WordPress Security

Don’t Be a Target

Will Chatham
@willc
www.willchatham.com

WordCamp Asheville, June 3, 2016

Will Chatham

BA, Certified Ethical Hacker, Certified Penetration Tester, Security+, A+

- Asheville Resident since 1992
- Longtime WordPress user, developer, fan
- Lover of secrets
  - Magician -> Locksmith -> Web Dev -> SEO -> Ethical Hacker
- Currently Cyber Security Analyst at the National Centers for Environmental Information (NOAA) in Asheville

Who Are You?

Questions from me!

Overview

- Security Threats: Why & Who
- How WordPress Gets Hacked
- **Don’t Be a Target**
- Disaster Recovery: Get Well Soon!
- Q&A Discussion (but feel free to ask at any time!)

WordPress Security Threats: Why Me?

“My little website is out of the way, and no one ever visits it.”

“My website isn’t important enough for some hacker to care about.”

“My website is a needle in a haystack. The chances that some hacker would find it are too small for me to get hacked.”

Sound familiar?

This Is Why You Are a Target

Spam injection/Black Hat SEO

Resource theft - spammers

Botnets

Data Theft / Deletion

Ransomware

Drive By Downloads

Defacement/Bragging Rights

WordPress Security Threats: Who Are They?

It is usually automated scripts run by:

- Script Kiddies (aka Skiddies)
- L33t H@xx0rs
- Blackhat SEOs

It is rarely:

- Guys in hoodies in dark rooms
- Competitors
- Spies
- Governments

Hacking WordPress: Common Attacks

- File upload
- Malicious Code Injection
- Brute Force
- Social Engineering & Phishing

Hacking WordPress: Example

The infamous “timthumb” exploit of 2012

- Timthumb is an image editing library built into many themes and plugins
- 0-day exploit impacting upwards of 40 million WordPress websites
- Hackers could upload files to take control of WP websites
- Easy to exploit, quickly proliferated
- Steal info, perform redirects, deliver Malware

Hacking WordPress: Example

To this day, the timthumb exploit lingers

Update, update, update….

Don’t Be a Target

Security is not about eliminating threats, it is about reducing them.

Basic WordPress Security

If you walk away and do nothing else, at least do this:

- Unique, strong password
- Unique, uncommon usernames
- Update, Update, Update

Plugins: The Biggest Threat

Plugins are why most WordPress hacks occur. Some best practices:

- Only use well-known, active, updated plugins
- Do not use abandoned plugins
- Do your research
- Keep them up to date!

This plugin keeps your plugins updated automatically, and it’s free:

Update Control

More Stuff to Update

Update WordPress Core

- WordPress itself has an excellent track record in security

Update your Themes

- Theme frameworks bring risk
- Included functionality in themes

Your Web Host Matters

Shared Hosting: You are the company you keep

Virtual Private Server (VPS): Taller fences

Dedicated Hosting: Have an IT staff?

Managed WordPress Hosting: Best option for many businesses

With web hosting, you really do get what you pay for!

Incrementally Making The Target Smaller

The “admin” username

Password security

Add Two-Factor Authentication

Employ Least Privileged principles

Hide wp-config.php and .htaccess

Use WordPress security keys for authentication

Disable file editing

Limit login attempts

Be selective with XML-RPC

Hosting & WordPress security

Stay up-to-date

(Free) plugins & themes

WordPress Security Plugins

Two of the better freemium WP plugins:

iThemes Security (formerly Better WP Security)

WordFence

Quick demo?

SSL

Encrypts your website’s traffic

- Gain visitor trust, especially for ecommerce sites
- Protect your login, cookies, sessions
- Preferential treatment from Google

It is now free, so there is no reason not to get a SSL certificate for your website

https://letsencrypt.org/

Disaster Recovery

Backups make recovery a breeze

BackupBuddy ($6.66/mo)

Updraft (Free)

VaultPress ($5/mo)

Remote Backup Storage:
Amazon S3, Google Drive, DropBox, etc etc etc

Ask your web host
If they provide backups!

Getting Help

The WordPress Codex Guide - help for when you have been hacked

Repair Services:

Sucuri

WordFence

RescueWP (soon?)

Ask your web host
If they restore backups!

References and More Info

https://yoast.com/wordpress-security/

https://wordpress.org/plugins/google-authenticator/

https://blog.sucuri.net/2015/02/why-websites-get-hacked.html

https://www.wordfence.com/blog/2016/03/attackers-gain-access-wordpress-sites/

https://codex.wordpress.org/Configuring_Automatic_Background_Updates

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

http://www.wpbeginner.com/beginners-guide/what-why-and-hows-of-wordpress-security-keys/

Contact Me

Will Chatham

will@willchatham.com

@willc

These slides will be available at:
www.willchatham.com

Happiness Bar at 2:45 today!