ds communications

web and graphic solutions

The Care and Nurturing of your WordPress Site

Dave Adams

daveadams@ds-communications.com

www.ds-communications.com

....I can build you a site for 500 bucks!!

Challenges to your site

- Local viruses
- DOS
- Spam
- Admin Incompetence
- SQL Attacks
- Bad Plugins
- Poor Hosts
- Bloated Code
- Too much functionality

File Permissions

Core:

- Should be writable only by your server user account.
  - files = 0644
  - directories = 0755 (less restrictive)
  - These settings ensure that the core is writable only by the user account and readable by the web (ie. the world)
  - {demo: http://permissions-calculator.org/}

.HTACCESS

- codex suggests setting looser permissions in order to make it writable by WordPress.

Themes

- same as core
- Exception: if modifing themes via dashboard. If so, make it group writable.

Plugins

- use defaults and then evaluate case by case

File Permissions (cont.)

wp-content/uploads (and wp-content/cache if applicable)

- Needs to be writable for users to upload files
- Set to 777 but try 755 or 750. 777 is considered vulnerable.

Disabling Directory Views

- can be done via htaccess file, hosts control panel or blank index file.

Golden Eggs

WP Specific	Generic
• wp-config.php • install.php • /wp-admin	• .htaccess • .htpasswd • php.ini • PHP scripts • Flash source files (.fla format) • Photoshop files (.psd format) • Log files

Tip 1: {demo: see .htaccess}
Tip 2: Just nuke install.php

Tips

- Protect the login page
  - Use Strong Passwords, Change Often
  - Don't use username of 'admin'
  - Limit by IP via htaccess file
    - {demo: see .htaccess}
- Limit the number of login attempts

- Remove tidbits of information
  - Login {demo: see cycle.ottawacitizen.com & functions.php}
- Get away from defaults
  - change table prefix of "wp_" to "xyz_"
    - {demo: see wp-config_new.php}

.....and for the lazy

- WP Security Scan
- LockDown Plugin

Spam - The NON Plugin Approach

- Disallow PingBacks and TrackBacks
- Require authors to provide name and email
- Users must be registered (if possible)
- Disallow comments on old documents
- Monitoring via email alerts (if possible)
- Admin approval (if possible)
- Requiring approval for documents with multiple links
- Black Lists

Spam - The .htaccess Approach

Problem: Automated spam bots typically target the comment processing scripts directly, bypassing your comments.php form altogether. Such activity results in HTTP referrers that are not from your domain

Solution: {demo: see .htaccess}

http://perishablepress.com/press/2006/11/20/block-spam-by-denying-access-to-no-referrer-requests/

Spam - The Plugin Approach

{Demo: see http://www.505.ca/blog/nor-2011-ontario-championships/}

Shields Up and Site Monitoring

- Inspector WordPress {demo: see plugin and log files}
- www.changedetection.com

Database

- Demo: How to Optimize
- Demo: Portable PMA
- Demo: Backups using **WP-DBManager**
- How to recover Lost Passwords

WordPress Optimization

- Split long posts into multiple pages
- Hardcode database calls to improve performance
- Disable unused/unnecessary plugins
- Caching {demo: See Plugins}

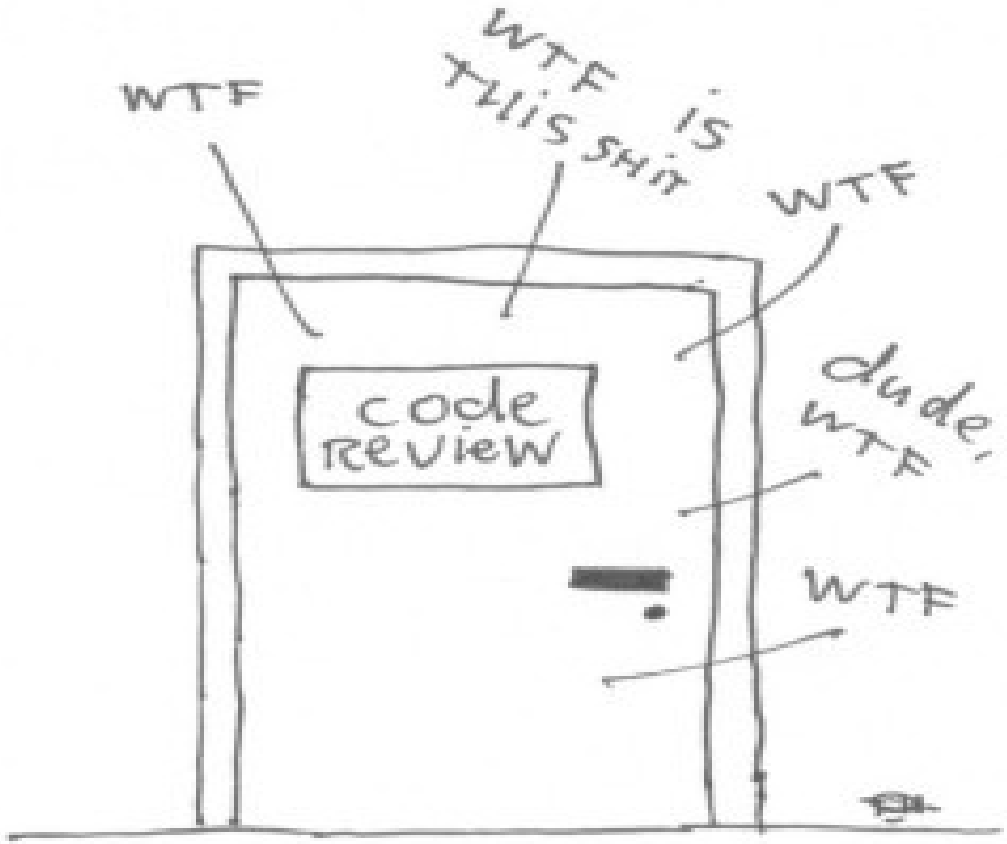
Plugins - My Love Hate Relationship

Signs of Bad Plugins:

- Unable to deactivate
- Does not clean up after itself
- Bloats the wp_options table
- Does not come from WordPress.org
- Not active (ie. no current updates)
- Unvalidated User Inputs (SQL Injections)

The ONLY VALID MEASUREMENT OF CODE QUALITY: WTFs/MINUTE

Good code.



BAd code.

Web Hosts

- Register Domain Seperately from your host
- Pay with PayPal
- Avoid Black Holed ISP. Bad Neighbours kill your SEO
- Good ISPs should have a Spam Policy
- Trial Period should be long and reasonable refund policy
- Language Factor
- Don't go with the cheapest
- Do you own backups

Site Migrations

Option 1: Mess with DB (a too simplistic explanation with serialization being the GOTCHA)

```
UPDATE wp_options
SET option_value = 'http://NEWsite.com'
WHERE option_value = 'http://OLDsite.com'
```

Option 2: Plugins

Option 3: {demo: see Under Construction http://www.rockandbauble.com/}

References:

- The Codex
- Digging into Wordpress (http://digwp.com/)