

# Wordpress Security



# The Goal of this Presentation...



...Is to scare the crap out of you!

# The Goal of this Presentation...



...and then make everything better  
with the best security tips!



# Topics

- ◉ Example Link Injection Hack
- ◉ Securing your WordPress Website
- ◉ Recommended Plugins



# The Scary



# Link Injection

Hacker bots look for known exploits (SQL Injection, folder perms, etc).  
This allows them to insert spam files/links into  
your WordPress Themes, plugins, and core files.



# 375 Spam Links Per Page

```
<p><!--linksb--><br />
<b style="display:none"><br />
<a href='http://major-pharmacy.com/' title='The Lowest Drugs Online-Offers' alt='The Lowest Drugs Online-Offers'>The Lowest Drugs Online-Offe
<a href='http://your-pharmacy-shop.com/' title='The Best Offers for Viagra, Cialis and Levitra' alt='The Best Offers for Viagra, Cialis and L
<a href='https://addons.mozilla.org/en-US/firefox/user/4342957' title='Buy Cialis Without Prescription' alt='Buy Cialis Without Prescription'
<a href='http://forum.utorrent.com/profile.php?id=141094' title='Order Viagra' alt='Order Viagra' >Order Viagra</a>
<a href='http://cutephp.com/forum/index.php?showuser=30117' title='Cheap Cialis' alt='Cheap Cialis' >Cheap Cialis</a>
<a href=http://www.iscb.org/mambots/yanc/cialis/index.html' title='Buy Cialis fast shipping' alt='Buy Cialis fast shipping' >Buy Cialis fast
<a href=http://www.iscb.org/mambots/yanc/cialis/buy-cialis-fda.html' title='Buy Cialis fda' alt='Buy Cialis fda' >Buy Cialis fda</a>
<a href=http://www.iscb.org/mambots/yanc/cialis/buy-cialis-free-shipping.html' title='Buy Cialis free shipping' alt='Buy Cialis free shipping
<a href=http://www.iscb.org/mambots/yanc/cialis/buy-cialis-from-usa-online.html' title='Buy Cialis from usa Online' alt='Buy Cialis from usa
<a href=http://www.iscb.org/mambots/yanc/cialis/buy-cialis-generic.html' title='Buy Cialis generic' alt='Buy Cialis generic' >Buy Cialis gene
<a href=http://www.iscb.org/mambots/yanc/cialis/buy-cialis-generic-online.html' title='Buy Cialis generic Online' alt='Buy Cialis generic Onl
<a href=http://www.iscb.org/mambots/yanc/cialis/buy-cialis-generic-pharmacy-online.html' title='Buy Cialis generic pharmacy Online' alt='Buy
Online</a>
<a href=http://www.iscb.org/mambots/yanc/cialis/buy-cialis-in-canada.html' title='Buy Cialis in canada' alt='Buy Cialis in canada' >Buy Ciali
<a href=http://www.iscb.org/mambots/yanc/cialis/buy-cialis-in-the-uk.html' title='Buy Cialis in the uk' alt='Buy Cialis in the uk' >Buy Ciali
<a href=http://www.iscb.org/mambots/yanc/cialis/buy-cialis-in-uk.html' title='Buy Cialis in uk' alt='Buy Cialis in uk' >Buy Cialis in uk</a>
<a href=http://www.iscb.org/mambots/yanc/cialis/buy-cialis-line.html' title='Buy Cialis line' alt='Buy Cialis line' >Buy Cialis line</a>
<a href=http://www.iscb.org/mambots/yanc/cialis/buy-cialis-mail-online.html' title='Buy Cialis mail Online' alt='Buy Cialis mail Online' >Buy
<a href=http://www.iscb.org/mambots/yanc/cialis/buy-cialis-money-order.html' title='Buy Cialis money Order' alt='Buy Cialis money Order' >Buy
<a href=http://www.iscb.org/mambots/yanc/cialis/buy-cialis-no-online-prescription.html' title='Buy Cialis no Online prescription' alt='Buy Ci
prescription</a>
```

# CSS Hides the Spam

`<b style="display:none">Any text you want to hide</b>`



# Aftermath

- Website was dropped by Google completely
- Pagerank went from 6 to 5
- Hack also infected phpBB forum
- Organic traffic for “viagra” started showing up

Hack happened in April 2009, website just received PR6 back a few weeks ago



# Scared Yet?



# How about now?



# Securing WordPress



# Don't use the admin account

If you are using the admin account you are wrong!

Either change the username in MySQL:

```
update wp_users set user_login='newuser' where user_login='admin';
```

Or create a new/unique account with administrator privileges.

3. Create a new account. Make the username very unique
4. Assign account to Administrator role
5. Log out and log back in with new account
6. Delete admin account

Make it hard on the hacker!

