WORDPRESS SECURITY: FUNDAMENTALS FOR PROFESSIONALS

ABOUT ME

WEB DESIGN AND INFORMATION SECURITY

Committed to WordPress since 2008.

SUCURI – RESEARCHER AND ACCOUNT MANAGER

Removing malware and protecting websites.

Personally cleaned over 5,000 websites

SUCURI.NET

TWITTER: @JHERBRANDSON

ABOUT SUCURI

Over 45 Security Professionals Making a Safer Web

SECURITY SCANNING & ANALYSIS

Checking the health over 3 Million websites every month through our free Sitecheck Scanner:
http://sitecheck.sucuri.net

ATTACK PROTECTION

Blocking over 33 million attacks and instances of malicious traffic every month

MALWARE CLEANUP

Cleaning and remediating 300 – 400 hacked or infected websites everyday.

EDUCATION

Providing detailed and actionable security information through our blog at
http://blog.sucuri.net

SUCURI

JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

ATTACK TRAFFIC ORIGINS

Map.Ipviking.com

A QUICK DEMO

Attack in Progress:

https://www.youtube.com/watch?v=v4Xr3LrixVg&list=UUzkxqKA_bkNlj1-nX5f2LNA

Sooo… WHY?

It's Just Business…probably

- The Short Answer: Fame and Fortune
- $BILLION Spam – Generic Pharmaceuticals, Payday Loans, Gambling, Designed Brand Knock Offs
- Hacktivism – Politics and religion at the speed of download
- Immaturity – Kids being kids

Start with the Basics

I

THE NEED FOR SECURITY

THE STATE OF THE INTERNET

2,981,011,519

Internet Users in the world

34,476

Websites hacked today

1,073,467,940

Total number of Websites

www.internetlivestats.com

SUCURI

JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

HOSTING OPTIONS

Choose wisely

Shared Hosting

Dedicated Hosting

Managed Hosting

SUCURI

JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

MANAGED-HOSTING PROVIDERS

WordPress Experts for Everyone!

pagely

synthesis

WP engine

SiteGround

bluehost

SUCURI

JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

SPEAKING OF ENVIRONMENT...

JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

II

No Easy Path

WORD OF WARNING

No chance of 0% risk.

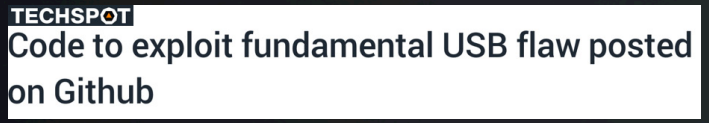
The next '0-Day' attack is always around the corner...

SUCURI

JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

SECURITY HEADLINES

Proof: Seen the news lately?



SUCURI
JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

ALWAYS
Backup

BUT I'VE NEVER HAD A PROBLEM BEFORE...

HAVE A LOW PROFILE, NON-THREATENING SITE? YOU ARE STILL GETTING ATTENTION

JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

FREE WEBSITE REBRAND

- HACKERS HARD AT WORK
- PHARMACEUTICAL SPAM MAKES HACKERS TWO BILLION DOLLARS/YEAR
- **SOLUTION:** OFFSITE BACKUPS
- **RESULT:** CLEAN SITE IMMEDIATELY

SUCURI

JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

AUTOMATED BACKUPS

Know you have a backup plan

BACKUP BUDDY

ithemes.com/
backupbuddy/

VAULTPRESS

Vaultpress.com

SUCURI BACKUPS

Sucuri.net

WEBHOSTING BACKUPS

Your hosting
company

JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

IV

Take Password Policy Seriously

Top 5 passwords used in 2013

Seriously....

