WordPress Website Hardening Methodology

1.0 – Updates to WordPress Themes and Plug-ins

#	Hardening Procedures	Status
1.1	Ensure that WordPress is updated to the latest version.	
1.2	Consider configuring automatic WordPress updates.	
1.3	Ensure that all WordPress themes and plug-ins are updated to the latest version.	
1.4	Consider configuring automatic WordPress theme and plug-in updates.	
1.5	Delete all unused themes or plugins.	

Plug-ins to consider:

1. Enable automatic WordPress Core updates. (More Here)
2. Enable automatic Theme and plug-in updates. (Advanced Automatic Updates)

2.0 – Accounts and Passwords

#	Hardening Procedures	Status
2.1	All passwords should be updated to meet minimum password strength requirements.	
2.2	Consider a WordPress plug-in to enforce strong password requirements.	
2.3	Create a new administrator account with a unique username and strong password.	
2.4	Delete any default administrator or user accounts.	
2.5	Consider enabling two-step authentication.	
2.6	Limit the number of login attempts to 3 attempts.	
2.7	Require a CAPTCHA for all login pages.	
2.8	Utilize automatic password generators and storage tools	

Plug-ins to consider:

1. Enforce strong password requirements. (Wordfense)
2. Utilize password generators. (WP Password Generator, Norton Password Generator)
3. Enable two-step authentication. (Plug-in options here)
4. Enforce limited login attempts. (Wordfense, Limit Login Attempts)
5. Enforce CAPTCHA requirements for login. (Jetpack)
6. Automatic password generator and storage (LastPass)

3.0 - File Permissions and Securing Key Folders

#	Hardening Procedures	Status
3.1	The following folders/files should be configured to be writable to only the administrator account: - /wp-admin/ - /wp-includes/ - /wp-content/ - /wp-content/themes/ - /wp-content/plugins/	
3.2	Add server-side password protection to the wp/admin/ page.	
3.3	Disable file editing within WordPress (more here)	
3.4	Secure wp-includes (more here)	
3.5	Consider the installation of a Web Firewall (WAF) to the web server.	

Plug-ins to consider:

1. Security Plug-ins (iThemes Security, All in One WP Security)
2. Open Source Web Firewall (ModSecurity)

4.0 – Data Backups, Logging, and Monitoring

#	Hardening Procedures	Status
4.1	Automatically backup the MySQL database on a periodic basis.	
4.2	Encrypt all data backups and/or backup to read only media.	
4.3	Install forensic logging devices or plugins.	
4.4	Install an intrusion detection device or plugins.	

Plug-ins to consider:

1. Security Plug-ins (iThemes Security, All in One WP Security)
2. Automatic backup plugin (VaultPress, BackUpWordPress)
3. Security Logging and Monitoring Plug-in (Securi Security)
4. Open Source Intrusion Detection (OSSEC)

5.0 – Manual Control Considerations

#	Hardening Procedures	Status
5.1	Gather key login detail from Website developer and ensure ownership is completely transferred including: - Server login - WordPress login - url ownership and hosting* - all files and images**	
5.2	Ensure individuals are assigned to perform the following functions: - receive and respond to backup alerts and failures - receive and respond to intrusion detection alerts - receive and respond to password failures - receive and respond to alerts for updates, theme updates, and plug-in updates	
5.3	Develop a documented incident response plan in the event of website security breach of defacement. Events include: - backup alerts and failures - intrusion detection alerts - password failures - alerts for updates, theme updates, and plug-in updates	
5.4	Develop a documented backup and disaster recovery plan in the event of website outage.	

*If you had someone develop your WordPress website don't leave your domain name and hosting behind. Be sure to ask for the domain and hosting registration and payment details!

**Any images and logos developed for your website belong to you. Be sure to ask for the raw image files. This will be important if you want to use your logo for other marketing purposes.