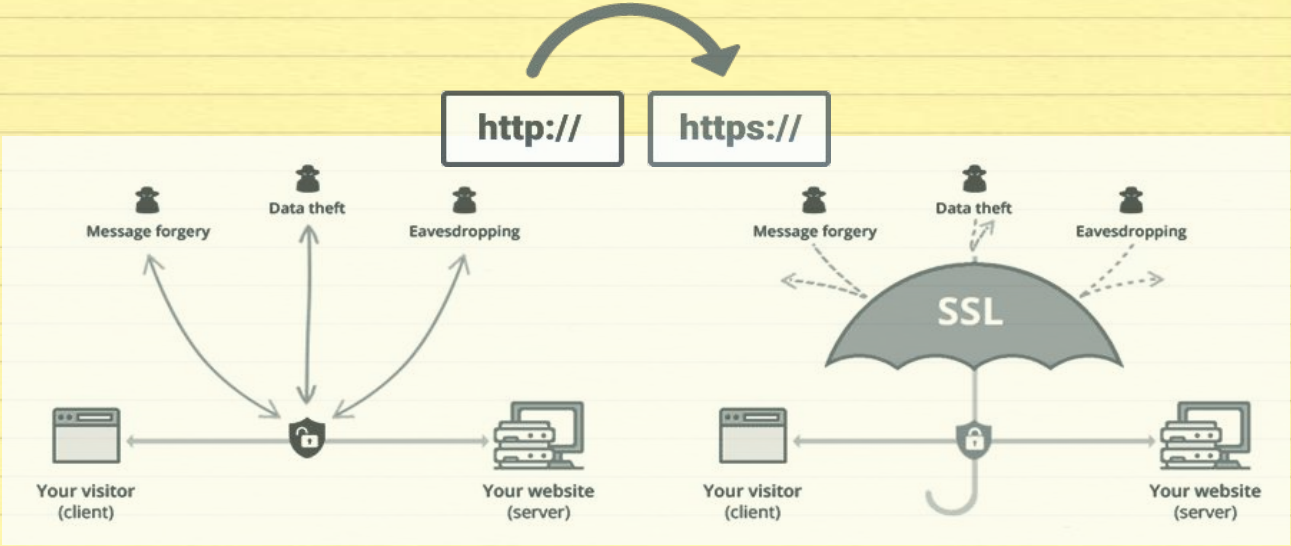
Lehigh Valley WordPress Meetup

Securing Your WordPress Site

February 13, 2020

What Is HTTPS and Why Do I Need It

- HyperText Transport Protocol Secure
  - Allows an encrypted connection to your website (secure).



Passwords:

