Wells Foundation
a century of social innovation

www.wellsfound.org

Technical Documentation
Including URLs, User IDs, Passwords

May 9, 2018

Version 1.2

Author ~ Bob Oganovic
bob_oganovic@msn.com

The Wells Foundation
c/o St. Mark's Episcopal Cathedral
519 Oak Grove
Minneapolis, MN 55403

Document Revisions

Date	Version Number	Document Changes
January 10, 2018 with additional minor updates on January 11, 2018 and January 16, 2018	1.0	Initial document
March 12, 2018	1.1	• Added chapter describing how the website uses Google Drive. • Added information about the "Embed Any Document" plugin and clarified verbiage around subscriptions to other premium plugins. • Corrected typos and font inconsistencies.
May 9, 2018	1.2	Added Chapter 8 describing a known security vulnerability within the Media Library of WordPress and the plugin-based solution to that problem.

Table of Contents

1   Introduction and WordPress basics

1.1   Introduction

The purpose of this document is to provide a deeper dive into some points around the Wells Foundation website above and beyond that which is found in the user documentation that is found on a page under the "Board Members" menu. It basically formalizes and organizes the notes that the webmaster has routinely used and as such would allow a new administrator who has basic WordPress knowledge to come in and take over with relative ease.

1.1   Technical documentation

This document has been given the name **Technical Documentation Including URLs, User IDs, Passwords User/Board Member Documentation** to distinguish it from a separate document entitled **Technical Documentation Including URLs, User IDs, Passwords**. Both are stored under the passworded menu "Board Members (Private)".

This new document:

- Is more technical in nature and as such **is not designed for general board member use**.
- Includes, among other things, detail about all the "under-the-hood" such as theme/child theme choice, plugins used, hosting provider accounts/user IDs/passwords (AUPs), cPanel AUPs, WordPress administrator AUPs, domain registrar AUPs, and the process for making database changes.
- Is password-protected. This password is available from the webmaster and two other board members.

1.2   Theme and best practices

The current website was developed using the **twentyseventeen** theme[1]. At the time it was chosen it was the newest, most generic open source theme offered by the WordPress parent foundation. All best practices related to WordPress have been followed in the development and maintenance of the Wells site. These include:

- Creating a child theme and making changes only to that child theme[2].
- Assuring backups occur (this is managed through ASO).
- Minimizing the number of plugins.
- Choosing plugins with high user ratings and a large installed user base.

---

[1] A theme is "...*a collection of files that work together to produce a graphical interface with an underlying unifying design for a weblog. These files are called template files. A theme modifies the way the site is displayed, without modifying the underlying software*." Article "*Using Themes*" https://codex.wordpress.org/Using_Themes.

[2] The whys and wherefores here require some lengthy explanation. Suffice it to say that correctly managing "parent" and "child" themes assures that any updates to *twentyseventeen* occur without a hitch while at the same time permitting users to customize the website as needed.

- Confirming that pages display correctly across multiple platforms and browsers.
- Optimizing and scaling images.
- Making the SSL-compatible (SSL being the "S" in HTTPS and the current standard for website security established by Google).
- Keeping core WordPress and plugin versions up-to-date.
- Using a favicon (the little icon that shows up next to our page title in the browser window).
- Giving permalinks (the links between pages, documents, and images that occur **within** the website) logical names.
- Including contact links.
- Applying additional security where appropriate (for example, on the board members pages).
- Posting documents in PDF format unless compelling reasons dictate otherwise.
- Removing Media Library items and un-installing plugins that are no longer needed.
- Auditing for broken links (both internal and external).

1.3   Plugins used on the Wells website

Plugin	Description	Wells-specific comment
Accordion Pro	Creates FAQ (frequently asked questions) sections on pages that can open and close thereby saving space.	Premium plugin; subscription began on May 8, 2017 (██ /year). Because this is premium product we have an account with the vendor: • URL: https://wpshopmart.com/ • User: ██████████ • Password: ██████
Advanced Twenty Seventeen	Allows some customizing of that theme.	← As stated.
Akismet Anti-Spam	Protects site from spam.	Comes as part of WordPress load.
Child Themify	Creates child themes easily.	Accomplishes what is described footnote 2.

