

Extending WordPress

Plugins

- Developer Center

Themes

Mobile

Ideas

Kvetch!

Search Plugins

Search

Popular

Tags

More »

widget (3,827)

Post (2,420)

plugin (2,308)

admin (1,914)

posts (1,829)

sidebar (1,569)

twitter (1,305)

google (1,304)

Jetpack by WordPress.com

Supercharge your WordPress site with powerful features previously only available to WordPress.com users.

[Download Version 2.9.3](#)

- [Description](#)
- [Installation](#)
- [FAQ](#)
- [Screenshots](#)
- [Changelog](#)
- [Stats](#)
- [Support](#)
- [Reviews](#)
- [Developers](#)

2.9.3

- Important security update. CVE-2014-0173

2.9.2

- Bugfix: Publicize: When publishing from a mobile app or third-party client, Publicize now works again.

2.9.1

Requires: 3.7 or higher

Compatible up to: 3.9

Last Updated: 2014-4-16

Downloads: 9,943,993

Ratings



3.9 out of 5 stars

“The Jetpack plugin [...] before 2.9.3 for WordPress does not properly restrict access to the XML-RPC service, which allows remote attackers to bypass intended restrictions and publish posts ”

Source: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0173>

WordPress Security

How to think about security

- Confidentiality
- Integrity
- Availability

What an attacker can do with a vulnerable plugin

- Publish posts (*Jetpack between 1.9 and 2.9.3*)
- Display the entire contents of the users table (*BuddyPress 1.7.1*)
- Steal usernames and passwords when users log in (*Unconfirmed 1.2.3*)
- Do pretty much whatever an admin can - and more (*WP Super Cache 1.2*)
 - Create new users, delete existing users
 - Create posts and delete existing posts
 - Take complete control of the server
- Make your site totally unresponsive (*GA Dashboard 2.0.4*)

How to protect your site

- Keep WordPress and your plugins updated
- Keep your server updated
- Choose your plugins carefully
- Use strong passwords
- Lock down your wordpress installation

