The What and Why of WordPress Security

Paul Gilzow

University of Missouri

The What and Why of WordPress Security

Paul Gilzow

University of Missouri

The What and Why of WordPress Security

Paul Gilzow

University of Missouri

The What and Why of WordPress Security

Make sure to submit questions during this presentation via Twitter. Use the hashtag #WPCampus and @gilzow (me). You'll earn points toward the conference game for each question you submit!

TL;DR

Minimizing Risk

What is “Risk”?

- Risk is the intersection of assets, threats, and vulnerabilities.
- Asset
  - People, Property, Information
  - An asset is what we are trying to protect
- Threat
  - Anything that that represents a potential danger to an asset, whether deliberately or by accident
  - A threat is what we’re trying to protect against
- Vulnerability
  - Weakness or holes/gaps in security procedures or program that can be exploited by a threat to affect assets

What is “Risk”?

- Asset = You
- Threat = Rain
- Vulnerability = Hole in your umbrella
- Risk = you getting wet

What is “Risk”?

The potential for loss, damage or destruction of
an asset(s) as a result of a threat exploiting a vulnerability
multiplied by the impact of the threat occurring

Why Education is an Attractive Target

- Network bandwidth and availability
- Rich in hardware infrastructure
- Poor in human resources
- Resistant to blacklisting
- SEO reputation

Why Education is an Attractive Target

- Personally Identifiable Information (PII) / Sensitive Personal Information (SPI)
- Protected Health Information (PHI)
- Confidential Intellectual Property
- Export Controlled Data
- National Security Interest (NSI)

#1: Backups

- What
  - A snapshot of your
    - the files that make up your site
    - database
- Why

#1: Backups

Mizzou
University of Missouri

#1: Backups

- What
  - A snapshot of your
    - the files that make up your site
    - database
- Addresses two types of threats:
  - Data loss/damage
  - Disruption in service/site downtime
- How does it reduce risk?
  - Lowering Impact

#1: Backups

- Bonus points
  - How Often?
  - What should you back up?
  - Types of backups
  - Protection of the backups

#1: Backups

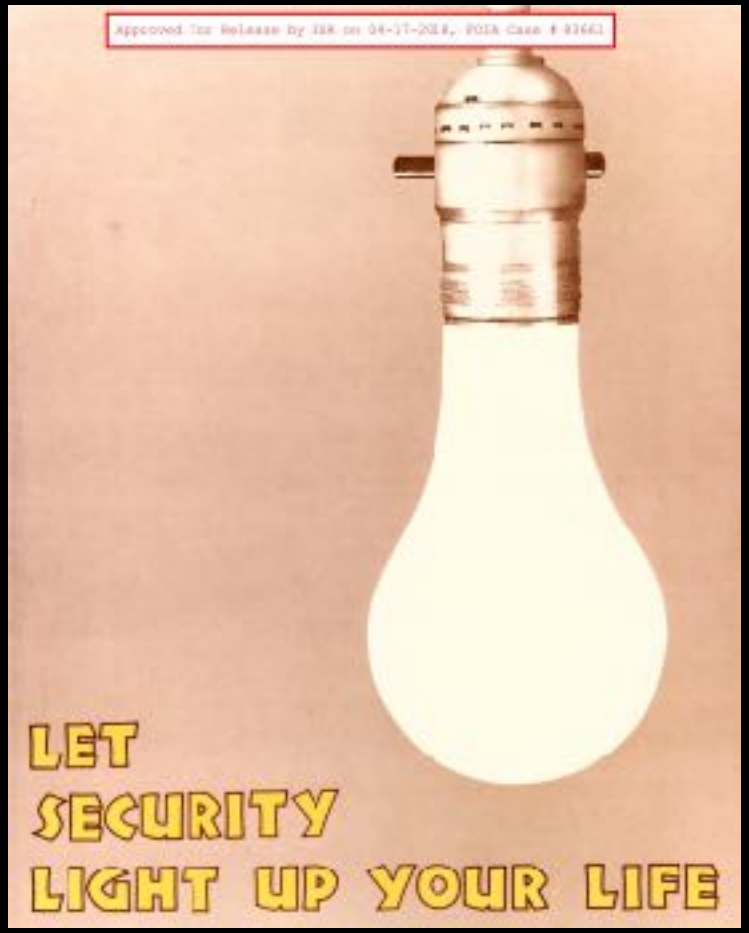
- How Often?
  - Will depend on how much data you're willing to lose or recreate
  - If unsure, start with daily backups and adjust from there
- What should you back up?
  - Ideally
    - contents of the uploads directory
    - database

#1: Backups

- How long should you keep a back up?
  - Depends on how much data you're willing to lose or recreate
  - Start with 3 months and adjust from there
- Backups should be in triplicate
  - Hot backup
  - Cold backup
  - Remote cold/long-term backup

#1: Backups

- Bonus points
  - Protect your backups
  - Don’t keep your back ups in a publicly accessible area
  - Test your backups!



