ACCESS DENIED

KEEPING YOURSELF OFF AN ATTACKER'S RADAR

Paul Gilzow
gilzow@missouri.edu
Twitter: @gilzow
Facebook: https://fb.com/gilzow
https://www.linkedin.com/in/gilzow

A LITTLE ABOUT ME

- With the University of Missouri since 2000
- Programmer/Analyst since 2005
- Developing WordPress sites since 2009
- Maintainer and current author of the wpDirAuth plugin
- Author and maintainer of a WordPress MVC development framework

WHAT WE WILL TALK ABOUT

- Why WordPress is an attractive target
- Why Education is an attractive target
- Current state of web application security
- Tools available
- WPScan
- Counter-measures

WHY WORDPRESS IS AN ATTRACTIVE TARGET

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

"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

WHY EDUCATION IS AN ATTRACTIVE TARGET

- Network bandwidth and availability
- Rich in hardware infrastructure
- Poor in human resources
- Resistant to blacklisting
- SEO reputation
- Personally Identifiable Information (PII) / Sensitive Personal Information (SPI)

CURRENT STATE OF WEB APPLICATION SECURITY

- Education, 49% of sites had at least one vulnerability every day of the year[1]
- Education, average of 28 vulnerabilities per site, 15 of those serious[1]
- Education, took an average of 4 months to remediate issues[1]

1 - White Hat Security Web Applications Security Statistics Report 2016

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  - Wordpress out-of-date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

AVAILABLE TOOLS

- BuiltWith.com
- Wappalyzer (Firefox, Chrome, Opera + bookmarklet)
- CMSmap : https://github.com/dionach/CMSmap
- Droopescan : https://github.com/droope/droopescan
- WPScan : http://wpscan.org/

