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

TL;DSWTGMC SUMMARY

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

- Implicitly Deny
- Defense-in-Depth

BEYOND THE BASICS

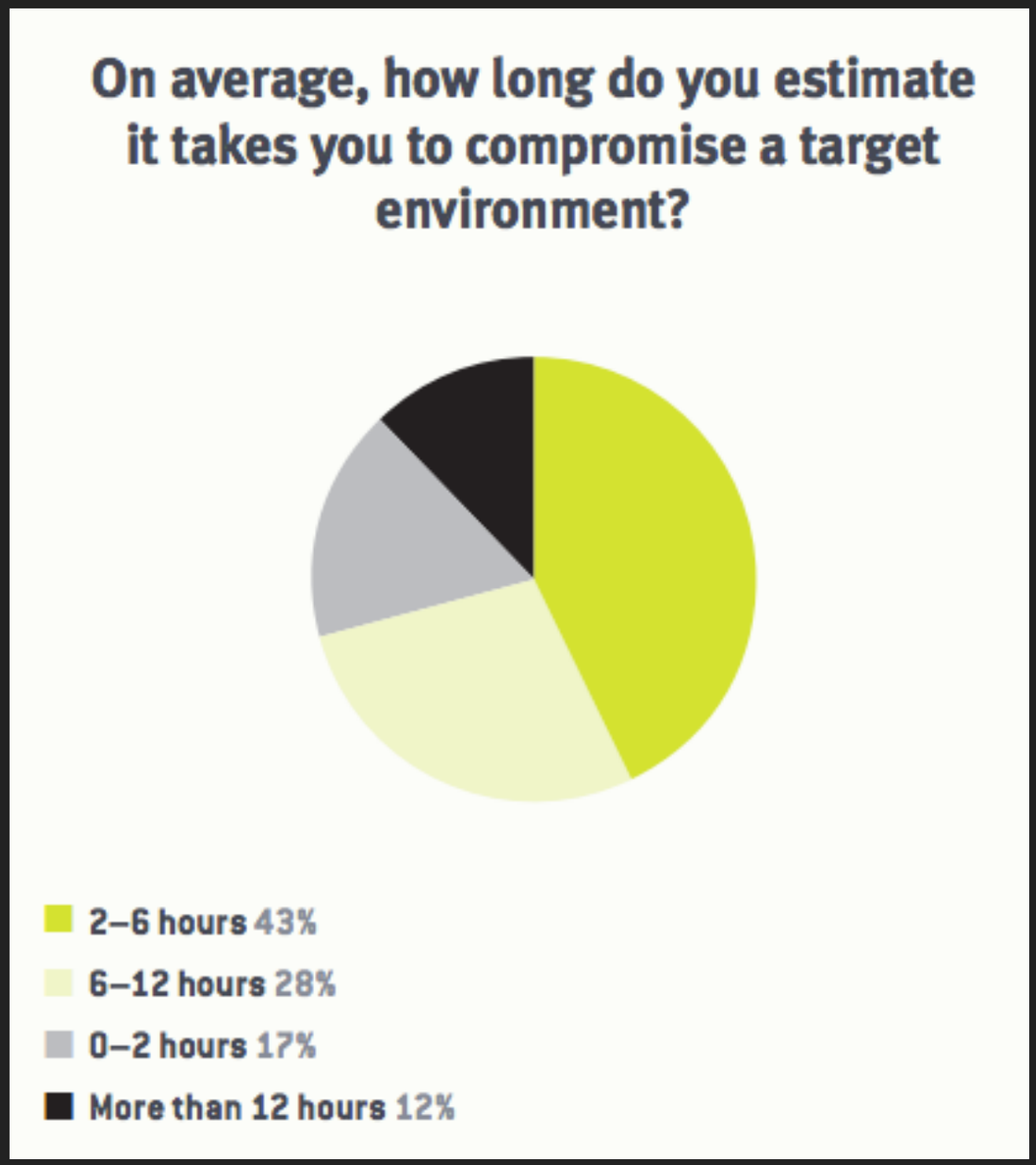
- Why do attackers target you
- Why WordPress is an attractive target
- Current state of WordPress security
- WPScan
- Counter-measures

CURRENT STATE OF WEB APPLICATION SECURITY

- 44% of sites had at least one vulnerability every day of the year[1]
- Average of 14 vulnerabilities per site, 7 of those serious[1]
- Took an average of 5 months to remediate issues[1]

1 - White Hat Security Web Applications Security Statistics Report 2016

CURRENT STATE OF WEB APPLICATION SECURITY CONT.