#2: Keep WordPress Up-to-date

- Why/How does it reduce risk?
  - Updates often address security issues
  - Potentially removes an exploitable vulnerability
- How
  - Don’t turn off automatic minor updates*
  - Upgrade and stay on the latest branch release*
- Security principle : *Don’t use components with known vulnerabilities*

* Where possible

#3: Strong Passwords

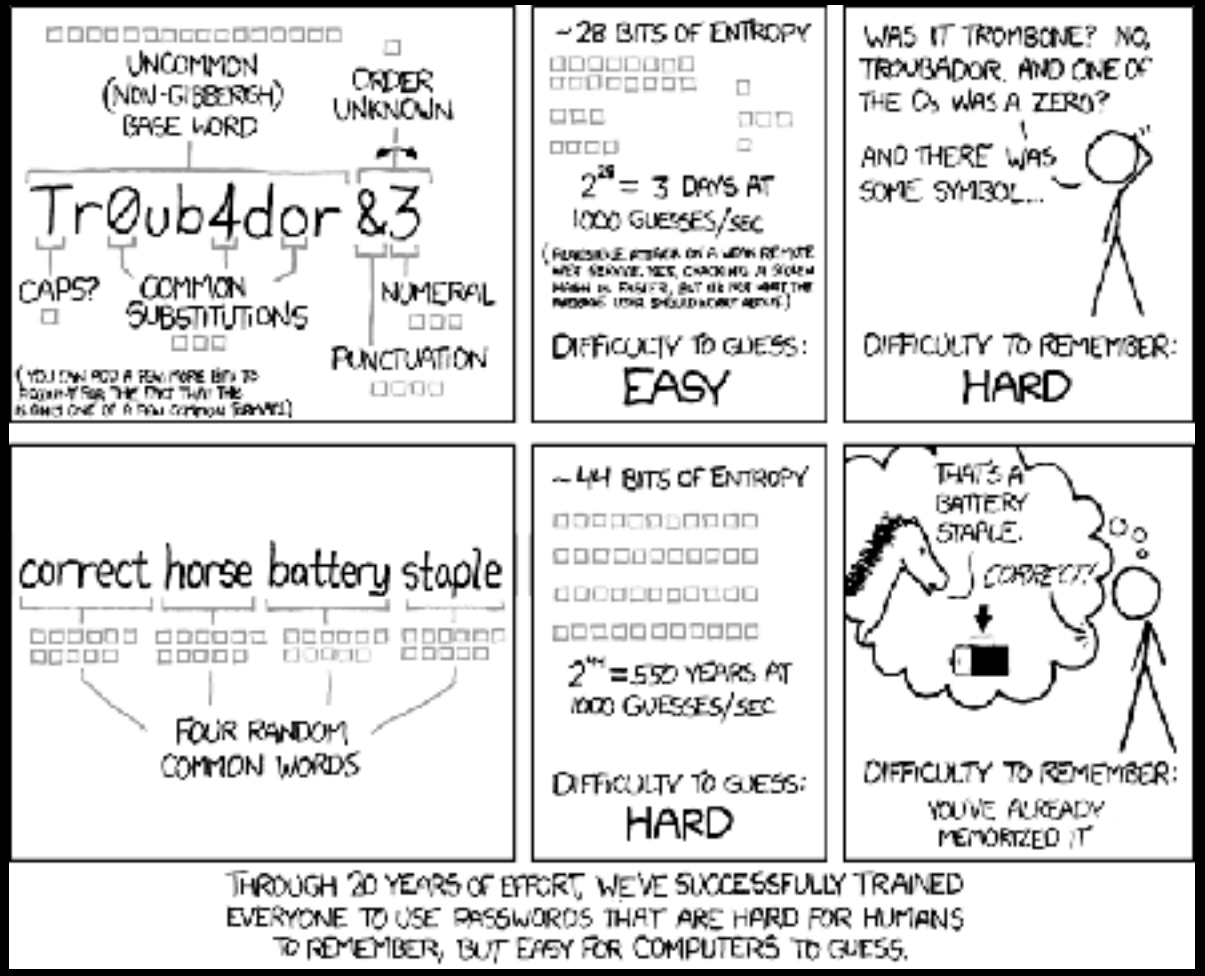
- What
  - Use a password that is long and contains randomized alpha characters, numbers and special characters
  - Does not contain common words in the dictionary
- Why/How does it reduce risk?
  - More difficult for attackers (threat agents) to guess, and, historically, brute force
  - Prevent unauthorized access

