**DIGM-243: Web Authoring II**

**Week 08**

**WordPress Security**

The worst thing that can happen with WordPress is to have your site, or your client's site, hacked.

You need to have a back up plan. Every host has their own process but you cannot rely on this. Read your terms of service. Here is a section from the terms from HostMonster:

**Backups.** For its own operational efficiencies and purposes, Hostmonster.com from time to time backs up data on its servers, but is under no obligation or duty to Subscriber to do so under these Terms. IT IS SOLELY SUBSCRIBER'S DUTY AND RESPONSIBILITY TO BACKUP SUBSCRIBER'S FILES AND DATA ON HOSTMONSTER.COM SERVERS, AND under no circumstance will Hostmonster.com be liable to anyone FOR DAMAGES OF ANY KIND under any legal theory for loss of Subscriber FILES AND/or data on any Hostmonster.com server. Hostmonster.com will not attempt to back up accounts that exceed 50,000 files or 30 Gigs of space for any reason.

Simply downloading a copy of your all your ftp server files is only half of a complete backup strategy! Wordpress stores all of your post and page content within several tables, in a database. This database and it's tables are NOT stored in any one file or folder. Fortunately you can easily export ALL of your database/table content via the WP Dashboard (Tools - Export). I suggest you download a complete backup of your site AND your export Wordpress database at least once a month, just in case! If you do not want to manually backup your Wordpress site you can always buy a plug-in to help automate the process

To my experience the [backupBuddy](http://pluginbuddy.com/purchase/backupbuddy/) plug-in is the best currently on the market.

**Backup your entire WordPress install.** Widgets, themes, plugins, and SQL database - the entire package! You should not leave the backup process up to your web host. Just like your laptop or desktop computer, you should be doing regular backups of your blog or website. With BackupBuddy you can schedule backups and have them sent off-site to Amazon S3, Rackspace Cloud, an FTP/FTPS account, or to your email.

**Restore your WordPress site fast.** The restore function in BackupBuddy is super simple. You upload the importbuddy.php script and your backup file, and it restores WordPress: your themes, widgets, plugins, and everything else. No need to install WordPress first! Other backup solutions only backup; BackupBuddy restores too!

If possible have two different domains on different hosting providers. Use one domain as your main site. Use the other domain for backup, development, and testing. If you have backed up to your main domain (.com) to your backup domain (.net) on a regular bases. You still have a way to get your content out to your public (or clients) in case disaster strikes.

**WP Security Measures**

**Rule #1: Stay Up-to-Date**

WordPress developers are constantly working to make Word-Press a better, more secure and stable platform. This is one of the key advantages to open source software. Many developers, each with different skill sets, are looking over the code every day and performing various audits and updates to improve the overall codebase.

Updates often fix security concerns before there are exploits in the wild. In fact, many of the recent exploits have been targeting outdated versions of WordPress while consistently updated sites are immune.

WordPress implemented new notices in the Dashboard letting you know when there is a new version available. Another new feature is the ability to upgrade WordPress directly from the Dashboard. The WordPress team has been working to make upgrading as painless as possible. This new feature lets the site administrator update the WordPress Core right from inside the web interface.

If your web server has the ability to write to the files in your WordPress directories, then the automatic upgrade functionality works. If not, WordPress prompts for your FTP credentials to update the files for you. Both of these situations concern us. In general, your web user should not have write permissions to your entire web root. This is just asking for trouble, especially on a shared hosting platform; realizing, of course, that certain directories such as the uploads folder must be writable by the web user in order to function.

**Secure the .htaccess and wp-config.php files**

One thing hackers try to do in order to take control of your system is to either get access to the .htaccess file or the wp-config file. In order to protect these you just add the following to your .htaccess file:

<Files .htaccess>

Order Allow,Deny

Deny from all

</Files>

<Files .wp-config.php>

Order Allow,Deny

Deny from all

</Files>

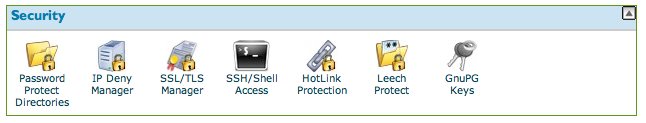
**Remove /wp-admin/install.php**

Delete this file from your server. WordPress used to instruct you to do this, but a lot of people overlooked it. They now claim you do not need to, but also that it wouldn't hurt to remove it. Better safe than sorry.

**Password protect the wp-admin folder**

One of the biggest causes of WordPress hacks if choosing weak passwords. You can password protect your wp-admin folder using your cpanel, and at least that way you have 2 passwords that need to be broken in order to gain access to the wp-admin.

To do this in HostMonster's cpanel see the Password Protect Directories option in the Security Section.



**Force SSL on Login and Admin**

You can force your visitors and administrators to log in via an SSL encrypted page, assuming you have that set up already. You have a few options when it comes to SSL. You can force WordPress to use SSL for logins only, or you can use SSL for all administration sessions. To do this, edit your WordPress config file and add the following flag:

define('FORCE\_SSL\_LOGIN', true);

You can also force the entire WordPress Dashboard to be served over HTTPS. Again, edit your config file and add the following line:

define('FORCE\_SSL\_ADMIN', true);

With the SSL login option, your username and password will be handled in a secure transaction (encrypted). All your other traffic, including the authorization cookies you receive from WordPress, will be sent in the clear. While this is obviously somewhat more secure, it is slower.

There are also plugin options to force SSL, including:

* **Admin SSL**
* **WordPRess HTTPS**

**Change file permissions to read only when possible**

It is best to lock down the file permissions as much as you can. Letting people/application to have write access to your clients files can be quite dangerous.