If they already know your username that's half the battle





**YOU SUCK**

The truth had to be told



# The Great Permission Debate

What folder permissions should you use?

Good Rule of Thumb:

- Files should be set to **644**
- Folders should be set to **755**

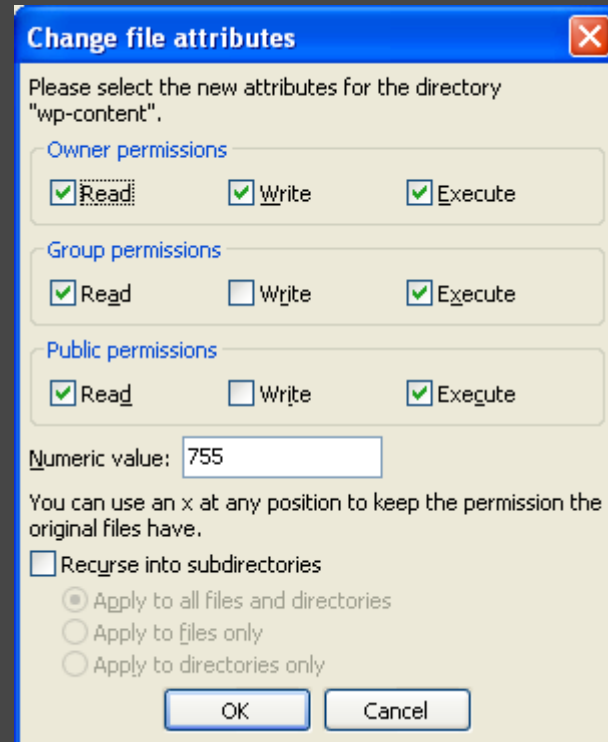
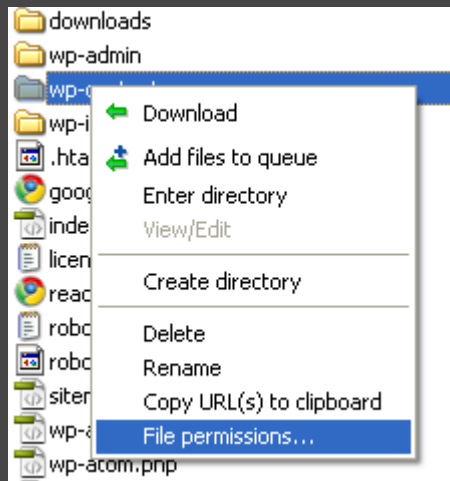
Start with the default settings above  
if you can't upload increase privileges (ie 775, 777)

Permission levels vary depending on server configuration



# The Great Permission Debate

Permissions can be set via FTP



Or via shell access with the following commands

```
find [your path here] -type d -exec chmod 755 {} \;  
find [your path here] -type f -exec chmod 644 {} \;
```

# Move the wp-config.php file

WordPress 2.6 added the ability to move the wp-config.php file one directory above your WordPress root

If WordPress is located here:

```
public_html/wordpress/wp-config.php
```

You can move your wp-config.php file to here

```
public_html/wp-config.php
```

WordPress automatically checks the parent directory if a wp-config.php file is not found in your root directory

This makes it nearly impossible for anyone to access your wp-config.php file as it now resides outside of your website's root directory



# Move the wp-content Directory

WordPress 2.6 added the ability to move the wp-content directory

1. Move your wp-content directory
2. Make two additions to wp-config.php

```
define( 'WP_CONTENT_DIR', $_SERVER['DOCUMENT_ROOT'] . '/blog/wp-content' );  
define( 'WP_CONTENT_URL', 'http://domain.com/blog/wp-content');
```

If you have compatibility issues with plugins there are two optional settings

```
define( 'WP_PLUGIN_DIR', $_SERVER['DOCUMENT_ROOT'] . '/blog/wp-content/plugins' );  
define( 'WP_PLUGIN_URL', 'http://domain.com/blog/wp-content/plugins');
```



If hackers can't find your wp-content folder, they can't hack it!

# Remove WordPress Version from Header

Viewing source on most WP sites will reveal the version they are running

```
<meta name="generator" content="WordPress 2.8" /> <!-- leave this for stats -->
```

This helps hackers find vulnerable WP blogs running older versions

To remove find the code below in your header.php file of your theme and remove it

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

The `wp_head` function also includes the WP version in your header  
To remove drop this line of code in your themes `functions.php` file

```
remove_action('wp_head', 'wp_generator');
```

Themes and plugins might also display versions in your header.

