https://wordpress.org/plugins/jetpack/changelog/

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)

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

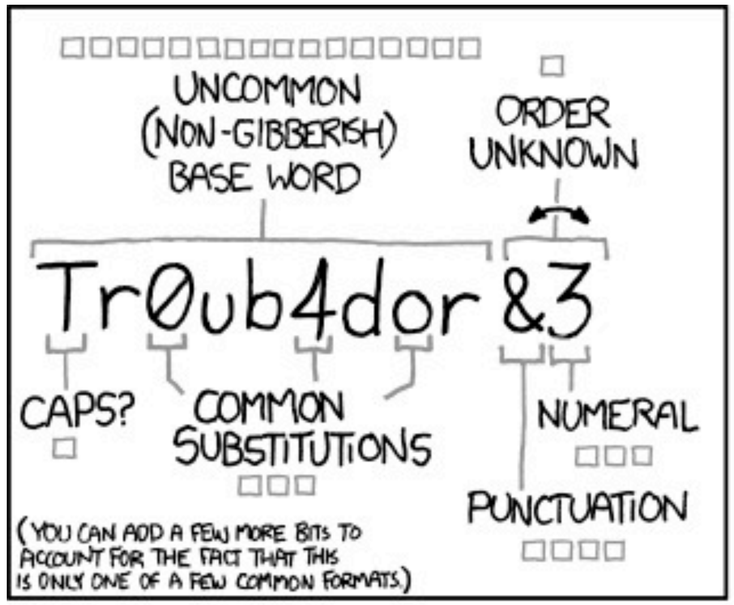
Checking for advisories

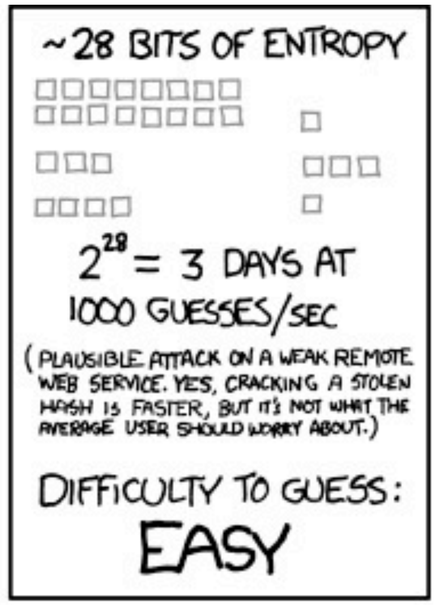
- https://cve.mitre.org/
- http://osvdb.org/
- https://secunia.com/community/advisories/
- http://www.exploit-db.com/
- https://security.dxw.com/

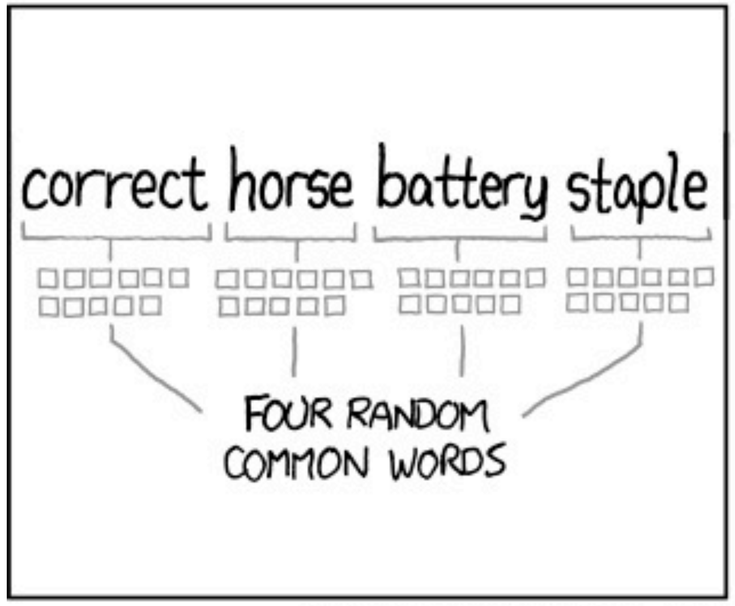
Plugin developers - how to not be part of the problem

