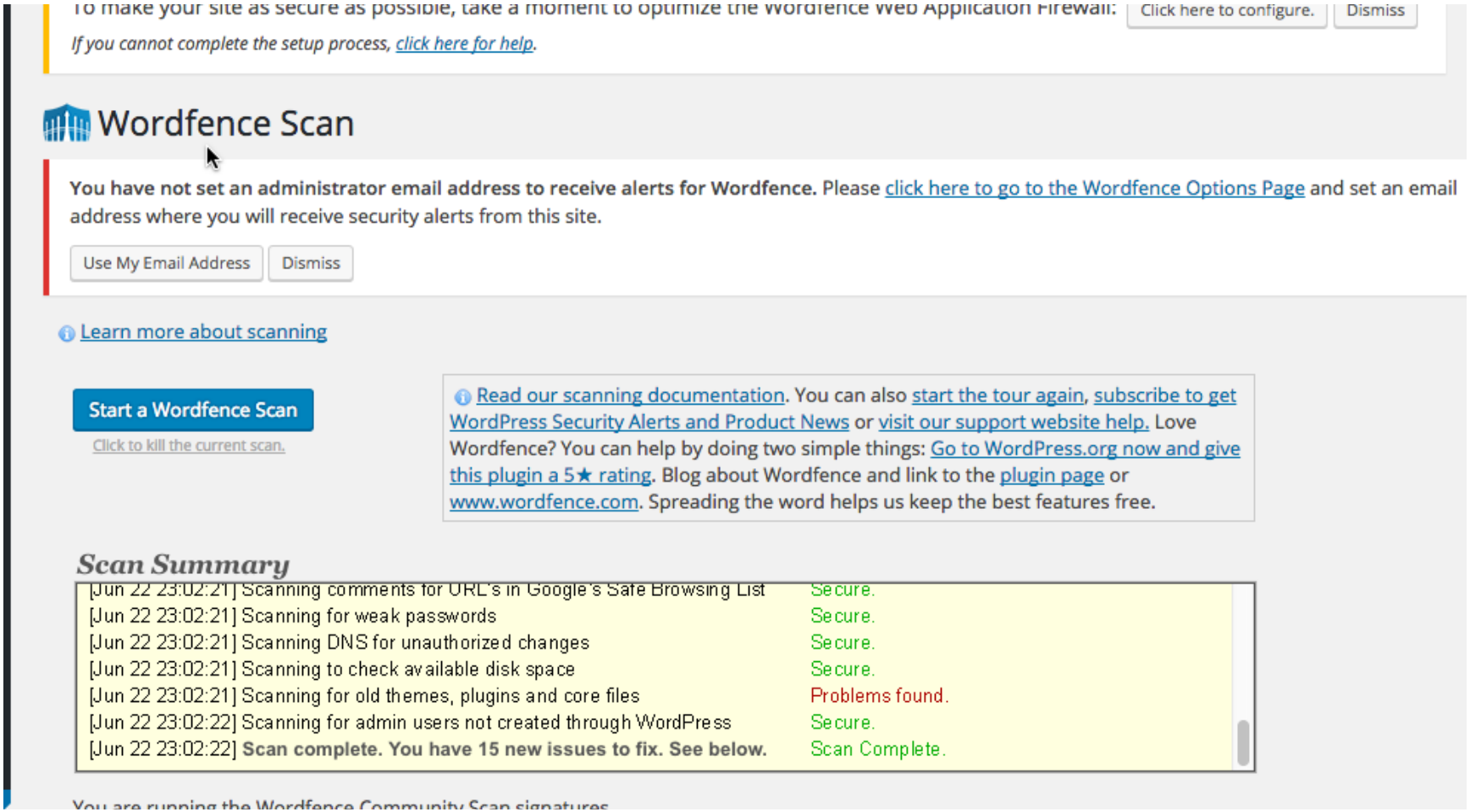
- Its worth installing just for the security scan
- Its complicated to learn and use
- Be patient and take your time and always install the additional assistant plugin – so you can get in if and when you lock yourself out of the site

