

BEYOND THE BASICS

TAKING THE NEXT STEPS IN SECURING YOUR SITE

Paul Gilzow

gilzow@missouri.edu

Twitter: @gilzow

Facebook: <https://fb.com/gilzow>

<https://www.linkedin.com/in/gilzow>

BEYOND THE BASICS

TAKING THE NEXT STEPS IN SECURING YOUR SITE

Paul Gilzow

gilzow@missouri.edu

Twitter: @gilzow

Facebook: <https://fb.com/gilzow>

<https://www.linkedin.com/in/gilzow>

TL;DSWTGMC SUMMARY

(Too Long; Didn't Stay, Went to Get More Coffee)

- ▶ Implicitly Deny
- ▶ Defense-in-Depth

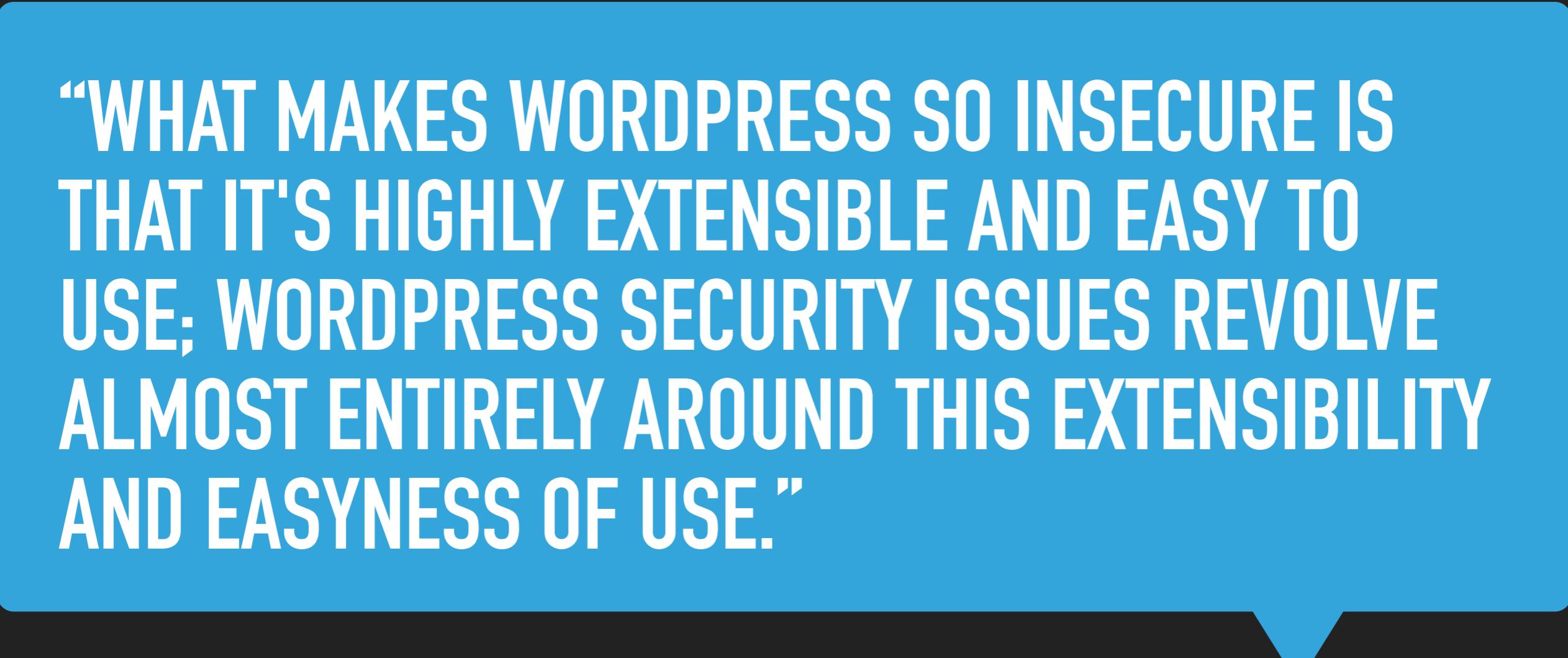
WHY DO ATTACKERS TARGET YOU

- ▶ Your site resources
- ▶ Your domain
- ▶ Your SEO reputation
- ▶ Your visitors

WHY WORDPRESS IS AN ATTRACTIVE TARGET

- ▶ Market share
- ▶ Open Source
- ▶ Extremely easy to set up and get running, not so easy to secure
- ▶ Anyone can create and submit a theme/plugin

“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 EASYNESS OF USE.”