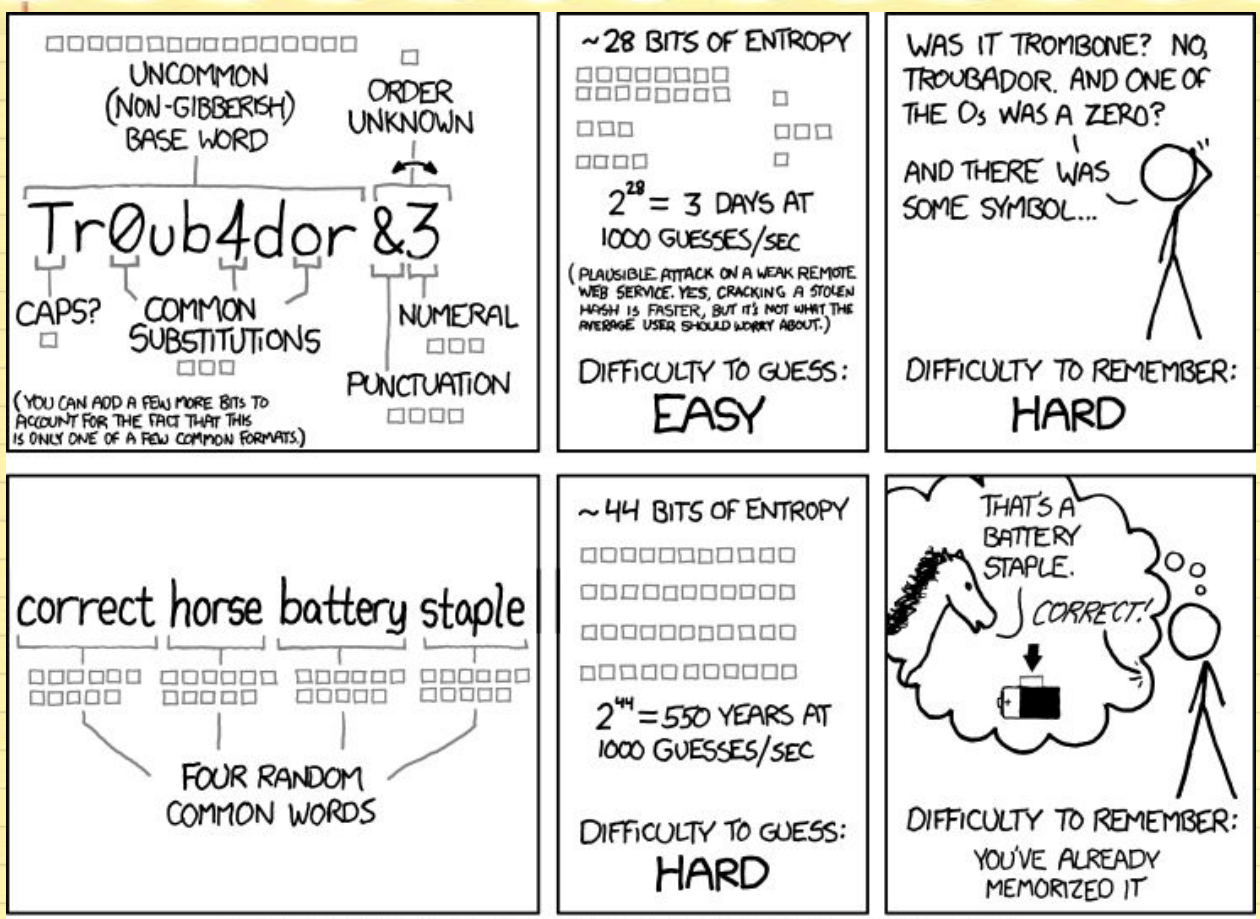
You expect me to remember all this?

- Passwords (a mindset of strong passwords)
- 2FA (two-factor authentication)
- Password Managers (1-Password, LastPass, Bitwarden, DashLane)
- Yuibkey (fingerprint control over passwords -
  for the security geek
  in all of us)

Passwords:

You expect me to remember all this?

- Passwords (a mindset of strong passwords)
- 2FA (two-factor authentication)
- Password Managers (1-Password, LastPass, Bitwarden, DashLane)
- Yuibkey (fingerprint control over passwords -
  for the security geek
  in all of us)



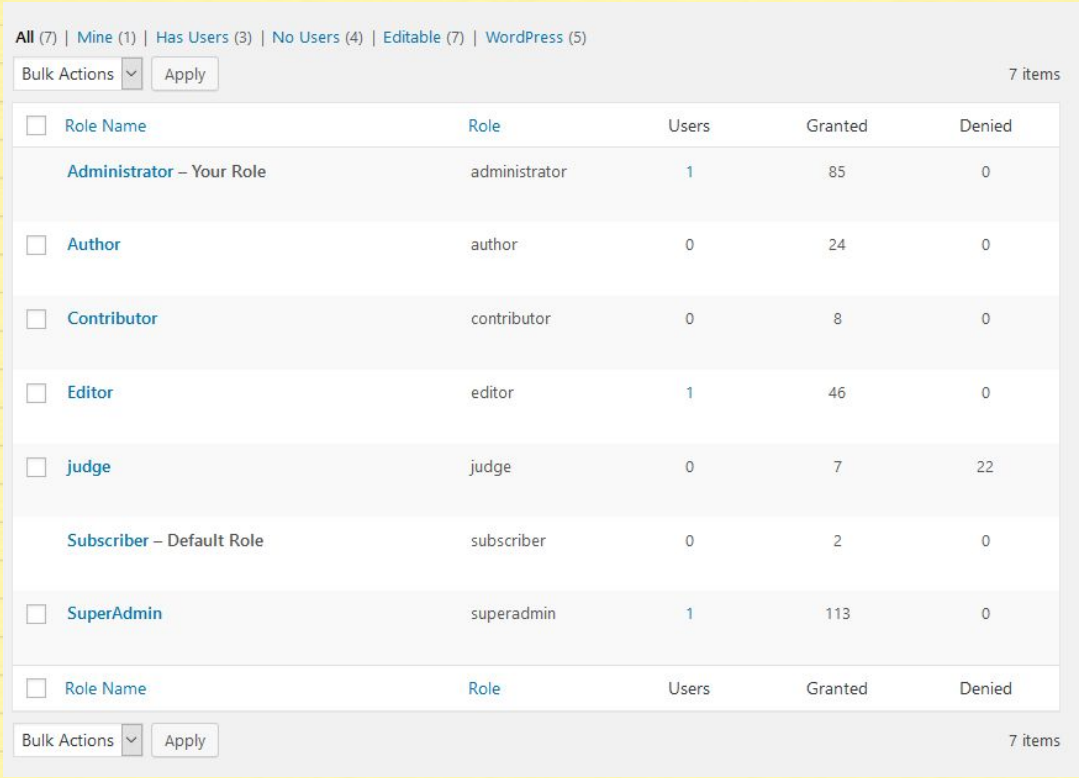
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

