EDHP-SIG Maintenance

The following document provides help and resources for the EDHP-SIG website.

Contents

Background Information

This website was developed by Tom Smalling under the guidance of Dr. Atsusi Hirumi in the spring & summer semesters of 2020. Along with the website, a social media presence for the EDHP-SIG was concurrently developed by Dr. Efren De La Mora Velasco.

Developer Contact Information

Tom Smalling
407-461-1888
tom@smallingstudios.com
https://smallingstudios.com

Template & Builder System

This website was developed using the *Avada* template and *Fusion Builder* system. This template was chosen because it is highly flexible and offers many options for website owners. *Fusion Builder* provides a simple system for developing pages using a fluid box-based approach. Furthermore, the template offers comprehensive documentation and help files for beginners and professionals.

Working with Fusion Builder

The *Fusion Builder* uses a system of containers, columns, and boxes to develop pages quickly. Each column is responsive, and depending on the width of the browser, the columns will appear normal or stacked.

Video Objectives:

1. Demonstrate how to create pages.
2. Demonstrate how to use the *Fusion Builder* system.
3. Demonstrate how responsive pages work in the *Avada* template.
4. Demonstrate how to add pages to the menu system.

https://vimeo.com/421687450/2f9b1bd326

Support Documentation

All Support Documents
https://theme-fusion.com/support/

Avada Template Documentation
https://theme-fusion.com/documentation/avada/

Fusion Builder Documentation
https://theme-fusion.com/documentation/fusion-builder/

Additional Resources

ThemeFusion YouTube Channel
https://www.youtube.com/user/ThemeFusionVideos

Padlet Resource Wall

Padlet is a simple tool for aggregating different sources for an audience in one area. Padlet provides an easy interface to upload and share different files, PDFs, links, and images. A positive aspect is the open nature of *Padlet*, and the ability to embed *Padlets* in websites and share with a community of people.

Video Objectives:

1. Describe how *Padlet* is connected to the EDHP-SIG website.
2. Demonstrate how to upload a Word Document.
3. Demonstrate how to upload a PDF file.
4. Demonstrate how to link to a Google Drive folder.

https://vimeo.com/421184304/6081502923

Additional Resources

Padlet YouTube Channel
https://www.youtube.com/channel/UC9YVlt7eSTTYOFNw0kyJhiA/videos

Website Maintenance

WordPress is an actively developed, content management system. Consistent maintenance is critical for WordPress websites to ensure they run without issues and remain secure from hackers. The following section reviews procedures for backups and updates on the server.

Website Backups

Please note, when using GoDaddy Managed WordPress, the backups are included in the price and automatically set up. The status of the backups is checked in the hosting dashboard. In an emergency, the website can be restored from the past 30 days. If another hosting level or service is utilized, the location and implementation of the backup system may be different. Backups can also be purchased through external plugins such as *JetPack.*

Video Objectives:

1. Demonstrate how to access backups in GoDaddy managed WordPress accounts.

https://vimeo.com/421687057/e449848f57

WordPress Updates

Please note, In a managed WordPress hosting environment, this maintenance task is handled by the web host. For other hosting setups, the administrator must update the WordPress installation. WordPress has frequent "point" updates to the core system. As these updates become available, they should be applied to the website. Many of these updates provide security updates. Major releases are less frequent and should be applied after they are released. It is prudent to wait a few days before installing a major release to ensure there are no significant issues for early adopters.

Video Objectives:

1. Demonstrate how to update WordPress.

https://vimeo.com/421687254/93c64a68a4

Theme Updates

Similar to WordPress, *Avada* is consistently developed and improved. As updates are delivered for the themes, they should be applied. It is important to note; there are two themes required to maintain the website. The first theme is *Avada*, which contains all of the files required to run the theme. The second theme, which should remain active, is *Avada Child*. The child theme holds custom CSS styles, and PHP overrides created by the designer. Furthermore, the *Twenty Twenty* theme should remain for emergency testing purposes.

Video Objectives:

1. Discuss themes and running a lean WordPress installation.
2. Explain child themes.
3. Demonstrate how to update themes.

https://vimeo.com/421686815/c1f60388d0

Plugin Updates

One of the most significant vulnerabilities in terms of security of WordPress is the open implementation of plugins (Subsign, 2017). WordPress plugins allow the website administrator to add functions and features to a website. Plugins are provided by many different companies and are consistently developed and updated. Plugins must be consistently updated to ensure that potential security flaws are handled.

Video Objectives:

1. Discuss premium and standard plugins.
2. Demonstrate the update process for premium plugins.
3. Demonstrate the update process for standard plugins.

https://vimeo.com/421686322/4e7bd171ed

Update Failures

First and foremost, do not panic. It is a sporadic occurrence that a website cannot be fixed when an update fails. In the worst-case scenario, the website can be retrieved from the latest backup. Use the following techniques to determine what kind of issue is present:

Identify if it is a caching or server issue
When a failure occurs, begin by double-checking the connection to the website. Sometimes, there is an issue with browser caching or server caching. Open a private browser session and view the website to see how the website appears. If the website appears or appears but is broken, then re-login into the website and try to update the offending plugin.