Plugin	Description	Wells-specific comment
Content Anchor Links	Adds content anchors to pages and posts.	Makes it easier to create "jumps" from one page or paragraph within the website to another.
Draw Attention	Creates interactive images in WordPress.	Used to create link on the homepage to the page publicizing the annual concert Honoring Veterans.
Duplicate Page	Duplicates posts, pages and custom posts easily.	← As stated.
Embed Any Document	Lets you upload and embed your documents on a WordPress website without any additional browser plugins like Flash or Acrobat reader.	Used for the pages storing documents from grant years 2016 and before that are stored on Google Drive.
Google Apps Login	Provides secure login for WordPress through users' Google Apps accounts.	Same as above.
Google Drive Embedder Premium	Browse for Google Drive documents and embed directly in your posts and pages. Extends the Google Apps Login plugin so no extra user authentication (or admin setup) is required.	Same as above. Premium plugin; subscription began on July 23, 2018 ($██.00/year).
Simple Membership Custom Messages	Customizes content protection messages.	Part of solution for board member menu security.
Simple WordPress Membership	Protects content within WordPress site.	Same as above.
Slick Sitemap	Adds an HTML sitemap.	Used to create sitemap page.

Plugin	Description	Wells-specific comment
TablePress	Embeds tables into pages.	Used on several pages that have "table-ized" or spreadsheet-like content and display.
TinyMCE Advanced	Enables advanced features and plugins in TinyMCE, the visual editor in WordPress.	Standard editing enhancement.
Wordfence	Provides functionality to, among other things, address a known security vulnerability within the Media Library of WordPress	See Chapter 8 for a detailed explanation.
WP Header image slider and carousel	Creates image slider.	Creates the moving grant recipient images on the home page.
WP Mail SMTP	This is an "under-the-hood" email manager.	Comes as part of WordPress load.
WP Smush	Compresses photos to save space and speed up page loading time without sacrificing image resolution quality.	← As stated.
WP Staging	Creates a staging clone site for testing & developing.	← As stated.
WPForms	Provides drag & drop form builder to create WordPress forms.	Premium plugin set; subscription began on May 4, 2017 ($▮▮▮/year). These provide the support processes related to the forms entry by applicant
WPForms Conditional Logic	Provides conditional logic for WPForms.	

Plugin	Description	Wells-specific comment
WPForms Custom Captcha	Provides "Captcha" fields with WPForms.	organization that are described in the other user documentation. All 3 are loaded but only the first one is currently being used. Because this is a premium product we have an account with the vendor: • URL: ██████████████ • User:████████ • Password██████████

2   Hosting Provider – A Small Orange (ASO)

2.1   CAVEAT about URLs that follow

There is an elusive browser issue of some sort such that the URLs in the tables below may not work by clicking on the links. If that is the case, then copy and paste the links into your browser.

2.2   ASO client support area

In the table below the URL, user ID, and password bring you to the page that tells you everything about the Wells account with ASO. The support code is only needed for online chat support sessions.

URL	███
User ID	███
Password ID	███
Support code	███

2.3   ASO cPanel login

cPanel is the standard web-based hosting control panel provided by ASO and other hosting providers. cPanel allows Wells to manage websites from a web-based interface. Most work in terms of maintaining and updating the website is not done on cPanel but, rather, is performed on the WordPress Administrator page discussed in section 3.1.

URL	███
User ID	███
Password	███

2.4   ASO Webmail – General

The Webmail account is a requirement of WordPress but as a practical matter it has no active use. Wells uses Gmail accounts for communication.

