The Ultimate Guide to WordPress Security

Part One

Who I Am

David Schargel

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

- 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!

Overview

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

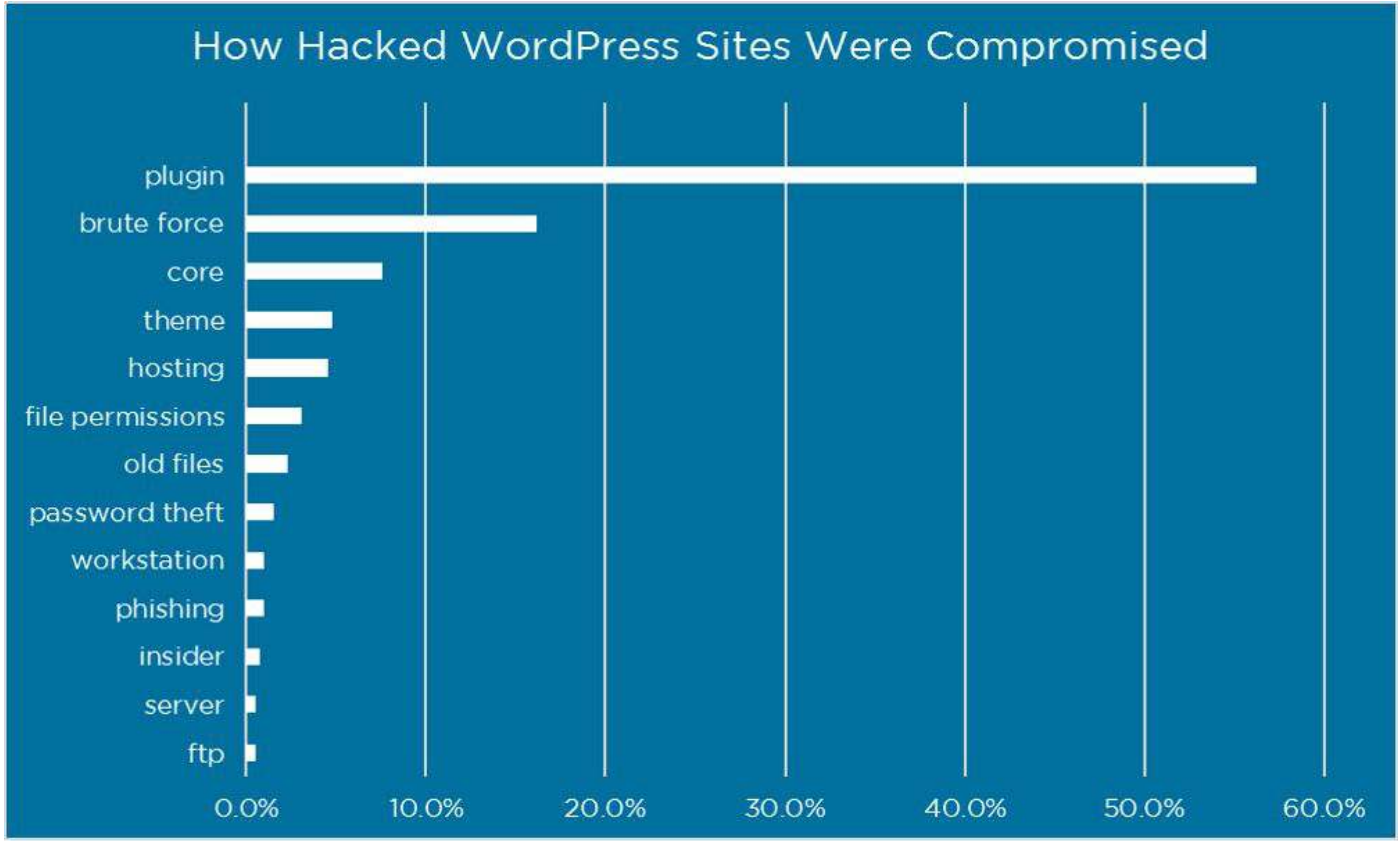
“Easy” & Common WordPress Attack Vectors

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
Basic Security Recommendations

101 Security Basics - 1 of 2

Backup

Keep WordPress & plugins & themes up-to-date.