Tony Perez, @perezbox

CURRENT STATE OF WORDPRESS SECURITY

- ▶ Most compromises occur through
 - ▶ vulnerable plugins and themes
 - ▶ Weak passwords
 - ▶ Wordpress out-of-date

**AS AN OWNER/MAINTAINER OF A
WORDPRESS SITE, IT IS YOUR
RESPONSIBILITY TO BE PARANOID**

SO WHAT DO WE DO?

DEFENSE-IN-DEPTH



WPSCAN

Passive (non-intrusive) Scan

- ▶ Robots.txt
- ▶ Interesting headers
- ▶ Multisite
- ▶ Must-use plugins
- ▶ Xml-rpc
- ▶ Wordpress version
- ▶ Plugins/themes

WPSCAN

Active scan

- ▶ Scans for signs of vulnerable plugins
- ▶ Scans for signs of vulnerable themes
- ▶ Scans for signs of timthumb
- ▶ Attempts to enumerate user account names

vagrantpress.dev/wp-admin/users.php

Apps Bookmarks reboots home access-denied work accessdenied 20160723 Other Bookmarks

Access Denied 3 0 + New Howdy, Access Denied Admin

Dashboard Posts Media Pages Comments Appearance Plugins 3 Users

All (5) | Administrator (1) | Editor (1) | Author (1) | Contributor (1) | Subscriber (1)

Screen Options Help

Users Add New

	Username	Name	Email	Role	Posts
<input type="checkbox"/>	admin	Paul Gilzow	gilzow@missouri.edu	Administrator	1
<input type="checkbox"/>	gilzow-author	Paul-Author Gilzow	paul@gilzow.com	Author	1
<input type="checkbox"/>	gilzow-contributor	Paul-Contributor Gilzow	paul.gilzow@gmail.com	Contributor	0
<input type="checkbox"/>	gilzow-editor	Paul-Editor Gilzow	gilzowp@missouri.edu	Editor	1
<input type="checkbox"/>	gilzow-subscriber	Paul-Subscriber Gilzow	wkdirauth@gilzow.com	Subscriber	0

Bulk Actions Apply Change role to... Change

5 items

Username Name Email Role Posts

5 items

Thank you for creating with WordPress.

vagrantpress.dev/wp-admin/users.php Version 4.7.2

vagrantpress.dev/wp-admin/edit.php

Apps Bookmarks reboots home access-denied work accessdenied 20160723 Other Bookmarks

Access Denied 2 0 + New Howdy, Access Denied Admin

Dashboard

Posts Add New

All (3) | Mine (1) | Published (3)

Bulk Actions Apply All dates All Categories Filter 3 items

		Author	Categories	Tags	Date
<input type="checkbox"/>	Title				
<input type="checkbox"/>	Author first post	Paul-Author Gilzow	Uncategorized	—	Published 2016/07/01
<input type="checkbox"/>	Editor very first post	Paul-Editor Gilzow	Uncategorized	—	Published 2016/07/01
<input type="checkbox"/>	Hello world!	Access Denied Admin	Uncategorized	—	1 Published 2013/01/22
<input type="checkbox"/>	Title	Author	Categories	Tags	Date

Bulk Actions Apply 3 items

Thank you for creating with [WordPress](#). Version 4.7.2

← → C vagrantpress.dev/wp-admin/plugins.php

Apps Bookmarks reboots home access-denied work accessdenied 20160723 Other Bookmarks

Access Denied 2 0 + New Howdy, Access Denied Admin

Dashboard Posts Media Pages Comments Appearance Plugins 2

All (8) Active (1) Inactive (7) | Update Available (2)

Search installed plugins... 8 items

Bulk Actions Apply

<input type="checkbox"/> Plugin	Description
<input type="checkbox"/> Akismet Anti-Spam	Used by millions, Akismet is quite possibly the best way in the world to protect your blog from spam. It keeps your site protected even while you sleep. To get started: activate the Akismet plugin and then go to your Akismet Settings page to set up your API key. Activate Edit Delete Version 3.3 By Automattic View details
<input type="checkbox"/> Anti-Recon	Attempts to prevent recon data gathering Deactivate Edit Version 0.0.1 By WpCampus
<input type="checkbox"/> Aspose Cloud eBook Generator	Aspose Cloud eBook Generator is a plugin for exporting content from Posts/Pages and then downloading it in desired format. Activate Edit Delete Version 2.0 By Fahad Adeel View details
<input type="checkbox"/> Download Manager	Manage, track and control file download from your WordPress site Activate Edit Delete Version 2.6.96 By Shaon View details
There is a new version of Download Manager available. View version 2.9.44 details or update now.	
<input type="checkbox"/> Gravity Forms	Easily create web forms and manage form entries within the WordPress admin. Activate Edit Delete Version 1.9.10.2 By rocketgenius Visit plugin site
<input type="checkbox"/> Hello Dolly	This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong: Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page. Activate Edit Delete Version 1.6 By Matt Mullenweg View details

