Secure Wordpress

Bachaav Session
A Null Community Initiative
30 – Nov - 2013

Agenda

- Understand
- How to Setup
- Security Configuration

Agenda

- Understand
  - How Wordpress Works
  - File and Folder Co-relations
- How to Setup
- Security Configuration

Demo Setup

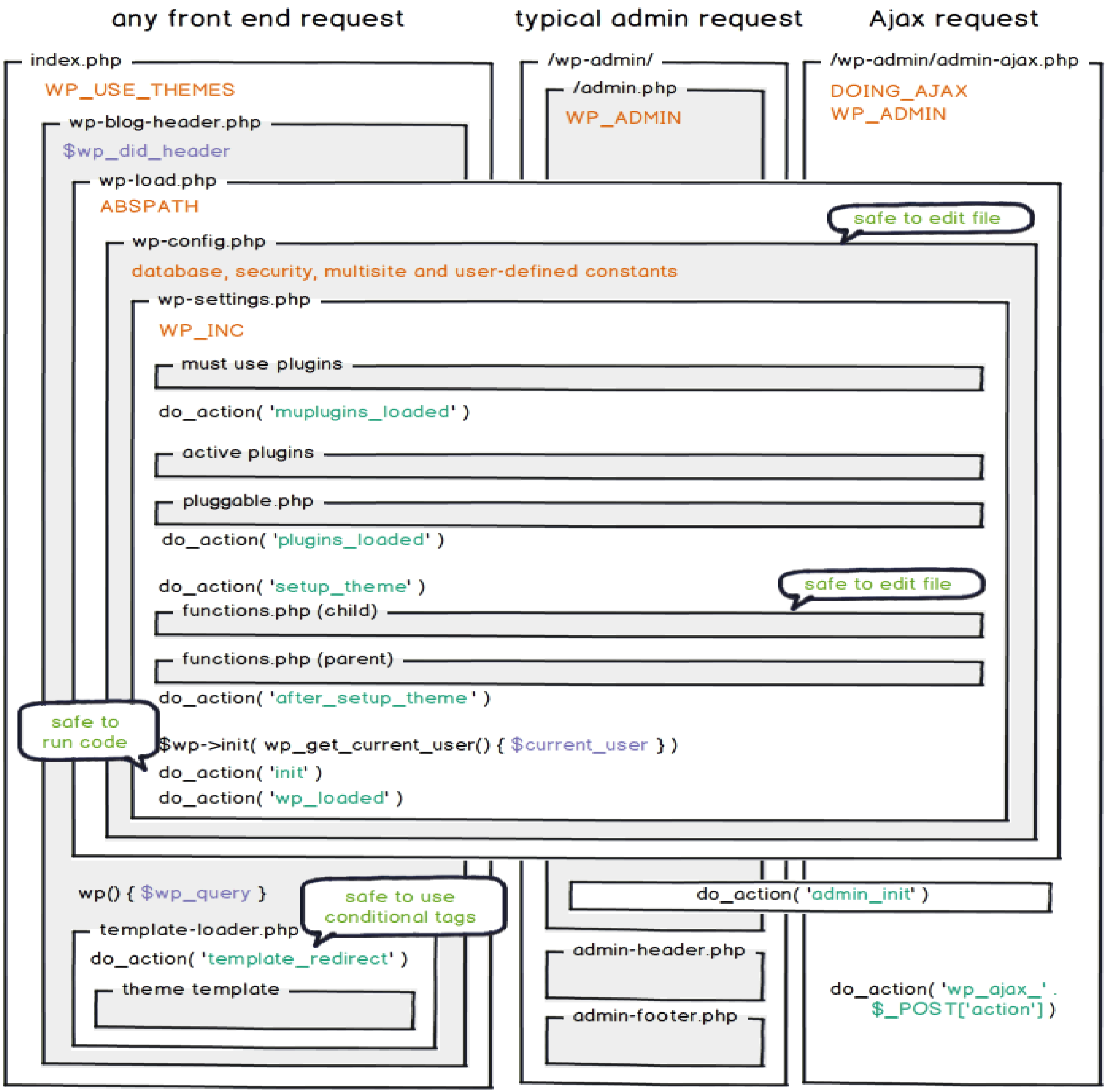
- VirtualBox VM
  - NAT interface for Internet Access
  - Hostonly connection for normal testing
  - sudo ifconfig => get the IP Address
- Various URL
  - http://IP/wordpress
  - http://IP/phpmyadmin
- Credentials
  - Username:wordpress
  - Password:wordpress