#3: Strong Passwords

- Even more important than complexity is length

3 to 4 additional characters has the same entropy (number of possible combinations) as passwords using a more complex set of characters

#3: Strong Passwords



https://xkcd.com/936/

#3: Strong Passwords

But wait!

#3: Strong Passwords

What if we COMBINE them?!

#3: Strong Passwords

Your new password!

MF>E,D4,C!q^m,uSwVh.[2AD+JHsM^6}

Assuming one hundred billion guesses per second will take 6.22 million trillion trillion trillion centuries to brute force

#3: Strong Passwords

- They need to be unique, **for every account, on every site**
  - As of 2017, 7 **billion** credentials have been leaked/exposed
  - Credential stuffing

#3: Strong Passwords

"R=.b8q%P5(fR74cZd3n<srtE?6c{X%`

$;@(:B&%hY^gt&QHV7t.4}y2:nnED:fe

Ah=4Rp9gb{zb5qW!`:K;5=R6]nDXD'PM

?fF*c,Xk&B<`WsCeeVLPNp{*/n5Nn4bC

ZkD=w{)PKG`<Z8*{)&RdjV{$XZ#L:RnA

7E?#!+5+b){CyM,p@r.U;WW6sFM%%5j"

b-46dy+=V-_Vu-8tU=k.*]Ne%/5k2D#e

#3: Strong Passwords

- Use a password manager
- No, really: use a password manager
- Enforce strong, unique passwords for **everyone**
  - Integrate with your institution's single-sign-on system
- Use a strong, *unique,* and **long** password **everywhere**, not just in WordPress

#3: Keep Themes/Plugins Up-to-date

- Why/How does it reduce risk?
  - Similar to WordPress core updates, plugin and theme updates can also contain security fixes, removing potential vulnerabilities
- Bonus points
  - Know what you have installed and **why** you have it installed
  - Remove those that are no longer in use (#6t)
  - Limit your plugin/theme use (#13t)

#4: Hosting Provider

If WordPress is the brain, and your content the heart and soul of your site…

…the hosting provider is the rest of the body

#4: Hosting Provider

- Why
  - Doesn't matter how well you've secured WordPress, if the host is compromised
  - Remains one of the top vectors for compromised sites
- Security principles :
  - *Don't use components with known vulnerabilities*
  - *Establish Secure Defaults / Fail safely*
  - *Separation of Duties/Segmentation*
- Bonus points
  - Know what your host is running and what versions they have installed
  - Engage with the team responsible for hosting and work with them to keep the stack up-to-date

#5: Limit Login Attempts

- What
  - Locks an account or blocks an IP address after so many failed attempts
- Why/How does it reduce risk?
  - Threat is unauthorized access
  - Vulnerability is a weak/common password
  - Reduces the ability of the threat agent to exploit the vulnerability
  - Security principle: *Minimize the attack surface*

What is “Attack Surface”?

- The sum of all paths for data/commands into and out of the application
- Plus all of the code that protects those paths
- Plus all of the data used in the application
- Plus all of the code that protects this data

What is “Attack Surface”?

#5: Limit Login Attempts

- What
  - Locks an account or blocks an IP address after so many failed attempts
- Why/How does it reduce risk?
  - Slows down an attacker from brute forcing/credential stuffing
  - Frees up your site resources
- Bonus points
  - Ensure the method you're using takes into account XMLRPC

#5: Default Credentials

- What
  - Remove or rename the default “admin” account
- Why/How does it reduce risk?
  - In automated attacks, attackers will typically start with the admin account
- Bonus points
  - Remove account enumeration

#6: Two/Multi-Factor Authentication

- What
  - Adds a secondary (or multiple) step that must be completed in order to authenticate
- Why/How does it reduce risk?
  - Adds an extra layer of defense against authentication attacks
  - Security principle: *Defense-in-depth*