Password	Last Year's Rank
'123456'	2
'PASSWORD'	1
'12345678'	3
'QWERTY'	5
'ABC123'	4

credit: SplashData.com

PASSWORD MANAGER

Remembers your passwords so you don't have to

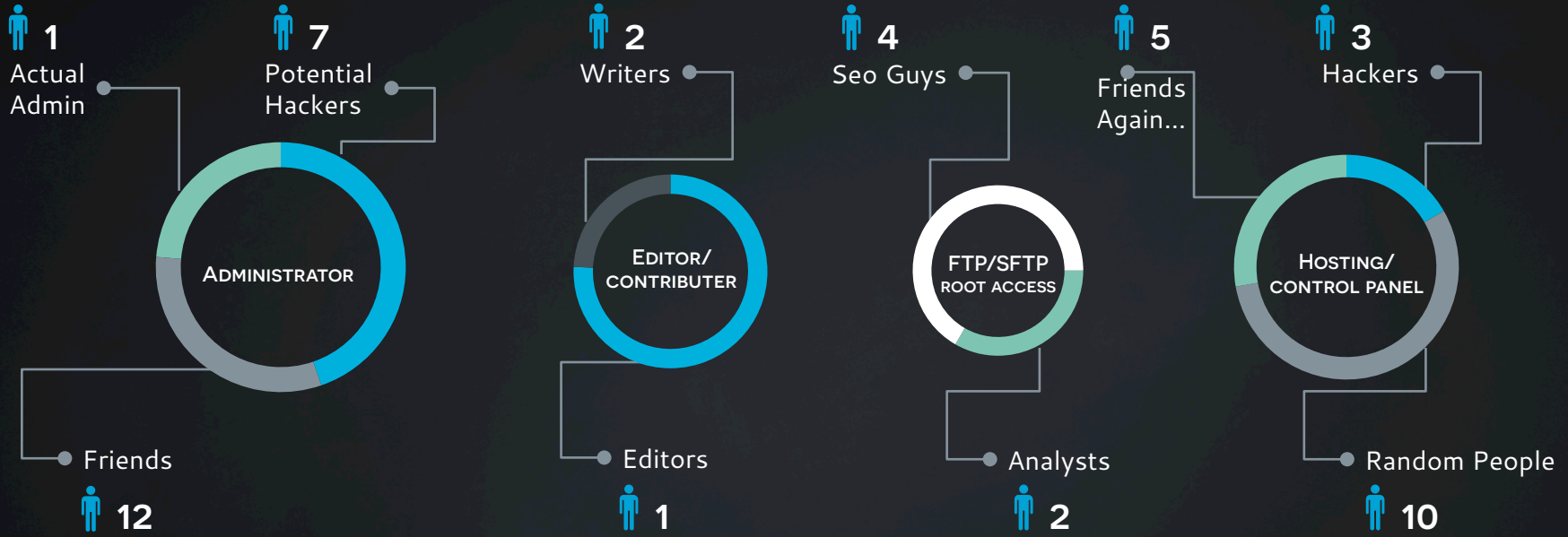
LASTPASS	1PASSWORD	KEYPASS	DASHLANE
			
lastpass.com	agilebits.com	keepass.info	dashlane.com

SUCURI

JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

LEAST PRIVILEGE

Does your user setup look like this?



JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

Steal and Be Stolen From

NOT THE CODE YOU'RE LOOKING FOR...

Assisting the enemy

THIS PROBABLY SHOULDN'T BE IN YOUR THEME:

```
if(isset($_GET['pwd'])) {

eval(base64_decode("CiRhdXRoX3Bhc3MgPSAiN2U5NBhY3RpdmF0ZXM
sIGNoYW5nZWQgZWxlbWVudHMgaW4gdGhlIG9yaWdpbmFsIHBsdWdp
biwgZGVzaWduZWQgdG8gYmVoYXZlIGxpa2UgY2xlYW4gY29kZSwgc2ln
bmFsIHRoZSBoYWNrZXIgdG8gbGV0IGl0IGtub3cgdGhhdCBpdOKAmXMg
aW4uIEEgY2xlYW4gYmFjayBkb29yIGhhcyBiZWVuIG9wZW5lZCwgYW5k
IHlvdXIgc2l0ZSBpcyBub3cgb24gYW4gYXV0b21hdGVkIGF0dGFjayBsaXN
0LCBtZWFudCB0byBxdWlldGx5IGluZmVjdCBhbmQgcmVpbmZlY3QgeW9
1ciBzaXRlIGFnYWluIGFuZCBhZw==“)); }
```

MORE THAN EXPECTED

Powered by Albanian Hackers ©

// Joomla Index Changer / Wordpress Index Changer / Cpanel Cracker / Sql Scanner / Joomla Bruter //
// Backdoor / Joomla Server Scanner / Wordpress Server Scanner / Admin Finder / Shell Finder //
// CmsDetector / MassPASSChange / Wp Mass Defacer / Uploader //

To Generate PHP.ini Click the button below [Generate PHP.ini]

Check The Smylink Dump Click the button below [use to Extract usernames]

Have a System

VI

A SYSTEM TO LIVE BY

1. Protect! – Your computer has a firewall, why doesn't your website?
2. Detect! – The same goes for AntiVirus.
3. Respond! – Clean up the mess. You have a backup right?

