



Securing Your WordPress Website

Jim Grant, Owner Simply Creative Media
@Jim_Grant - jim@simplycreativemedia.com

Why?

Confidentiality
Integrity
Availability



Why?

Why does a hacker bother with me?

ALL Websites are attacked - \$\$\$\$\$

- Traffic/Pharma/Affiliate
- Blackhat SEO - Link Injection
- Hacktivism - Defacements
- Drive-by Downloads
- Malicious Redirects
- Hidden Pages
- Email Spam



Where Are The Weaknesses?

Leaked Passwords

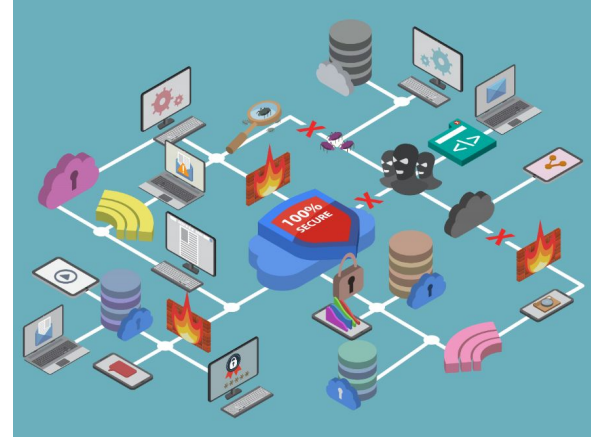
Software Vulnerabilities

Hosting



Where Are The Weaknesses?

- Leaked Passwords
 - Public Wifi
 - Social Engineering
 - Sending them in the clear
- Software Vulnerabilities
 - Plugins - even the inactive
 - Themes - yes, even the inactive
 - WordPress Core
- Hosting



Where Are The Weaknesses?

SSL

- Who works from a coffee shop?
- Get a certificate
 - LetsEncrypt - <https://letsencrypt.org/>
 - From your hosting provider
 - SSLs.com
- Enforce HTTPS in WordPress wp-config.php
 - `define('FORCE_SSL_ADMIN', true);`
- Use a VPN
- Also avoid shared or public computers



Where Are The Weaknesses?

Use Secure Passwords!

- Don't email or text passwords and userids - or other unsecure messaging apps
- At least 12 characters long - length is important....
- Different passwords everywhere
 - Get a password manager

Also - Limit WordPress admins, give only necessary permissions for the time needed

Don't use the userid "admin"

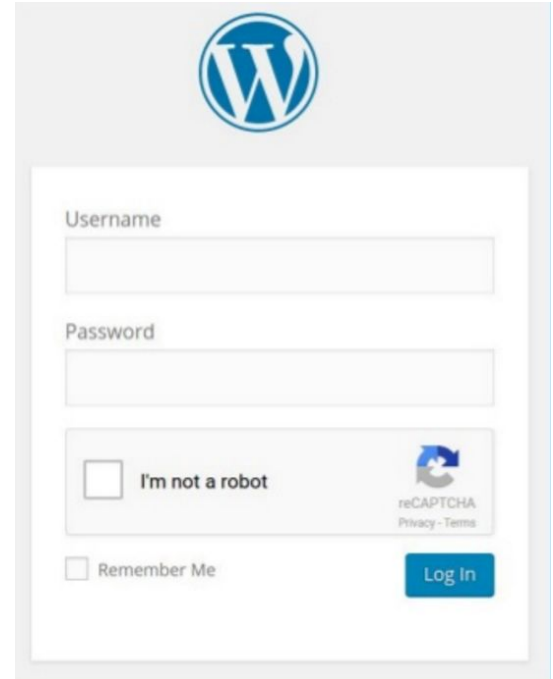
Where Are The Weaknesses?

Use Captcha

WP Login reCAPTCHA

Login No Captcha reCAPTCHA

<https://www.google.com/recaptcha>



The image shows a screenshot of a WordPress login page. At the top center is the WordPress logo (a blue 'W' in a circle). Below the logo are two input fields: 'Username' and 'Password'. Underneath the password field is a reCAPTCHA widget with the text 'I'm not a robot' and a checkbox. To the right of the checkbox is the reCAPTCHA logo and the text 'reCAPTCHA Privacy - Terms'. At the bottom left of the form is a 'Remember Me' checkbox, and at the bottom right is a blue 'Log In' button.

Where Are The Weaknesses?

Software Vulnerabilities

- UPDATE, UPDATE, UPDATE
- Don't use pirated software or suspicious "free" themes
- Limit your exposure by reducing plugins
 - Not all plugins are written by security experts....
- Remove all inactive plugins and themes
- `define('DISALLOW_FILE_EDIT', true);` `wp-config.php`
- Move `/wp-config.php` - WordPress will find it
- Don't use the default database prefix `wp_`
- Don't share database among multiple sites

Where Are The Weaknesses?

Hosting

- Shared hosting has more exposure
 - Cross Contamination - Especially if you are a developer and keep multiple projects in the same shared space with no isolation
- VPS offers additional isolation from other sites but is not necessarily more secure in other ways
- Most major hosting companies provide good security and updated environments because it's ultimately cheaper for them, but....
 - Look up their environment, latest PHP, Linux, etc.
 - Security or status blog, good support
 - Can you use an Letsencrypt SSL cert or cert you provide
 - Do they offer WordPress specific hosting?
 - Consider SSH, not basic ftp, don't share folders on website

Security Plugins

DO YOU HAVE A BACKUP??

- BackupBuddy
- Store off-site copies, Pull and Push
- Backup as often as your data changes and you can afford to reconstruct it
- Automatic - scheduled

Security Plugins

Monitoring - Scanning

- WPScan
- Google Search Console
- Jetpack Protect
- Sucuri - scanner plugin (free)



Security Plugins

Defense

- VaultPress - Subscription Service
- Wordfence
- iThemes Security
- All in One WP Security
- Google Authenticator
- Clef Two-Factor Authentication
- BulletProof Security - Firewall

DON'T install all of them!

Security Plugins

Remediation - Cleanup

- Wipe the environment CLEAN including new database
- Restore your backup
- Don't have a backup... review every file
 - Replace everything you can with new copies
- Change all of your passwords and salts again
- Eli - Anti-Malware Security and Brute-Force Firewall
- Sucuri - professional services
- Check Cron Jobs