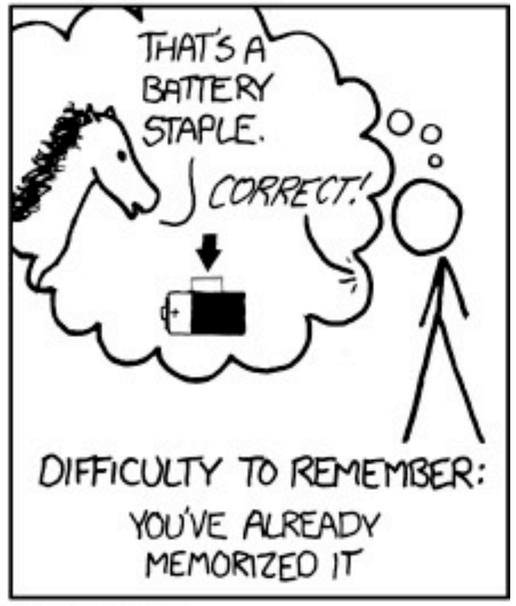
Be careful about untrusted data

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









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

C0mmunications

C0mm1ss10n

C1vilservice

Letmein456

stupidpassword

government12

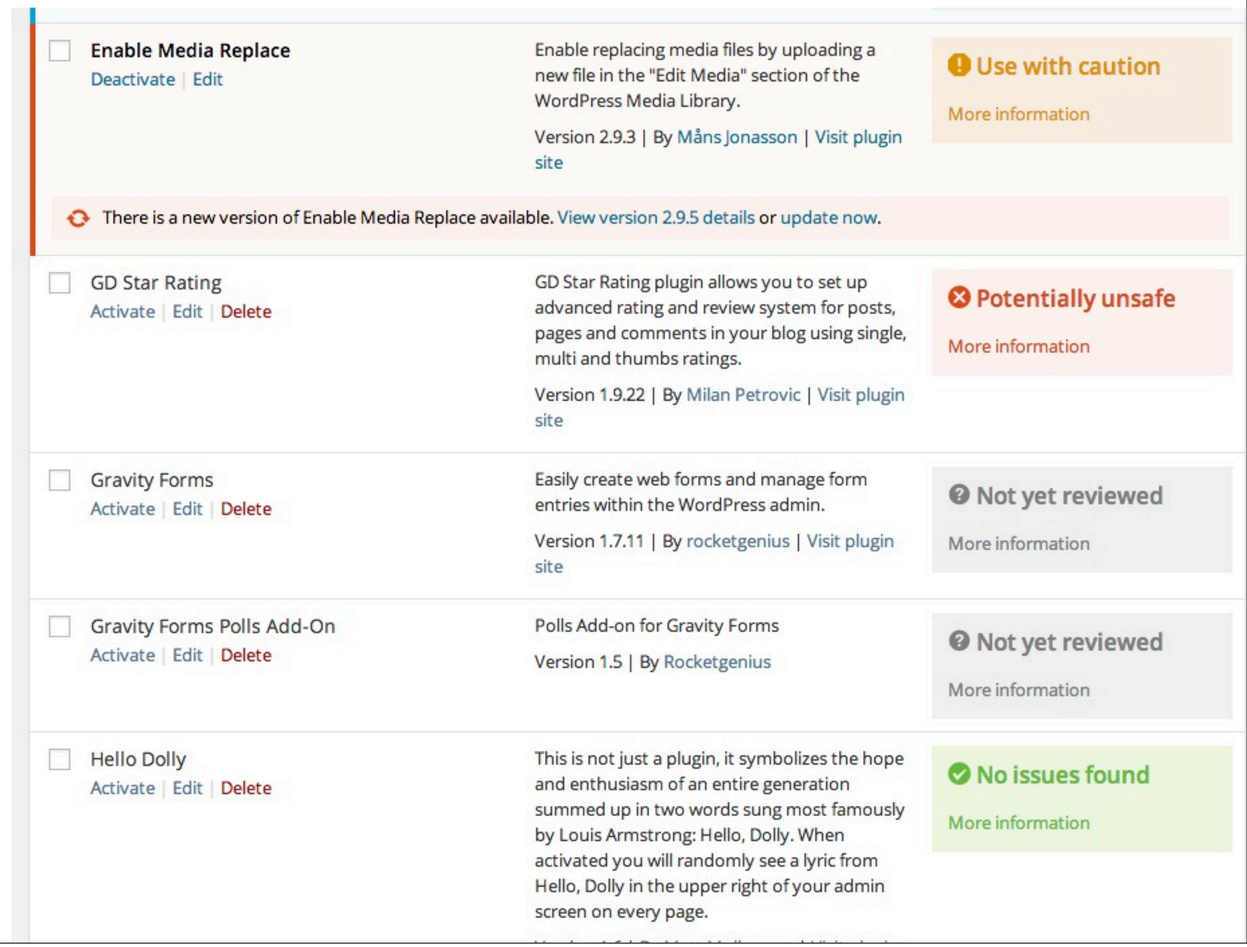
government99

Security at dxw

(shameless plug)

dxw
dexterous digital

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



Questions?

@dgmstuart

@thedxw

http://www.dxw.com/