Delete unused plugins & themes.

Use Strong (complex and long) Passwords.

Use Two Factor Authentication (2FA).

Make sure your site is only on HTTPS (aka has a SSL certificate).

101 Security Basics - 2 of 2

Secure your website from the very start.

The role of a good website host.

Don’t use shady, pirated, nulled plugins.

Understand attacks and which ones are important to avoid...

...and decide how much effort you want to place into this.

Updating…
WordPress Themes & Plugins

What is 2FA?

“Two Factor Authentication”

What is 2FA “Two Factor Authentication”?

Protect your WordPress Login backend.

An additional login security feature.

Relies on ***something you know*** together with ***something in your possession***, like your molbile phone or email account.

Thus...two factors are involved in authenticating your access.

How To Implement 2FA

1) Download and install a free 2FA app on smartphone or desktop.
2) Install a plugin within WordPress and set it up.
3) Then, at sign-in, you enter a username and password (as usual), and then, when prompted, you enter the code shown on the app.

Note: Good 2FA systems also have “backup codes” in case 2FA fails

Three Free 2FA Plugin Options

Two-Factor (two-factor) by Plugin Contributors.

Two Factor Authentication (two-factor-authentication) by UpdraftPlus.

Wordfence Login Security (wordfence-login-security) by Wordfence.

Brute Force Attacks

What is a Brute Force Attack?

Multiple usernames and passwords over & over until a successful one is discovered.

Usually comes from automated tools or botnets, not people.

These automated tools send 100s or 1000s of login requests using a list of random usernames and passwords.

Website Backups

Make Backups of Your Website

Don't rely on your host as the only mechanism..

Automate your backups.

Test Restore & Recovery Process!

Download & store your backups off the server.

The 3-2-1 Rule of Backups...

➔ 3 copies or versions of your data on…
➔ 2 different media (local computer + external drive) with…
➔ 1 copy off-site for disaster recovery.

WordPress Built-in Site Health

WordPress Built-in Site Health feature

Potentially Public files

File Integrity

PHP Warnings

Inactive Themes or Plugins

Delete Unused Plugins

Are Things Up To Date

201
After The Basics

201 Beyond the Basics - 1 of 2

Minimize Plugin Use.

Bad user names: administrator, admin, webmaster, or testadmin

Use Cloudflare or a true Firewall if your hosting company does not do that for you.

Watch out for expired paid/premium plugins & themes

Ensure there's no "mixed content" warnings. http:// vs. https://

201 Beyond the Basics - 2 of 2

Use a Password Keeper.

Only Install Software From Trusted Sources.

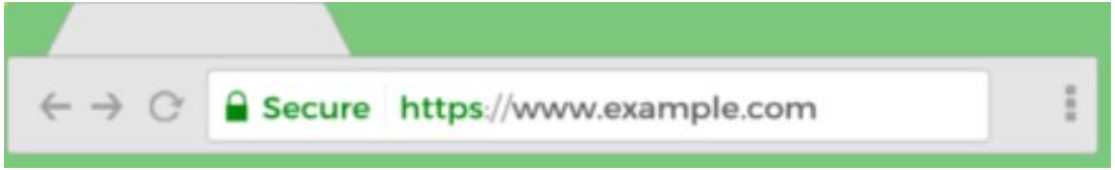
Limit Access and Have Very Few Administrator Users.

Off-Site Backups, Lots Of Backups.

Limit Failed Login Attempts.

SSL and “Mixed Content”

SSL - https://



SSL/TLS (https://) = Encryption, Authentication, Integrity.

Browsers flag websites as “Not Secure.”

It’s a major ranking factor for search engines.

If your host does not provide this for free, then find a new host.

Check your pages as you may have "mixed content!"

Choosing Quality Plugins & Themes

Choosing Quality Plugins & Themes

Always run “less” software.

Always use the WordPress Repository.

Don't use pirated plugins or themes.

For Premium Plugins & Themes: Are they respected & reputable developers?