URL	███
User ID	███
Password	███

3   Accessing the WordPress Administrator site

3.1   Basic dashboard access

The dashboard is the first screen you see when you log into the administration area of any WordPress website. Notice below that the link for the administrator is simply the website URL with "/wp-admin" tacked on the end. In the words of one online training site:

> *The main idea of the dashboard is to give you a place where you can get an at-a-glance overview of what's happening with your blog. You can catch up on news, view your draft posts, see who's linking to you or how popular your content's been, quickly put out a no-frills post, or check out and moderate your latest comments. It's like a bird's eye view of operations, from which you can swoop down into the particular details.*[3]
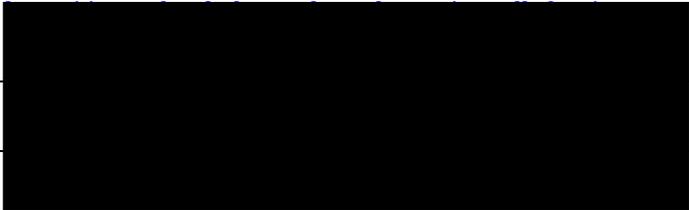
URL	
User ID	
Password	

3.2   More about "user role management"

In addition to members of the public, WordPress comes with an **internal** user role management system which defines what a specific user can and cannot do on the website. Out of the box when you install WordPress, there are five default user roles with **decreasing** (as the number gets higher) ability to do things on the website.

1. Administrator
2. Editor
3. Author
4. Contributor
5. Subscriber

3.3   User role management at Wells

For Wells only #1 (Administrator) has been implemented. If it is desired a second user ID with a clone Administrator role could be (but has not yet been) set up.

Roles #2 through #5 are designed for websites that are more oriented toward blogging and collecting content from multiple players wherein differing levels of review and editorial control are necessary.

---

[3] See article entitled "*Support*" at https://en.support.wordpress.com/dashboard/ .

4 Management of the Wells domain

4.1 Initial registration through DomainIT.com

The Wells domain was secured through a domain registrar company called DomainIT. Our account information is as follows:

URL	█████████████
User ID	█████████████
Password	█████████████

According to information on this site the domain was established/purchased by ████████ ████ on May 20, 2008 and expires on May 19, 2019. Even though ████████ has long since left the Wells Board the user ID was established with her initials and last name and as such it will be there in perpetuity. However, other information on this account has been updated to show Bob Oganovic.

4.2 Renewing the domain

I have consulted with experts from the Twin Cities WordPress Small Business User Group who have told me the following:

- Sometime before May 19, 2019 I will receive a notice asking us to renew the URL.
- **What was done here regarding Wellsfound.org is unusual.** That is – nowadays no domain registrar would set us up for 11 years with (what appears to be) only a single up-front payment (the amount of which is unknown – there is no record of that anywhere on Domait.com).
- So, going forward (i.e., starting after May 19, 2019) we can renew on a sliding scale of[4]:
  - 1 year for $█████
  - 2 years for ████████
  - 5 years for ████████

---

[4] These are the terms on DomainIT.com as of January 10, 2018.