1. Nuix White Paper, The Black Report 2017: https://www.nuix.com/download/White%20paper%20-%20The%20Black%20Report

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  - Wordpress out-of-date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

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 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	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 4.7.2

vagrantpress.dev/wp-admin/users.php

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
  - 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 4.7.2

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
  - Installed Plugins
  - Add New
  - Editor
- Users
- Tools
- Settings
- Collapse menu

Screen Options | Help

Plugins Add New

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

Search installed plugins...

Bulk Actions Apply

8 items

Plugin	Description
Akismet Anti-Spam 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: activate the Akismet plugin and then go to your Akismet Settings page to set up your API key. Version 3.3 | 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 2.9.44 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

VirtualBox-5.0.32-11....dmg

Show All

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

```
gilzow@kali:~$ sudo wpscan --url vagrantpress.dev
```

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

        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 12:00:35 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
[!] 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 4.7.3 (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 plugins from passive detection ...
[+] No plugins found

[+] Finished: Tue Mar 14 12:00:41 2017
[+] Requests Done: 67
```

```
gilzow@kali:~$ sudo wpscan --url vagrantpress.dev
```

```
      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 12:00:35 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
[!] 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 4.7.3 (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 plugins from passive detection ...
[+] No plugins found

[+] Finished: Tue Mar 14 12:00:41 2017
[+] Requests Done: 67
```

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

```
gilzow@kali:~$ sudo wpscan --url vagrantpress.dev
```

```
      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 12:00:35 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
[!] 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 4.7.3 (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 plugins from passive detection ...
[+] No plugins found

[+] Finished: Tue Mar 14 12:00:41 2017
[+] Requests Done: 67
[+] Memory used: 17.625 MB
```

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

```
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 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/
 |  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

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 - 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/aribitrary-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, 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>
```

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>
```

```
gilzow@kali:~$ sudo wpscan --url vagrantpress.dev --enumerate u --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 12:27:49 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

[+] 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 Mar 14 12:27:55 2017
[+] Requests Done: 83
[+] Memory used: 19.41 MB
[+] Elapsed time: 00:00:05
```

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);
```

```
gilzow@kali:~$ sudo wpscan --url vagrantpress.dev --enumerate u --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 12:27:49 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

