The Ultimate WordPress Security Checklist

A must follow security checklist for WordPress users!

Stevie. DIGITAL

Plug & Play Magento Protection against Bots, Malware & Threats

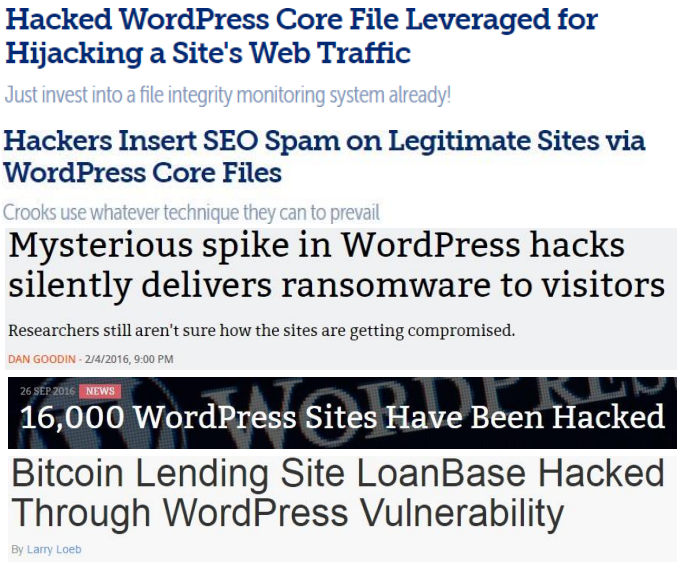
www.stevie.digital/website-security

Ultimate WordPress Checklist

WordPress is the Most Attacked CMS!

WordPress is used by 35% of the web! It's easy to use, open-source and has more than 54,000 extensions making it the choice of bloggers, small business and even news agencies like CNN. However, all these factors attract community of hackers too. In the past WordPress has seen its share of vulnerabilities ranging from SQL injection to Cross Site Scripting attacks. This creates a need to strengthen your WordPress and have a real-time firewall protecting it 24x7.

You don't want to be one of them!



We recover hacked WordPress websites on daily basis. One thing we have realised is that ~75% website owners haven't taken of even the most basic WordPress security practices. A website not having even basic security checks attracts more hackers and makes their work easy. This led us to compile a high level security checklist which assures basic checks and balances are in place. In addition, Stevie's always there to protect your website in real time against bots, hackers, malware and other threats!

Presenting a must-follow checklist for WordPress owners:

Ultimate WordPress Checklist

WordPress Security Checklist

Server side

- ☐ Disable FTP, use SFTP
- ☐ Do not save SFTP passwords, malware harvests them
- ☐ Keep /boot as read-only (reduces the risk of unauthorized modification of critical boot files)
- ☐ Monitor User Activities psacct or acct
- ☐ Install Fail2ban (protects computer servers from brute-force attacks & give option to block IP)
- ☐ From php.ini file, disable show_source, popen, shell_exec, proc_open functions, phpinfo, passthru
- ☐ Lockdown Cronjobs
- ☐ Disable directory indexing by adding Options –Indexes in .htaccess file
- ☐ Adaptive filtering recommendations for NGINX and Apache
- ☐ Remove KDE/GNOME Desktops
- ☐ Check Listening Network Ports
- ☐ Delete */readme.html* file
- ☐ Enable Iptables (Firewall)

Database

- ☐ Change Database prefix to something other than wp_
- ☐ Schedule periodic backup for database (Updraft, WP DB Backup etc.)
- ☐ Use a strong password containing uppercase, lowercase, numbers, and special characters for the database user (password generator)

Ultimate WordPress Checklist

Login Page

- ☐ Change login url
- ☐ Implement limit login attempts
- ☐ Enable Two-factor Authentication (2FA)
- ☐ Use an email address instead of username
- ☐ Create a strong password
- ☐ Change your WordPress credentials regularly
- ☐ Change Generic error message for an incorrect username or password
- ☐ Administrative Panel
- ☐ Use latest version of the theme
- ☐ Delete the unused themes
- ☐ Download and use themes only from trustworthy sources. Avoid using null themes
- ☐ Remove the WordPress version from the theme. You can use our WP Hardening Plugin to fix common security issues.
- ☐ Disable Ctrl+Alt+Delete in Inittab
- ☐ Disabling the REST API on WordPress

Use Free WP Hardening plugin to fix 14+ security issues with a click.

Ultimate WordPress Checklist

WordPress Files

- ☐ Use recommended file & folder permissions
- ☐ Assign No-Owner Files to appropriate users
- ☐ Move wp-config.php out of the root folder as it contains sensitive information
- ☐ Use Wp-intel Chrome extension for basic security audit

Use a WordPress security plugin that offers

- ☐ Malware scanning & removal
- ☐ Firewall that stops XSS, SQLi, Bad bots & 100+ WordPress attacks & updates it rules set regularly
- ☐ Brute-force login protection
- ☐ Rate based throttling and blocking
- ☐ Two-factor authentication
- ☐ Password auditing
- ☐ Country/IP blocking
- ☐ Basis security audit

Secure your store now with rock solid Stevie Security Suite