5 Google Drive Access

Google Drive is used to store archival documents that appear on the Board Member's website page "Google Drive Documents 2010-2016". The page has a "Questions and Answers" section at the bottom describing the rationale for, and steps taken with regard to, keeping these documents where they always resided rather than bringing them into the WordPress Media Library. This is the high level folder structure where these documents reside:
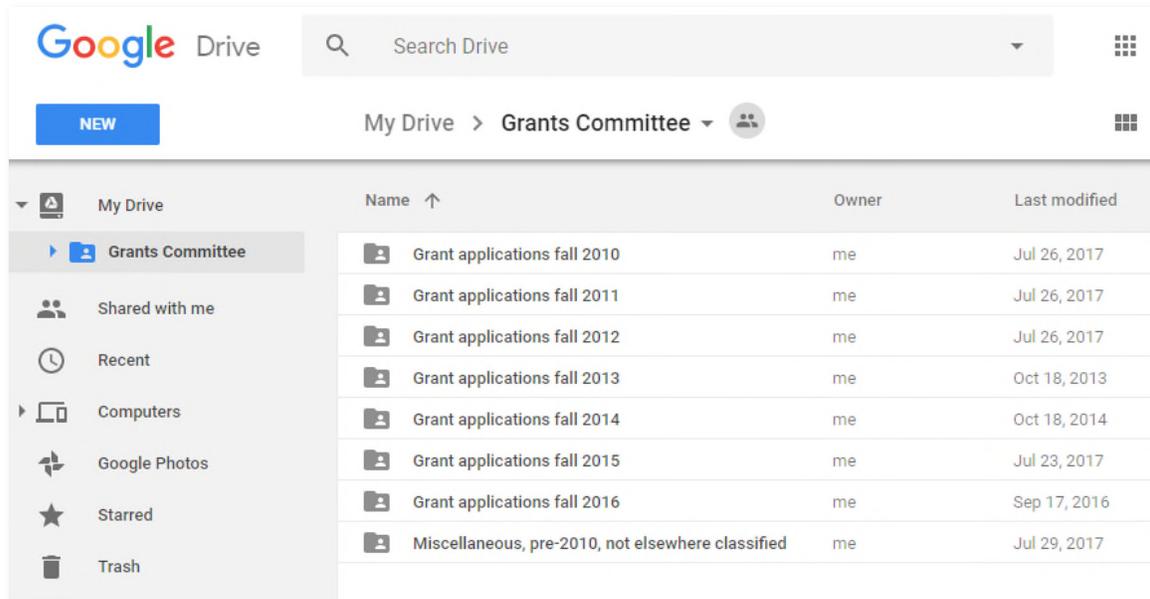
Security with respect to accessing these documents is enabled by the Google Drive Embedder Premium plugin described earlier.

Google Mail Address	
Password	

6   YouTube access

WordPress limits the size of media files (sound, video, images) that can be stored on the database. Therefore – especially in the case of videos – the best practice is to create links within WordPress pages to a separate YouTube account. On the Wells website this is the case for the video that appears on the page "Slide Show – Photos from the Wells Archive".

URL	
User ID	
Password	

7 Updating/correcting applicant records entered through WPForms

7.1 Background

As discussed elsewhere Wellsfound.org uses a form plugin called WPForms that allows organizations to apply online for grants. See screenshot below for how the data content looks once it has been entered. WPForms has worked very well for collecting user data but it has no means for correcting data that's already been entered and submitted. This might be caused by an applicant fat-fingering the entry on the form or, alternatively maybe there was turnover in the applicant organization and therefore a point-of-contact needs to be changed.

This is not a huge deal considering the relatively small number of records we are talking about, but it is something of an irritant when it comes to generating acceptance and rejection letters. That is because WPForms can export a CSV file with all the applicant organization data content. That CSV file is then brought into a Word mail merge letter. Any changes or corrections must be made at that point.

So, my "ask" of ▮▮▮▮▮▮▮▮ of the WordPress User Group was, "*Is there a way I could correct the record within the underlying SQL database?*" A description of the solution follows.