[+] 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 Mar 14 12:27:55 2017
[+] Requests Done: 83
[+] Memory used: 19.41 MB
[+] Elapsed time: 00:00:05
```

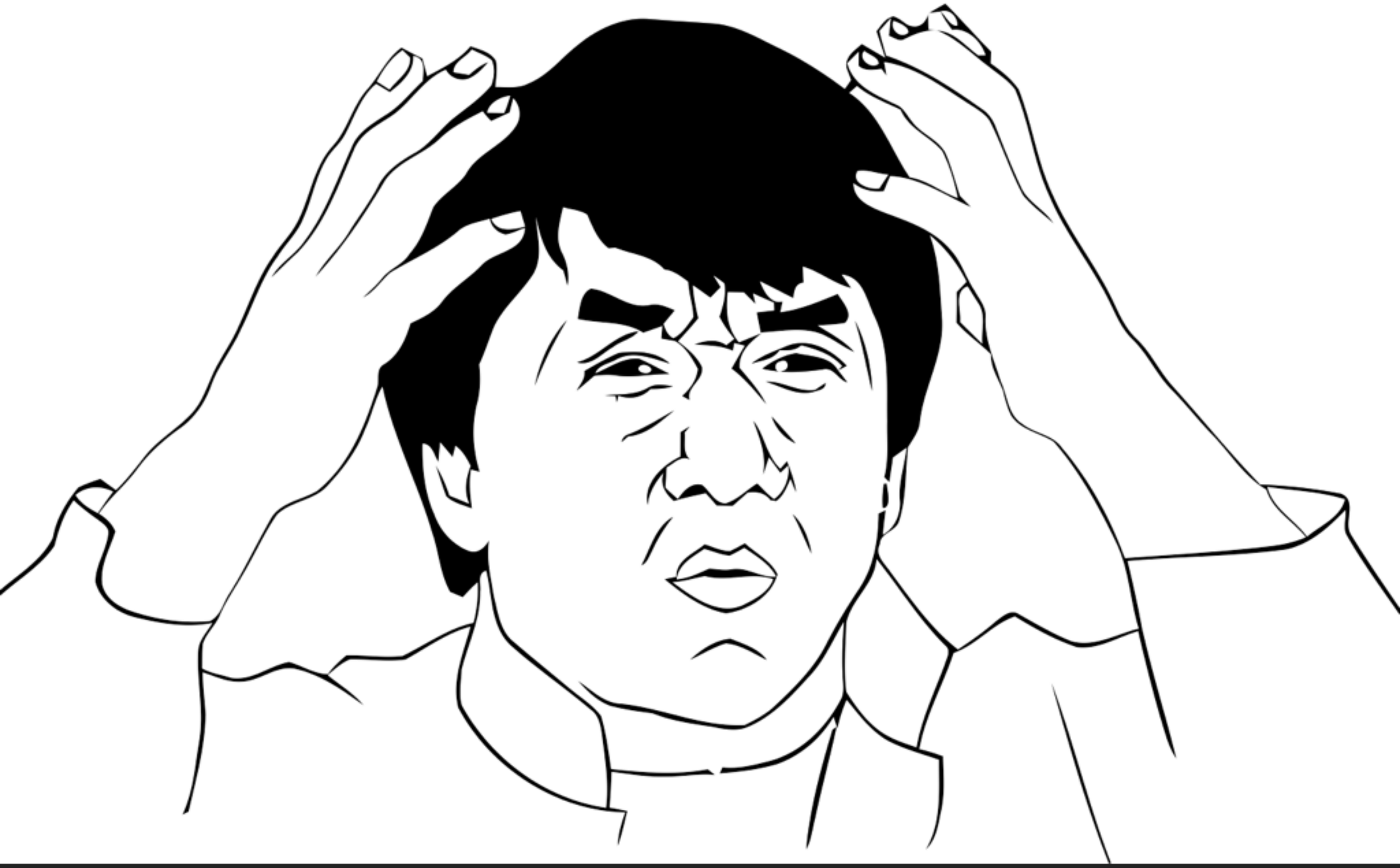
COUNTER MEASURES

Account enumeration

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

```php
/**
* Changes author permalink to use author=# instead of username
*
* @param $strLink   string  Prepared link to Author's archive page
* @param $intID     integer Author User ID
*
* @return string    Link to Author's archive page
*/
add_filter('author_link',function($strLink,$intID){
    return home_url('/') . '?author=' . $intID;
},10,2);

/**
* Corrects author feed link after filtering author_link
*
* @param $strLink   string  Prepared link to author feed
* @param $strFeed   string  Feed type
*
* @return string Prepared link to author feed
*/
add_filter('author_feed_link',function ($strLink,$strFeed){
    if(1 == preg_match('/^\/([^\/]+)/',$strLink,$aryMatch)){
        return $aryMatch[0] . '&feed=' . $strFeed;
    }
},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 Oct 11 18:00:44 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 Oct 11 18:00:48 2016
[+] Requests Done: 53
[+] Memory used: 7.254 MB
[+] Elapsed time: 00:00:03
```



```
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);
```

```
gilzow@kali:~$ sudo wpscan --url vagrantpress.dev --enumerate u --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 12:27:49 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


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

[+] Enumerating usernames ...
[!] Stop User Enumeration plugin detected, results might be empty. However a bypass exists for v1.2.8 and below, see stop_user_enumeration_b
pass.rb in /usr/share/wpscan
[+] Identified the following 5 user/s:
    +----+-------+-------------------------+
    | Id | Login | Name                    |
    +----+-------+-------------------------+
    | 1  | 1     | Access Denied Admin     |
    | 2  | 2     | Paul-Editor Gilzow      |
    | 3  | 3     | Paul-Author Gilzow      |
    | 4  | 4     | Paul-Contributor Gilzow |
    | 5  | 5     | Paul-Subscriber Gilzow  |
    +----+-------+-------------------------+