#6: File/Directory Permissions

- What
  - Ensure that files and directories are set to the lowest access necessary
- Why/How does it reduce risk?
  - Improper permissions allow an attacker to access restricted files or directories and potentially modify or delete their contents
- Security principle : *least privilege*

Principle of Least Privilege

- Grant necessary permissions required to perform the intended activities
- For a limited time
- But with the *minimum* rights required for the task(s)
- Removing permissions when no longer needed

#6: File/Directory Permissions

- Bonus points
  - Lock down all area of WordPress to read-only except for those areas that specifically require the ability to write
  - Ideally, only the wp-content/uploads directory is writable, and then only writeable by the php process
  - If your environment allows it, set files to only readable (0400) by the owner of the process that php runs under

#6:Remove Unused Themes/Plugins/Users

- What
  - Remove everything that isn't in active use
- Why/How does it reduce risk?
  - Even if a plugin/theme is disabled, the files are still there and are publicly accessible
  - A non-active user is one more account that can be compromised
  - Removes potential vulnerabilities
- Bonus points
  - Make plugin, theme and user audits a routine

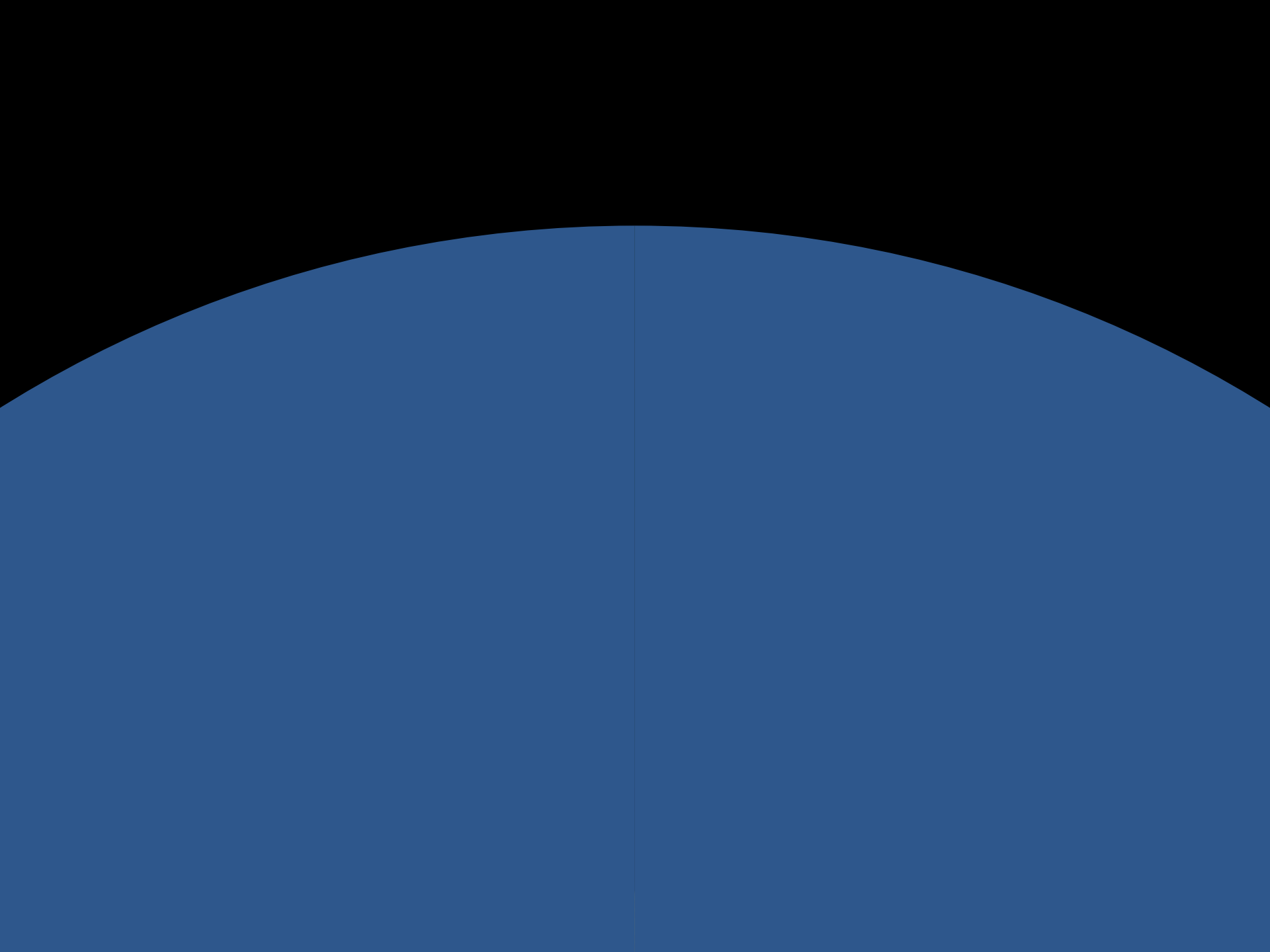
#7: Protect WP-Config.php

- What
  - Add rules to prevent direct access