* Files - set permission to 644
* Folders - set permission to 755

This also can be done in cpanel with the File Manager option under the Files Section. This has a Change Permissions option on the top level navigation.

**Generate Authentication Security Keys**

We did this at the time of install. Since WordPress 2.6, there has been the ability to add authentication keys. These encrypt the information stored in cookies more difficult to crack. This is a really simple step, just go here: https://api.wordpress.org/ secret-key/1.1/salt/ and paste the information into your wp-config.php file.

**Block Bad Queries Plugin**

This plugin protects WordPress against malicious URL requests. Many WordPress sites gets attacked with extremely malicious code, fortunately Jeff Starr wrote a simple script that checks for excessively long request strings (i.e., greater than 255 characters), as well as the presence of either eval( or base64 in the request URI.

**WP-FileMonitor Plugin**

This plugin monitors your WordPress installation for any added/deleted/ changed files. When a change is detected an email alert is sent out to you. The reason why this is so important is that if a site does get hacked, it will help you get to the bottom of which file caused it, which will help you prevent an attack in the future. You donʼt want to be left in a situation, where you have fixed the site, but donʼt know how it happened.

**WP Security Scan Plugin**

Scans your WordPress installation for security vulnerabilities and suggests corrective actions.

**WordPress Exploit Scanner Plugin**

WP-Exploit Scanner is another plugin that scans your files, posts, and comments for suspicious information. Basically, this is a forensics tool for you to use to make sure your site has not been compromised. This plugin does not remove anything, but creates a list of suspicious content for you to review.

**Change your admin user name**

Such a obvious step, but one that hardly anyone thinks about. Every automated install sets up an account named admin. This means hackers are half way to accessing your data. Make this part of your setup process.

If you do have an account with username:admin, you cannot change the name while you are logged in as 'admin'. You will need to create a new account with admin rights, log in as that new user, then delete the username:admin account.

**Secure passwords**

This seems so obvious, but as mentioned above, weak passwords are the most common way for sites to get hacked. Try and use alphanumeric passwords. If you donʼt have 1Password or Roboform, then checkout http://goodpassword.com

**Change database prefix**

Most hacks target the database, so one of the most important steps you can take is to change the database prefix. Do not be put off by the perceived complexity of doing something like this, the plugin BuddyBackup (as mentioned earlier), which we will automate this process.

**Remove WordPress Version from header**

It is probably not a good idea to advertise to hackers which version of WordPress you are using. If there are known security holes in a given system version, and you are using it, it will tip them off on how to hack your site.

In the header.php file remove the following line:

<meta name="generator" content="WordPress <?php bloginfo('version');?."" /><!-- leave this for stats -->

The wp\_head function also includes the WP version in your header. To remove it, add this line of code in your functions.php

remove\_action('wp\_head', 'wp\_generator');

**Hardcore Security for WP**

**Limiting Access To wp-admin by IP Address**

Create a .htaccess file inside your wp-admin directory. Then add the following

code:

AuthUserFile / dev/null

AuthGroupFile / dev/null

AuthName "Access Control"

AuthType Basic

order deny,allow

deny from all

#IP address to Whitelist

allow from xx.xxx.xx.xx

Replacing xx.xxx.xx.xx with your specific IP address will only allow you access to the wp-admin directory.

<http://whatismyipaddress.com/>

Or you can use a plugin:

**Login Lockdown**

The Login Lockdown plugin helps protect you from brute force password attacks by disabling the login function for a range of IP addresses after several failed attempts in a short period of time

**Further Hardcore Security Reading**

* <http://codex.wordpress.org/Hardening_WordPress>
* <http://digwp.com/2010/07/wordpress-security-lockdown/>
* <http://net.tutsplus.com/tutorials/wordpress/20-steps-to-a-flexible-and-secure-wordpress-installation/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%253A+nettuts+%2528NETTUTS%2529>

## Removing Comments

There are a few ways to remove comments from your wordpress installation. The first step is to go to Settings > Discussions and under *Default Article Settings*, uncheck the box for

* Allow people to post comments on new articles"

Then under *Other Comment Settings*, check the boxes for

* Comment author must fill out name and e-mail
* Users must be registered and logged in to comment

Then for extra added security, check the boxes for

*E-mail me whenever*

* Anyone posts a comment
* A comment is held for moderation

*Before a comment appears*

* An administrator must always approve the comment
* Comment author must have a previously approved comment

Be sure to SAVE CHANGES at the bottom of the page

This will remove the comment form, but replace it with something like:

**Leave A Reply**

You must be logged in to post a comment.

Make sure you go to Settings > General and uncheck "Anyone can register" . This will remove the Register link from the wp-login page.

To completely remove comments, you will need to scrub through each template file and look for the following code:

comments\_popup\_link

comments\_template();

If you find these codes in your template files, remove them and all appropriate surrounding tags.

Or if you just want to disable it, but be able to reenabe it an any time easy just comment it out like such:

<?php //comments\_template(); ?>

**Homework**

**Read:**

* **Beginning WordPress 3: Make Great Websites the Easy Way**Chapter 11 - Performance and Security
* **Professional WordPress: Design and Development**Chapter 11 - Statistics, Scalability, Security, and Spam

**Build:**

Continue coding your theme

Bring your files to class for review.

Be able to show your instructor what progress you have made on your lists:

* Changes you believe you will be able to make in the Dashboard.
* Changes you believe you will be able to make in CSS.
* Changes you believe you will have to make with PHP.

**Submit:**

N/A

**[Instructor NOTE: Check it see if students have made progress, if students has NOT made progress ask them why, offer assistance (during class lab time), and remind him/her that their final project is the Majority of their grade for the class]**