[+] Finished: Fri Mar 17 15:48:46 2017
[+] Requests Done: 85
[+] Memory used: 18.488 MB
[+] Elapsed time: 00:00:04
```

But Wait...
THERE'S
MORE!

vagrantpress.dev/wp-json/wp/v2/users


```
{
    "id": 3,
    "name": "Paul-Author Gilzow",
    "url": "",
    "description": "",
    "link": "http://vagrantpress.dev/?author=3",
    "slug": "gilzow-author",
    "avatar_urls": {
        "24": "http://2.gravatar.com/avatar/b836d5429d6b43f820c8e867f4246d72?s=24&d=mm&r=g",
        "48": "http://2.gravatar.com/avatar/b836d5429d6b43f820c8e867f4246d72?s=48&d=mm&r=g",
        "96": "http://2.gravatar.com/avatar/b836d5429d6b43f820c8e867f4246d72?s=96&d=mm&r=g"
    },
    "meta": [],
    "_links": {
        "self": [
            {
                "href": "http://vagrantpress.dev/wp-json/wp/v2/users/3"
            }
        ],
        "collection": [
            {
                "href": "http://vagrantpress.dev/wp-json/wp/v2/users"
            }
        ]
    }
},
```

COUNTER MEASURES

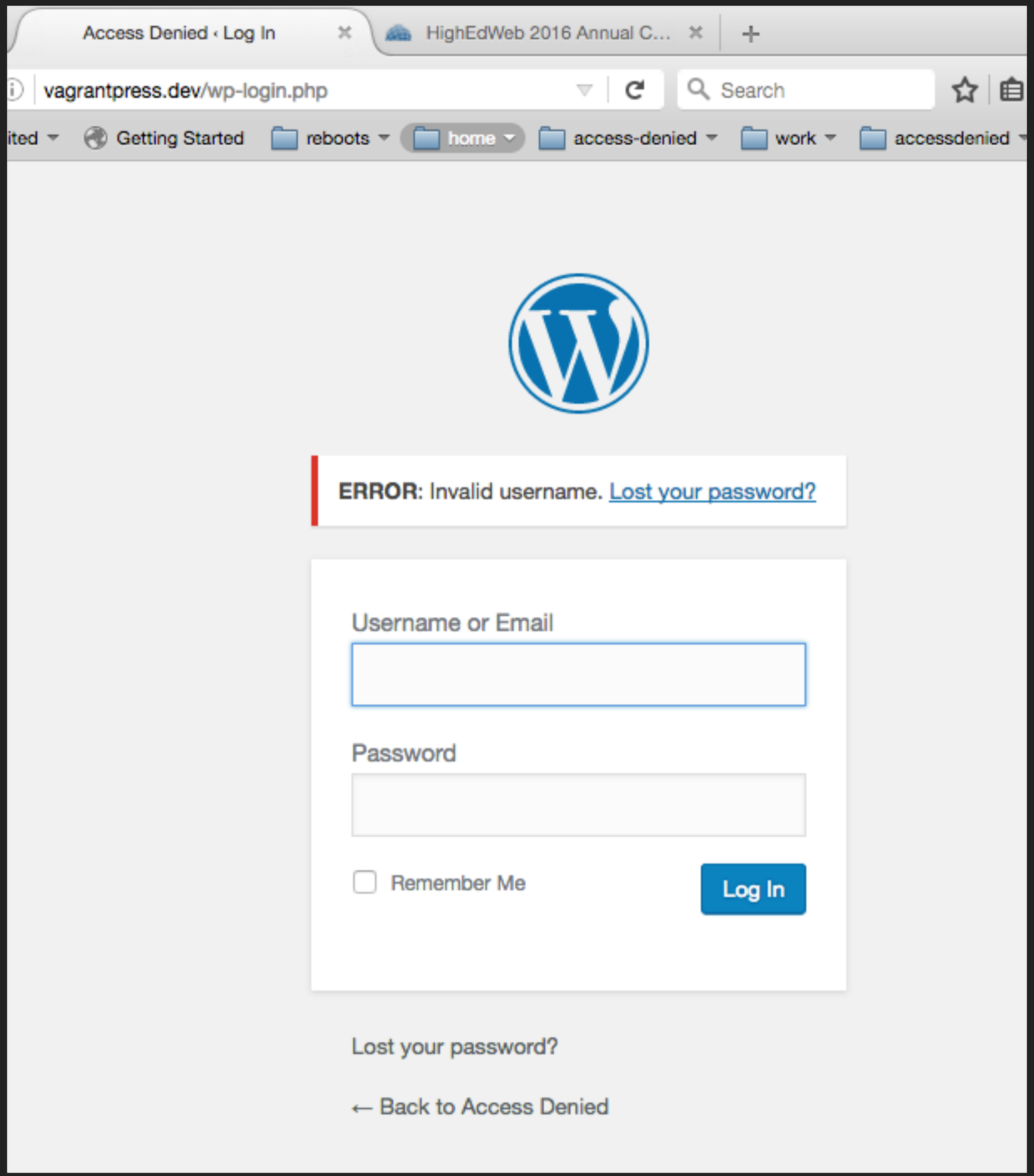
Account enumeration

- Prevent ?author= redirection
- Disable account name as author permalink
- Remove author account from classes
- Remove user “slug” property from users endpoint in REST API

