The Ultimate Guide to WordPress Security

Part Two

This will be recorded

It will be on YouTube and the URL will be in Meetup event comments

Who I Am

David Schargel

david@ambient.vision
@DavidSchargel
+1 503-405-8999

https://ambient.vision

- Using computers since the Apple //
- Started with Macintosh in 1984
- Technical Editor at MacUser Magazine
- Started Aladdin Systems (“the StuffIt company”)
- Started with the Internet before the web
- Started consulting in 1996
- Started with WordPress 2007 (version 2.2!)
- Since started 5 other companies
- Technology, IT, Tourism, Team Building,
- Site Building, Security, Optimization, Hosting

I don’t “do” Wordpress, I live and breathe it.

Who I Am

David Schargel

david@ambient.vision
@DavidSchargel
+1 503-405-8999

Please contact me with any questions!

Part One Review

Increasing in complexity as we go on

How Hackers Get In

Basic Security Options for Anyone

After the Basics

Advanced & Expert To Dos

Backups and You

Fixing A Hacked Site

Plugin Issues

Defining Brute Force Attacks

Protecting Your Admin Access

Firewalls

Security Plugins & Monitoring

Why WordPress Security is Important?

Is WordPress Secure?

Is WordPress Secure?

Yes, WordPress itself is safe.

The rest depends entirely on you,

Security is though is risk reduction, not risk elimination.

Use “Best Practices” and stay informed.

Security in general is complex and use your head, not "just because."

How Do Most Sites Get Hacked?

Websites mostly get hacked because of a few things:

- Software Vulnerabilities & Third-Party Integrations
- Brute Force Attacks
- Access Control
- Social Engineering like Phishing

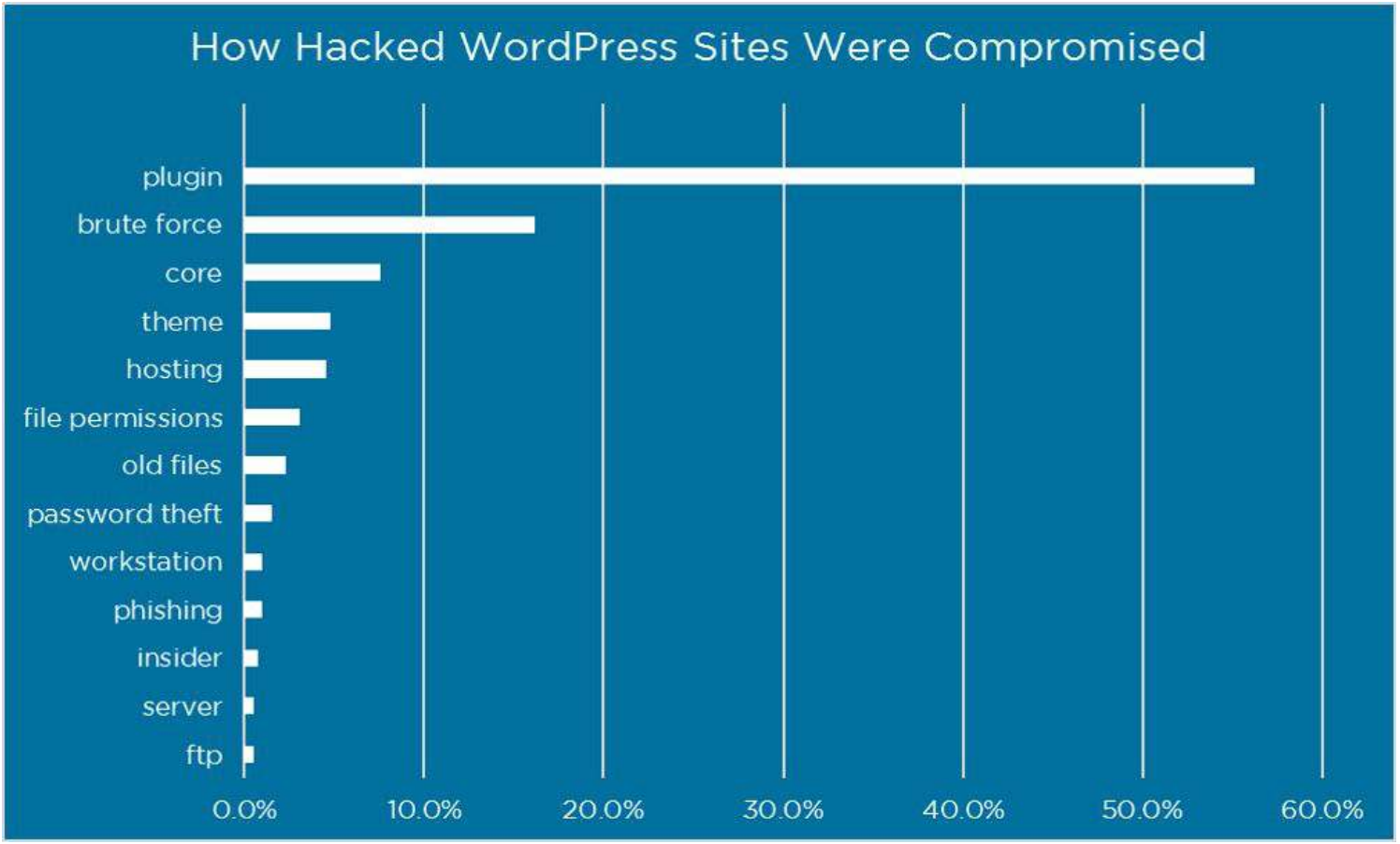
“Easy” & Common WordPress Attack Vectors