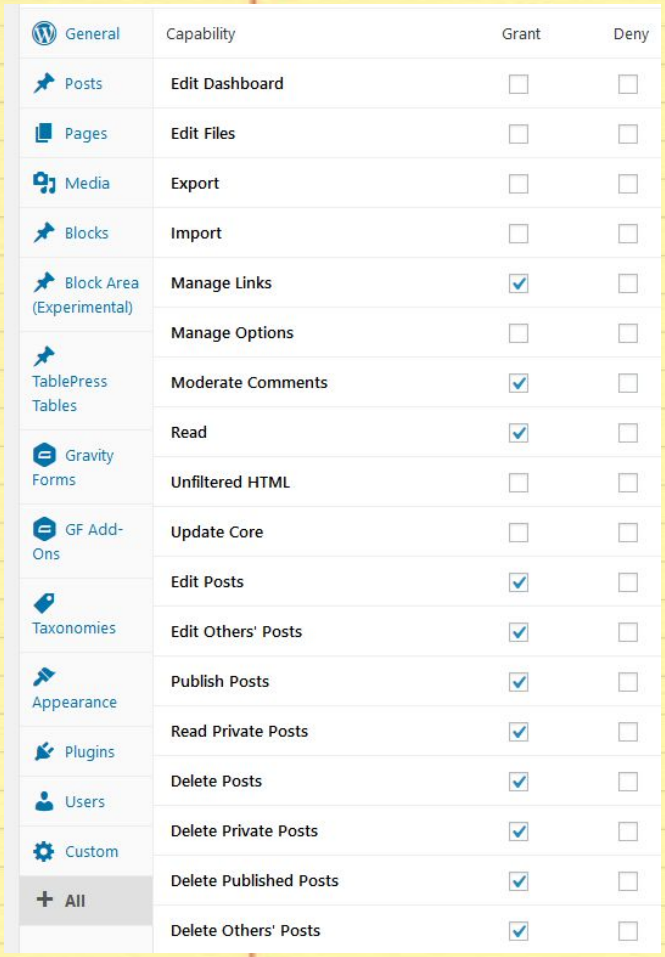
Surface Area:
Limiting Users Who Can Do Everything

