WordPress Security

Don’t Be a Mark

(with apologies to anyone named Mark)

Will Chatham
@willc
www.willchatham.com

Asheville Area WordPress Group, August 17, 2016

Overview

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

Will Chatham

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

- Asheville Resident since 1992, graduate WWC ‘96
- 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

What?

You are up against:

Spam injection/Black Hat SEO

Resource theft - spammers

Botnets

Data Theft / Deletion

Ransomware

Drive By Downloads

Defacement/Bragging Rights

The easiest way to defeat security is to go around it.

WordPress Security Threats: Who Are They?

It is usually automated scripts run by:

- Script Kiddies (aka Skiddies)
- Blackhat SEOs
- Malware/Adware

It is rarely:

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

Hacking WordPress: Common Attacks

Finding Vulnerabilities to:

- Gain Access
- Escalate Privileges
- Upload Files
- Malicious Code Injection

Don’t Be a Target

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

Basic WordPress Security

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

- *Update everything weekly or more (WordPress, plugins, themes)*

- Unique, strong password

- Unique, uncommon usernames

Plugins: The Biggest Threat

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

- Only use well-known, active, updated plugins, preferably from the WP Plugin Directory
- 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

Or you can do it on your own in wp-config.php

More Stuff to Update

Update WordPress Core

- WordPress itself has an excellent track record in security
- Quick to patch, auto-updates enabled by default now (is yours?)

Update your Themes

- Theme frameworks bring risk
- Included functionality in themes (sliders, forms, etc)

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!

Using Defense-In-Depth (sort-of)

The “admin” username

Password security

Add Two-Factor Authentication

Employ Least Privileged principles

Hide the admin area

Use WordPress security keys for authentication

Disable file editing

Limit login attempts

Be selective with XML-RPC

(Free) plugins & themes

SSL

Update, update, update

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

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