WPSCAN

Passive Scan

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

```
root@kali:~# wpscan --url wpcampus.org
```

```
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.1
          Sponsored by Sucuri - https://sucuri.net
      @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[i] The remote host tried to redirect to: https://wpcampus.org/
[?] Do you want follow the redirection ? [Y]es [N]o [A]bort, default: [N]y
[+] URL: https://wpcampus.org/
[+] Started: Sun Jul 10 06:56:21 2016

[+] robots.txt available under: 'https://wpcampus.org/robots.txt'
[+] Interesting entry from robots.txt: https://wpcampus.org/wp-admin/admin-ajax.php
[+] Interesting header: KEEP-ALIVE: timeout=20
[+] Interesting header: LINK: <https://wpcampus.org/wp-json/>; rel="https://api.w.org/"
[+] Interesting header: LINK: <https://wpcampus.org/>; rel=shortlink
[+] Interesting header: SERVER: nginx
[+] Interesting header: X-CACHE: HIT: 3
[+] Interesting header: X-CACHE-GROUP: normal
[+] Interesting header: X-CACHEABLE: SHORT
[+] Interesting header: X-PASS-WHY:
[+] Interesting header: X-TYPE: default
[+] This site seems to be a multisite (http://codex.wordpress.org/Glossary#Multisite)
[+] This site has 'Must Use Plugins' (http://codex.wordpress.org/Must_Use_Plugins)
[+] XML-RPC Interface available under: https://wpcampus.org/xmlrpc.php

[+] WordPress version 4.5.3 identified from advanced fingerprinting (Released on 2016-06-21)

[+] Enumerating plugins from passive detection ...
 | 1 plugin found:

[+] Name: google-maps-builder-pro - v2.0.1
 |  Location: https://wpcampus.org/wp-content/plugins/google-maps-builder-pro/
 |  Readme: https://wpcampus.org/wp-content/plugins/google-maps-builder-pro/README.txt

[+] Finished: Sun Jul 10 06:56:30 2016
[+] Requests Done: 47
[+] Memory used: 63.008 MB
```

```
        </script>
        <style type="text/css">
img.wp-smiley,
img.emoji {
    display: inline !important;
    border: none !important;
    box-shadow: none !important;
    height: 1em !important;
    width: 1em !important;
    margin: 0 .07em !important;
    vertical-align: -0.1em !important;
    background: none !important;
    padding: 0 !important;
}
</style>
<link rel='stylesheet' id='give-styles-css'  href='https://wpcampus.org/wp-content/plugins/give/templates/give.min.css?ver=1.5.2' type='text/css' media='all' />
<link rel='stylesheet' id='google-maps-builder-plugin-styles-css'  href='https://wpcampus.org/wp-content/plugins/google-maps-builder-pro/assets/css/google-maps-builder.min.css?ver=2.0.1' type='text/css' media='all' />
<link rel='stylesheet' id='google-maps-builder-map-icons-css'  href='https://wpcampus.org/wp-content/plugins/google-maps-builder-pro/includes/libraries/map-icons/css/map-icons.css?ver=2.0.1' type='text/css' media='all' />
<link rel='stylesheet' id='wpcampus-fonts-css'  href='https://fonts.googleapis.com/css?family=Open+Sans%3A600%2C400%2C300&#038;ver=4.5.3' type='text/css' media='all' />
<link rel='stylesheet' id='wpcampus-css'  href='https://wpcampus.org/wp-content/themes/wpcampus/css/styles.min.css?ver=0.58' type='text/css' media='all' />
<script type='text/javascript' src='https://wpcampus.org/wp-includes/js/jquery/jquery.js?ver=1.12.4'></script>
<script type='text/javascript' src='https://wpcampus.org/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1'></script>
<script type='text/javascript'>
/* <![CDATA[ */
var give_global_vars = {"ajaxurl":"https:\/\/wpcampus.org\/wp-admin\/admin-ajax.php","checkout_nonce":"1f42ab319a","currency_sign":"$","currency_pos":"before","thousands_separator":",","decimal_separator":".","no_gateway":"Please select a payment method","bad_minimum":"The minimum donation amount for this form is","general_loading":"Loading...","purchase_loading":"Please Wait...","number_decimals":"2","give_version":"1.5.2"};
var give_scripts = {"ajaxurl":"https:\/\/wpcampus.org\/wp-admin\/admin-ajax.php","loading":"Loading","select_option":"Please select an option","default_gateway":"manual","permalinks":"1","number_decimals":"2"};
/* ]]> */
</script>
<script type='text/javascript' src='https://wpcampus.org/wp-content/plugins/give/assets/js/frontend/give.all.min.js?ver=1.5.2'></script>
<script type='text/javascript' src='https://cdnjs.cloudflare.com/ajax/libs/modernizr/2.8.3/modernizr.min.js?ver=4.5.3'></script>
```

vagrantpress.dev/wp-admin/users.php

Apps | Bookmarks | reboots | home | access-denied | work | Other Bookmarks

Access Denied | 2 | 0 | New | Howdy, Access Denied Admin

- Dashboard
- Posts
- Media
- Pages
- Comments
- Appearance
- Plugins 2
- Users
  - All Users
  - Add New
  - Your Profile
- Tools
- Settings
- Collapse menu

Screen Options | Help

Users

Add New

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

Search Users

Bulk Actions | Apply | Change role to... | Change

5 items

	Username	Name	Email	Role	Posts
	admin	Paul Gilzow	gilzow@missouri.edu	Administrator	1
	gilzow-author Edit | Delete	Paul-Author Gilzow	paul@gilzow.com	Author	1
	gilzow-contributor	Paul-Contributor Gilzow	paul.gilzow@gmail.com	Contributor	0
	gilzow-editor	Paul-Editor Gilzow	gilzowp@missouri.edu	Editor	1
	gilzow-subscriber	Paul-Subscriber Gilzow	wpdirauth@gilzow.com	Subscriber	0
	Username	Name	Email	Role	Posts

Bulk Actions | Apply | Change role to... | Change

5 items

Thank you for creating with WordPress.

Version 4.5.3

vagrantpress.dev/wp-admin/edit.php

Apps | Bookmarks | reboots | home | access-denied | work | Other Bookmarks

Access Denied | 2 | 0 | New | Howdy, Access Denied Admin

- Dashboard
- Posts
  - All Posts
  - Add New
  - Categories
  - Tags
- Media
- Pages
- Comments
- Appearance
- Plugins 2
- Users
- Tools
- Settings
- Collapse menu

Screen Options | Help

Posts

Add New

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

Search Posts

Bulk Actions | Apply | All dates | All Categories | Filter

3 items

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

Bulk Actions | Apply

3 items

Thank you for creating with WordPress.