Old WordPress versions & Old Plugins & Old Themes

The backend; /wp-admin/

XML-RPC

Too many login points with potentially poor passwords


How Hacked WordPress Sites Were Compromised
plugin
brute force
core
theme
hosting
file permissions
old files
password theft
workstation
phishing
insider
server
ftp
0.0%
10.0%
20.0%
30.0%
40.0%
50.0%
60.0%

101-301
Quick Review???

101 to 301 Quick Review?

Watch previous video and download slides

More on Firewalls

Previous Slides on Firewalls?

webpagetest.org security score

Previous Slides on Firewalls?

401
College-Level Advanced
(Can Be Done With Most Webhosts)

401 College-Level Advanced - 1 of 3

Enforce strong password policies with something like the “Password Policy Manager”.

Disable PHP File Execution in "/wp-content/uploads".

Disable Directory Indexing & Browsing.

Disable XML-PRC without using a plugin.

Put SMTP email info in functions.php & wp-config.php and not via plugins.

401 College-Level Advanced - 2 of 3

Revisit PHP version - 5.6, 7.2, 7.3, or 7.4?

Aggressively limit IP access - even geographically.

Remove “User 1”: Which is (was?) the default Administrator user.

Disable the Theme Editor.

Employ User Roles better.

401 College-Level Advanced - 3 of 3

Automatically log out idle users.

Place some backups in Amazon Deep Glacier or a Safe Deposit Box.

Avoid WordPress Multisite Network.

If using WooCommerce, take extra steps to enforce strong password policies.

Register your website with Search Engines “Webmaster Tools”

Security Through Obscurity?

Changing WordPress Database Prefix?

Renaming the Administrator account (user with the ID of 1)?

Changing your wp-login.php URL or /wp-admin/ URL?

- Some plugins & themes don't play well!

402
Email Security
Outbound from WordPress

402 - Email from WordPress

Plugins usually place the SMTP info into a database, so...

Put SMTP info in functions.php & wp-config.php.

Add Email DNS entries - SPF, DKIM, and DMARC.

Check it on https://www.mail-tester.com/

Sendgrid, Mailgun, AWS SES, MailPoet

Eric L Presentation?

403
DNS Security

402 - Domain Name Service (DNS) Security

The DNS system was not designed with security in mind.

Use DNSSEC with your Domain Registrar.

Use Privacy with your Domain Registrar.

Add Email DNS entries - SPF, DKIM, and DMARC.

Other Security Issues are Mostly Local

Questions?

Post-Hack Actions

Post-Hack Actions and Remediation

Have a Professional do it for you.

Check with your hosting company.