How Wordpress Works

- Index.php
  - Define WP_USE_THEMES
  - include(wp-blog-header.php)
- Wp-blog-header
  - include(wp-config.php) -> db and other constants
  - include(wp-settings.php)
    - lots and lots of includes
    - Plugins from PLUGIN_DIR
    - Pluggable_functions loaded (can be overridden by plugins)
  - Path Declaration
  - Query Parsing and assignment
  - HTTP Headers
  - Request Parsing
  - Template Redirections
  - Theme
    - Header
    - Loop
    - Widget / Sidebar
    - Footer

Reference : http://codex.wordpress.org/User:DavidHouse/Wordpress_Code_Flow

Make sense of WP core load



any front end request

index.php

WP_USE_THEMES

wp-blog-header.php

$wp_did_header

wp-load.php

ABSPATH

wp-config.php

database, security, multisite and user-defined constants

safe to edit file

wp-settings.php

WP_INC

must use plugins

do_action('muplugins_loaded')

active plugins

pluggable.php

do_action('plugins_loaded')

do_action('setup_theme')

safe to edit file

functions.php (child)

functions.php (parent)

do_action('after_setup_theme')

safe to run code

$wp->init(wp_get_current_user() { $current_user })

do_action('init')

do_action('wp_loaded')

wp() { $wp_query }

safe to use conditional tags

template-loader.php

do_action('template_redirect')

theme template

typical admin request

/wp-admin/

/admin.php

WP_ADMIN

do_action('admin_init')

admin-header.php

admin-footer.php

Ajax request

/wp-admin/admin-ajax.php

DOING_AJAX

WP_ADMIN

do_action('wp_ajax_' .
$_POST['action'])

File and Folders Co-relations

- wp-config.php
- wp-settings.php
- index.php
- .htaccess
- /wp-admin/
- /wp-content
  - /plugins
  - /themes
- /wp-includes

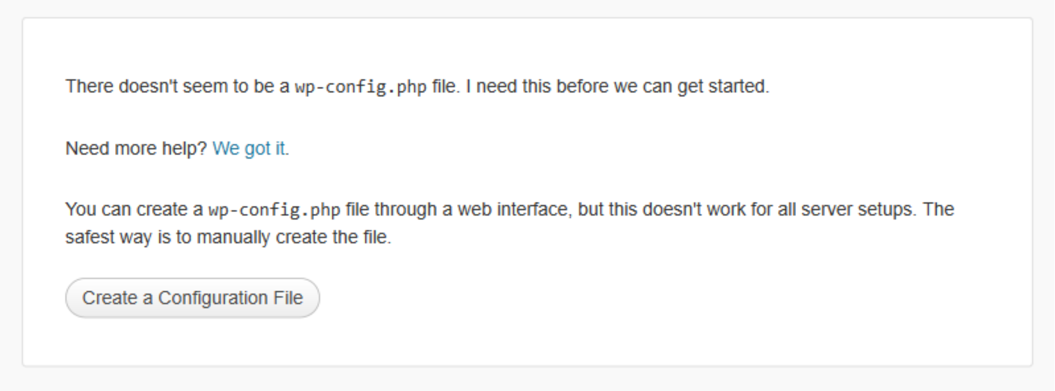
Agenda

- Understand
- How to Setup
  - Setup over FTP / SSH
  - Setup via SVN
- Security Configuration

Setup

- Shared hosting
  - Use Hosting Control Panel
  - Upload Via FTP and run install.php
- VPS / Dedicated / Cloud Server
  - Upload via ssh / ftp
  - Sync via SVN