Wordfence Assistant

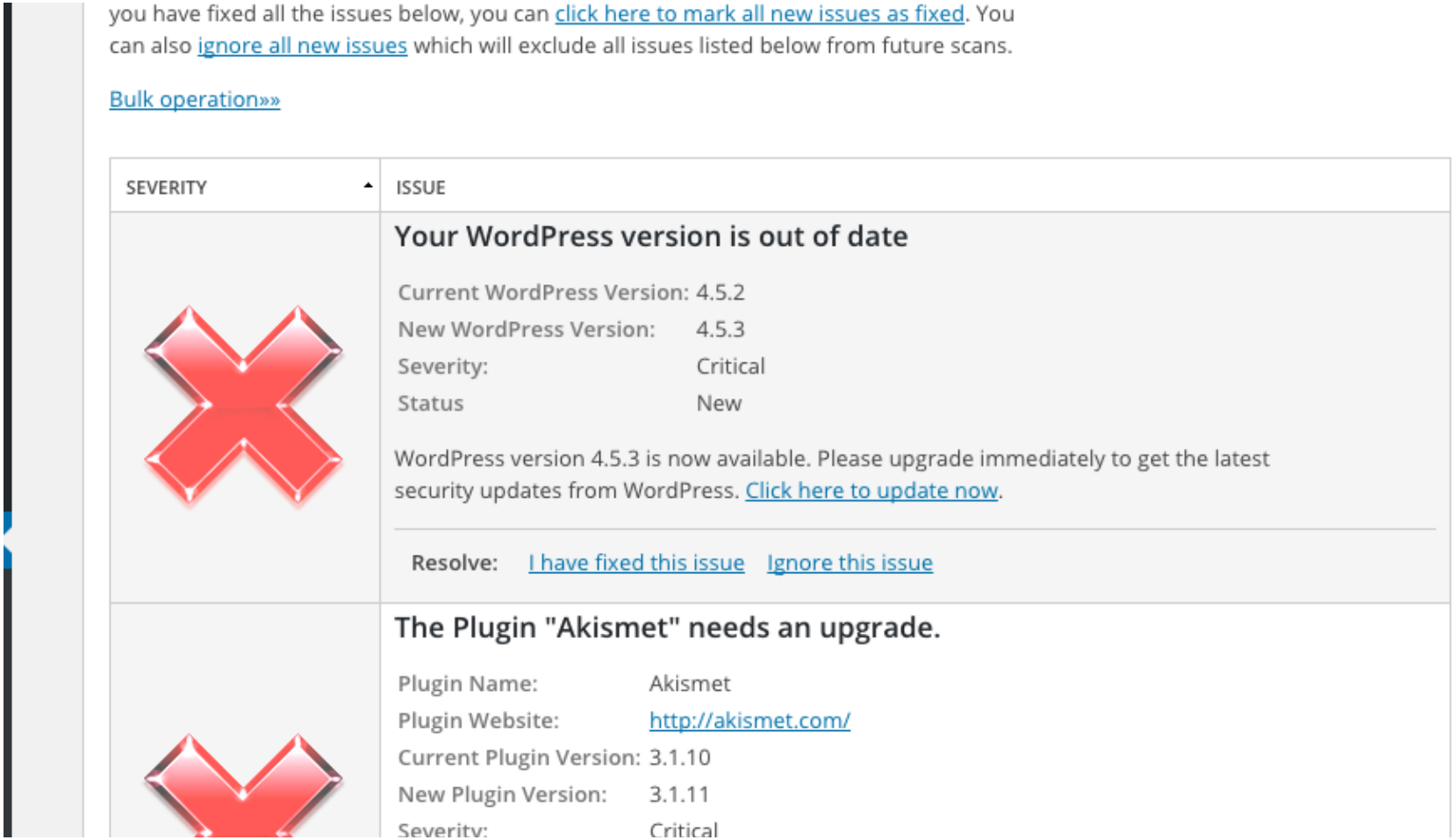
Why does this additional plugin exist?

- 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.