# Stay Current on Updates

Keep WordPress core, plugins, and theme files up to date

Recent WordPress hack only affected outdated WordPress installs

## Shadowbox JS

[Description](#) [Installation](#) [Faq](#) [Screenshots](#) [Other Notes](#) [Changelog](#) [Stats](#)

### 3.0.0.1 (2009-06-30):

- Bring back PHP4 support
- Increase speed by reducing the number of queries
- Code cleanup
- Add changelog output to upgrade notice in admin. Requires WordPress 2.8
- Do not display majority of the settings page form if the options have been removed from the database
- Fix broken localization directory name in code and update localization template
- Remove unused javascript files
- Add Russian translation - Props [Fat Cow](#)

### 3.0.0.0 (2009-06-10):

The newly added plugin Changelog tab makes it very easy to view what has changed in a new plugin version

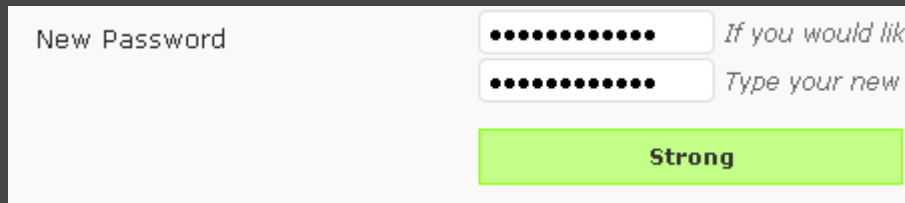
Expect wider adoption in the coming months as this was just added a few weeks ago

# Use Secure Passwords

Use strong passwords to protect your website from dictionary attacks  
Not just for WordPress, but also FTP, MySQL, etc

BAD PASSWORD: bradocks

GOOD PASSWORD: S-gnop2D[6@8



New Password

..... If you would like to use a long password, please enter it here.

..... Type your new password again.

**Strong**



WordPress will tell you when you have it right

Great resource:  
**goodpassword.com**

Creates random passwords



 **Random Password**

Generate Password

12 Size 1 # Passwords

(0-9)  (a-z)

(A-Z)  (?!:,)





**YOU SUCK**

The truth had to be told



# Use Secret Keys

A secret key is a hashing salt which makes your site harder to hack by adding random elements to the password.

1. Edit wp-config.php

2. Visit this URL to get your secret keys: <https://api.wordpress.org/secret-key/>

## BEFORE

```
define('AUTH_KEY', 'put your unique phrase here');  
define('SECURE_AUTH_KEY', 'put your unique phrase here');  
define('LOGGED_IN_KEY', 'put your unique phrase here');  
define('NONCE_KEY', 'put your unique phrase here');
```

## AFTER

```
define('AUTH_KEY', '<6R=V1:Hak 6x0`yZ*teE PaG-kw9;|5yS]f%*D0VV+stO9lq?QuV]VR*dy,ggZB');  
define('SECURE_AUTH_KEY', 'MduY%x#o!P?6n`[4LU~Ca/,:_mMp++j|om3J'8A{-qStd WVGvaa),9|U{n({>FB');  
define('LOGGED_IN_KEY', '!:8,+O+@Z,!7F+. = )YmhGaYjV6@~rq:1W0^/uK& MSoo==v(a EOM}oM;4J,V');  
define('NONCE_KEY', 'KOWQmp~[[z{+Q=n(7-Zll/+:#Rw-1||2GSNrpo +VX6)tYN)Bj;s3yy4:OQTD9`r');
```

You can add/change secret keys at anytime.

This will invalidate all existing cookies and require your users to login again

# Change WordPress Table Prefix

1. Edit wp-config.php before installing WordPress
2. Change the prefix wp\_ to something unique:

```
/**
 * 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 = 'zztop_';
```

All database tables will now have a unique prefix (ie zztop\_posts)



# Force SSL Login and Admin Access

Set the below option in wp-config.php to force SSL (https) on login

```
define('FORCE_SSL_LOGIN', true);
```

Set the below option in wp-config.php to force SSL (https) on all admin pages

```
define('FORCE_SSL_ADMIN', true);
```



# .htaccess lockdown

1. Create a .htaccess file in your wp-admin directory
2. Add the following lines of code:

```
AuthUserFile /dev/null
AuthGroupFile /dev/null
AuthName "Access Control"
AuthType Basic
order deny,allow
deny from all
#IP address to Whitelist
allow from 67.123.83.59
```

Only a user with the IP 67.123.83.59 can access wp-admin



# Recommended Security Plugins



# WP Security Scan

## Initial Scan

**WordPress version: 2.8** You have the latest stable version of WordPress.

Your table prefix should not be `wp_`. [Click here](#) to change it.

Your WordPress version is successfully hidden.

WordPress DB Errors turned off.