VirtualBox-5.0.32-11...dmg Show All X

```
gilzow@kali:~$ sudo wpscan --url vagrantpress.dev --enumerate vp --random-agent
```



WordPress Security Scanner by the WPScan Team

Version 2.9.2

Sponsored by Sucuri - <https://sucuri.net>

@WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_

```
[+] URL: http://vagrantpress.dev/
```

```
[+] Started: Tue Mar 14 12:09:30 2017
```

```
[+] robots.txt available under: 'http://vagrantpress.dev/robots.txt'
```

```
[!] The WordPress 'http://vagrantpress.dev/readme.html' file exists exposing version number
```

```
[!!] A wp-config.php backup file has been found in: 'http://vagrantpress.dev/wp-config.php.bak'
```

```
[+] Interesting header: LINK: <http://vagrantpress.dev/wp-json/>; rel="https://api.w.org/"
```

```
[+] Interesting header: SERVER: Apache/2.4.7 (Ubuntu)
```

```
[+] XML-RPC Interface available under: http://vagrantpress.dev/xmlrpc.php
```

```
[+] WordPress version 4.7.3 (Released on 2017-03-06) identified from meta generator, links opml
```

```
[+] WordPress theme in use: twentyseventeen - v1.1
```

```
[+] Name: twentyseventeen - v1.1
```

```
| Latest version: 1.1 (up to date)
```

```
| Location: http://vagrantpress.dev/wp-content/themes/twentyseventeen/
```

```
| Readme: http://vagrantpress.dev/wp-content/themes/twentyseventeen/readme.txt
```

```
| Style URL: http://vagrantpress.dev/wp-content/themes/twentyseventeen/style.css
```

```
| Theme Name: Twenty Seventeen
```

```
| Theme URI: https://wordpress.org/themes/twentyseventeen/
```

```
| Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a...
```

```
| Author: the WordPress team
```

```
| Author URI: https://wordpress.org/
```

```
[+] Enumerating installed plugins (only ones with known vulnerabilities) ...
```

```
Time: 00:01:18 <===== (1437 / 1437) 100.00% Time: 00:01:18
```

```
[+] We found 5 plugins:
```

vagrantpress.dev/wp-admin/plugins.php

Access Denied 2 0 + New Howdy, Access Denied Admin

Dashboard Posts Media Pages Comments Appearance Plugins 2

All (8) Active (1) Inactive (7) | Recently Active (2) | Update Available (2)

Screen Options Help

Search Installed Plugins 8 items

Plugin Description

Akismet Used by millions, Akismet is quite possibly the best way in the world to protect your blog from spam. It keeps your site protected even while you sleep. To get started: 1) Click the "Activate" link to the left of this description, 2) Sign up for an Akismet plan to get an API key, and 3) Go to your Akismet configuration page, and save your API key.

Version 3.1.11 | By Automattic | View details

Anti-Recon Attempts to prevent recon data gathering

Version 0.0.1 | By WpCampus

Aspose Cloud eBook Generator Aspose Cloud eBook Generator is a plugin for exporting content from Posts/Pages and then downloading it in desired format.

Version 2.0 | By Fahad Adeel | View details

Download Manager Manage, track and control file download from your WordPress site

Version 2.6.96 | By Shaon | View details

There is a new version of Download Manager available. [View version 2.8.98 details](#) or update now.

Gravity Forms Easily create web forms and manage form entries within the WordPress admin.

Version 1.9.10.2 | By rocketgenius | Visit plugin site

Hello Dolly This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong: Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page.

