

SECURING WORDPRESS

Randall Rode

Security Vulnerabilities

2

- University address offers trusted domain and high-volume internet access – attractive to spammers.
- Properly maintained and configured WordPress installations are very secure – i.e. WordPress.com .
- “Create” efforts from faculty, students and other users can complicate the security footprint.

General Considerations

3

- Maintain regular server/software updates
 - Apache, PHP, MySQL, MyPHPAdmin
- Implement best security practices for core software
 - Apache: i.e. No directory browsing (wp-content/plugins)
 - PHP: i.e. No error messages
- Have Monitoring tools in place
 - Regularly check web sites
- Implement service level agreement
 - Do users expect content to stay up forever? What is the lifecycle? When archive it to an html site (<http://www.httrack.com/>)?
- Minimize security footprint
 - Only keep content that is actively being used
 - Only allow access that is specifically required

WordPress Security Principles

4

- Avoid default settings
 - ▣ Reset table names
 - ▣ Rename default admin account
- Implement security standards
 - ▣ Restrict database user account
 - ▣ Force https for user log-in
- Restrict public access
 - ▣ Restrict wp-admin access by IP
 - ▣ Deny *.php files in wp-content, wp-config.php
- Remove unneeded files
 - ▣ Readme.html, license.txt, etc., inactive plug-ins/themes

Installing WordPress

5

- At least 2 options
 - ▣ Do it yourself – create the database, create a database user account, upload the WP files, configure wp-config.php, run the installer
 - ▣ Run an installer script – i.e. Fantastico, Dreamhost – Most common with commercial web host accounts
- Security through plug-ins
 - ▣ Blogsecurity.net, wpsecurity.net

Step 1 – create directory

6

The screenshot shows an SSH Secure File Transfer window for 'yds4.its.yale.edu'. The main window displays a directory listing with columns for Local Name, Size, Type, Mod, and Remote Name. The 'z_exam' folder is highlighted in the listing. A 'z_exam Properties' dialog box is open, showing the 'General' tab. The dialog box displays the folder name 'z_exam', its type as 'Folder', location as '/home/tr236/www/wwwroot', size as '0 Bytes', and modified date as 'Tuesday, January 27, 2009 01:47:38 PM'. The 'Permissions' section shows a table with columns for Read, Write, and Execute, and rows for Owner, Group, and Other. The 'Permission mode' field is set to '775'. A yellow arrow points from the 'z_exam' folder in the listing to the dialog box, and a blue arrow points from the '775' field to the text on the right.

Permissions:	Read	Write	Execute
Owner:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Other:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Permission mode: 775

775 should be sufficient folder setting for most server configurations

644 for files

Step 2 -- set up data user account

7

Server: localhost

Databases SQL Status Variables Charsets Engines Privileges

Processes Export Import

User overview

User	Host	Password	Global privileges	Grant	
<input type="checkbox"/>	root	localhost	No	ALL PRIVILEGES	Yes

[Check All / Uncheck All](#)

[Add a new User](#)

Add a new User

Login Information

User name: Use text field: wp_123

Host: Local

Password: Use text field:

Re-type:

Generate Password:

Global privileges ([Check All / Uncheck All](#))

Note: MySQL privilege names are expressed in English

Data	Structure	Administration
<input checked="" type="checkbox"/> SELECT	<input checked="" type="checkbox"/> CREATE	<input type="checkbox"/> GRANT
<input checked="" type="checkbox"/> INSERT	<input checked="" type="checkbox"/> ALTER	<input type="checkbox"/> SUPER
<input checked="" type="checkbox"/> UPDATE	<input type="checkbox"/> INDEX	<input type="checkbox"/> PROCES
<input checked="" type="checkbox"/> DELETE	<input checked="" type="checkbox"/> DROP	<input type="checkbox"/> RELOAI
<input type="checkbox"/> FILE	<input type="checkbox"/> CREATE TEMPORARY TABLES	<input type="checkbox"/> SHUTDC
	<input type="checkbox"/> CREATE VIEW	<input type="checkbox"/> SHOW I

Step 3 – create database, access

8

Server: localhost

Databases SQL Status Variables Charsets Engines Privileges Processes

User overview

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

	User	Host	Password	Global privileges	Grant	
<input type="checkbox"/>	root	localhost	No	ALL PRIVILEGES	Yes	
<input type="checkbox"/>	wp_123	localhost	Yes	SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, ALTER	No	

↑ Check All / Uncheck All

Add a new User

Remove selected users
(Revoke all active privileges from the users and delete them afterwards.)
 Drop the databases that have the same names as the users.