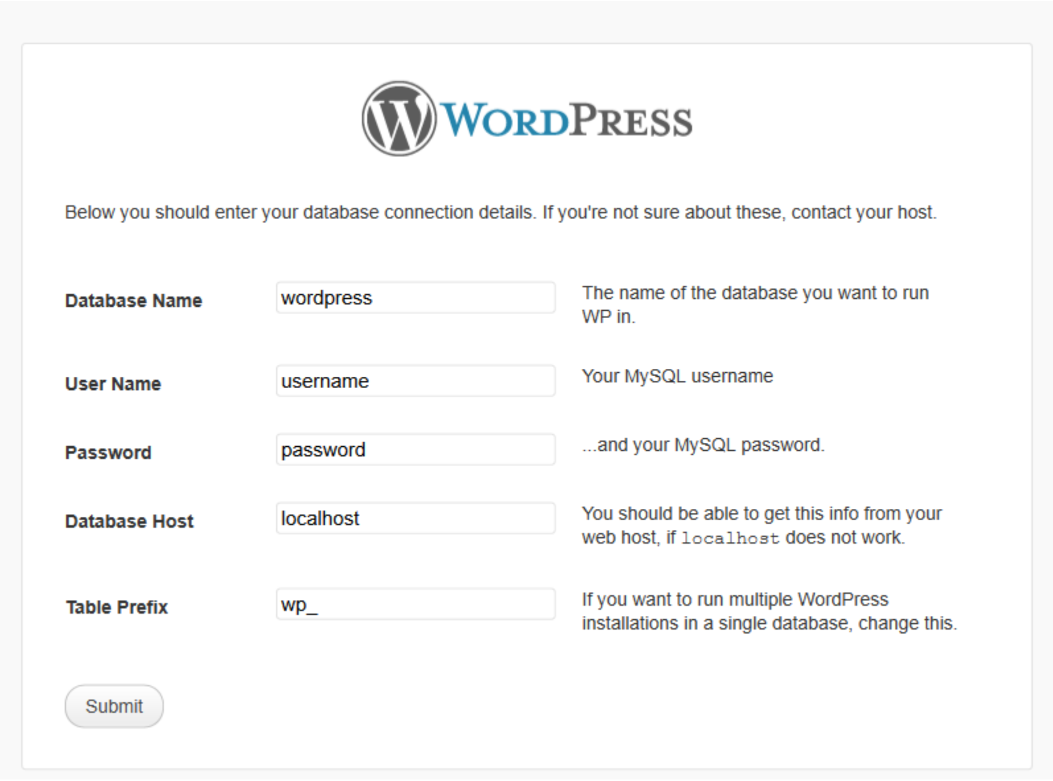
Wordpress Setup



There doesn't seem to be a `wp-config.php` file. I need this before we can get started.