7.2 Example
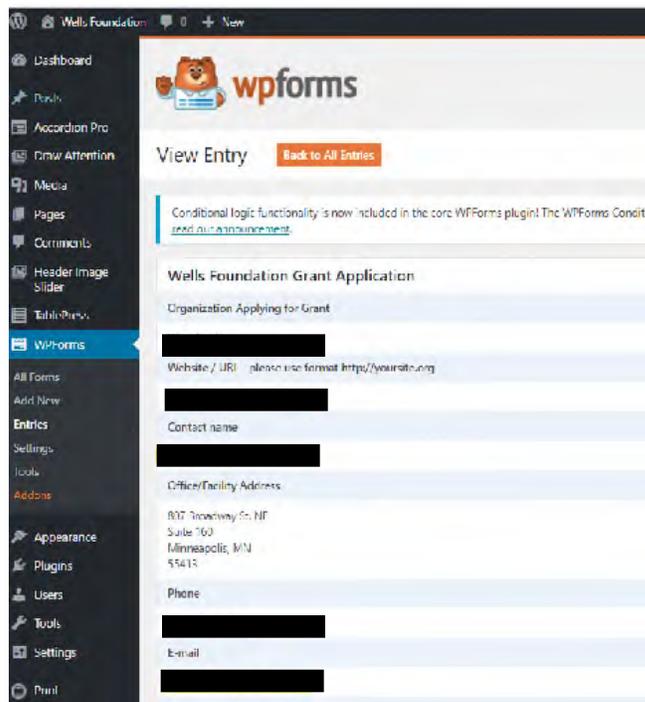
Figure 7-1

The contact person for the applicant ███████████ (as shown above) has changed to Eliza Wright, ████████████████████ (from her predecessor, ████████████).

7.3   Steps to follow

7.3.1   Go into cPanel and update the table wells_wpforms_entry_fields

Access to cPanel is discussed in section 2.3. The **phpMyAdmin** page opens up the fields and values of the table **wells_wpforms_entry_fields**.[5]
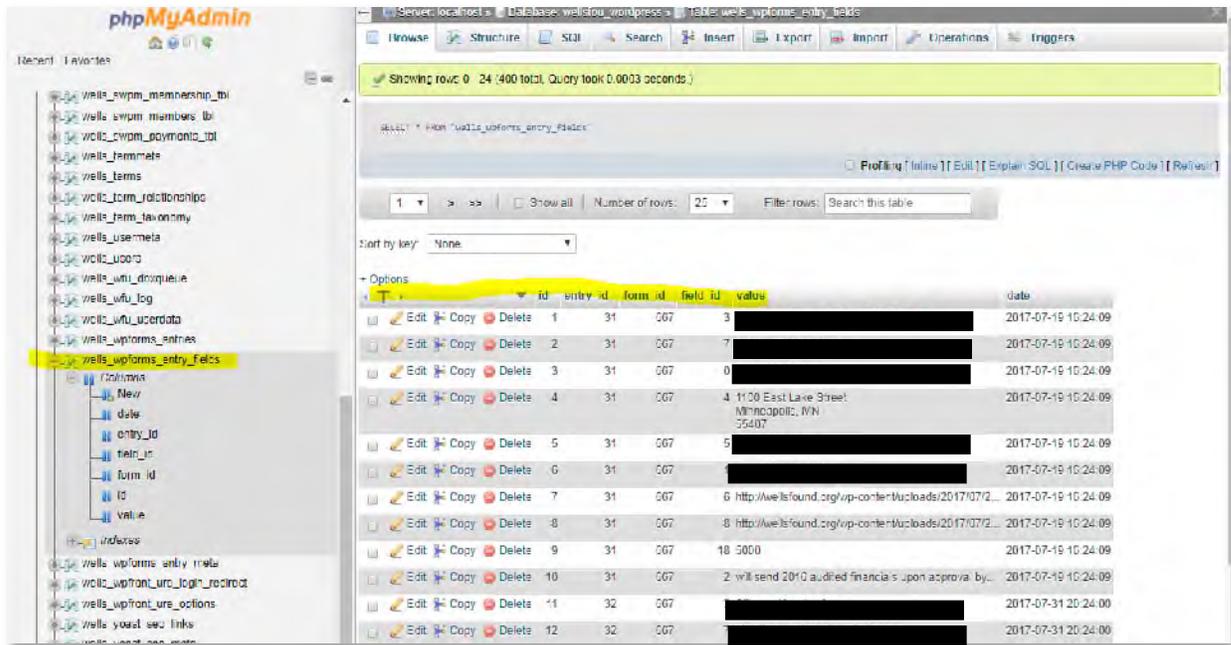
Figure 7-2

7.3.2   Find the record(s) that need(s) to be changed

Note here and in what follows that this applicant is identified by **entry_id** "48".

Figure 7-3

---

[5] I am *guessing* this table is where the data entered by the applicant organization is stored as soon as they click on the WPForms submit button.