```php
/**
* Remove slug property from response to user query
*
* @param $objResponse   WP_REST_Response    Prepared response object to REST API call
* @param $objUser       WP_User             User object used to create response
* @param $objRequest    WP_REST_Request     Requested object
*
* @return WP_REST_Response
*/
add_filter('rest_prepare_user',function($objResponse,$objUser,$objRequest){
    if(isset($objResponse->data['slug']) && '' !== $objResponse->data['slug']){
        unset($objResponse->data['slug']);
    }

    return $objResponse;
},10,3);
```

vagrantpress.dev/wp-json/wp/v2/users


```
{
    "id": 3,
    "name": "Paul-Author Gilzow",
    "url": "",
    "description": "",
    "link": "http://vagrantpress.dev/?author=3",
    "avatar_urls": {
        "24": "http://2.gravatar.com/avatar/b836d5429d6b43f820c8e867f4246d72?s=24&d=mm&r=g",
        "48": "http://2.gravatar.com/avatar/b836d5429d6b43f820c8e867f4246d72?s=48&d=mm&r=g",
        "96": "http://2.gravatar.com/avatar/b836d5429d6b43f820c8e867f4246d72?s=96&d=mm&r=g"
    },
    "meta": [],
    "_links": {
        "self": [
            {
                "href": "http://vagrantpress.dev/wp-json/wp/v2/users/3"
            }
        ],
        "collection": [
            {
                "href": "http://vagrantpress.dev/wp-json/wp/v2/users"
            }
        ]
    }
},
```


Access Denied ‹ Log In
HighEdWeb 2016 Annual C...
vagrantpress.dev/wp-login.php
Search
Getting Started
reboots
home
access-denied
work
accessdenied
ERROR: Invalid username. Lost your password?
Username or Email
Password
Remember Me
Log In
Lost your password?
← Back to Access Denied

Access Denied ‹ Log In