Version 4.5.3

vagrantpress.dev/wp-admin/plugins.php

Apps | Bookmarks | reboots | home | access-denied | work | Other Bookmarks

Access Denied | 2 | 0 | New | Howdy, Access Denied Admin

- Dashboard
- Posts
- Media
- Pages
- Comments
- Appearance
- Plugins 2
  - Installed Plugins
  - Add New
  - Editor
- Users
- Tools
- Settings
- Collapse menu

Screen Options | Help

Plugins Add New

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

Search Installed Plugins

Bulk Actions Apply

8 items

Plugin	Description
Akismet Activate | Edit | Delete	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 Deactivate | Edit	Attempts to prevent recon data gathering Version 0.0.1 | By WpCampus
Aspose Cloud eBook Generator Activate | Edit | Delete	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 Activate | Edit | Delete	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 Activate | Edit | Delete	Easily create web forms and manage form entries within the WordPress admin. Version 1.9.10.2 | By rocketgenius | Visit plugin site
Hello Dolly Activate | Edit | Delete	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

anti-recon.php

```php
<?php
/*
Plugin Name: Anti-Recon
Description: Attempts to prevent recon data gathering
Author: WpCampus
Version: 0.0.1
*/
```

vagrantpress.dev/wp-admin/plugins.php

Apps | Bookmarks | reboots | home | access-denied | work | Other Bookmarks

Access Denied | 2 | 0 | New | Howdy, Access Denied Admin

- Dashboard
- Posts
- Media
- Pages
- Comments
- Appearance
- Plugins 2
  - Installed Plugins
  - Add New
  - Editor
- Users
- Tools
- Settings
- Collapse menu

Screen Options | Help

Plugins Add New

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

Search Installed Plugins

Bulk Actions Apply

8 items

Plugin	Description
Akismet Activate | Edit | Delete	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 Deactivate | Edit	Attempts to prevent recon data gathering Version 0.0.1 | By WpCampus
Aspose Cloud eBook Generator Activate | Edit | Delete	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 Activate | Edit | Delete	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 Activate | Edit | Delete	Easily create web forms and manage form entries within the WordPress admin. Version 1.9.10.2 | By rocketgenius | Visit plugin site
Hello Dolly Activate | Edit | Delete	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

```
root@kali:~# wpscan --url vagrantpress.dev
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.1
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[+] URL: http://vagrantpress.dev/
[+] Started: Sun Jul 10 07:43:13 2016

[+] robots.txt available under: 'http://vagrantpress.dev/robots.txt'
[!] The WordPress 'http://vagrantpress.dev/readme.html' file exists exposing a version number
[+] 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
[!] Upload directory has directory listing enabled: http://vagrantpress.dev/wp-content/uploads/
[!] Includes directory has directory listing enabled: http://vagrantpress.dev/wp-includes/

[+] WordPress version 4.5.3 identified from meta generator (Released on 2016-06-21)

[+] WordPress theme in use: twentysixteen - v1.2

[+] Name: twentysixteen - v1.2
 |  Latest version: 1.2 (up to date)
 |  Location: http://vagrantpress.dev/wp-content/themes/twentysixteen/
 |  Readme: http://vagrantpress.dev/wp-content/themes/twentysixteen/readme.txt
 |  Style URL: http://vagrantpress.dev/wp-content/themes/twentysixteen/style.css
 |  Theme Name: Twenty Sixteen
 |  Theme URI: https://wordpress.org/themes/twentysixteen/
 |  Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout — the horizontal masthe...
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Finished: Sun Jul 10 07:43:17 2016
[+] Requests Done: 37
[+] Memory used: 7.062 MB
[+] Elapsed time: 00:00:03
```

vagrantpress.dev/wp-content/plugins/wp-mobile-detector/

Apps Bookmarks reboots home access-denied work

Index of /wp-content/plugins/wp-mobile-detector

Name	Last modified	Size	Description
Parent Directory		-	
admin/	2016-06-03 00:30	-	
cache/	2016-07-15 14:55	-	
default-widgets.php	2010-12-07 09:26	42K	
functions.php	2016-01-19 05:50	67K	
js/	2016-06-03 00:30	-	
locale/	2016-06-03 00:30	-	
readme.txt	2016-06-03 00:30	7.8K	
resize.php	2016-06-22 19:42	1.5K	
themes/	2016-06-03 00:30	-	
timthumb.php	2016-01-19 04:28	50	
websitez-wp-mobile-detector.php	2016-01-19 04:28	4.9K	