  - move the file somewhere not publicly accessible
- Why
  - Contains your database credentials and salts
  - Prevents accidental exposure of those assets
- Bonus points
  - Set file permissions to 0400*
  - See #4 Hosting Provider

#7: Protect/Limit Access to Login/Admin Areas

- What
  - Add an extra layer of protection to the login area
    - Basic Access Authentication
    - Captcha
- Why/How does it reduce risk?
  - Similar to 2FA/MFA in that it adds an extra layer
- Security principle: *Minimize attack surface* and *Defense-in-Depth*
- Bonus points
  - Limit access to the login/admin areas to specific IP ranges

64.85.59.68 —> 64.85.0.0/16



#7: Protect/Limit Access to Login/Admin Areas

- Bonus points
  - Limit access to the login/admin areas to specific IP ranges
  - Require users to use a Virtual Private Network
  - Disable XMLRPC if not in use, or limit access to known network ranges

#7: Limit User Roles

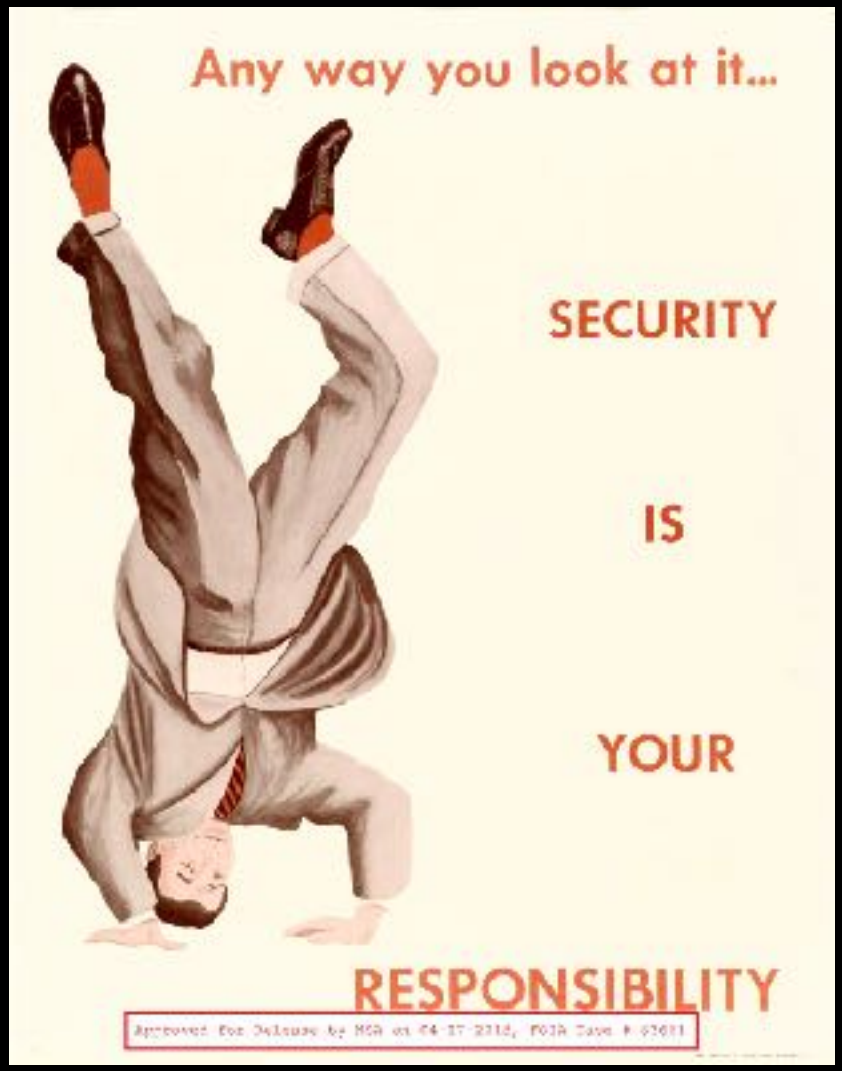
- What
  - Give users the lowest possible role that allows them to complete their tasks
  - Only login with a higher privileged account when performing actions that require elevated privileges
- Security principle: Least privilege
- Why/How does it reduce risk?
  - Minimizes the damage if an account is compromised
  - Reduces the opportunity for a rogue user to inflict damage
  - Reduces the opportunity for someone to make a mistake