Version 1.6 | By Matt Mullenweg | View details

```
[+] Name: download-manager v2.6.96
| Location: http://vagrantpress.dev/wp-content/plugins/download-manager/
| README: http://vagrantpress.dev/wp-content/plugins/download-manager/readme.txt
[!] The version is out of date, the latest version is 2.8.98

[!] Title: Download Manager <= 2.7.4 - Code Execution / Remote File Inclusion
Reference: https://wpvulndb.com/vulnerabilities/7700
Reference: http://blog.sucuri.net/2014/12/security-advisory-high-severity-wordpress-download-manager.html
Reference: https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_downloadmanager_upload
Reference: https://www.exploit-db.com/exploits/35533/
[i] Fixed in: 2.7.5

[!] Title: Download Manager 2.7.2 - Privilege Escalation
Reference: https://wpvulndb.com/vulnerabilities/7827
Reference: http://security.szurek.pl/wordpress-download-manager-272-privilege-escalation.html
Reference: http://packetstormsecurity.com/files/130690/
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9260
Reference: https://www.exploit-db.com/exploits/36301/
[i] Fixed in: 2.7.3

[!] Title: WordPress Download Manager <= 2.7.94 - Authenticated Stored XSS
Reference: https://wpvulndb.com/vulnerabilities/8101
Reference: https://plugins.trac.wordpress.org/changeset/1199505/download-manager
Reference: http://packetstormsecurity.com/files/132716/
[i] Fixed in: 2.7.95

[!] Title: WordPress Download Manager <= 2.8.7 - Multiple Vulnerabilities
Reference: https://wpvulndb.com/vulnerabilities/9265
Reference: http://www.protect.net/blog/wordpress-download-manager-2-8-8-critical-security-vulnerabilities
Reference: http://www.wpdownloadmanager.com/wordpress-download-manager-security-maintenance-release/
[i] Fixed in: 2.8.8

[+] Name: gravityforms
| Location: http://vagrantpress.dev/wp-content/plugins/gravityforms/

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: Gravity Forms <= 1.8.19 - Arbitrary File Upload
Reference: https://wpvulndb.com/vulnerabilities/7820
Reference: http://blog.sucuri.net/2015/02/malware-clean-up-to-arbitrary-file-upload-in-gravity-forms.html
Reference: http://www.gravityhelp.com/gravity-forms-v1-8-20-released/
[i] Fixed in: 1.8.20

[!] Title: Gravity Forms 1.8 <= 1.9.3.5 - Authenticated Blind SQL Injection
```

```
[+] Name: wp-mobile-detector - v2.7
| Location: http://vagrantpress.dev/wp-content/plugins/wp-mobile-detector/
| Readme: http://vagrantpress.dev/wp-content/plugins/wp-mobile-detector/readme.txt
[!] The version is out of date, the latest version is 3.7
[!] Title: WP Mobile Detector <= 3.2 - Stored Cross-Site Scripting (XSS)
Reference: https://wpvulndb.com/vulnerabilities/8059
Reference: https://research.g0blin.co.uk/g0blin-00050/
[i] Fixed in: 3.3
[!] Title: WP Mobile Detector <= 3.5 - Arbitrary File Upload
Reference: https://wpvulndb.com/vulnerabilities/8505
Reference: https://blog.sucuri.net/2016/06/wp-mobile-detector-vulnerability-being-exploited-in-the-wild.html
Reference: https://www.pluginvulnerabilities.com/2016/05/31/arbitrary-file-upload-vulnerability-in-wp-mobile-detector/
Reference: https://wordpress.org/plugins/wp-mobile-detector/changelog/
[i] Fixed in: 3.6
[+] Finished: Wed Mar 1 17:03:57 2017
[+] Requests Done: 1513
[+] Memory used: 142.25 MB
[+] Elapsed time: 00:01:24
gilzow@kali:~$
```


COUNTER MEASURES

- ▶ Prevent php execution in /wp-content/uploads/

```
#we dont want to allow access directly to any php files
<FilesMatch "\.(?i:php)$">
    <IfModule !mod_authz_core.c>
        Order allow,deny
        Deny from all
    </IfModule>
    <IfModule mod_authz_core.c>
        Require all denied
    </IfModule>
</FilesMatch>
```