WordPress Install

- Download latest WordPress from wordpress.org/download
- Rename `wp-config-sample.php` to `wp-config.php`
- Configure `wp-config.php`
 - Enter database name, db user name, db user password in appropriate lines
 - Customize table name, key settings, add forced SSL

Wp-config.php notes

10

```
wp-config.php - WordPad
File Edit View Insert Format Help
[Icons]
/*
/** SPECIAL SETTING - force https in admin directory login */
define('FORCE_SSL_ADMIN', true); */
/**#@+
 * Authentication Unique Keys.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link http://api.wordpress.org/secret-key/1.1/ Wo
 *
 * @since 2.6.0
 */
define('AUTH_KEY',          'X%#GHUzA+EdlTjA=]r4E{@&S8%YCcSaMvnAd:nE/Igy*-ER!MRdspL+Q2<
define('SECURE_AUTH_KEY',  '8E()_N6(3yfc2,--,4TEH$NVQj)3d,pE-[@bGKgQpRl_N/ljKA*-z/xEjy:
define('LOGGED_IN_KEY',    'hBc!X+DquScKJ{ea]L>U:KHVQ>_5PsQ8G+OldRvO~t+LP.;B5byx~Dc/46#
define('NONCE_KEY',        'Cc1[GxiF5ZtEF.)Apc=*9M!Ka>Y q#lM|+?RvN-|L<uazMC=(t+asKCXX$/
/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each a unique
 * prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wp_5af3';
```

Comment out for initial install – then add back

Upload WordPress

11

- First remove unneeded files:
 - ▣ Readme.html, license.txt, wp-content/plugins/hello.php, etc.
- Upload to web server
- Run <http://siteaddress/wp-admin/install.php>
- After install complete uncomment secure FTP line in wp-config.php

htaccess

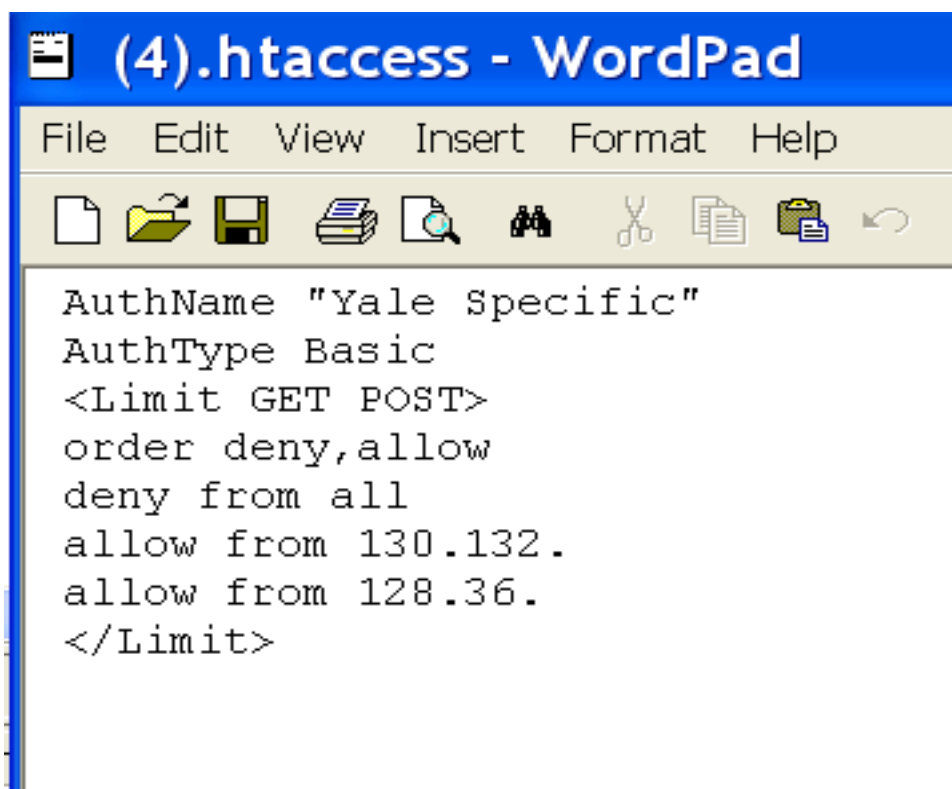
12

- Special server file used to control server behaviors
- Will create our own special ones for the main directory, /wp-content and /wp-admin
- I prefer to manually edit this and not allow WordPress to access them.