HighEdWeb 2016 Annual C…

vagrantpress.dev/wp-login.php

Search

ited | Getting Started | reboots | home | access-denied | work | accessdenied

ERROR: The password you entered for the username **admin** is incorrect. Lost your password?

Username or Email

admin

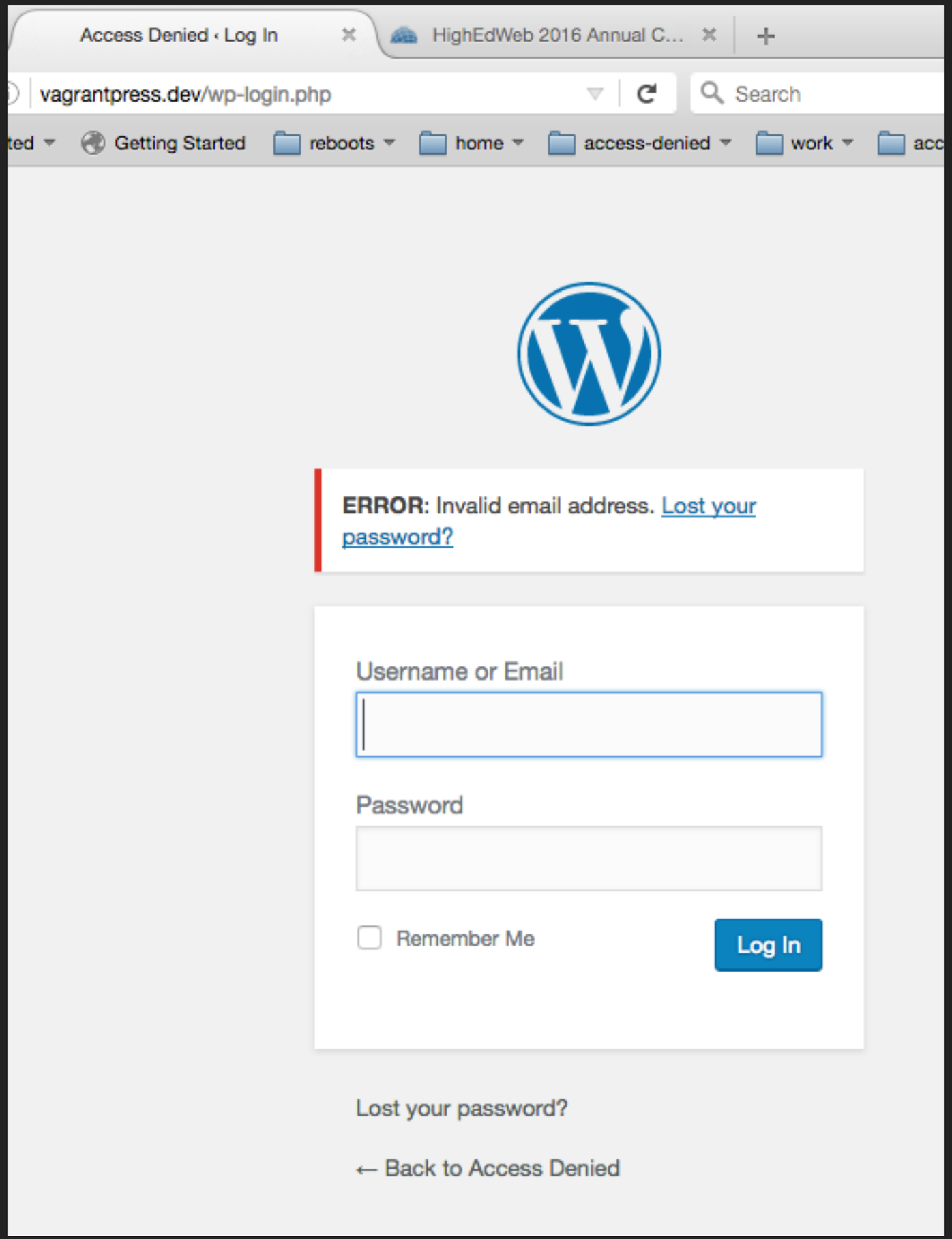
Password

Remember Me

Log In

Lost your password?

← Back to Access Denied


Access Denied ‹ Log In
HighEdWeb 2016 Annual C…
vagrantpress.dev/wp-login.php
Search
Getting Started
reboots
home
access-denied
work
ERROR: Invalid email address. Lost your password?
Username or Email
Password
Remember Me
Log In
Lost your password?
← Back to Access Denied

vagrantpress.dev/wp-login.php

Search

ed Getting Started reboots home access-denied work accessdenied

ERROR: The password you entered for the email address **paul@gilzow.com** is incorrect. Lost your password?

Username or Email

paul@gilzow.com

Password

Remember Me

Log In

Lost your password?

← Back to Access Denied

COUNTER MEASURES

Account enumeration

- Prevent ?author= redirection
- Disable account name as author permalink
- Remove author account from classes
- Remove users endpoint from REST API
- 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);

```

vagrantpress.dev/wp-login.php

Search

d Getting Started reboots home access-denied work ac

ERROR: Invalid username, email address or incorrect password.

Username or Email

admin

Password

Remember Me

Log In

Lost your password?

← Back to Access Denied

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/
- Additional tools that are handy
  - BuiltWith.com
  - Wappalyzer (Firefox, Chrome, Opera + bookmarklet)