It ***is*** possible to do an in-place repair, but not advised unless you know how to do it

- Identify the Hack.
- Restore from Backup
- Restore backup to another web host under a different domain name.
- Re-install WordPress from scratch
- Manually add known-good plugins back in.
- Import content.

Questions?

501
Masters-Level Expert

501 Masters-Level Expert - 1 of 3

Stop user enumeration

BasicAuth Password Protect /wp-admin/ and /login.php.

Optional WP fail2ban plugin.

Check server crontab and wp-cron events with crontrol

Consider disabling allow_url_include & allow_url_include

Move the wp-config.php file to the directory above your WordPress install

501 Masters-Level Expert - 2 of 3

Server-level backups.

Update WordPress salts.

Remove pingbacks/trackbacks via functions.php.

Restrict access or Disable the REST API.

Add/Change HTTP Response Headers...

- Adding Strict-Transport-Security
- X-Frame-Options
- X-Xss-Protection
- X-Content-Type-Options
- Referrer-Policy
- Feature-Policy
- X-Robots-Tag
- X-Powered-By
- X-Pingback & Link

501 Masters-Level Expert - 3 of 3

If you ever mucked with file permissions…reset them:

- Directories 755.
- Files 644 (exceptions may apply to some themes and plugins).
- wp-config.php 600.
- Apache .htaccess 644 or 600.

Similarly, be sure that everything has the appropriate *user*:*group*.

Checking HTTP Headers

Inspect

Strict Transport Security (HSTS)

HSTS Preloading?

- Adding Strict-Transport-Security
- X-Frame-Options
- X-Xss-Protection
- X-Content-Type-Options
- Referrer-Policy
- Feature-Policy
- X-Robots-Tag
- X-Powered-By
- X-Pingback & Link

Questions?

601
Doctorate-Level Expert

601 Doctorate-Level Expert - 1 of 3

- Avoiding DDoS attacks
- Review Hardening Techniques.
- Do not rely on command line-only setups and stop there. Keep server software updated, including apache/nginx, PHP, MySQL/MariaDB/Percona, etc. updated.
- Jeff Starr's 6G "Firewall" 6G was originally intended for Apache's .htaccess files, so it has inherent limitations.
- If using Cloudflare, add a Firewall Rule matching backend login (/wp-login.php) with action JS Challenge.
- SSH: Escalate a band-new user to allow sudo and deny root user logins
- SSH: SSH-key login only (no passwords).
- Consider allowing SSH only from your IP address(es).
- IPTables/UFW/CSF/lfd and Fail2ban.

601 Doctorate-Level Expert - 2 of 3

- Setup fail2ban on origin server and configure it to talk with CF Firewall API so fail2ban jail rules you specify for bad request type.
- Lock down unused ports (keep 80, 443, 22, 53).
- Linux Malware Detect (LMD/maldet) & clamAV.
- OS, nginx, Apache, PHP Updates. Constantly.
- Keep each site running under its own user:group. If not, then consider keeping 1 site per server.
- Strong (and rotating) passwords.
- Only use SSH with SSH Keys (no passwords) only.
- Bad bot blocker, including denying of WPScan identifiers.

601 Doctorate-Level Expert - 3 of 3

- (Carefully) ModSecurity 3+ WAF and OWASP 3+ ruleset with granular per site control (brute force/DDOS + +). "ModSec is a biatch"
- Overkill for most brochure sites.
- Force Security Headers for web traffic.
- Consider geo filtering/banning /wp-admin/ at the apache/nginx level.
- Consider changing some of the default php.ini settings.
- Disable server signature in HTTP Response Header.
- Consider an occasional WPScan via command line.
- Employ server-level rate limiting.
- IP Deny Lists (even though its in some plugins)

Questions?

Resources & Sites to Watch

Resources & Sites to Watch

- Security Glossary:
  - https://www.wpwhitesecurity.com/wordpress-security-glossary/
- WPScan Vulnerability Database
  - https://wpvulndb.com/
- Wordfence Monthly Blog
- WebARX Blog
- WP Scan Blog
- Think Like a Hacker Podcast

Thanks!

David Schargel
david@ambient.vision
@DavidSchargel
+1 503-405-8999

https://ambient.vision

Please contact me with *any* questions!