Htaccess for /wp-admin

13

- Limit access to a range of, or specific IP addresses



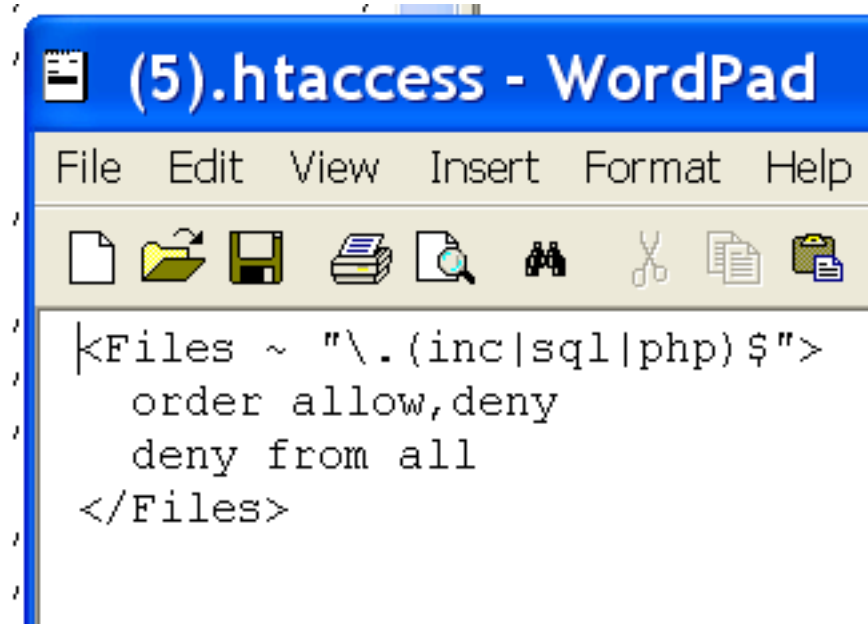
The image shows a screenshot of a WordPad window titled "(4).htaccess - WordPad". The window has a menu bar with "File", "Edit", "View", "Insert", "Format", and "Help". Below the menu bar is a toolbar with icons for file operations. The main text area contains the following configuration:

```
AuthName "Yale Specific"  
AuthType Basic  
<Limit GET POST>  
order deny,allow  
deny from all  
allow from 130.132.  
allow from 128.36.  
</Limit>
```