Checking the WordPress Repository…

- When was it last updated?
- What is the rating and why?
- Number of user reviews?
- Number of installations?
- Does the author answer support Qs?

301
Refining and Improving

301 Refining and Improving - 1 of 2

Convince your boss that 2FA is a great thing.

Enforce 2FA wherever you can.

Administrator account usernames should be hard to guess.

Employ the principle of "Least Privileged."

Consider creating a new Administrator user and ‘disabling’ the old one.

301 Refining and Improving - 2 of 2

Check Must-Use & Drop In Plugins.

Keep your 2FA codes separate from your main Password Keeper

Have an allowlist of IP addresses.

Be careful how you duplicate the wp-config.php file.

Hide WordPress version.

What is a Firewall?

Firewall Before WordPress

Infrastructure/Hardware Firewall

DNS-Level Firewall (aka Reverse Proxies)

Network/Server Firewall

Web Server Configuration Files

Firewall Within (Or Just Before) WordPress

Application-layer firewall.

Often referred to as a Web Application Firewall (WAF).

Filter attacks as WordPress is loading, but before it is fully processed.

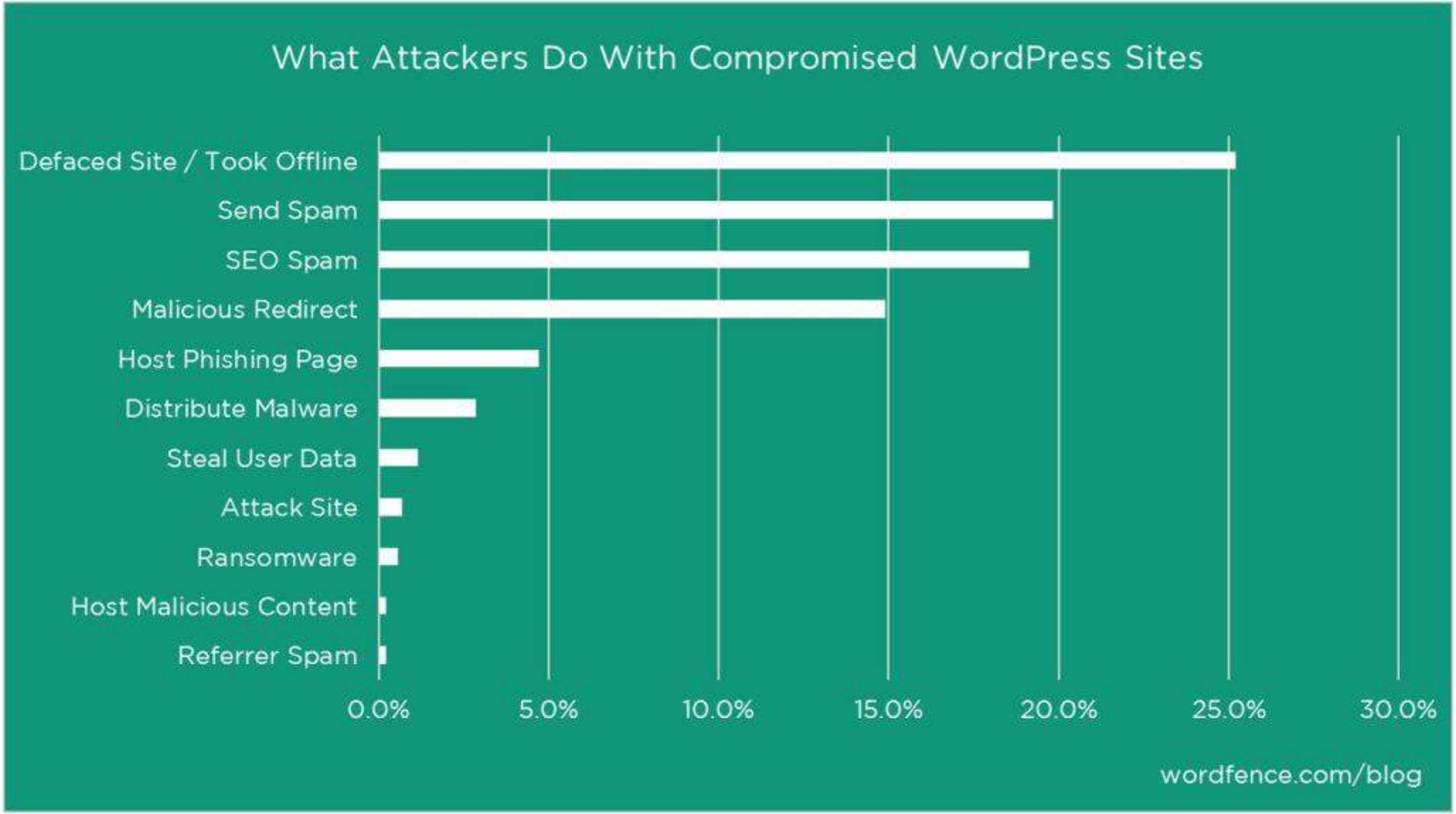
WordPress-Specific Rules

What a Hack Looks Like

How To Tell if I Have Been Hacked

- Defacement.
- Redirection
- Bad links.
- Strange emails being sent.
- Blog posts not from you.
- Search results show impossible results or other languages.
- Website suspended by Web host or denylisted by Google
- Ad injections.