Choosing Plugins Carefully

- Size
- Age
- Forum responses
- Downloads
- Author

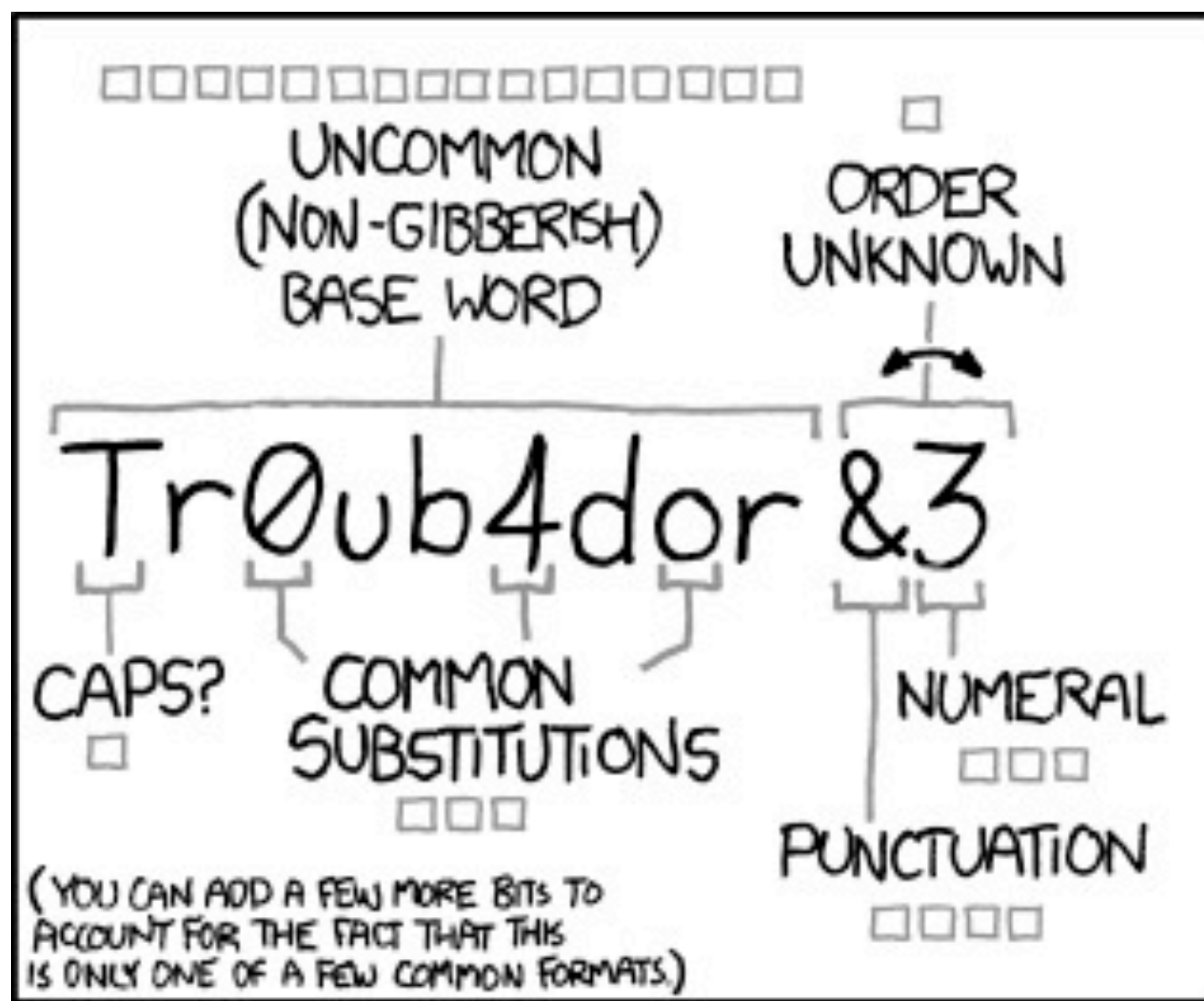
Checking for advisories

- <https://cve.mitre.org/>
- <http://osvdb.org/>
- <https://secunia.com/community/advisories/>
- <http://www.exploit-db.com/>
- <https://security.dxw.com/>

Plugin developers - how to not be part of the problem

Be careful about untrusted data

- *Database Queries: \$wpdb->prepare()*
- *Data in the page: esc_html(), esc_attr(), esc_url()*
- *Use with extreme caution: eval()*