7.3.3 Double click on field(s) to be changed

Placing the cursor on the field automatically opens it up for editing.

Figure 7-4

7.3.4 Similarly edit the wells_wpforms_entries table

There is another table – **wells_wpforms_entries** – that appears to **hold the data in the formatted manner displayed in** *Figure 7-1*.[6] Updating the first table **does not appear to update the second**. Here is a screenshot updating the second table.

Figure 7-5

7.3.5 Confirm changes

The screen where the record is displayed now shows the correct information.

---

[6] Here again I'm guessing.

8 Media Library security access solution using Wordfence plugin
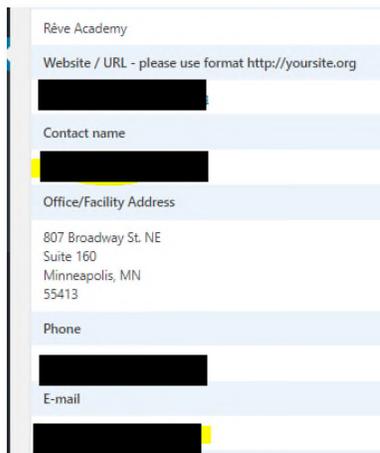
8.1 Where/how the WordPress Media Library is stored

The Media Library typically holds every document that a WordPress page is linked to. [It may also hold images, audio files, etc.]. These files are organized automatically in a predictable way – i.e., usually (although not always) in folders that are automatically created and named according to a pattern. The default naming/storage convention is the month and year in which an upload first occurs; we are using that default for Wells.

8.2 Example of the naming convention

If, say, on April 1st a new document is uploaded then WordPress will create an "04" subfolder under the "2018" subfolder. If a few days later another document is uploaded it DOES NOT create a new folder -- /2018/04 already exists – but instead just drops the document into "/2018/04". This is like what we do on the PC except WordPress creates the folders automatically according to these rules.

8.3 What is the security problem with Media Library items?

Start with the fact that our website URL is wellsfound.org.

- If I am (a) a malicious hacker, (b) knowledgeable about WordPress, and (c) savvy enough to recognize that a website has been developed in WordPress [sometimes this is easy to deduce, other times not] then …
- … It's not too hard to know the folder structure where these documents live. This is shown in *Figure 8-1* and reflects the VULNERABILITY THAT MUST BE ADDRESSED.

Figure 8-1

- Notice what is highlighted in yellow at the top – it's the Wells URL followed by a drilldown from a root-level folder/subfolder (wp-content/uploads) into the YYYY/MM folder mentioned earlier.
- You could click on any one of these document links and the document will open. [Ignore the fact that there are multiple files similarly named; that's a long explanation around a feature of WordPress that's not relevant to the question at hand].
- Figure 8-2 shows that it is possible to open one of the Beacon documents just using the browser. I (as an outsider) can do this *even though I am not signed on as WordPress administrator nor am I even signed onto the website as a board member.*
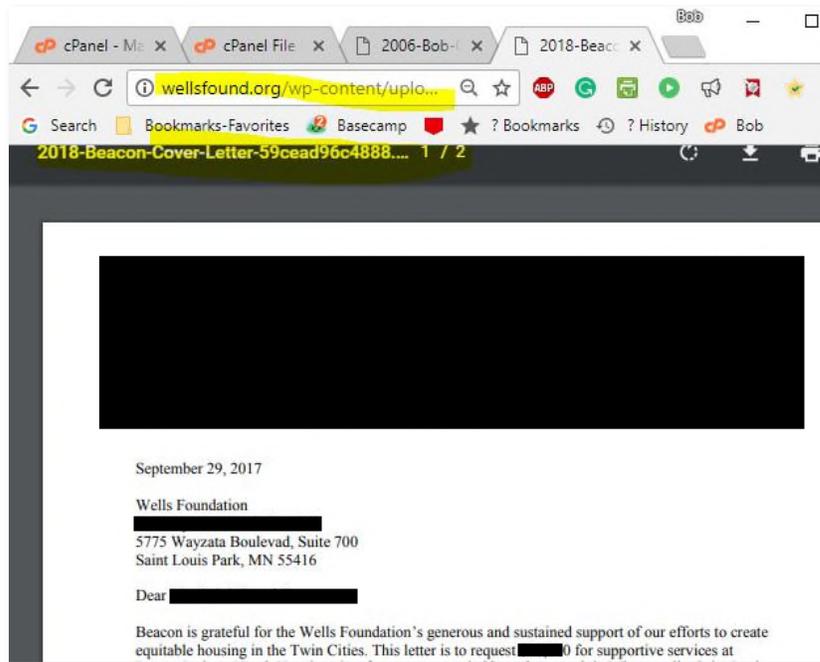