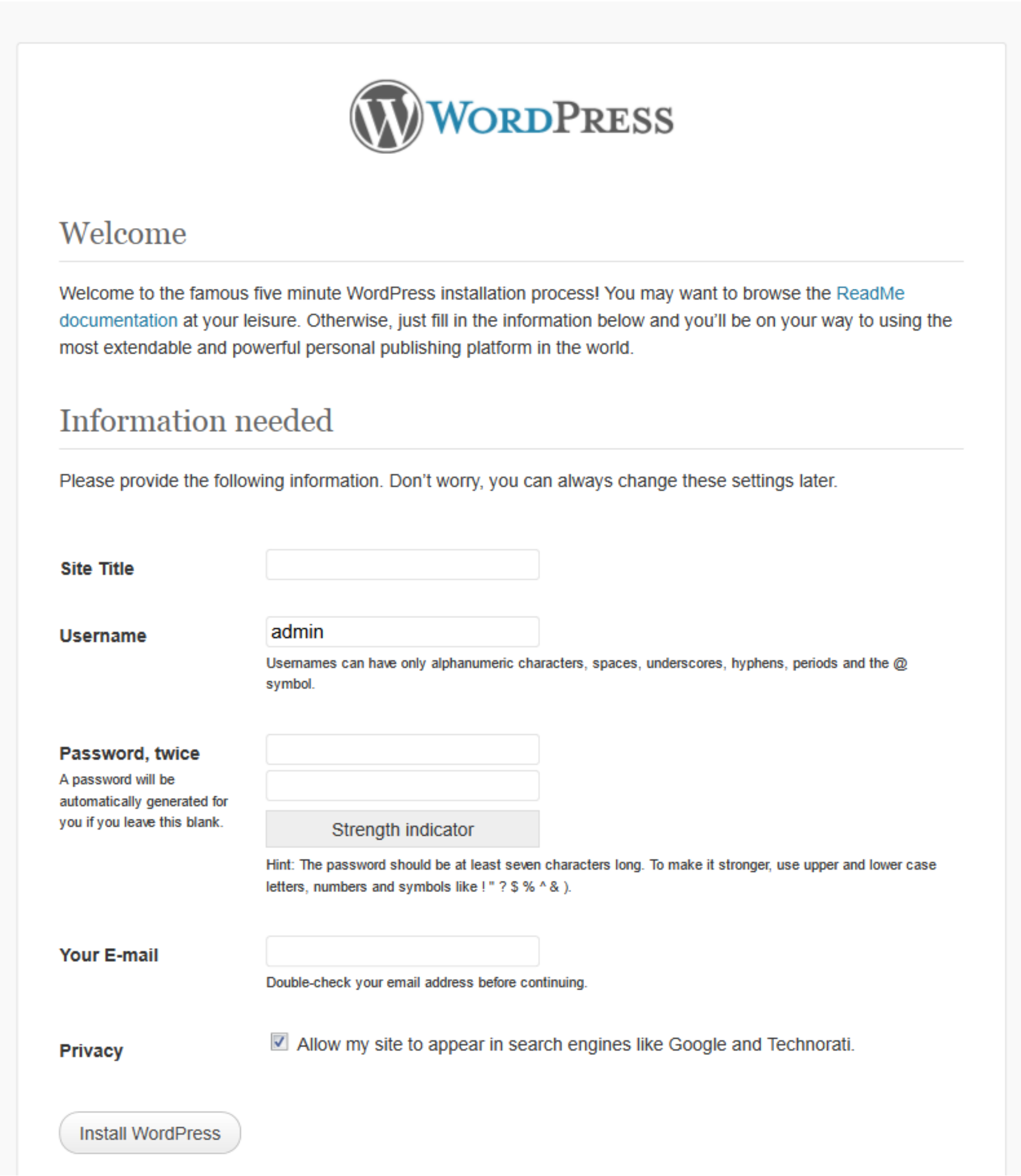
Need more help? We got it.

You can create a `wp-config.php` file through a web interface, but this doesn't work for all server setups. The safest way is to manually create the file.



Below you should enter your database connection details. If you're not sure about these, contact your host.

Database Name	wordpress	The name of the database you want to run WP in.
User Name	username	Your MySQL username
Password	password	...and your MySQL password.
Database Host	localhost	You should be able to get this info from your web host, if `localhost` does not work.
Table Prefix	wp_	If you want to run multiple WordPress installations in a single database, change this.



Welcome

Welcome to the famous five minute WordPress installation process! You may want to browse the ReadMe documentation at your leisure. Otherwise, just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

Information needed

Please provide the following information. Don't worry, you can always change these settings later.

Site Title	
Username	admin Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods and the @ symbol.
Password, twice A password will be automatically generated for you if you leave this blank.	Strength indicator Hint: The password should be at least seven characters long. To make it stronger, use upper and lower case letters, numbers and symbols like ! " ? $ % ^ &).
Your E-mail	Double-check your email address before continuing.
Privacy	☑ Allow my site to appear in search engines like Google and Technorati.

Agenda

- Understand
- How to Setup
- Security Configuration
  - Basic Server hardening
  - Understanding attack vectors
  - Implement Protections

Base Server Hardening

- This session is wordpress focused so we will not cover about server hardening in details

Core Level Attacks

- Present Unpatched Issues
  - Full Path Disclosures
  - Enumeration Issues
    - Username
    - Attachment
    - Plugins
    - Themes
  - Account Bruteforce
  - Version disclosure and Multiple places
- Previously exploited issues
  - XMLRPC based SSRF attack
  - D-DoS and more

Other Attacks

- Plugin / Theme using old Files
- Vulnerable Code in Core
- Vulnerable Code in Plugin / Themes
- Permission and Access Issues

How to Defend

- Core Modifications is not recommended as every upgrade modifies core files.
- Implement Custom HTACCESS based restrictions
- Implement Hook / function override via custom theme templates
- Even theme modification is a absolute no – no as new update will override it.