COUNTER MEASURES

- ▶ Prevent php execution in /wp-content/uploads/
- ▶ Protect wp-content completely
 - ▶ Not only prevent php execution, but
 - ▶ Implicit deny (only allow what is necessary and expected)

```
RewriteEngine On

#allow images jpg,jpeg,gif,png,svg,bmp,ico
RewriteCond %{REQUEST_URI} !\.(?i:jpe?g|gif|png|svg|bmp|ico)$ [NC]

#allow js, css and fonts
RewriteCond %{REQUEST_URI} !\.(?i:css|js|eot|ttf|woff|woff2)$ [NC]

# allow documents: pdf, doc, docx, xls, xlsx, pps, ppsx, ppt, pptsx, psd, odt, key
RewriteCond %{REQUEST_URI} !\.(?i:pdf|docx?|xlsx?|pp[st]x?|psd|odt|key)$ [NC]

# allow audio, video: mp2, mp3, mp4, mp5, mpg, m4a, m4v, ogg, ogv, wav, mov, wma, wmv, avi, 3gp, 3g2
RewriteCond %{REQUEST_URI} !\.(?i:mp[2-5g]|m4[av]|og[gv]|wav|mov|wm[av]|avi|3g[p2])$ [NC]

#allow data
RewriteCond %{REQUEST_URI} !\.(?i:xml|json)$ [NC]

RewriteRule .* - [F,L]
```

```
RewriteEngine On
ErrorDocument 403 /404

#Don't allow screenshots
RewriteCond %{REQUEST_URI} screenshot(?:\-\d+)?\.(?:jpe?g|png|gif)$ [NC,OR]

#uncomment if you have a specific file you need
RewriteCond %{REQUEST_URI} !plugins/baz/foo\.php$ [NC]

#allow images jpg,jpeg,gif,png,svg,bmp,ico
RewriteCond %{REQUEST_URI} !\.(?i:jpe?g|gif|png|svg|bmp|ico)$ [NC]

#allow js, css and fonts
RewriteCond %{REQUEST_URI} !\.(?i:css|js|eot|ttf|woff|woff2)$ [NC]

# allow documents: pdf, doc, docx, xls, xlsx, pps, ppsx, ppt, pptx, psd, odt, key
RewriteCond %{REQUEST_URI} !\.(?i:pdf|docx?|xlsx?|pp[st]x?|psd|odt|key)$ [NC]

# allow audio, video: mp2, mp3, mp4, mp5, mpg, m4a, m4v, ogg, ogv, wav, mov, wma, wmv, avi, 3gp, 3g2
RewriteCond %{REQUEST_URI} !\.(?i:mp[2-5g]|m4[av]|og[gv]|wav|mov|wm[av]|avi|3g[p2])$ [NC]

#allow data
RewriteCond %{REQUEST_URI} !\.(?i:xml|json)$ [NC]

RewriteRule .* - [F,L]
```

```
gilzow@kali:~$ sudo wpscan --url vagrantpress.dev --enumerate vp --random-agent
```



WordPress Security Scanner by the WPScan Team
Version 2.9.2

Sponsored by Sucuri - <https://Sucuri.net>
 @_WPScan_, @_ethicalhack3r, @_erwan_lr, pvdL, @_FireFart_

```
The plugins directory 'wp-content/plugins' does not exist.  
You can specify one per command line option (don't forget to include the wp-content directory if needed)  
[?] Continue? [Y]es [N]o, default. [N]  
Y  
[+] URL: http://vagrantpress.dev/  
[+] Started: Wed Mar 22 09:14:42 2017  
  
[+] robots.txt available under: 'http://vagrantpress.dev/robots.txt'  
[!] The WordPress 'http://vagrantpress.dev/readme.html' file exists exposing a version number  
[!] A wp-config.php backup file has been found in: 'http://vagrantpress.dev/wp-config.php.bak'  
[+] Interesting header: LINK: <http://vagrantpress.dev/wp-json/>; rel="https://api.w.org/"  
[+] Interesting header: SERVER: Apache/2.4.7 (Ubuntu)  
[+] XML-RPC Interface available under: http://vagrantpress.dev/xmlrpc.php  
  
[+] WordPress version 4.7.3 (Released on 2017-03-06) identified from meta generator, links opml  
  
[+] WordPress theme in use: twentyseventeen - v1.1  
  
[+] Name: twentyseventeen - v1.1  
| Latest version: 1.1 (up to date)  
| Location: http://vagrantpress.dev/wp-content/themes/twentyseventeen/  
| Style URL: http://vagrantpress.dev/wp-content/themes/twentyseventeen/style.css  
| Theme Name: Twenty Seventeen  
| Theme URI: https://wordpress.org/themes/twentyseventeen/  
| Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a...  
| Author: the WordPress team  
| Author URI: https://wordpress.org/  
  
[+] Enumerating installed plugins (only ones with known vulnerabilities) ...  
  
Time: 00:01:19 <===== (1443 / 1443) 100.00% Time: 00:01:19  
[-] No plugins found
```

COUNTER MEASURES

- ▶ Protect wp-content
 - ▶ Prevent php execution
 - ▶ Implicit deny (only allow what is necessary and expected)
- ▶ Protect wp-includes

```
RewriteEngine On
RewriteCond %{REQUEST_URI} !(?:wp-tinymce|ms-files)\.php$ [NC]
RewriteCond %{REQUEST_URI} \.php$ [NC]
RewriteRule .* - [F,L]
```