Apache/2.4.7 (Ubuntu) Server at vagrantpress.dev Port 80

COUNTER MEASURE

- Disable Directory listings
  - In .htaccess in the root of the site

```
OPTIONS -INDEXES
```

  - ask your host to disable in your account

```
root@kali:~# wpscan --url vagrantpress.dev
_____________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.1
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_____________________________________________________________

[+] URL: http://vagrantpress.dev/
[+] Started: Sun Jul 10 07:43:13 2016

[+] robots.txt available under: 'http://vagrantpress.dev/robots.txt'
[!] The WordPress 'http://vagrantpress.dev/readme.html' file exists exposing a version number
[+] 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
[!] Upload directory has directory listing enabled: http://vagrantpress.dev/wp-content/uploads/
[!] Includes directory has directory listing enabled: http://vagrantpress.dev/wp-includes/

[+] WordPress version 4.5.3 identified from meta generator (Released on 2016-06-21)

[+] WordPress theme in use: twentysixteen - v1.2

[+] Name: twentysixteen - v1.2
 |  Latest version: 1.2 (up to date)
 |  Location: http://vagrantpress.dev/wp-content/themes/twentysixteen/
 |  Readme: http://vagrantpress.dev/wp-content/themes/twentysixteen/readme.txt
 |  Style URL: http://vagrantpress.dev/wp-content/themes/twentysixteen/style.css
 |  Theme Name: Twenty Sixteen
 |  Theme URI: https://wordpress.org/themes/twentysixteen/
 |  Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout — the horizontal masthe...
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Finished: Sun Jul 10 07:43:17 2016
[+] Requests Done: 37
[+] Memory used: 7.062 MB
[+] Elapsed time: 00:00:03
```

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

```
root@kali:~# wpscan --url vagrantpress.dev --enumerate vp
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.1
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[+] URL: http://vagrantpress.dev/
[+] Started: Mon Jul 11 02:20:24 2016

[+] robots.txt available under: 'http://vagrantpress.dev/robots.txt'
[!] The WordPress 'http://vagrantpress.dev/readme.html' file exists exposing a version number
[+] 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 4.5.3 identified from meta generator (Released on 2016-06-21)

[+] WordPress theme in use: twentysixteen - v1.2

[+] Name: twentysixteen - v1.2
 |  Latest version: 1.2 (up to date)
 |  Location: http://vagrantpress.dev/wp-content/themes/twentysixteen/
 |  Readme: http://vagrantpress.dev/wp-content/themes/twentysixteen/readme.txt
 |  Style URL: http://vagrantpress.dev/wp-content/themes/twentysixteen/style.css
 |  Theme Name: Twenty Sixteen
 |  Theme URI: https://wordpress.org/themes/twentysixteen/
 |  Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout — the horizontal masthe...
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/

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

   Time: 00:01:05 <=============================================================================================================> (1344 / 1344) 100.00% Time: 00:01:05

[+] We found 5 plugins:

[+] Name: akismet
 |  Latest version: 3.1.11
 |  Location: http://vagrantpress.dev/wp-content/plugins/akismet/
```

vagrantpress.dev/wp-admin/plugins.php

Apps | Bookmarks | reboots | home | access-denied | work | Other Bookmarks

Access Denied | 2 | 0 | New | Howdy, Access Denied Admin

- Dashboard
- Posts
- Media
- Pages
- Comments
- Appearance
- Plugins 2
  - Installed Plugins
  - Add New
  - Editor
- Users
- Tools
- Settings
- Collapse menu