- Your Administrator(s) access is gone.
- Site goes offline.
- Alert(s) from host or scanning/monitoring software.

Sometimes, attacks sit dormant, keep old backups!


What Attackers Do With Compromised WordPress Sites
Defaced Site / Took Offline
Send Spam
SEO Spam
Malicious Redirect
Host Phishing Page
Distribute Malware
Steal User Data
Attack Site
Ransomware
Host Malicious Content
Referrer Spam
0.0%
5.0%
10.0%
15.0%
20.0%
25.0%
30.0%
wordfence.com/blog

The Role of Security Plugins

False Hope vs Future Hope

Security Plugins - Monitoring & Reports

Display on WordPress Dashboard.

Logging of users and suspicious activities.

Vulnerability monitoring & reports.

File scanning and file integrity reports

Malware & Virus scanning

Notify if you’re on Google’s Safe Browsing list.

Uptime monitoring.

Security Plugins - Alerts & Notifications

Alerting of File Changes on Your Site.

Alerting of Malware scan results.

Alerts via Email.

Alerts via Text Messages

- 10digitphonenumber@tmomail.net
- 10digitphonenumber@messaging.sprintpcs.com
- 10digitphonenumber@vtext.com
- 10digitphonenumber@txt.att.net

Security Plugins - Active Security

“Security hardening.”

Old/abandoned Plugin Notifications.

Brute force attack protection.

Two-Factor Authentication (2FA) and other login protections.

Notifications for when a security threat is detected.

Some have Firewall capability.

Security Plugins - Prevention & Protection

Managed Web Application Firewall (WAF).

Virtual Patching via WAF.

Blocklist monitoring.