Htaccess for wp-content, wp-includes

14

- Restrict access to certain file types



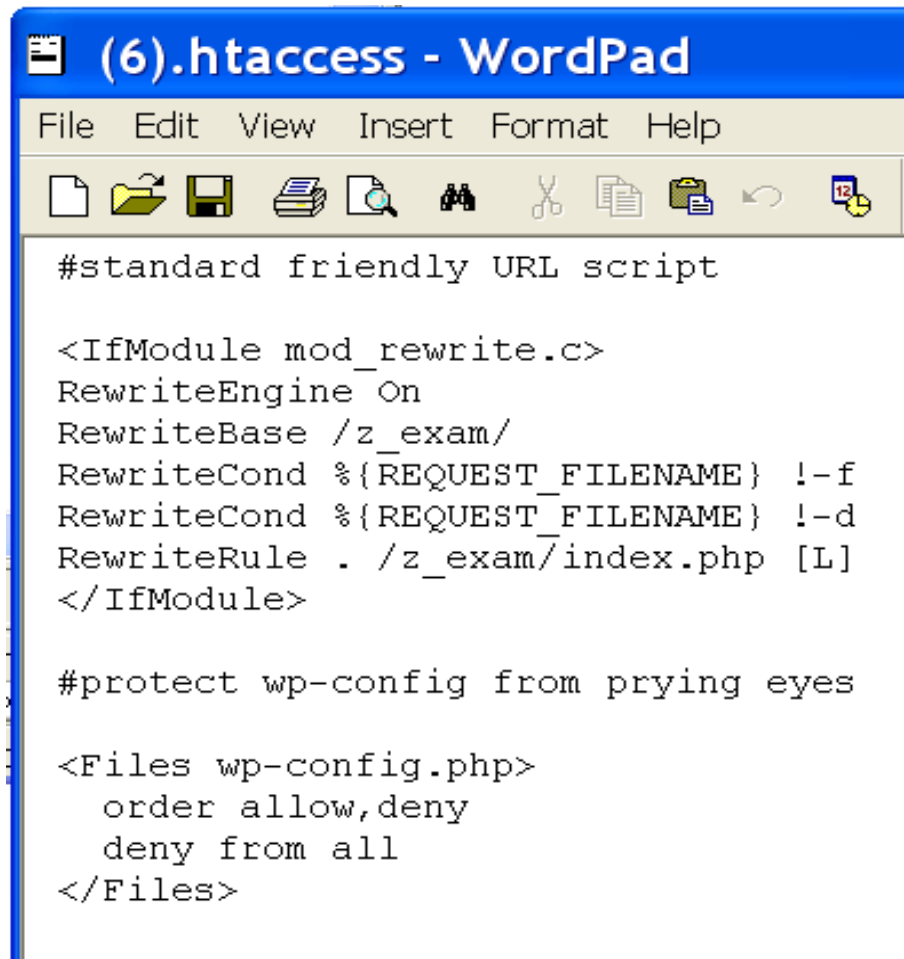
The image shows a screenshot of a WordPad window titled "(5).htaccess - WordPad". The window has a menu bar with "File", "Edit", "View", "Insert", "Format", and "Help". Below the menu bar is a toolbar with various icons for file operations. The main text area contains the following .htaccess configuration:

```
<Files ~ "\.(inc|sql|php)$">  
    order allow,deny  
    deny from all  
</Files>
```

Htaccess for main directory

15

- Set friendly URLs
- Restrict access to wp-config.php



The screenshot shows a WordPad window titled "(6).htaccess - WordPad". The window contains the following text:

```
#standard friendly URL script

<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /z_exam/
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /z_exam/index.php [L]
</IfModule>

#protect wp-config from prying eyes

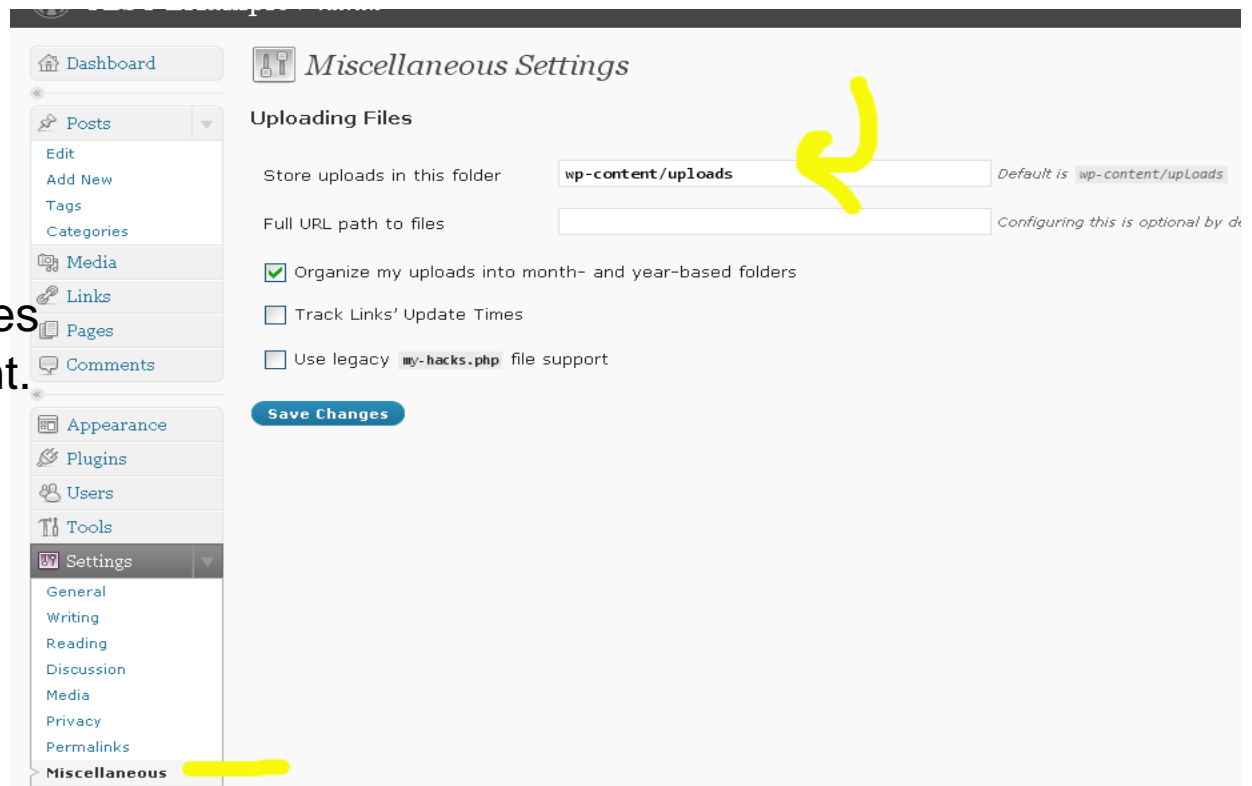
<Files wp-config.php>
  order allow,deny
  deny from all
</Files>
```