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

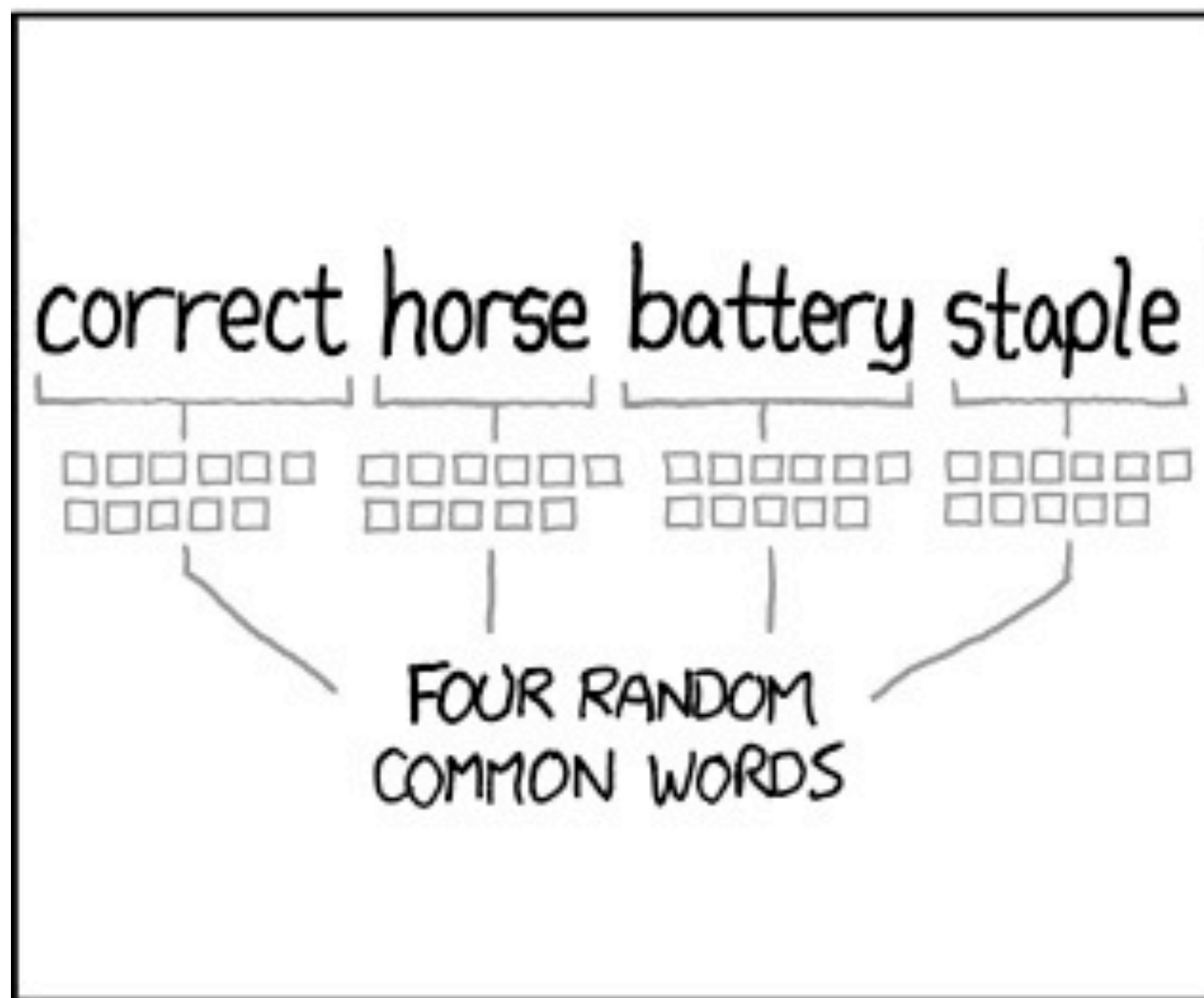
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Password Security

- Usually the easiest way to get into a system
- Long and memorable > Short and complex
- Is your admin user still called admin?

For the lols

1communication

Letmein456

C0mmunications

stupidpassword

C0mm1ss10n

government12

C1vilservice

government99

Security at dxw

(shameless plug)



- Secure hosting
- Password restrictions
- security.dxw.com
- dxw Security plugin

A screenshot of the WordPress dashboard's plugin security scan results. It shows a list of installed plugins with their security status, version, and author information. The 'Enable Media Replace' plugin is marked as 'Use with caution', 'GD Star Rating' as 'Potentially unsafe', 'Gravity Forms' and 'Gravity Forms Polls Add-On' as 'Not yet reviewed', and 'Hello Dolly' as 'No issues found'.

Plugin Name	Status	Description	Version	Author
Enable Media Replace	Use with caution	Enable replacing media files by uploading a new file in the "Edit Media" section of the WordPress Media Library.	2.9.3	Måns Jonasson
GD Star Rating	Potentially unsafe	GD Star Rating plugin allows you to set up advanced rating and review system for posts, pages and comments in your blog using single, multi and thumbs ratings.	1.9.22	Milan Petrovic
Gravity Forms	Not yet reviewed	Easily create web forms and manage form entries within the WordPress admin.	1.7.11	rocketgenius
Gravity Forms Polls Add-On	Not yet reviewed	Polls Add-on for Gravity Forms	1.5	Rocketgenius
Hello Dolly	No issues found	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.		

Questions?

@dgmstuart

@thedxw

<http://www.dxw.com/>