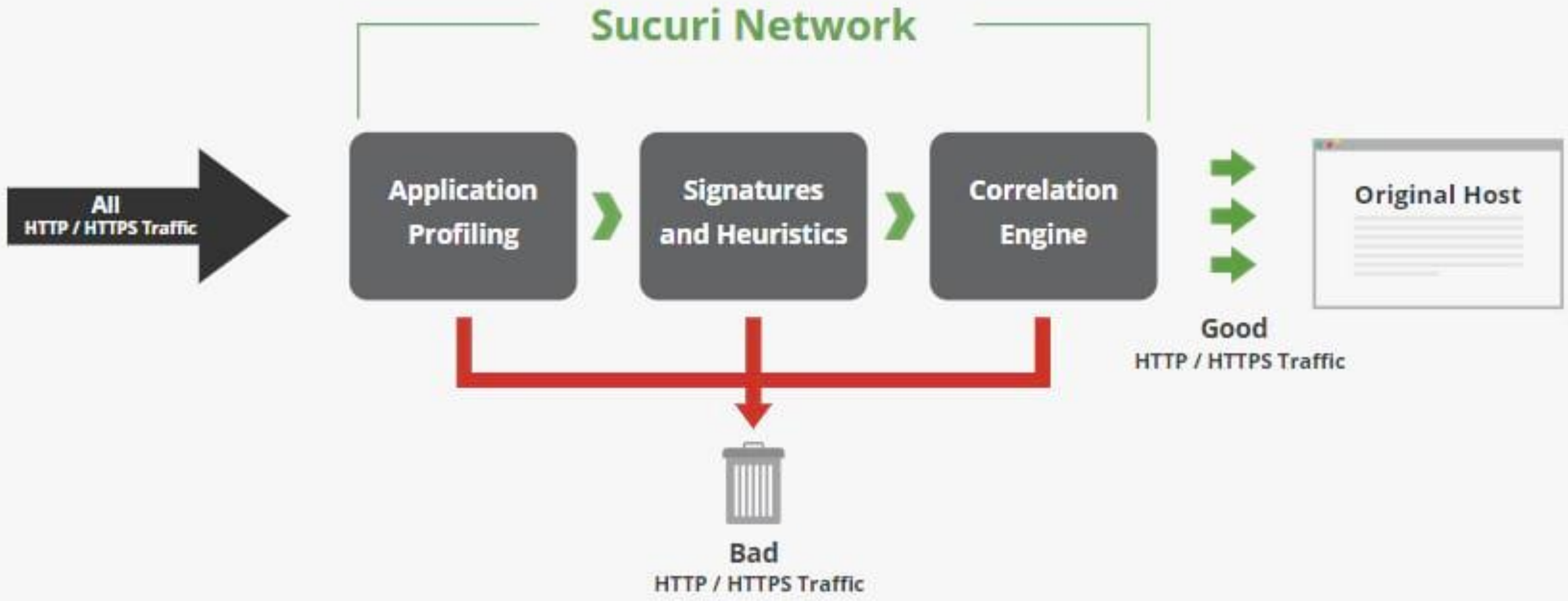
Permit or restrict IP access with an allowlist and a blocklist.

Insert Security Headers.

Disable or restrict access to REST API, XML-RPC, Pingbacks, Trackbacks, RSS feeds.

Website Application Firewall (WAF)

Protect and Speed Up Your Website



Security Plugins - Cloud Dashboards

Single interface to view and manage findings across multiple websites.

Uptime Monitoring & Is My Site Down?

Wordfence Premium, WebARX, Securi Premium, and others.

ManageWP & MainWP

Choosing a Security Plugin

Choosing a Security Plugin

DO: Get one with 2FA.

DO: Get one with a true Firewall (which you will need to pay for).

DO: Research based on your needs & abilities.

DON’T: Choose the “100% most complete security” plugin.

DON’T: Use multiples.

“I Want Free” Security Plugins/Tools

One of previously mentioned 3 Free 2FA Plugin Options.

Disable XML-RPC.

Logging and notification.

Limit Login Attempts via "Limit Login Attempts Reloaded" OR "Login LockDown”.

Image Security

Image Security

Image watermarks.

Prevent right-click to save image.

Prevent hotlinking.

Copyright/copyleft notices.

Social Engineering Concerns

Social Engineering

1. Phishing & Vishing (voice phishing).

2. Information Sharing: Sharing too much information on social media

3. Surveillance. Spear phishing & email interceptions.

4. Social grooming. Building trusted relationships and creating empathy with targeted staff can help ensure a scam is successful.

302
Additional Security For Clients

302 - Additional Security For Client Sites

Disable theme editing.

Disable plug-in uploads.

Disable file modification.

Document this for them in case they are no longer your client down the road.

Use ManageWP, MainWP, or Infinite WP monitoring for clients.

304
Other Security Considerations

304 - Other Security Considerations

Trust Signals

eCommerce Security

Password hygiene & annual #passwordday

Local computer backups.

Local computer should have a strong password and disallow auto-logins.

Don’t store Passwords in browser

Working with children, seniors, or people with disabilities on what security is and what they should pay attention to.

Legal issues – Terms of Service, Privacy Polices, Cookie Compliance – opt-in vs. opt-out.

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!