Customize file uploads

16

- Principle – change defaults!

Add .htaccess restriction to limit executable file types as you did with wp-content.



The screenshot shows the WordPress 'Miscellaneous Settings' page. The left sidebar menu has 'Settings' expanded, with 'Miscellaneous' highlighted in yellow. The main content area is titled 'Miscellaneous Settings' and contains the 'Uploading Files' section. A yellow arrow points to the 'Store uploads in this folder' text input field, which contains the value 'wp-content/uploads'. The default value is shown as 'wp-content/uploads'. Below this, there is a 'Full URL path to files' text input field with the note 'Configuring this is optional by default'. There are three checkboxes: 'Organize my uploads into month- and year-based folders' (checked), 'Track Links' Update Times' (unchecked), and 'Use legacy my-hacks.php file support' (unchecked). A 'Save Changes' button is located at the bottom of the settings area.

Hide WordPress version tag

17

- Header includes WordPress version number – can be exploited by hackers – the more they have to guess the better!
- Add command to functions.php for selected theme:

```
1 <?php
2 /**
3  * @package WordPress
4  * @subpackage Default_Theme
5  */
6
7 /** Remove WordPress version tag */
8 remove_action('wp_head', 'wp_generator');
9
```

User accounts

18

- Create admin-only accounts and editor accounts for every day use.
- Get more granular control over user permissions through a plug-in such as Role Manager (<http://www.im-web-gefunden.de/wordpress-plugins/role-manager/>)
Not listed in WordPress plug-in repository (<http://wordpress.org/support/topic/200087>) and not listed as working with 2.7, but seems to be OK.
- Always limit users to fewest permissions – it is always easy to add, not always easy to remember to delete

Comments

19

- Comment spam is a huge problem
- Use Akismet, SpamBam (BlogSecurity) plugins
- Consider limiting comments
 - ▣ Turn comments off by default
 - ▣ Comments only by logged in users – no user self-registration
 - ▣ Require all comments to be held for moderation
 - ▣ Require user name/email address/ registration
 - ▣ Employ a Captcha device (plug-in)

Plug-ins to consider

20

□ BlogSecurity.net

▣ WPIDS – Detect Intrusions

<http://blogsecurity.net/wordpress/wpids-wordpress-intruder-detection-system/>

▣ WordPress Online Security Scanner

<http://blogsecurity.net/wordpress/news-140707/>

▣ SpamBam

<http://blogsecurity.net/wordpress/spambam-comment-anti-spam-plugin/>

□ Maximum Security

▣ <http://wpsecurity.net/>

Keep WordPress/plugins updated

21

The screenshot shows the WordPress dashboard for 'RodeWorks'. At the top right, there is a notification: 'WordPress 2.7 is available! [Please update now.](#)'. Below this, the 'Manage Plugins' section is visible. It includes a table of 'Currently Active Plugins' with columns for Plugin, Version, and Description. The table lists 'WordPress Related Posts' (version 1.0), 'Akismet' (version 2.1.4), and 'Bot Counter'. A yellow highlight is drawn around the 'Akismet' row, and another yellow highlight is drawn around a notification at the bottom of the table: 'There is a new version of Akismet available. [View version 2.2.3 Details](#) or [upgrade automatically.](#)' The left sidebar shows the 'Comments' and 'Plugins' menu items highlighted with yellow circles.

