BEGINNER AND ADVANCED STEPS FOR WP SECURITY

GEORGETOWN WORDPRESS MEETUP
03 APR 2019 @ GEORGETOWN LIBRARY

www.BEACON.agency

SCHEDULE

6:00p NETWORKING

6:30p SECURITY DISCUSSION

8:00p Q&A

8:30p NETWORKING

9:00p Done!

www.BEACON.agency

AGENDA

- Why WordPress Security is Important
- The Role of Web Hosting
- The Role of Core, Themes, and Plugins
- WordPress Security in Easy Steps
- Advanced WordPress Security
- Fixing a Hacked Site

ABOUT ME- ED PERRY
PRESIDENT, THE BEACON AGENCY
ED@BEACONAGENCY.NET
@THEEDPERRY
LINKEDIN.COM/IN/EDTECH

www.BEACON.AGENCY

SLIDES: WWW.BEACON.AGENCY/WPGT

www.BEACON.agency

WORDPRESS SECURITY OVERVIEW

www.BEACON.agency

WHY WORDPRESS SECURITY IS IMPORTANT

- Prevents hacking
- Loss of time/energy
- Loss of Revenue
- Loss of Sensitive Data/PII
- Downtime

www.BEACON.agency

THE ROLE OF WEB HOSTING

Who You Host With Makes A Difference

- Basic Server Security
- Shared vs Dedicated
- VPS
- Managed
- SSL

www.BEACON.agency

THE ROLE OF CORE, THEMES, AND PLUGINS

Update them, or pay the price!

www.BEACON.agency

- Avoid Known Vulnerabilities
- Core, Theme, and Plugin Updates
- Automatic Core Updates
- Automated Updates (with backups)
- Use Supported Themes
- Avoid Free Versions of Paid Plugins

WORDPRESS SECURITY IN EASY STEPS

www.BEACON.agency

CHANGE THE DEFAULT “ADMIN” USERNAME

Anything but admin.

- Three Methods:

1. Create a new admin username and delete the old one.
2. Use the Username Changer plugin
3. Update username from phpMyAdmin

www.BEACON.agency

INSTALL A WORDPRESS BACKUP SOLUTION

Back that site up!

www.BEACON.agency

- Choose a plugin
  - VaultPress (with Jetpack)
  - BackupBuddy
  - UpdraftPlus
- Full Backups vs. Snapshots
- Automated Backups, How Often?
- Backups before Updates
- Off-site Storage

INSTALL A WORDPRESS SECURITY PLUGIN

Choose Wisely...

- Sucuri Security
- Wordfence
- iThemes Security
- Follow the Instructions / Read the Directions

www.BEACON.agency

ENABLE WEB APPLICATION FIREWALL (WAF)

Stop Problems Before They Get To Your Site

- Sucuri
- CloudFlare
- Paid Services
- “Set and Forget”

www.BEACON.agency

USE 2-FACTOR AUTHENTICATION FOR LOGIN

All The Cool Kids Are Doing It...

www.BEACON.agency

- Two types of algorithms
  - Time-based One-time Password (TOTP)
  - HMAC-based One-time Password (HOTP)
- Two Factor Authentication Plugin
- Supports Google Authenticator and more
- Don’t use SMS or Email

DISABLE TRACKBACKS

What Have You Done For Me Lately?

- Spamy, Fake, and Annoying
- Settings > Discussion
- Uncheck “Allow link notifications from other blogs (pingbacks and trackbacks)”

DISCOURAGE SPAMMERS

Add a human touch.

- Human Interface Form
- Akismet Anit-Spam
- Captcha Plugins (there are many)
- Some Contact Form Plugins already include as an option
- Disable Comments
- Or outsource comments to Disqus

DON'T ADD SECURITY QUESTIONS TO LOGIN

Nope. Just nope.

- Decreases security because the answers are almost always public data!
- Don't use them. Period.

www.BEACON.agency

ADVANCED WORDPRESS SECURITY

www.BEACON.agency

DISABLE FILE EDITING

Lock it down.

www.BEACON.agency

You can easily do this by adding the following code in your wp-config.php file.

```
1 // Disallow file edit
2 define( 'DISALLOW_FILE_EDIT', true );
```

DISABLE PHP FILE EXECUTION

No php, no cry.

- disable PHP file execution where it's not needed e.g. /wp-content/uploads/
- Open a text editor

```
<Files *.php>
deny from all
</Files>
```

- Save as ".htaccess" in /wp-content/uploads/
- can also be done with specific directories using `php.ini` if host allows

www.BEACON.agency

LIMIT LOGIN ATTEMPTS

Three strikes and you're (locked) out.

- Easily done with Plugins
- Login LockDown Plugin
- Wordfence Security Plugin
- Limit number of login attempts
- Block invalid Usernames

CHANGE WORDPRESS DATABASE PREFIX

NOTE: This can break your site if this is not done properly. Only proceed if you feel comfortable with your coding skills.

www.BEACON.agency

- Change Table Prefix in wp-config.php from “wp_” to something else like this “wp_a123456_”
- Change all Database Tables Name
- Change all Database Tables Name
- Search the options table for any other fields that is using “wp_ “
- Search the usermeta for all fields that is using “wp_”
- Backup and Done

PW PROTECT WP-ADMIN AND LOGIN

Extra PWs for extra safety.

www.BEACON.agency

- Only if SSL is enforced
- Can be done in Cpanel OR:
- Create a .htpasswd file using this generator
- Upload this file outside your /public_html/ directory
- Create a .htaccess file and upload it in /wp-admin/
- Add this and save:

```
1 AuthName "Admins Only"
2 AuthUserFile
  /home/yourdirectory/.htpasswds/public_html/wp-
  admin/passwd
3 AuthGroupFile /dev/null
4 AuthType basic
5 require user putyourusernamehere
```

DISABLE DIRECTORY INDEX/BROWSE

Reveal nothing.

www.BEACON.agency

- Open the .htaccess file in your root directory
- Add the following line at the end of the .htaccess file

```
Options -Indexes
```

- Save and upload .htaccess file back to your site

DISABLE LOGIN HINTS

NOTE: This can break your site if this is not done properly and may affect future core updates.

www.BEACON.agency

- Open functions.php file
- Add this code:

```
function no_wordpress_errors(){
  return 'What the heck are you doing?! Back off!';
}
add_filter( 'login_errors', 'no_wordpress_errors' );
```

- Change the “What the heck are you doing?! Back off!” message to better fit your mood.

FIXING A HACKED SITE

www.BEACON.agency

YOU'VE BEEN HACKED

Now What?

- Archive current site directory and database for forensic analysis
- Restore from backups (hopefully?)
- Malware Scan and removal

www.BEACON.agency

YOU'VE BEEN HACKED

Cleaning up.

- Update Plugins and Core
- Verify permissions are minimal (most malware makes things 777)
- Force PW change at next login
- Change admin PW
- Change DB PW and secret keys

www.BEACON.agency

THANKS FOR JOINING ME!

GOT QUESTIONS?

EMAIL: ED@BEACONAGENCY.NET
TWITTER: @THEEDPERRY

www.BEACON.agency