#7: Limit User Roles

- Bonus points
  - Create or add custom roles that give you the ability to be more granular with permissions
  - Do routine account audits and remove permissions/roles from accounts that don’t require them

#7: Use a Security Plugin

- What
  - Install a plugin that has been designed to implement multiple “best measures”
- Why/How does it reduce risk?
  - Can make it easier to implement multiple security measures
  - Useful if you’re not comfortable with some of the actions
  - Auditing, Detection, Prevention



#8: Disable File Editing

- What
  - Disable the built-in Theme and Plugin file editor
- Why/How does it reduce risk?
  - Prevents a user from altering Theme/Plugin code from the WordPress dashboard
  - Security principle: *Minimize attack surface*

#9: Trusted Sources

- What
  - Don’t obtain plugins/themes from unknown sources
- Why
  - Code may have been altered/infected

#9: Implement SSL

- What
  - Add a SSL/TLS certificate to your site
- Why/How does it reduce risk?
  - Encrypts the data as it is transferred between your site and the end user
- Security principle: *Minimize attack surface*
- Bonus steps
  - Enforce https over the *entire* site, not just login areas and wp-admin

#10: Do Your Homework on Theme/Plugin Selection

- What
  - Research a theme/plugin before installing
- Why/How does it reduce risk?
  - Every piece of code you add to your system increases your attack surface
  - Every piece of code you add to your system has the potential to introduce new exploitable vulnerabilities

#10: Do Your Homework on Theme/Plugin Selection

"WHAT MAKES WORDPRESS SO INSECURE IS THAT IT'S HIGHLY EXTENSIBLE AND EASY TO USE; WORDPRESS SECURITY ISSUES REVOLVE ALMOST ENTIRELY AROUND THIS EXTENSIBILITY AND EASINESS OF USE."

Tony Perez, @perezbox

#10: Do Your Homework on Theme/Plugin Selection

- What
  - Research a theme/plugin before installing
- Why/How does it reduce risk?
  - Every piece of code you add to your system increases your attack surface
  - Every piece of code you add to your system has the potential to introduce new exploitable vulnerabilities
  - Security principle: Be paranoid, be skeptical

#10: Do Your Homework on Theme/Plugin Selection

~~Jessica~~ Paul, your paranoia is exhausting

#10: Do Your Homework on Theme/Plugin Selection

- Security principle: *Treat all third party code/data as tainted and hostile*
- Bonus steps
  - https://wpvulndb.com/
  - https://php-grinder.com/
  - Run third party code through PHP-CS Security Audit
  - Run local static code analysis

#11

- Web Application Firewall
- Move/Hide Login Location
- Routine Security Scan
- Log actions/activities
- Secure your local machine

Items I believe should be higher in the list

- Block PHP execution (#14t)
- Logging (#11t)
- Segmentation/Isolation (separation of duties)
- Be selective with XMLRPC
  - Remove software/services that aren't actively used
- Limit the number of plugins you use (#13t)
- Monitor for file changes (#12t)
- Stay informed!

Summary

- Always be thinking in terms of how you can reduce risk
- Minimize attack surface area
- Principle of least privilege
- Defense in depth
- Don’t use components with known vulnerabilities
- Be paranoid, be skeptical
  - Treat all third party code/data as tainted and hostile
- Security is a continual process; you’re never “finished”

Paul Gilzow

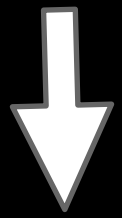
- Programmer/Analyst / Security Analyst at the University of Missouri
- Contact
  - gilzow@missouri.edu
  - @gilzow on twitter
  - https://http://fb.me/gilzow
  - https://profiles.wordpress.org/gilzow
- Slides: https://github.com/gilzow/whatwhywordpress/

Questions

WHAT QUESTIONS DO YOU HAVE FOR ME?

The What and Why of WordPress Security

Please be sure to submit session feedback through the WPCampus website. Not only will you earn additional points toward the conference game, you'll also be entered to win a door prize!



https://2018.wpcampus.org/schedule/security-chat-for-everyone/