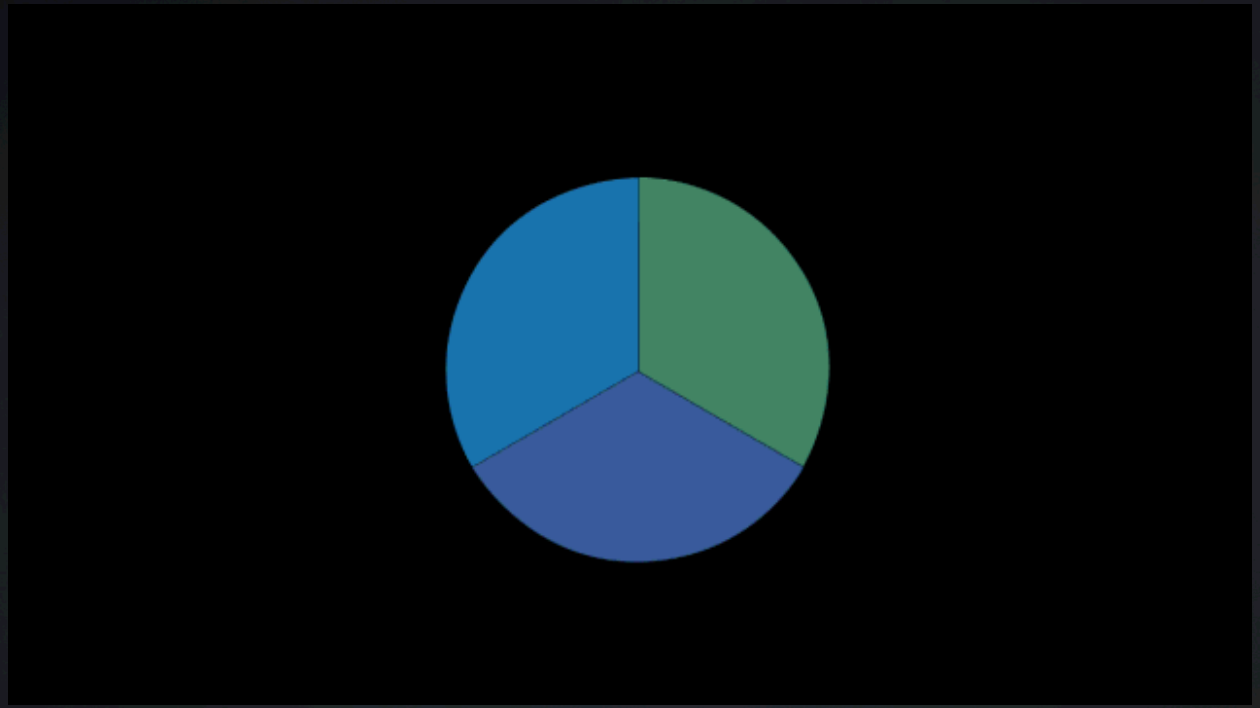
Encompassing Actions:

- Know the best practices
- Mind your maintenance

SUCURI

JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

SYSTEM IN ACTION



VII

Understand the Changing Landscape

WORDPRESS CORE

Strong and Secure

Dedicated Creators

Making WordPress
Solid and Secure

Auto-Updates

Get important
patches right away.