Screen Options | Help

Plugins Add New

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

Search Installed Plugins

Bulk Actions Apply

8 items

Plugin	Description
Akismet Activate | Edit | Delete	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 Deactivate | Edit	Attempts to prevent recon data gathering Version 0.0.1 | By WpCampus
Aspose Cloud eBook Generator Activate | Edit | Delete	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 Activate | Edit | Delete	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 Activate | Edit | Delete	Easily create web forms and manage form entries within the WordPress admin. Version 1.9.10.2 | By rocketgenius | Visit plugin site
Hello Dolly Activate | Edit | Delete	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/7306
    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/8104
    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/8365
    Reference: http://www.pritect.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-cleanup-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 - Persistent 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/aribitrary-file-upload-vulnerability-in-wp-mobile-detector/
    Reference: https://wordpress.org/plugins/wp-mobile-detector/changelog/
[i] Fixed in: 3.6

[+] Finished: Mon Jul 11 02:21:37 2016
[+] Requests Done: 1413
[+] Memory used: 128.262 MB
[+] Elapsed time: 00:01:13
```

COUNTER MEASURES

- Protect wp-content
  - Prevent php execution

```
#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

- Protect wp-content
  - Prevent php execution
  - 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, xslx, 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]
```

```
RewriteEngine On

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

#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, xslx, 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]
```

```
RewriteEngine On

#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, xslx, 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]
```

```
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, xslx, 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]
```

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>
```

```
root@kali:~# wpscan --url vagrantpress.dev --enumerate u
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.1
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[+] URL: http://vagrantpress.dev/
[+] Started: Tue Jul 12 08:05:37 2016

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Enumerating usernames ...
[+] Identified the following 5 user/s:
    +----+--------------------+--------------------------+
    | Id | Login              | Name                     |
    +----+--------------------+--------------------------+
    | 1  | admin              | Access Denied Admin      |
    | 2  | gilzow-editor      | Paul-Editor Gilzow       |
    | 3  | gilzow-author      | Paul-Author Gilzow       |
    | 4  | gilzow-contributor | Paul-Contributor Gilzow  |
    | 5  | gilzow-subscriber  | Paul-Subscriber Gilzow   |
    +----+--------------------+--------------------------+
[!] Default first WordPress username 'admin' is still used

[+] Finished: Tue Jul 12 08:05:42 2016
[+] Requests Done: 53
[+] Memory used: 7.887 MB
[+] Elapsed time: 00:00:04
```

COUNTER MEASURES

Account enumeration

- Prevent ?author= redirection

```php
<?php
/*
Plugin Name: Anti-Recon
Description: Attempts to prevent recon data gathering
Author: WpCampus
Version: 0.0.1
*/

/**************************************
 * username anti-enumeration stuff
 **************************************/
/**
 * Blocks remote attackers from enumerating user names
 * @param $strRedirectionURL
 * @param $strRequestedURL
 * @return mixed
 * @see https://developer.wordpress.org/reference/hooks/redirect_canonical/
 */
add_filter('redirect_canonical',function($strRedirectionURL, $strRequestedURL){
    if (1 === preg_match('/\?author=([\d]*)/', $strRequestedURL)) {
        $strRedirectionURL = false;
    }

    return $strRedirectionURL;
}, 10,2);
```

```
root@kali:~# wpscan --url vagrantpress.dev --enumerate u
_______________________________________________________________

        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.1
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[+] URL: http://vagrantpress.dev/
[+] Started: Tue Jul 12 08:05:37 2016

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Enumerating usernames ...
[+] Identified the following 5 user/s:
    +----+--------------------+--------------------------+
    | Id | Login              | Name                     |
    +----+--------------------+--------------------------+
    | 1  | admin              | Access Denied Admin      |
    | 2  | gilzow-editor      | Paul-Editor Gilzow       |
    | 3  | gilzow-author      | Paul-Author Gilzow       |
    | 4  | gilzow-contributor | Paul-Contributor Gilzow  |
    | 5  | gilzow-subscriber  | Paul-Subscriber Gilzow   |
    +----+--------------------+--------------------------+
[!] Default first WordPress username 'admin' is still used

[+] Finished: Tue Jul 12 08:05:42 2016
[+] Requests Done: 53
[+] Memory used: 7.887 MB
[+] Elapsed time: 00:00:04
```