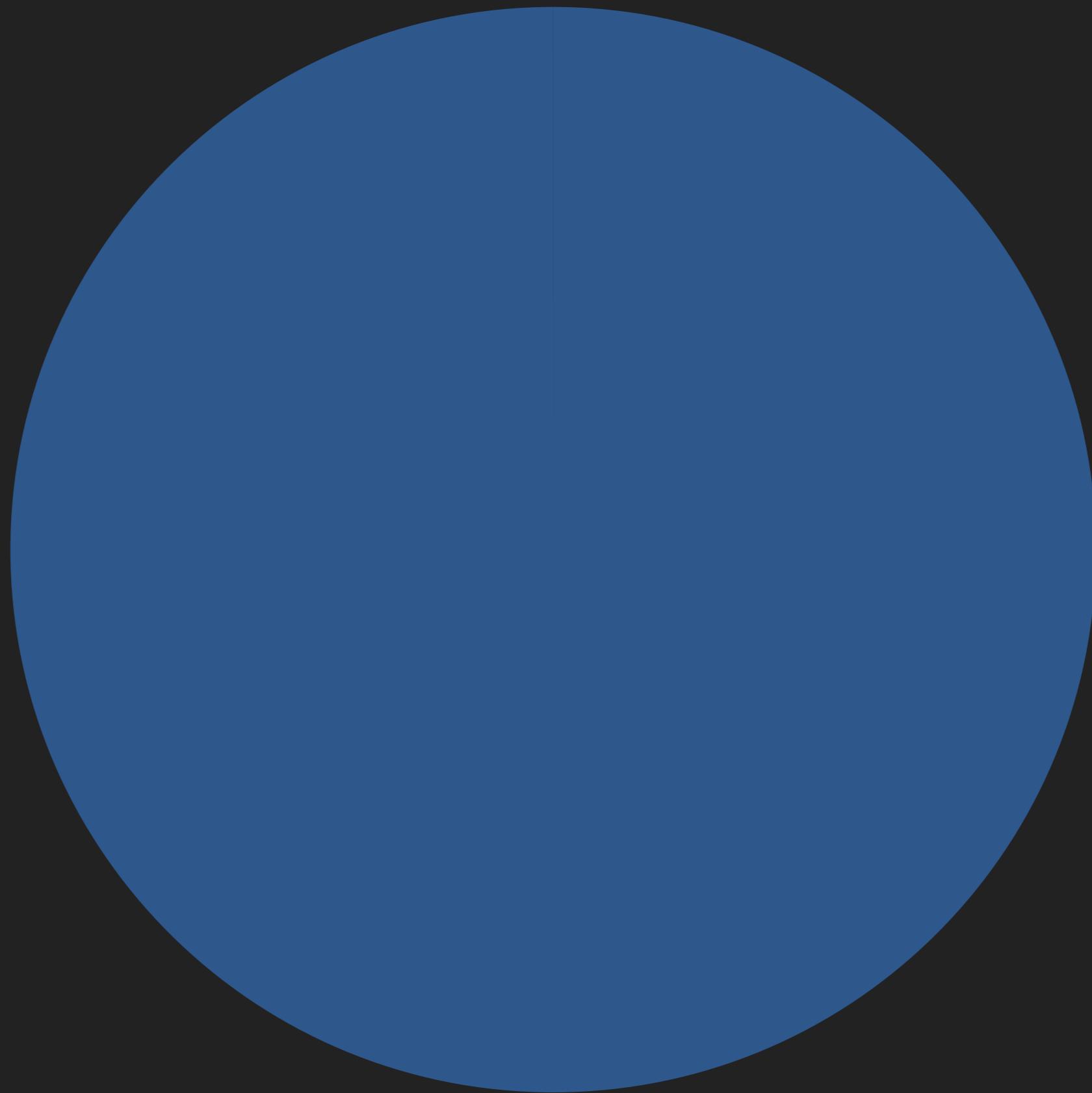
COUNTER MEASURES

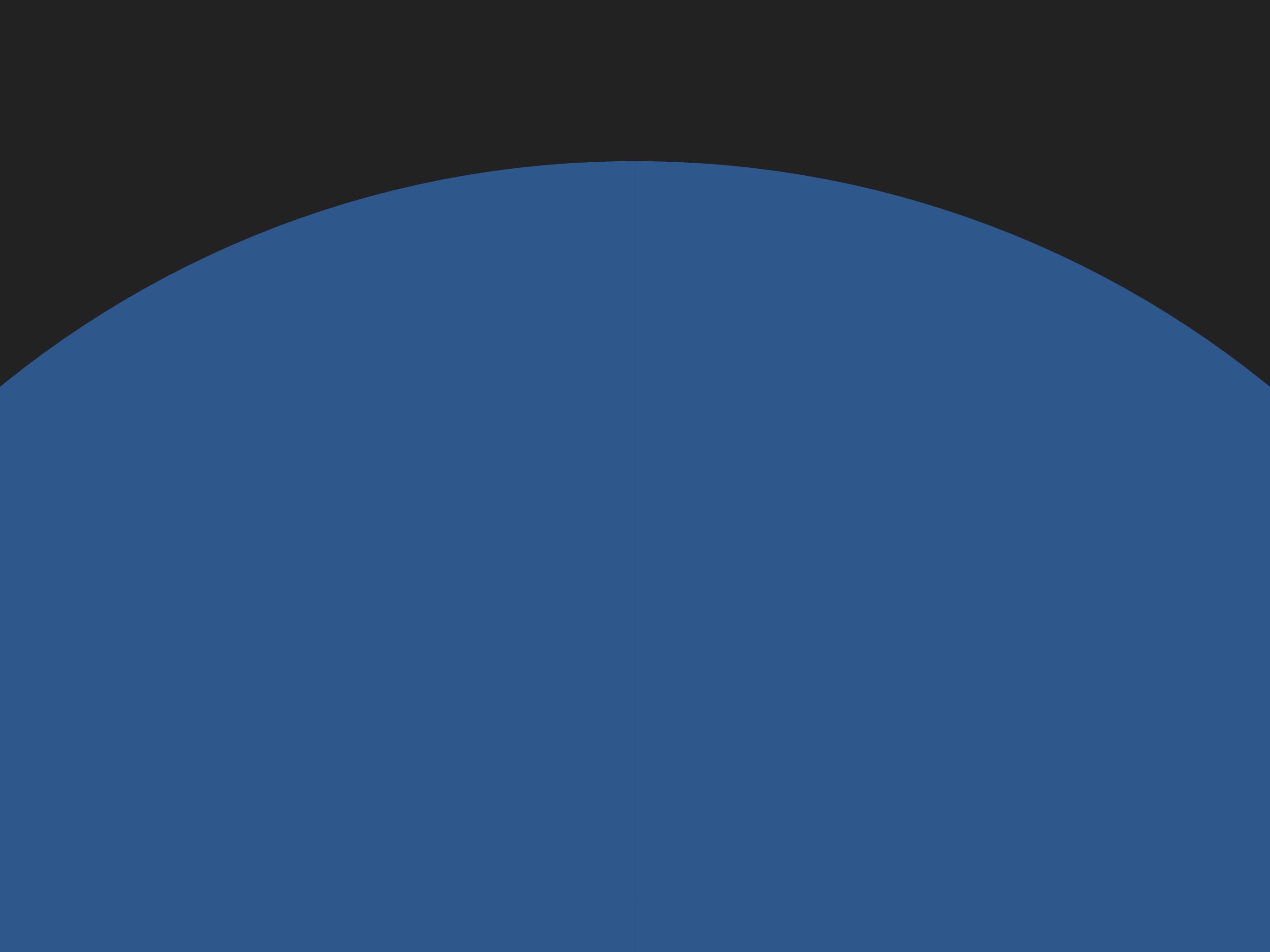
- ▶ Protect wp-content
 - ▶ Prevent php execution
 - ▶ Implicit deny (only allow what is necessary and expected)
- ▶ Protect wp-includes
- ▶ Protect wp-admin

```
# ideally, only allow access to those ip address/ranges that should have access
<FilesMatch ".*">
    <IfModule !mod_authz_core.c>
        deny from all
        allow from 128.206.
        allow from 161.130.
        allow from 10.7.
    </IfModule>
    <IfModule mod_authz_core.c>
        Require ip 128.206.
        Require ip 161.130.
        Require ip 10.7.
    </IfModule>
</FilesMatch>

#except for admin-ajax which needs to be accessible publicly
<Files admin-ajax.php>
    <IfModule !mod_authz_core.c>
        allow from all
    </IfModule>
    <IfModule mod_authz_core.c>
        Require all granted
    </IfModule>
</FilesMatch>
```

64.85.59.68 → 64.85.0.0/16





COUNTER MEASURES

- ▶ Protect wp-content
 - ▶ Prevent php execution
 - ▶ Implicit deny (only allow what is necessary and expected)
- ▶ Protect wp-includes
- ▶ Protect wp-admin
- ▶ Protect the root

```
# block access to login page from all external addresses
<Files wp-login.php>
    <IfModule !mod_authz_core.c>
        order allow,deny
        deny from all
        allow from 128.206.
        allow from 161.130.
        allow from 10.7.
    </IfModule>
    <IfModule mod_authz_core.c>
        Require ip 128.206.0.0/16
        Require ip 161.130.0.0/16
        Require ip 10.7.0.0/16
    </IfModule>
</Files>

# completely disable xmlrpc, block external access to readme and license
<FilesMatch "^(xmlrpc\.php|readme\.html|license\.txt)$">
    <IfModule !mod_authz_core.c>
        Order allow,deny
        Deny from all
    </IfModule>
    <IfModule mod_authz_core.c>
        Require all denied
    </IfModule>
</FilesMatch>
```