Support

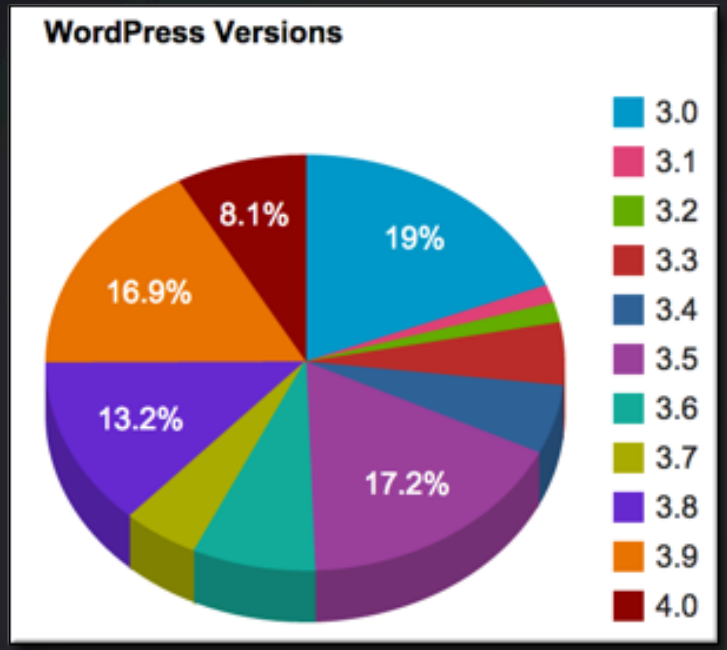
Everything you need
at WordPress.org

SUCURI

JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

WordPress Version Distribution

3.0 – 4.0 (wordpress.org/about/stats/)



JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

3RD PARTY VULNERABILITIES

Keep watch

Vulnerabilities disclosed at **http://blog.sucuri.net**

All-In-One SEO – 20 Million Downloads
WPtouch – 6 Million Downloads
MailPoet - 2.7 Million Downloads
Custom Contact Forms – 640k Downloads
Slider Revolution – Hundreds of Thousands (themeforest/codecanyon)

X

Going further

Tips, Tools, and Services

WEBSITE ANTIVIRUS & FIREWALL

Protection and Detection

Don't be the mark! Understand the changes you are implementing

"AntiVirus"

WordFence
Sucuri Website Antivirus

"Firewall"

CloudFlare
Sucuri Website Firewall

"Utilities"

iThemes Security
BruteProtect
Sucuri Security Plugin

JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

RESOURCES

Because you don't know what you don't know

General WordPress Security:
https://codex.wordpress.org/Hardening_WordPress
https://blog.sucuri.net

Hacking and General Security:
http://www.securityfocus.com/
http://blogs.sophos.com/