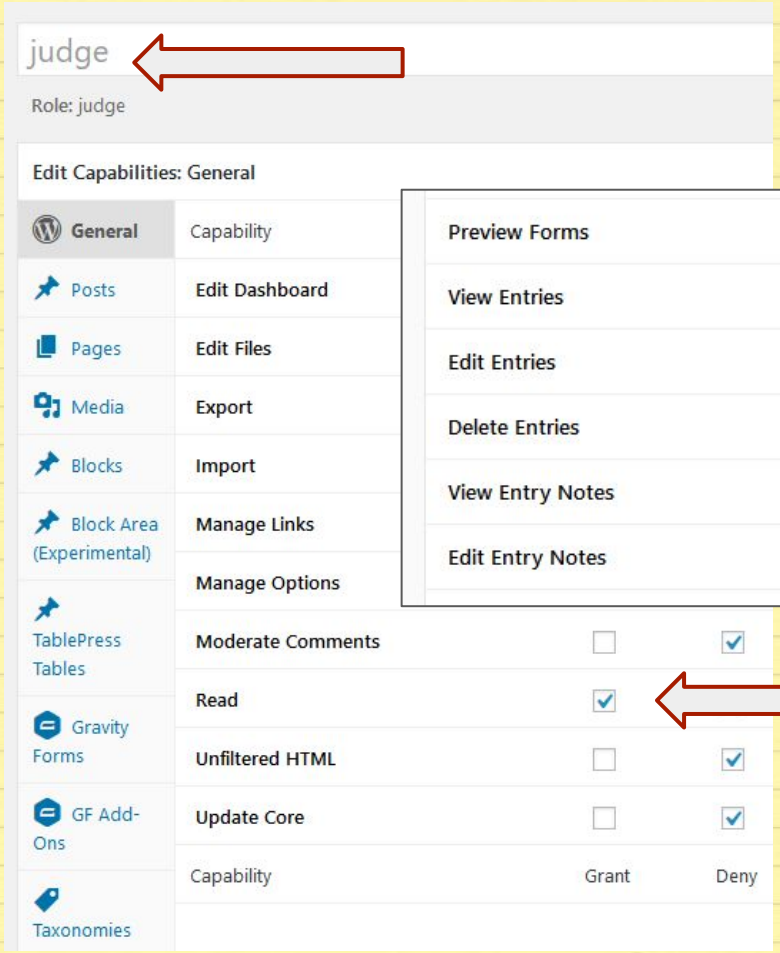
It’s not about Trust, it’s about unexpected consequences

- User Roles
- https://wordpress.org/plugins/user-role-editor/
- https://wordpress.org/plugins/members/

https://wordpress.org/plugins/members/




General
Posts
Pages
Media
Blocks
Block Area (Experimental)
TablePress Tables
Gravity Forms
GF Add-Ons
Taxonomies
Appearance
Plugins
Users
Custom
All
Capability
Grant
Deny
Edit Dashboard
Edit Files
Export
Import
Manage Links
Manage Options
Moderate Comments
Read
Unfiltered HTML
Update Core
Edit Posts
Edit Others' Posts
Publish Posts
Read Private Posts
Delete Posts
Delete Private Posts
Delete Published Posts
Delete Others' Posts


judge
Role: judge
Edit Capabilities: General
General
Posts
Pages
Media
Blocks
Block Area (Experimental)
TablePress Tables
Gravity Forms
GF Add-Ons
Taxonomies
Capability
Edit Dashboard
Edit Files
Export
Import
Manage Links
Manage Options
Moderate Comments
Read
Unfiltered HTML
Update Core
Capability
Grant
Deny
Preview Forms
View Entries
Edit Entries
Delete Entries
View Entry Notes
Edit Entry Notes

Simple Stuff

- Keeping WP/Plugins/Themes/PHP up to date
- Use Trusted Sources
- Form Security - Choose good Form Plugin
- Limit login attempts

More Simple Stuff

- Backups
- Firewalls
- Security Plugins

Security Plugins

- iThemes
  https://wordpress.org/plugins/better-wp-security/
- Sucuri
  https://wordpress.org/plugins/sucuri-scanner/
- Wordfence
  https://wordpress.org/plugins/wordfence/
- Vulnerability Listing
  https://ithemes.com/wordpress-vulnerability-roundup-january-2020-part-1/ (http://bit.ly/37iQfn5)

How Do You Know There Is a Problem?

Fixing a hacked site

I do not know why my picture pops up on this slide in the sidebar.

Not a “Thing”: Obscurity is not Security

- Usernames are “not a thing”
- Alternate login URLs are “not a thing”

Advanced Topics

HSTS (HTTP Strict Transport Security)

Enforces a secure connection (requires “server” rewrite access)

CSP (Content Security Policy)

A protocol to prevent “unauthorized” access to your site’s assets.

A “whitelist” of safe connections tlo you your site

Static Front End

Utilizing the WordPress REST API to access content to be displayed on a statically hosted website

TPS at a high level

Disallow file edits (edited)

Panelists

Kevin Cristiano: @kcristiano

Paul Wolke: @pwolke

pwolke@gmail.com (new biz site soon)

Kerch McConlogue: @kerchmcc

kerch@wefixbrokenwebsites.com