SUMMARY

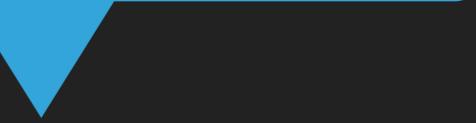
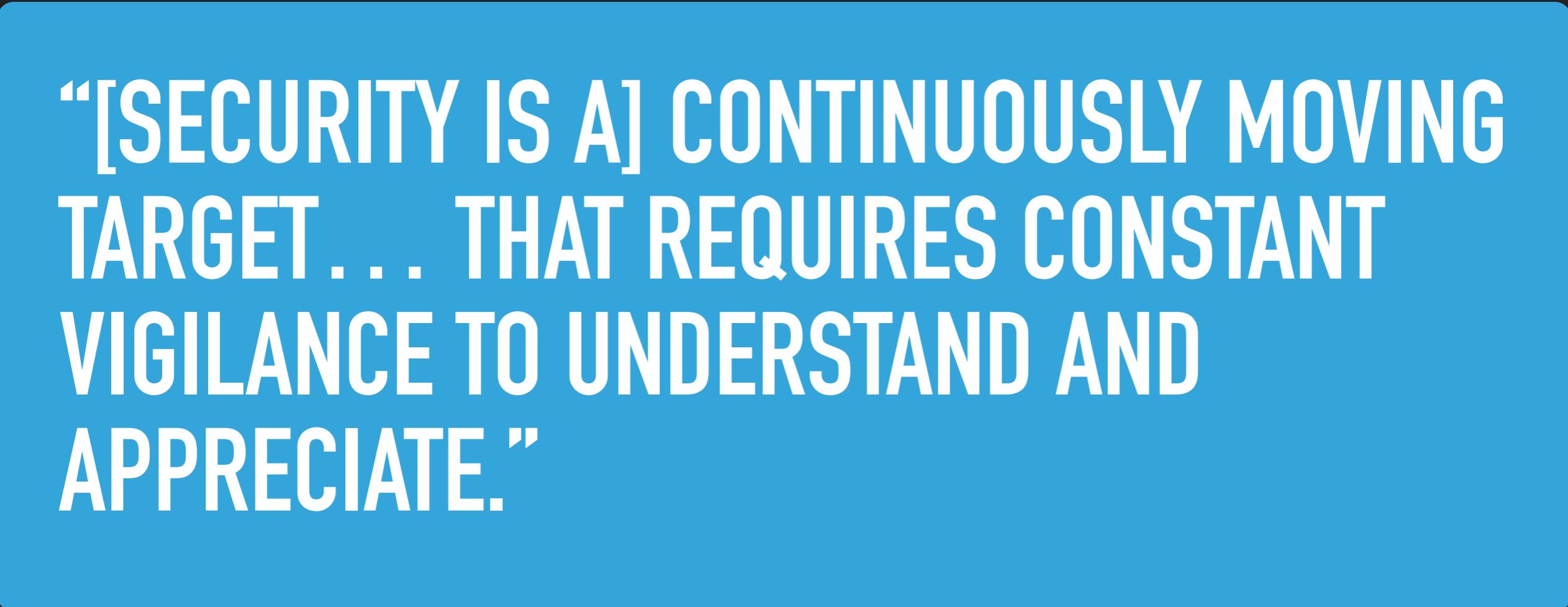
- ▶ Be paranoid; be skeptical
- ▶ Uninstall plugins/themes that aren't in use
- ▶ Disable php from executing where it shouldn't
- ▶ Limit access to **everything** where you can

SUMMARY CONT.

In other words...

- ▶ Implicitly deny
- ▶ Defense-in-depth

“[SECURITY IS A] CONTINUOUSLY MOVING TARGET... THAT REQUIRES CONSTANT VIGILANCE TO UNDERSTAND AND APPRECIATE.”



Tony Perez, @perezbox

**WHAT QUESTIONS DO
YOU HAVE FOR ME?**

CONTACT

- ▶ Contact
 - ▶ gilzow@missouri.edu
 - ▶ @gilzow on twitter
 - ▶ gilzow on wordpress.org
- ▶ Files: <https://github.com/gilzow/access-denied/>, wcmia2017 branch
- ▶ Additional tools that are handy
 - ▶ BuiltWith.com
 - ▶ Wappalyzer (Firefox, Chrome, Opera + bookmarklet)