Facebook Groups:
WordPress Security
Advanced WordPress

SubReddits:
Reddit.com/r/Hacking
Reddit.com/r/WordPress

JOSEPH HERBRANDSON | WWW.SUCURI.NET
1-888-873-0817| joseph@sucuri.net

EASY PATH TO CLEANUP

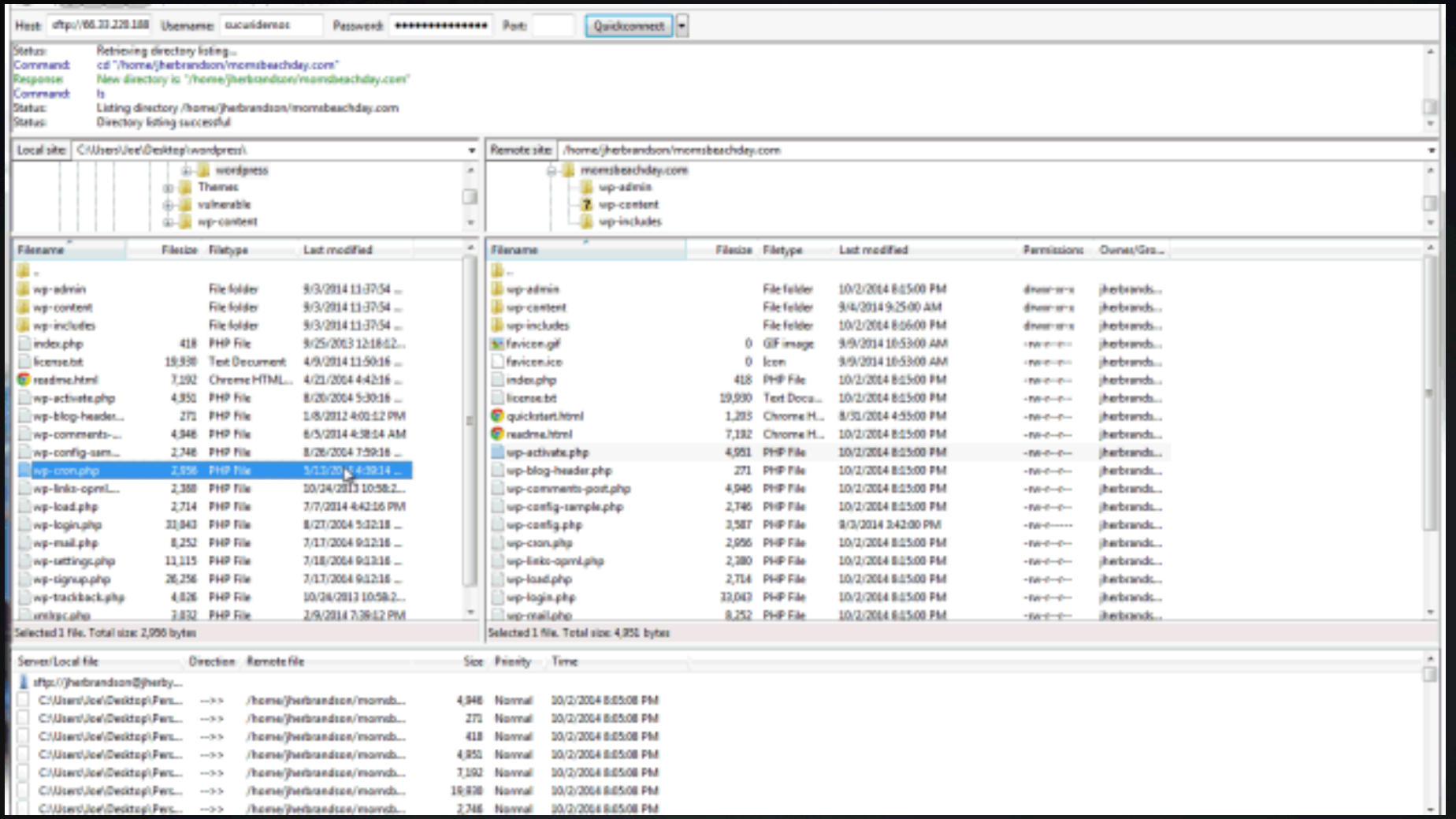
Response

NEED:

Releases of WordPress at:
https://wordpress.org/download/release-archive/

Clean backup of active theme and required plugins

New Passwords (WordPress, FTP, Hosting Control Panel, Everything Else)