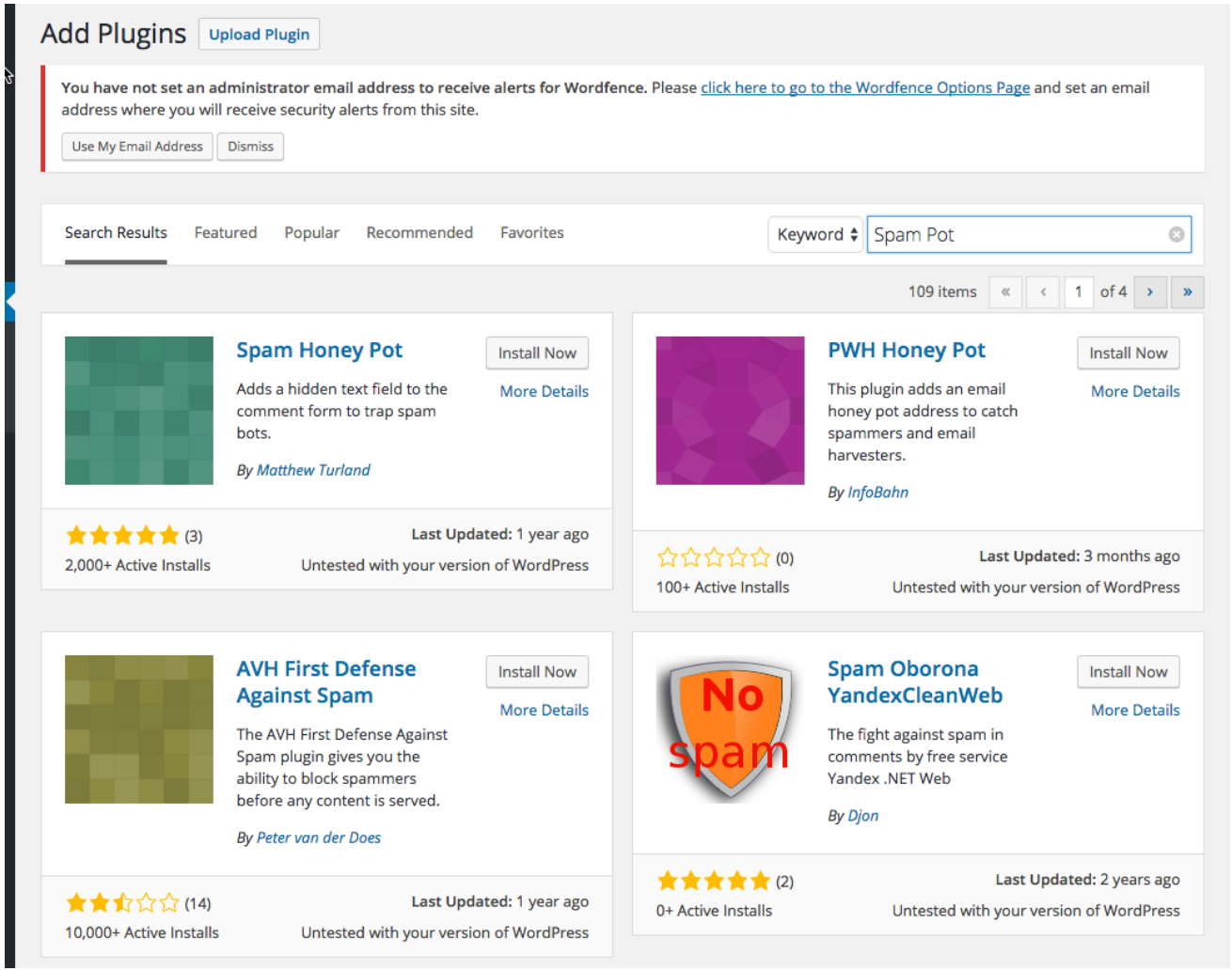
WordFence Scan



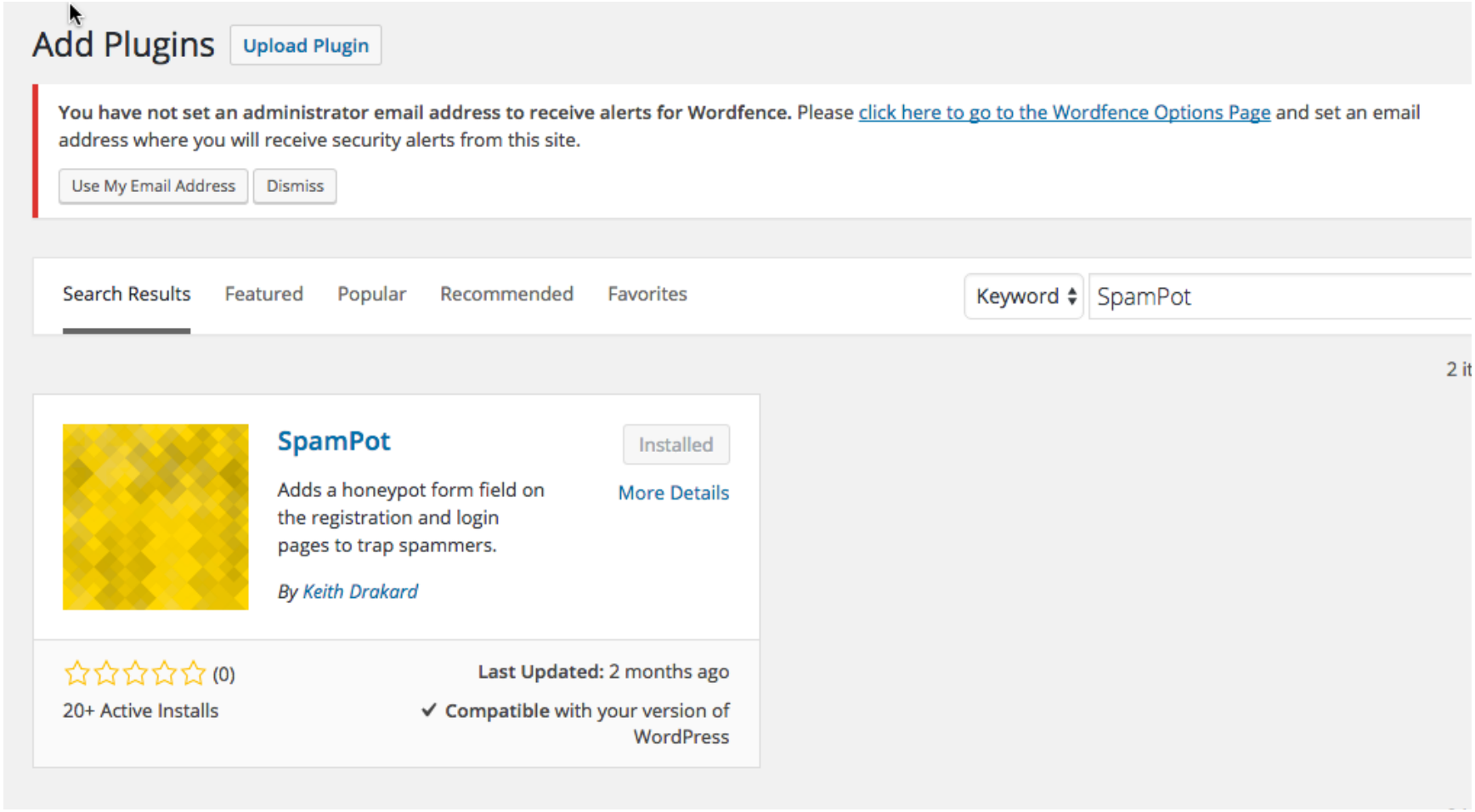
WordFence – Issue alters



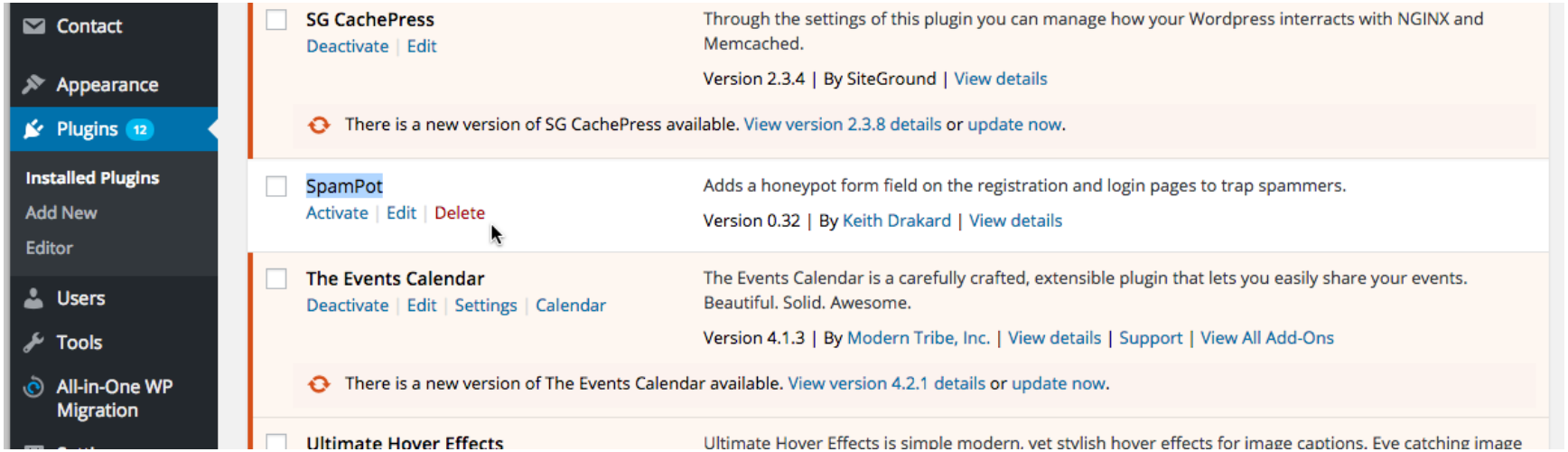
Spam Honey Pot



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
More Details
Adds a honeypot form field on the registration and login pages to trap spammers.
By Keith Drakard
(0)
20+ Active Installs
Last Updated: 2 months ago
Compatible with your version of WordPress