HTACCESS

- Redirections
  - RewriteCond %{REQUEST_URI} robots.txt
  - RewriteRule ^abracadabra/ http://google.com [R=301,L]
- Custom Directives
  - DirectoryIndex index.html
  - ServerSignature Off
  - Header unset Etag

Theme modification the right way

- Child Theme folder : all files picked first from this and then from parent
- style.css

  /*

  - Theme Name: Anantshri
  - Theme URI: http://www.anantshri.info/
  - Description: Child theme for the twenty twelve
  - Author: Anant Shrivastava
  - Author URI: http://anantshri.info/about/
  - Template: twentytwelve
  - Version: 0.1.0
  - */
  - @import url("../twentytwelve/style.css");
- functions.php : Can be used to provide all function overrides
  - remove_action('widgets_init', 'xyz_widgets_init');
  - add_action('widgets_init', 'abc_widgets_init');

User / Attachment Enumeration

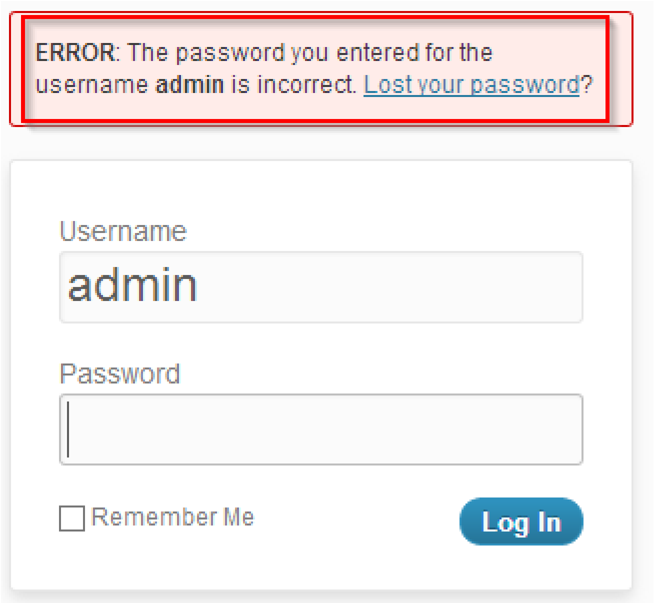
- Index.php?author=1
  - Redirects to /author/<username>
- Index.php?attachment=1
  - Redirects to Individual Attachment URL

Plugin / Theme Enumeration

- How it is identified
  - Predictable URL : wp-content/plugin , themes
  - Predictable file : readme.txt and plugin specific assets(js or css)

Account Bruteforce / Enumeration

- Possible to Enumerate Accounts due to different Error Messages

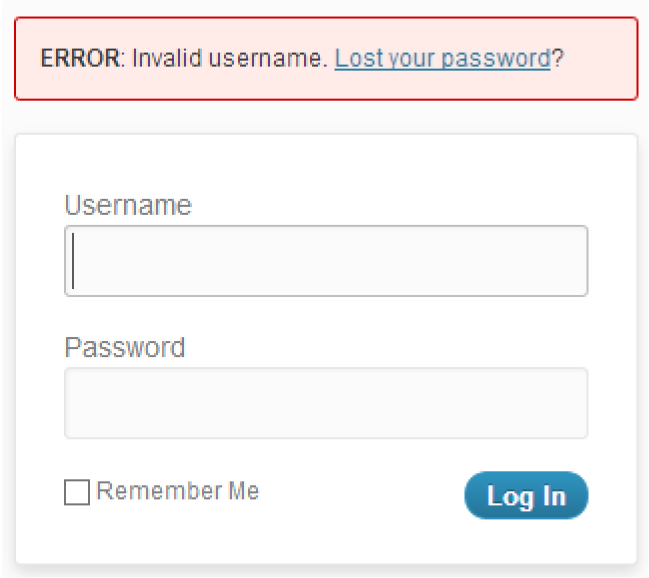


ERROR: The password you entered for the username **admin** is incorrect. Lost your password?

Username

admin

Password



ERROR: Invalid username. Lost your password?

Username

Password

More Issues

- Full Path Disclosures

  display_error : Off (php.ini)
- ClickJacking protection
- swf and timthumb related attacks
- Issues related to wp-includes folder
- Comment Spam
- Dangerous Methods (PUT and more)
- XMLRPC issues
- Automated scanners
- Wordpress header code

Plus a lot more

- This should help us in getting started and since you are now aware of various functions and ways to control them its an open playground now.