Host: sftp://66.33.220.188
Username: cucuridenos
Password: ••••••••••••••••
Port:
Quickconnect
Status: Retrieving directory listing...
Command: cd "/home/jherbrandson/momsbeachday.com"
Response: New directory is: "/home/jherbrandson/momsbeachday.com"
Command: ls
Status: Listing directory /home/jherbrandson/momsbeachday.com
Status: Directory listing successful
Local site: C:\Users\Joe\Desktop\wordpress\
wordpress
Themes
vulnerable
wp-content
Remote site: /home/jherbrandson/momsbeachday.com
momsbeachday.com
wp-admin
wp-content
wp-includes
Filename
Filesize
Filetype
Last modified
Permissions
Owner/Gro...
wp-admin File folder 9/3/2014 11:37:54 ...
wp-content File folder 9/3/2014 11:37:54 ...
wp-includes File folder 9/3/2014 11:37:54 ...
index.php 418 PHP File 9/25/2013 12:18:12...
license.txt 19,930 Text Document 4/9/2014 11:50:16 ...
readme.html 7,192 Chrome HTML... 4/21/2014 4:42:16 ...
wp-activate.php 4,951 PHP File 8/26/2014 5:30:16 ...
wp-blog-header... 271 PHP File 1/18/2012 4:01:12 PM
wp-comments-... 4,946 PHP File 8/5/2014 4:58:14 AM
wp-config-sam... 2,746 PHP File 8/26/2014 7:59:16 ...
wp-cron.php 2,956 PHP File 5/13/2014 4:39:14 ...
wp-links-opml... 2,388 PHP File 10/24/2013 10:58:2...
wp-load.php 2,714 PHP File 7/7/2014 4:42:16 PM
wp-login.php 33,843 PHP File 8/27/2014 5:32:18 ...
wp-mail.php 8,252 PHP File 7/17/2014 9:12:16 ...
wp-settings.php 11,115 PHP File 7/18/2014 9:13:16 ...
wp-signup.php 26,256 PHP File 7/17/2014 9:12:16 ...
wp-trackback.php 4,826 PHP File 10/24/2013 10:58:2...
xmlrpc.php 3,032 PHP File 2/9/2014 7:38:12 PM
Selected 1 file. Total size: 2,956 bytes
wp-admin File folder 10/2/2014 8:05:00 PM drwxr-xr-x jherbrands...
wp-content File folder 9/4/2014 9:25:00 AM drwxr-xr-x jherbrands...
wp-includes File folder 10/2/2014 8:06:00 PM drwxr-xr-x jherbrands...
favicon.gif 0 GIF image 9/9/2014 10:53:00 AM -rw-r--r-- jherbrands...
favicon.ico 0 Icon 9/9/2014 10:53:00 AM -rw-r--r-- jherbrands...
index.php 418 PHP File 10/2/2014 8:05:00 PM -rw-r--r-- jherbrands...
license.txt 19,930 Text Docu... 10/2/2014 8:05:00 PM -rw-r--r-- jherbrands...
quickstart.html 1,235 Chrome H... 8/31/2014 4:55:00 PM -rw-r--r-- jherbrands...
readme.html 7,192 Chrome H... 10/2/2014 8:05:00 PM -rw-r--r-- jherbrands...
wp-activate.php 4,951 PHP File 10/2/2014 8:05:00 PM -rw-r--r-- jherbrands...
wp-blog-header.php 271 PHP File 10/2/2014 8:05:00 PM -rw-r--r-- jherbrands...
wp-comments-post.php 4,946 PHP File 10/2/2014 8:05:00 PM -rw-r--r-- jherbrands...
wp-config-sample.php 2,746 PHP File 10/2/2014 8:05:00 PM -rw-r--r-- jherbrands...
wp-config.php 3,587 PHP File 8/3/2014 2:42:00 PM -rw-r----- jherbrands...
wp-cron.php 2,956 PHP File 10/2/2014 8:05:00 PM -rw-r--r-- jherbrands...
wp-links-opml.php 2,380 PHP File 10/2/2014 8:05:00 PM -rw-r--r-- jherbrands...
wp-load.php 2,714 PHP File 10/2/2014 8:05:00 PM -rw-r--r-- jherbrands...
wp-login.php 33,043 PHP File 10/2/2014 8:05:00 PM -rw-r--r-- jherbrands...
wp-mail.php 8,252 PHP File 10/2/2014 8:05:00 PM -rw-r--r-- jherbrands...
Selected 1 file. Total size: 4,951 bytes
Server/Local file
Direction
Remote file
Size
Priority
Time
sftp://jherbrandson@jherby...
C:\Users\Joe\Desktop\Pers... --> /home/jherbrandson/momsb... 4,946 Normal 10/2/2014 8:05:08 PM
C:\Users\Joe\Desktop\Pers... --> /home/jherbrandson/momsb... 271 Normal 10/2/2014 8:05:08 PM
C:\Users\Joe\Desktop\Pers... --> /home/jherbrandson/momsb... 418 Normal 10/2/2014 8:05:08 PM
C:\Users\Joe\Desktop\Pers... --> /home/jherbrandson/momsb... 4,951 Normal 10/2/2014 8:05:08 PM
C:\Users\Joe\Desktop\Pers... --> /home/jherbrandson/momsb... 7,192 Normal 10/2/2014 8:05:08 PM
C:\Users\Joe\Desktop\Pers... --> /home/jherbrandson/momsb... 19,930 Normal 10/2/2014 8:05:08 PM
C:\Users\Joe\Desktop\Pers... --> /home/jherbrandson/momsb... 2,746 Normal 10/2/2014 8:05:08 PM

THANK YOU!