SpamPot On WP Site



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.**

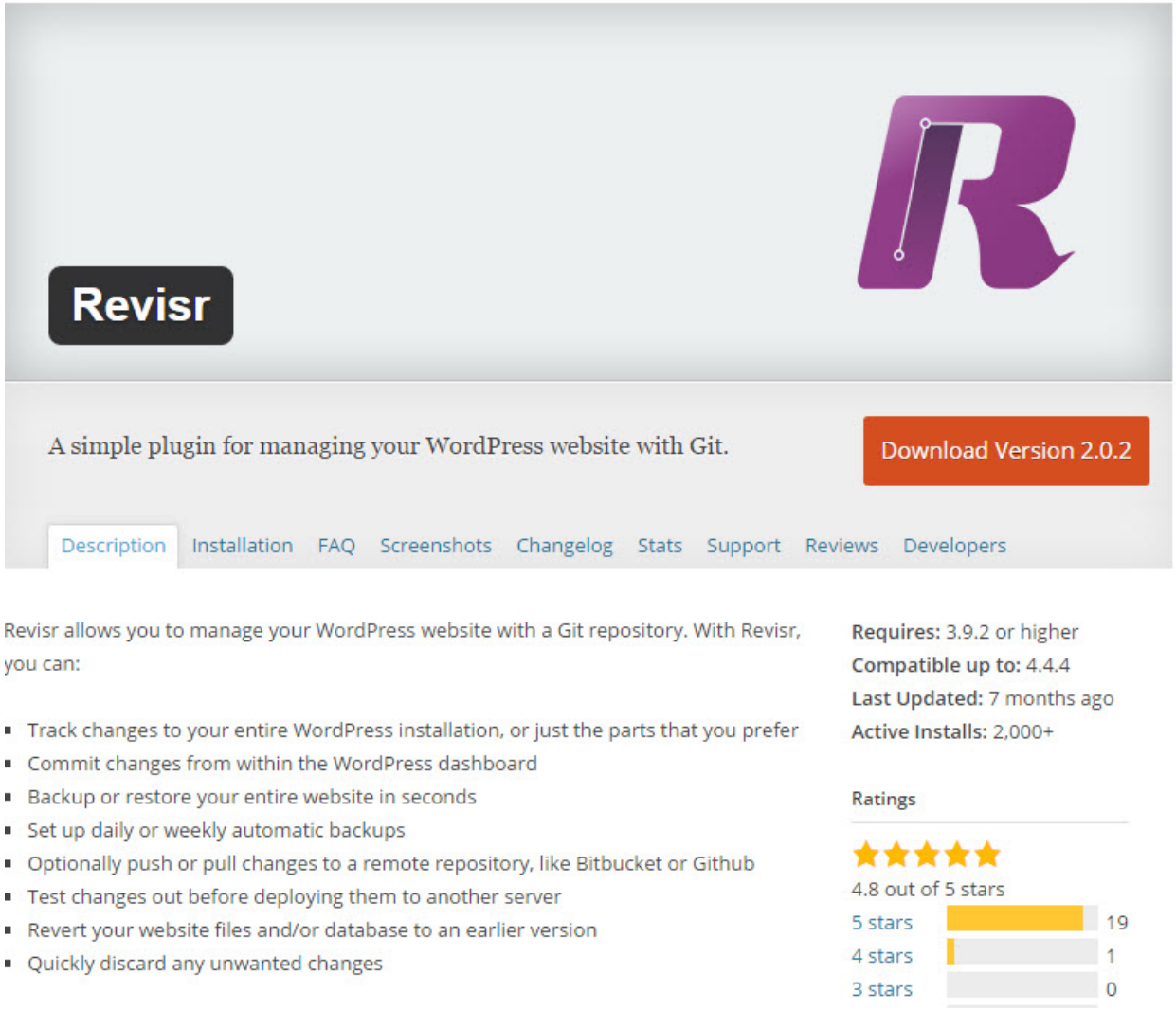
BackUpWordPress

- 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 – Revisor for any DePaul Web Hosted WP Sites



Revisor 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)