Shields Up For WordPress Websites and Blogs

Protecting and Securing Your WordPress Website
Bob Weiss  
MCSE, A+, CEH, CISSP

- Senior Cybersecurity Engineer at CIT
- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- Cybersecurity Blogger @ wyzguyscybersecurity.com
Additional Information

- (ISC)2 Twin Cities
  - Board and webmaster
- UMSA
  - Board member
- MnSec
- Bsides
- OWASP
- LinkedIn
  - www.linkedin.com/in/wyzguy
- Twitter handle
  - @wyzguys
- Conference
  - #Sec360
How This Presentation Happened

• Blogging since October 26, 2006
• Moved From Blogger to WordPress about 2013
• Decided I had to “walk the talk”
• When I installed WordFence I started seeing getting a barrage of alerts about brute force login attempts
• Decided this was a real threat.
This email was sent from your website "WyzGuys Computer and Network Support" by the Wordfence plugin at Monday 26th of September 2016 at 10:24:18 PM The Wordfence administrative URL for this site is: http://www.wyzguys.com/wp-admin/admin.php?page=Wordfence

A user with IP address 50.242.22.237 has been locked out from the signing in or using the password recovery form for the following reason: Used an invalid username 'wyzguys' to try to sign in.
User IP: 50.242.22.237
User location: Whitehouse, United States
Why Would Someone Hijack My Website?
Who Has Been Hacked?

• Brian Krebs – Krebs On Security - distributed denial of service attack took blog offline for several days
• Who in the room?
Non-Targeted Attacks

- Generally automated attacks
- Goal is to compromise as many sites as possible
- Website database information stolen
- Website content or information held for ransom
- Access to webserver may be “rented” to another cyber-criminal
  - Become part of a bot-net or DDoS collective
  - Used to host phishing scam landing pages
Targeted Attack

• The attacker specifically targeted your website
  – Ashley Madison was attacked to publicly expose the site users
  – Panama Papers stolen from Mossack Fonseca
  – DynDNS DDoS attack

• They may have an axe to grind
• They may be holding your site for ransom
What Do They Do With It

- Websites are used to distribute malware
- SEO – inserting backlinks to another site the attacker is promoting
- Steal client user, password, other information stored in a database
- Deface site
- Use site for phishing exploit, host replica landing pages
- Sending spam
- Host illegal content (porn, videos, music, software)
Taking Possession

• Getting your administrator user name and password
  – Phishing email
  – Asking for it
  – Keylogger
  – Password guessing
  – Automated brute force password cracking (software)
  – Buy a list of passwords on the Dark Web
Revelations

• When I added WordFence Security, I was able to see dozens of daily brute force log-in attempts for the first time. It was awe-inspiring.

• When I added miniOrange 2 Factor Authentication, brute force login software no longer worked, and they stopped almost completely.
Protecting Your Website
Secure Your Computer First

• If your computer is infected with Remote Access Trojan or Keylogger malware, cyber-attackers can watch what you are doing, and everything we are going to discuss would be pointless.
  – Install a good anti-malware product on Windows PCs and Macs, too.
  – Run a scan to find and destroy any malware
  – Set up automatic daily scanning. Once a week is not enough.
Use the Internet in a Secure Manner

• Learn how to recognize phishing emails.
• Avoid clicking on links or opening attachments in phishing emails.
• Keep your web browser version up-to-date.
• Watch for fake, clone, or malicious websites
  – If things seem strange – then get outta there!
When Starting a New Site

- These items are easiest to do if you are starting from scratch
  - Choose a good host
  - Rename the Administrator Account
  - Change the default table prefix from wp_ to something else
  - Delete the Sample Page
  - Delete the Sample Post ("Hello World")
Secure User Accounts

• Secure the Administrator Account
  – Do not use “admin” or your name for the administrator account name.
  – Too late? Create a NEW administrator account and delete or disable the old one.