WP ID META tag removed from WordPress core

**"admin" user exists.**

The file `.htaccess` does not exist in `wp-admin/`.

*\*\*WP Security Scan plugin must remain active for security features to remain\*\**

## Future Releases

one-click change file/folder permissions

test for XSS vulnerabilities

intrusion detection/prevention

lock out/log incorrect login attempts

user enumeration protection

WordPress admin protection/security

## WP - Security Scan

Name	File/Dir	Needed Chmod	Current Chmod
root directory	../	0755	755.
wp-includes/	../wp-includes	0755	755.
.htaccess	../.htaccess	0644	.0.
wp-admin/index.php	index.php	0644	644.
wp-admin/js/	js/	0755	755.
wp-content/themes/	../wp-content/themes	0755	755.
wp-content/plugins/	../wp-content/plugins	0755	777.
wp-admin/	../wp-admin	0755	755.
wp-content/	../wp-content	0755	777.

<http://wordpress.org/extend/plugins/wp-security-scan/>

# WordPress Exploit Scanner

[Search Files and Database](#) [Search Files Only](#) [Search Database Only](#)

Or search the files on your site for your own words:

**"iframe src"** *iframes can sometimes be used by hackers to load their own adverts and code on your site.*

1. `/var/www/html/lightspeed/wp-content/plugins/akismet/akismet.php`

```
tats.php?blog={ $blog}";
?>
<div class="wrap">
<iframe src="<?php echo $url; ?>" width="100%" height="100%" frameborder="0" id="akismet
</div>
<?php
}

function akismet_get_key() {
global $wpcom_api_key;
if ( !empty($wpcom_api_key) )
return $wpcom_api_key;
return get_
```

2. `/var/www/html/lightspeed/wp-content/plugins/exploit-scanner/exploit-scanner.php`

<http://wordpress.org/extend/plugins/exploit-scanner/>

# WordPress File Monitor

## WordPress File Monitor Options

Perform Scan Now

Dashboard Alert: Yes  (Notification on Dashboard when there is an active alert)

Scan Interval: 30  (in minutes, 0 for Manual Scan only)

Detection Method: Modification Date (faster, but less secure)  Note: Hash method

From Address: brad@webdevstudio: (for alerts)

Notify Address: brad@webdevstudio: (for alerts)

Notification Format: Detailed

Site Root: /var/www/html/lights (Default: /var/www/html/lightspeed/)

Exclude Paths:



# Login Lockdown

## *Login LockDown Options*

### Max Login Retries

### Retry Time Period Restriction (minutes)

### Lockout Length (minutes)

### Lockout Invalid Usernames?

Yes  No

### Mask Login Errors?

Yes  No

Update Settings

### Currently Locked Out

No current IP blocks locked out.

Release Selected



**ERROR:** We're sorry, but this IP range has been blocked due to too many recent failed login attempts.

Please try again later.

Username

Password

Login form protected by [Login LockDown](#).

Remember Me

Log In

[Register](#) | [Lost your password?](#)

<http://wordpress.org/extend/plugins/login-lockdown/>

From WPBeginner.com

Wordpress Security

# WordPress Security Resources

## Security Related Codex Articles

- > [http://codex.wordpress.org/Hardening\\_WordPress](http://codex.wordpress.org/Hardening_WordPress)
- > [http://codex.wordpress.org/Changing\\_File\\_Permissions](http://codex.wordpress.org/Changing_File_Permissions)
- > [http://codex.wordpress.org/Editing\\_wp-config.php](http://codex.wordpress.org/Editing_wp-config.php)
- > [http://codex.wordpress.org/htaccess\\_for\\_subdirectories](http://codex.wordpress.org/htaccess_for_subdirectories)

## Blog Security Articles

- > <http://www.wpbeginner.com/wp-tutorials/11-vital-tips-and-hacks-to-protect-your-wordpress-admin-area/>
- > <http://www.growmap.com/wordpress-exploits/>
- > <http://lorelle.wordpress.com/2009/03/07/firewalling-and-hack-proofing-your-wordpress-blog/>
- > <http://semlabs.co.uk/journal/how-to-stop-your-wordpress-blog-getting-hacked/>
- > <http://www.makeuseof.com/tag/18-useful-plugins-and-hacks-to-protect-your-wordpress-blog/>
- > <http://www.catswhocode.com/blog/10-easy-ways-to-secure-your-wordpress-blog>
- > <http://www.techjaws.com/php-script-injection-exploit-in-wordpress-271/>



# Contact Me

Nazly Ahmed

Blog : [www.nazly.net](http://www.nazly.net)

Email : [me@nazly.net](mailto:me@nazly.net)

Twitter: [@nazly](https://twitter.com/nazly)

