Hardening WordPress

(or, How Not To Get Hacked

And What To Do When You Are)

Gregory Ray
dot gray inc.
@dotgray

Resources

- Codex.WordPress.org
- WPSecure.net
- healthy dose of paranoia

Know Thy Enemy

Anatomy of an Attack

What?

- bulk password (dictionary attack)
  - POST /wp-login.php
  - POST /xmlrpc.php
- vulnerable plugin
  - All-in-One SEO
  - Contact Form 7
  - Custom Contact Forms
- vulnerable theme
  - TimThumb
- form spambot
  - comment spam
  - contact form spam
- SQL injection, XSS, etc.

When?

- ***2003*** *WordPress debuts*
- **2007-2008** WP core vulnerabilities (backdoor)
- ***Dec 2008*** *WP v2.7 adds one-click update feature*
- **2013** multiple vulnerable plugins, targeting Top 50
- ***2013*** *WP v3.7 adds automatic upgrades*
- **2014** brute force attacks, targeting wp-login and XML-RPC
- ***2014*** *Auttomatic acquires BruteForce*

How?

- brute force
- vulnerability scan / penetration testing
  - brobot | itsoknoproblembro DDOS toolkit
  - WPScan
  - Flunym0us
  - WP Security Scan
  - WordPress Auditor
  - WordPress Sploit framework
- targeted

Who?

- script kiddies
- hacker mafia -> mafia hackers
- state hackers

Why?

“Because that’s where the money is.”

- Willie “The Actor” Sutton, *bank robber*

“I never said that....Why
did I rob banks?
Because I enjoyed it.”

- Willie “The Actor” Sutton,
The Memoirs of a Bank Robber

Why WordPress?

- WordPress "has grown to be the largest self-hosted blogging tool in the world, used on millions of sites and seen by tens of millions of people every day." *(Wordpress.org)*
- "WordPress was used by more than 22.0% of the top 10 million websites as of August 2013. WordPress is the most popular blogging system, at more than 60 million websites." *(Wikipedia.org)*
- commonality = predictability
- infrequent updates
- botnets make it easy, low-risk, automated

Why your site?

- conscription (for later use e.g. DDOS, for resale)
- content manipulation (spam links, IFRAME injection e.g. fake AV scams, click selling)
- steal user profiles (for spam, identity theft)

= to make $

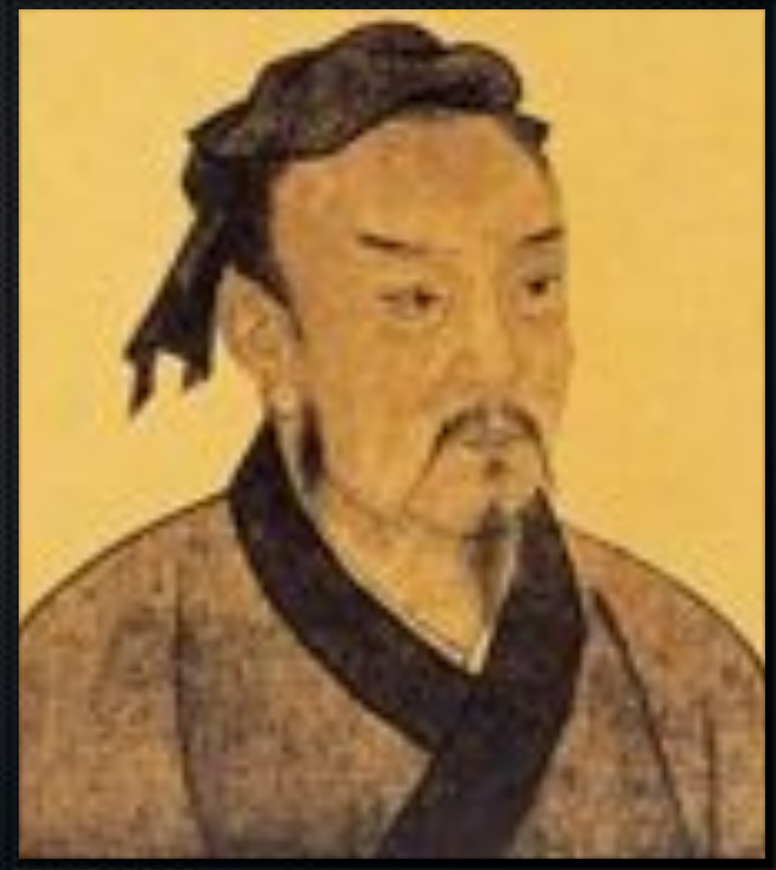
Preparing For War

or, If Sun Tzu Ran WordPress

“The opportunity to secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself.”

Sun Tzu,

The Art of War



Choose your ground

- trusted web host
- tested core version
- trusted theme
- necessary, vetted plugins

Stay current(-ish)

- update core WordPress
- update theme
- update plugins

caveat: test first!

Protect your general

- no 'admin' account
- strong, unique password

strongpasswordgenerator.com

password manager (1Password/LastPass)

Mac Keychain Password Assistant

S trong
O bscure
U nique
P assword

Secure the borders

- limit file permissions (check with web host)
  read-only except within /wp-content/uploads/
  conflicts with auto-updates
- .htaccess rules (check with web host)

Guard against spies

- change DB table prefix (not wp_*)
- disable WP version display (code, plugin)
- relocate wp-config.php (outside web root)

Prepare fallback positions

- site file & data backups!
  - preferably automatic
  - DB history

Responding to an Attack

- contact web host
- check & archive logs
- block IP (plugin, web server module, firewall)
- scan site files (WordFence)
- quarantine 'bad' files for forensic review
- revert DB
- change passwords & salts (wp-config.php)

Security Plugins

- prevention
  - All In One WP Security & Firewall
  - Better WP Security
    (now “iThemes Security”)
  - BruteProtect
  - Sucuri
  - WordFence

- detection
  - Exploit Scanner
  - TAC (Theme Authenticity Checker)
  - TimThumb Vulnerability Scanner

- comment spam prevention
  - Akismet
  - Antispam Bee
  - Bad Behavior
  - Cookies for Comments
  - WP Hashcash Extended