

Lehigh Valley WordPress Meetup

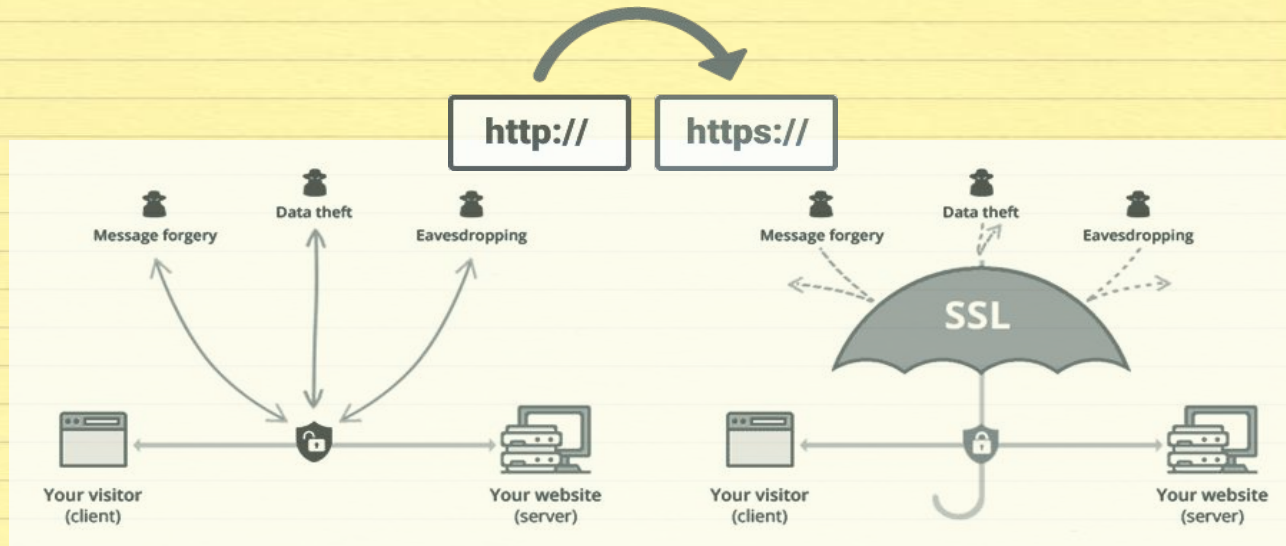
Securing Your WordPress Site

February 13, 2020



What Is HTTPS and Why Do I Need It

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

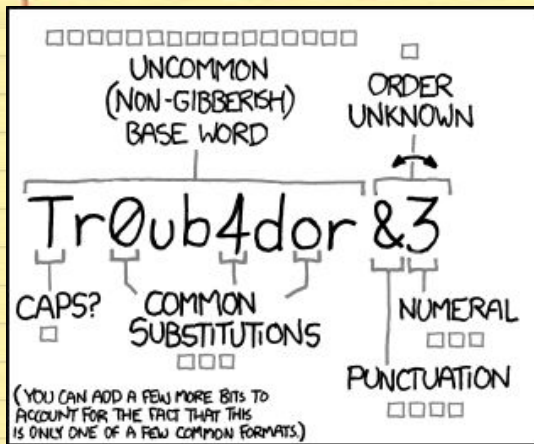


Passwords:

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)





~28 BITS OF ENTROPY

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

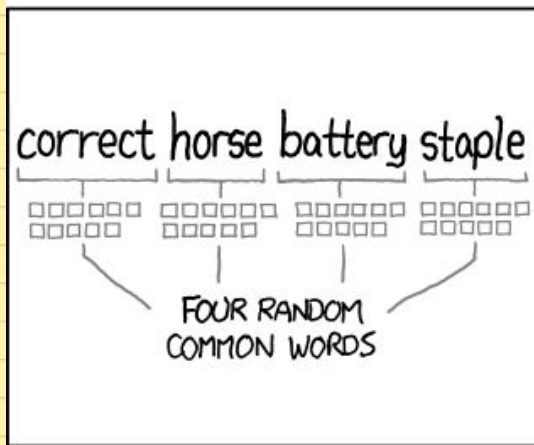
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

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.

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/>

All (7) | Mine (1) | Has Users (3) | No Users (4) | Editable (7) | WordPress (5)

Bulk Actions 7 items

<input type="checkbox"/>	Role Name	Role	Users	Granted	Denied
<input type="checkbox"/>	Administrator – Your Role	administrator	1	85	0
<input type="checkbox"/>	Author	author	0	24	0
<input type="checkbox"/>	Contributor	contributor	0	8	0
<input type="checkbox"/>	Editor	editor	1	46	0
<input type="checkbox"/>	judge	judge	0	7	22
<input type="checkbox"/>	Subscriber – Default Role	subscriber	0	2	0
<input type="checkbox"/>	SuperAdmin	superadmin	1	113	0
<input type="checkbox"/>	Role Name	Role	Users	Granted	Denied

Bulk Actions 7 items

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

judge ←

Role: judge

Edit Capabilities: General

General	Capability	Grant	Deny
Posts	Edit Dashboard	<input type="checkbox"/>	<input type="checkbox"/>
Pages	Edit Files	<input type="checkbox"/>	<input type="checkbox"/>
Media	Export	<input type="checkbox"/>	<input type="checkbox"/>
Blocks	Import	<input type="checkbox"/>	<input type="checkbox"/>
Block Area (Experimental)	Manage Links	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Manage Options	<input type="checkbox"/>	<input type="checkbox"/>
TablePress Tables	Moderate Comments	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Gravity Forms	Unfiltered HTML	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GF Add-Ons	Update Core	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Taxonomies	Capability	Grant	Deny

Preview Forms	<input type="checkbox"/>	<input checked="" type="checkbox"/>
View Entries	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit Entries	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete Entries	<input type="checkbox"/>	<input checked="" type="checkbox"/>
View Entry Notes	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit Entry Notes	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

A black rectangular box with yellow pixelated text that reads "YOU HAVE BEEN HACKED !". The text is arranged in two lines: "YOU HAVE BEEN" on the top line and "HACKED !" on the bottom line. The font is a simple, blocky, monospaced style.

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 to 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