Plugin refuses to update
Occasionally, some plugins are stubborn. A typical error message is "Could not create directory." In this instance, there is a permissions issue happening on the server. The most straightforward solution is to remove the plugin's folder under the *wp-content/uploads/plugins* directory via FTP. The plugin can then be reinstalled through WordPress.

Additional information:
https://kinsta.com/knowledgebase/installation-failed-could-not-create-directory/

Wordpress stuck in Maintenance Mode
"WordPress has a built-in maintenance mode that it activates whenever you update your software, themes, or plugins from the WordPress dashboard" (Kinsta, 2020). Sometimes there are issues in the WordPress system when conducting maintenance, and WordPress gets stuck maintenance mode. Turn off maintenance mode by removing the *.maintenance* file in the root directory. Use FTP to log in to the server and delete the file. Clear the browser cache and log into the website to ensure it is working correctly.

Additional Resources
WordPress Maintenance 101
https://kinsta.com/blog/wordpress-maintenance/

Website Security
The following section covers security for a WordPress installation. Running a secure website involves a mixture of maintenance and preventative actions. The Wordpress Installation and plugins should be consistently updated to ensure there are no easily exploited vulnerabilities. Furthermore, the website should be consistently backed up to ensure it can quickly be rebuilt in the instance of a hacker. Along with these maintenance items, it is essential to monitor for suspicious activity and control access to the website.

Sucuri Plugin
Hackers are a constant issue on the internet. The Sucuri plugin has been installed and activated as a preventative measure. The Sucuri plugin is a premium service, and it requires a yearly subscription for full monitoring. The free version of the Sucuri plugin provides preventative measures for hardening the server, email alerts, file integrity checks for core WordPress files, and malware scanning (Sucuri, n.d.).

Additional information can be found on Sucuri's website:
https://sucuri.net/wordpress-security-plugin/

Wordpress User Accounts

Providing users access to a website involves much trust between the organization and the person. To avoid issues of security, Wordpress has implemented a series of roles for the admin to choose for users. To control access and minimize security risks, please provide the appropriate level of access for users. These roles include:

- **Administrator** – An administrator is somebody who has access to all the administration features within a single site.
- **Editor** – An editor is somebody who can publish and manage posts, including the posts of other users.
- **Author** – An author is somebody who can publish and manage their posts.
- **Contributor** – A contributor is somebody who can write and manage their posts but cannot publish them.
- **Subscriber** – A subscriber is somebody who can only manage their profile. (WordPress.org, n.d.)

To learn more about user roles and capabilities, visit:
https://wordpress.org/support/article/roles-and-capabilities/

Additional Resources

The Ultimate WordPress Security Guide – Step by Step (2020)
https://www.wpbeginner.com/wordpress-security/

Appendix

Monthly Maintenance Checklist

Below is a list of tasks to complete monthly to ensure the website functions properly.

Double-check daily backups

In a managed Wordpress installation, the backups are performed through the hosting company. The status of the backups may be accessed on the hosting account overview page. There should be an option for *Files*, *Database,* or *Files & Database*. Choose any of the options to make sure the dates are recent.

Apply WordPress updates

In a managed Wordpress installation, WordPress updates are performed through the hosting company. In standard installations, the updates will appear next to the dashboard. Follow the instructions on the screen to complete the updates.

Apply theme updates

There are three themes on the website. *Avada*, *Avada Child*, and *Twenty-Twenty*. Update *Avada* and *Twenty-Twenty* as they become available. If additional themes are installed after a WordPress update, they can be safely deleted. Along with the theme updates, the *Avada* theme has its *Fusion Patcher* system. Apply these minor fixes as they appear.

Apply premium plugin updates

The *Avada* theme includes premium plugins with the installation. Before installing and updating these plugins, there must be a valid registration token in the system. To access the premium plugin update page, from the administration dashboard, click Avada > Plugins and then update the premium plugins.

Apply standard plugin updates

Standard plugins should be updated consistently. These updates can be accessed through the update button on the admin toolbar, or through the Plugins > Installed Plugins menu.

Empty WordPress caches

Once updates are complete, it is good practice to flush the cache, so the old website files are removed. On the top admin toolbar, click “Managed Wordpress” and choose “Flush Cache.”

Review the Sucuri plugin for suspicious events

Access the *Sucuri* plugin through the menu on the left. Click on “Sucuri Security” and choose “Dashboard.” On this page, the integrity of WordPress core files can be checked, along with validation, the website is clean of malware.

References

Kinsta. (2020, May 8). *How to fix WordPress stuck in maintenance mode*. Retrieved May 21, 2020, from Kinsta: https://kinsta.com/knowledgebase/wordpress-stuck-in-maintenance-mode/

Subsign. (2017, October 18). *Disadvantages of a WordPress website*. Retrieved May 21, 2020, from Medium: https://medium.com/@subsign/disadvantages-of-a-wordpress-website-92f0a799b823

Sucuri. (n.d.). *Sucuri WordPress Plugin*. Retrieved May 21, 2020, from Sucuri: https://sucuri.net/wordpress-security-plugin/

WordPress.org. (n.d.). *Roles and capabilities*. Retrieved May 21, 2020, from WordPress.org.