Figure 8-2

8.4   Solution to the vulnerability

This "Media Library visibility" issue is an inherent weakness that is handled in various ways by other WordPress websites. The solution recommended by the Twin Cities Small Business WordPress User Group for a site like that of Wells is a plugin known as Wordfence. With this plugin we can place a tiny file named *index.php* into the "MM" folder along with whatever other items are being stored there. Figure 8-3 shows this in action. The tool used to upload index.php is an FTP software called "Filezilla". It's a standard, free application used by website developers and others for moving files between a local PC and a remote server.

Figure 8-3

8.5   Proof that the Wordfence solution is working as expected

In Figure 8-4 you see the same URL shown in Figure 8-1. However, now the hacker is blocked from seeing anything. In addition, I checked to make sure that (a) as an example, the Beacon document is still visible from the Board Member page and (b) public items – like the photos that appear on the home page – are still visible to the public. Both checked out.

Figure 8-4

8.6 Other points

8.6.1 Wordfence <> Simple WordPress Membership plugin incompatibility

There was one odd outcome using this Wordfence solution that was addressed again with help from the user group.

- In WordPress parlance a "slug" is a series of words or numbers that define a page and appear after the website's URL. So, for example, the "Contact Us" page URL is https://wellsfound.org/contact-us/.
- The slug for that page is what is shown in *Figure 8-5*. This is a screenshot from the Wells Administrator console.
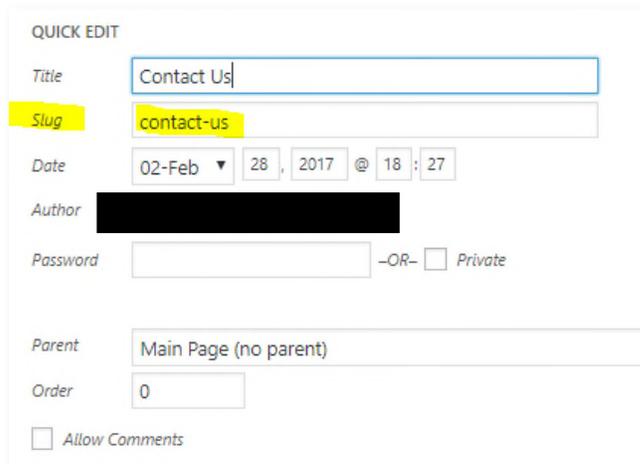

Figure 8-5

- WordPress generates these slug text strings automatically according to the name of the page, but they can be overridden.
- One of the pages began with "2018" and this caused the error message shown in Figure 8-4 to NOT appear as it should. A user group member determined that each WordPress page slug must NOT start with a 4-digit number that looks like a year.
- This appears to be an arcane problem of incompatibility between two plugins: Wordfence and Simple WordPress Membership (the plugin used to manage access to the board member menu). However, *incompatibilities between plugins like what is shown here are not uncommon in the WordPress world* and are dealt with through testing and troubleshooting along the lines of what happened here.

8.6.2 Going forward

The index.php file has been added to each "MM" subfolder for each year out there. Going forward *each time there is a new upload in a new month that step will be replicated*.