WordPress 2.7 is available! [Please update now.](#)

Manage Plugins

Plugins extend and expand the functionality of WordPress. Once a plugin is installed, you may activate it or deactivate

Currently Active Plugins

Actions

<input type="checkbox"/>	Plugin	Version	Description	
<input type="checkbox"/>	WordPress Related Posts	1.0	Generate a related posts list via tags of WordPress By Denis.	Deactiv
<input type="checkbox"/>	Akismet	2.1.4	Akismet checks your comments against the Akismet web service to see if they look like spam or not. You need a WordPress.com API key to use it. You can review the spam it catches under "Comments." To show off your Akismet stats just put <code><?php akismet_counter(); ?></code> in your template. See also: WP Stats plugin . By Matt Mullenweg.	Activ
<input type="checkbox"/>	Bot Counter			Activ

There is a new version of Akismet available. [View version 2.2.3 Details](#) or [upgrade automatically.](#)

Keep full WordPress backups

22

- Back up the database
 - ▣ Manual export through tool like PHPmyAdmin
 - ▣ Through WordPress plug-in such as:
<http://www.ilfilosofo.com/blog/wp-db-backup>
 - ▣ Export through WordPress admin panel – can also be used to transfer – only content, not settings
- Back up the file structure
 - ▣ Should be part of standard server maintenance
 - ▣ Can export locally via FTP program

Review themes/plugin-ins

23

- ❑ Themes include programming (functions.php) and can utilize vulnerable code
- ❑ Look for plug-ins and themes from official WordPress repository
- ❑ Write/design your own
(http://codex.wordpress.org/Writing_a_Plugin,
<http://www.devlounge.net/extras/how-to-write-a-wordpress-plugin>)
- ❑ Check security updates – i.e. Secunia Advisories,
<http://secunia.com/advisories/search/?search=WordPress>
- ❑ Read/subscribe to developer blogs
 - ❑ <http://lorelle.wordpress.com>, <http://blogsecurity.net>,
<http://wordpress.org/development/>

References

24

Used in this presentation:

- WordPress Security Whitepaper, Blogsecurity.net, Philipp Heinze - Primary Author, David Kierznowski - Co-author
•<http://blogsecurity.net/wordpress/wordpress-security-whitepaper/>
- 11 Best Ways to Improve WordPress Security, Pro Blog Design, Hendry Lee, <http://www.problogdesign.com/wordpress/11-best-ways-to-improve-wordpress-security/>
- WordPress Security -- How to Install WordPress Securely, BlogBuildingU.com, Hendry Lee, <http://blogbuildingu.com/wordpress/install-wordpress-securely>

Other resources:

- Maximum WordPress Security, Weblog Tools Collection, Jeff Chandler, <http://weblogtoolscollection.com/archives/2009/01/03/maximum-wordpress-security/>, AudioCast
- Wordpress Security Tips and Hacks, Noupe.com
•<http://www.noupe.com/how-tos/wordpress-security-tips-and-hacks.html>
- WordPress Tips Part 1, wpdesigner.com
•<http://www.wpdesigner.com/2008/01/30/wordpress-tips-part-1/>
- 9 easy ways to secure your WordPress blog, SimpleHelp.net, Ross McKillop, 9/10/09, <http://www.simplehelp.net/2007/09/10/9-ways-to-secure-your-wordpress-blog/>
- WordPress Security Predictions in 2009, Blogsecurity.net, David Kierznowski,
•<http://blogsecurity.net/wordpress/wordpress-security-predictions-in-2009/>
- WordPress Security Prevention, Reactions, and Scares, Lorelle on WordPress, Lorelle VanFossen
•<http://lorelle.wordpress.com/2008/04/28/wordpress-security-prevention-reactions-and-scares/>
- SecurityFocus SQL Injection Bogus, Ma.tt, Matt Mullenweg,
•<http://ma.tt/2008/04/securityfocus-sql-injection-bogus/>
- WordPress Security with Mark Jaquith, WordCamp Toronto 2008, <http://vimeo.com/1893250?pg=embed&sec=1893250>, VIDEO

Resources:

- National Vulnerability Database, search page, <http://web.nvd.nist.gov/view/vuln/search>: NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.
- Secunia Advisories, <http://secunia.com/advisories/search/?search=WordPress>