• Use “Editor” account for content work

• If you have a multi-user blog, limit permissions
  – Author can write and publish their own posts
  – Contributor can write their own posts but not publish
Strengthen Your Password

- Always use strong passwords
  - Use a unique and complex password of at least 12 characters
  - Test your password strength at Passfault.com
  - WordPress will calculate password strength for you
  - Sign up for a free LastPass account to make creating and remembering strong passwords easier.
Two Factor Authentication

• Use two factor authentication
  – **miniOrange 2 Factor Authentication** supports a variety of methods
  – Phone Call, SMS, Email Verification, QR Code, Push, Soft Token, Google Authenticator, Authy, Security Questions (KBA)

• Or use a CAPTCHA
  – (a backronym for "Completely Automated Public Turing test to tell Computers and Humans Apart")
Basic WordPress Security

- Allow WordPress to update automatically
- Update your Plug-ins and Themes
- Only Use Plugins and Themes From Trusted Sources
- Delete Plug-ins and Themes You Don’t Use
- Delete plug-ins that are reported as unsafe.
- Block or disable pingbacks and trackbacks
Backup Your WordPress Site

- Add a backup plug-in to your website – if you are hacked, at least you will have a recent copy.
  - BackupWordPress
  - Updraft Plus
  - BackupBuddy
- Download and save copy to your computer occasionally.
Install a Security Plug-in

- **Recommended Plug-ins**
  - **WordFence Security** – This is the one I use
  - **Sucuri** (also works with Joomla and other CMS sites) – Tried it, liked it
  - **BulletProof Security** – Another good option I tried.

- Limit logon attempts to thwart brute-force attempts
- Scan website for malware regularly.
Add a Web Application Firewall

• A web app firewall routes traffic to your site through servers that look for suspicious or malicious behavior, and block it from getting to your site.

• Often part of your security plug-in.
  – **WordFence** – endpoint firewall installed in WordPress
  – **Sucuri** – cloud firewall
  – **CloudFlare** – cloud firewall
Advanced Website Security

• Change your database prefix from wp_ to something else.
• Change your WordPress security keys.
• Use .htaccess – write your own or use a plug-in.
• Disable XML-RPC by deleting xmlrpc.php file.
• Read your security logs
  – **WP Security Audit Log**
More Advanced Security

- Disable PHP error reporting.
- **Google Search Console** (formerly Google Webmaster Tools) – you will be notified if malicious things are happening to your website by Google.
- Use **SSL** – we all know that HTTPS sites are secure and HTTP sites are not. Adding SSL is inexpensive and can help with page rank, too.
Educate Yourself

- Sign up for website security emails
  - WyzGuys Cybersecurity blog  www.wyzguyscybersecurity.com
  - WordFence Security blog  www.wordfence.com/blog/
  - Sucuri Security blog  https://blog.sucuri.net/
Recommended Plug-ins

- **WordFence** – pay for the Pro version and get the WAF
- **WP Security Audit Log**
- **miniOrange 2 Factor Authentication**
- **BackupWordPress** or **Updraft Plus**
Resources

• WordPress Security Learning Center www.wordfence.com/learn/
• How To Secure WordPress www.hostingfacts.com/how-to-secure-wordpress/
• WordPress Security Wizard: Lock Down Your WordPress Site From Hackers by Rolland Dhar
More Resources

- Google Search Console - [https://www.google.com/webmasters/tools/](https://www.google.com/webmasters/tools/)
- LastPass password manager – [www.lastpass.com](http://www.lastpass.com)
- Google Authenticator - [https://support.google.com/accounts/answer/1066447?hl=en](https://support.google.com/accounts/answer/1066447?hl=en)
- Authy - [https://www.authy.com/](https://www.authy.com/)
More Resources

- Editing wp-config - [https://codex.wordpress.org/Editing_wp-config.php](https://codex.wordpress.org/Editing_wp-config.php)
- Change the wp_ table prefix - [https://codex.wordpress.org/Editing_wp-config.php#table_prefix](https://codex.wordpress.org/Editing_wp-config.php#table_prefix)
More Resources

• Change security keys -
  https://codex.wordpress.org/Editing_wp-config.php#Security_Keys

• PHP error reporting -
  https://codex.wordpress.org/Editing_wp-config.php#Configure_Error_Logging
Thank You!
Questions?

- Bob Weiss
  - 651 387-1668
  - bob@wyzguys.com
  - Twitter @wyzguys
  - LinkedIn www.linkedin.com/in/wyzguy