COUNTER MEASURES

Account enumeration

- Prevent ?author= redirection
- Disable account name as author permalink

```php
/**
 * Force wordpress to use /?author=id for author permalink
 */
add_action('init',function(){
    global $wp_rewrite;
    $wp_rewrite->author_structure = '';

});
```

```
root@kali:~# wpscan --url vagrantpress.dev --enumerate u
_______________________________________________________________

        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.1
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[+] URL: http://vagrantpress.dev/
[+] Started: Tue Jul 12 08:05:37 2016

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Enumerating usernames ...
[+] Identified the following 5 user/s:
    +----+--------------------+--------------------------+
    | Id | Login              | Name                     |
    +----+--------------------+--------------------------+
    | 1  | admin              | Access Denied Admin      |
    | 2  | gilzow-editor      | Paul-Editor Gilzow       |
    | 3  | gilzow-author      | Paul-Author Gilzow       |
    | 4  | gilzow-contributor | Paul-Contributor Gilzow  |
    | 5  | gilzow-subscriber  | Paul-Subscriber Gilzow   |
    +----+--------------------+--------------------------+
[!] Default first WordPress username 'admin' is still used

[+] Finished: Tue Jul 12 08:05:42 2016
[+] Requests Done: 53
[+] Memory used: 7.887 MB
[+] Elapsed time: 00:00:04
```

```
54
55 <body class="archive author author-gilzow-author author-3 group-blog hfeed">
56 <div id="page" class="site">
57     <div class="site-inner">
58         <a class="skip-link screen-reader-text" href="#content">Skip to content</a>
59
60         <header id="masthead" class="site-header" role="banner">
61             <div class="site-header-main">
62                 <div class="site-branding">
63
64                                         <p class="site-title"><a href="http://vagrantpress.dev/" rel="
65                                         <p class="site-description">Just another exploitable WordPress
66                                 </div><!-- .site-branding -->
67
```

COUNTER MEASURES

Account enumeration

- Prevent ?author= redirection
- Disable account name as author permalink
- Remove author account from classes

```php
/**
 * Removes username from the body class list.  Why does wordpress include the user name in the body class?  So you can
 * add per-user custom classes, but that seems like a very fringe case vs giving hackers all of your user names.
 *
 * @param $aryClasses array of classes to include in the body element
 * @return array filtered list of classes
 */
add_filter('body_class',function($aryClasses){
    if(is_author() && in_array('author',$aryClasses)){
        /**
         * match all classes of 'author-<username>' but not 'author-id'
         *
         * match: author-admin
         * match: author-gilzowp
         * NO match: author-5
         *
         */
        $aryUserNames = preg_grep('/^author-(?!\d+$).+$/',$aryClasses);
        if(count($aryUserNames) > 0){
            $aryClasses = array_diff($aryClasses,$aryUserNames);
        }
    }
    return $aryClasses;
},100,1);
```

COUNTER MEASURES

Account enumeration

- Prevent ?author= redirection
- Disable account name as author permalink
- Remove author account from classes
- Remove default login failure error messages

```php
/**
 * Removes the error message indicating an invalid user, or incorrect password for a specific user
 * @param $objUser WP_User|WP_Error
 * @return WP_Error|WP_User|null
 */
add_filter('authenticate',function($objUser){
    if(is_wp_error($objUser)){
        if(
                isset($objUser->errors['incorrect_password'])
            ||  isset($objUser->errors['invalid_username'])
            ||  isset($objUser->errors['invalid_email'])
        ){
            $objUser = null;;
        }
    }

    return $objUser;
},99,1);

```

COUNTER MEASURES

Account enumeration

- Prevent ?author= redirection
- Disable account name as author permalink
- Remove author account from classes
- Remove default login failure error messages
- User your school's SSOID system

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

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

Tony Perez, @perezbox

QUESTIONS?

- Contact
  - gilzow@missouri.edu
  - @gilzow on twitter
- Files: https://github.com/gilzow/access-denied/