

WordPress Security

(in a non-dull way?)

Let's get going...

Sam Hotchkiss

BruteProtect

Bath, Maine, USA

@hotchkissweb

@bruteprotect

sam@getparka.com

Notes available at http://samhotchkiss.com/security_deck.pdf

Who am I?

A die-hard Cardinals fan

- I'm Sam (hi!)
- 4 months in the WordCamper
- PHP dev since the '97
- WP dev since '06
- Founder of Parka
- Principal of Hotchkiss Consulting Group



Disclaimer: You will never be 100% secure.



Types of Attacks

The How and The Why

- Pharma / Affiliate
- Link Injection
- Hacktivism
- Drive-by Downloads
- Redirection
- And the list goes on...

Question: My knitting
blog is safe, right?



Know your weaknesses

Don't be a fool, protect your tools.

- Public WiFi
- FTP
- Hosting environment
- Plugins (active and inactive)
- Themes (active and inactive)
- Is core up to date?

Basic Protections

You're already doing this stuff, right?

- Keep core up to date
- Keep plugins up to date
- Keep themes up to date
- Only use plugins you trust
- Don't give people more access than they need
- *Don't send passwords through email*

When setting up WordPress...

Change your Prefix!



Below you should enter your database connection details. If you're not sure about these, contact your host.

Database Name	<input type="text" value="wordpress"/>	The name of the database you want to run WP in.
User Name	<input type="text" value="username"/>	Your MySQL username
Password	<input type="text" value="password"/>	...and your MySQL password.
Database Host	<input type="text" value="localhost"/>	You should be able to get this info from your web host, if localhost does not work.
Table Prefix	<input type="text" value="wp_"/>	If you want to run multiple WordPress installations in a single database, change this.



When setting up WordPress...

Change your username!





Welcome

Welcome to the famous five minute WordPress installation process! You may want to browse the [ReadMe documentation](#) at your leisure. Otherwise, just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

Information needed

Please provide the following information. Don't worry, you can always change these settings later.

Site Title

Username

Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods and the @ symbol.

Protect against Brute Force Attacks

- Plugins
 - BruteProtect
 - Limit Login Attempts
 - Wordfence
 - Better WP Security
- .htaccess / .htpasswd

A little bit more about BruteProtect...

- As of this morning...
 - 47,553 sites protected
 - 50,711,851 attacks blocked
- It's free! (everything we do now will *always* be free)
- Available from Plugin directory or [BruteProtect.com](https://bruteprotect.com)

Develop a Backup Plan

It's not that hard...

- Don't trust your host
- Plugins
 - Backup Buddy
 - WordPress Backup to Dropbox
 - BackWPup
 - VaultPress

Connect Carefully

It's a scary world out there...

- When logging into wp-admin over public WiFi
 - Install SSL or
 - Use a VPN (I use Cloak- getcloak.com)
- Don't use FTP
- Don't send passwords through email, use a tool like QuickForget.com
- Use a password manager and secure passwords (I use [1Password- agilebits.com](http://1Password-agilebits.com))
- Consider Two-Factor Authentication

Any questions?

Sam Hotchkiss

BruteProtect

Bath, Maine, USA

@hotchkissweb

@bruteprotect

sam@getparka.com

Notes available at http://samhotchkiss.com/security_deck.pdf