

WordCamp UK 2014

How to Secure your WordPress Website

Mike Pead

www.primaryimage.com

primary image

About Me!

- ❖ Web design for 15 years
- ❖ Based in Essex & London
- ❖ Founded Primary Image in 2010
- ❖ Mainly work with small/medium sized businesses



primary image

About Me!

- ❖ Manage WordPress hosting for clients
- ❖ 100% WordPress
- ❖ Handle all their security, including WordPress updates



primary image

Today's Talk

- ❖ Why worry about WordPress security?
- ❖ Steps you can take to secure your site...



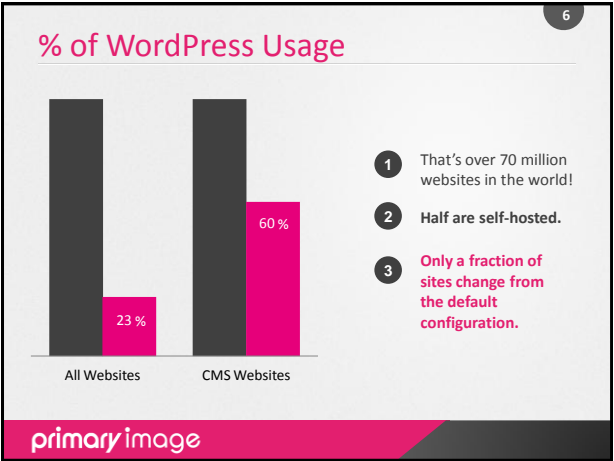
primary image



Why is WordPress vulnerable?



primary image





= WordPress is an attractive target to hackers due to its popularity – a victim of its own success!



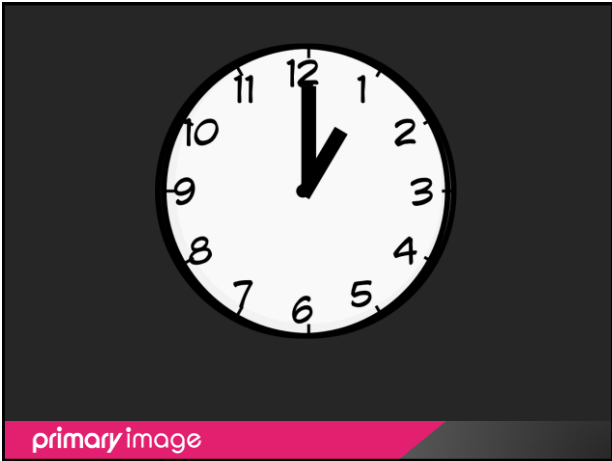
primary image

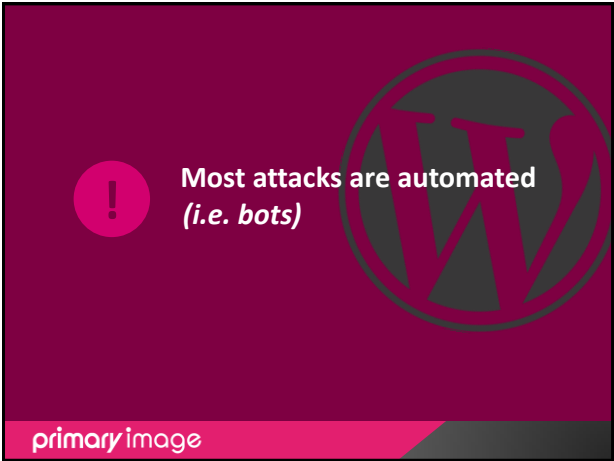


So why did I get interested in WordPress security?



primary image





15

Analysis by Wordfence

Looked at **26 million** "page not found" reports from **30,000 websites**

A cartoon illustration of Homer Simpson from 'The Simpsons'. He is standing with his hands on his head, looking confused. Above him is a large red 'D'oh!' in a speech bubble. Below that, it says 'Error 404 mundoflex'. There is some small, illegible text at the bottom of the illustration.

primary image

16

Bot URL requests


- 4th place: 102,800 requests: **/wp-login.php**
- 7th place: 31,800 requests: **/wp-login.php?action=register**
- 10th place: 24,000 requests: **/wp-comments-post.php**
- 11th place: 22,300 requests: **/administrator/**
- 23rd place: 14,200 requests: **/wp-content/themes/GeoPlaces/monetize/**
- 45th place: 8,500 requests: **/author=1**

Source: <http://www.wordfence.com/blog/2014/05/top-100-page-not-found-errors-for-wordpress/>

primary image

17

Bot URL requests



primary image




?

So what does a botnet attack look like?

primary image


19

Consequences of an attack...



primary image

20



primary image

So is WordPress Secure?

21

• YES IT IS!

- And trusted by some of the biggest names in the world:



primary image

Are you sure it's secure?

22

- Most vulnerabilities are found in plugins and hosting environment, **not the WordPress core.**
- WordPress is extremely good (& quick) at rolling out **security fixes** when issues are found.
- Many techniques used to attack WordPress could be applied to other types of CMS too.

primary image



But there are precautions you can take to secure your site ...



primary image



And the WordPress Codex itself gives some tips:

http://codex.wordpress.org/Hardening_WordPress



primary image

?

What **simple steps** can I take to secure my site?



primary image

26

01Keep WordPress updated

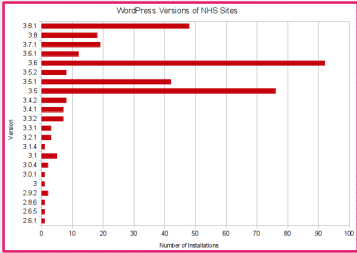
- **WHY?** WordPress is **open-source** – means anyone can see what vulnerabilities have been fixed between versions.
- **HOW?**
 - ❑ **One-click upgrades** are easy, quick & reliable.
- *Today you should all be using WordPress 3.9.1.*

primary image

27

01Keep WordPress updated

- Survey of 350+ NHS WordPress websites:



Source: Terence Eden
<http://shkspt.mobi/blog/2014/03/2000-nhs-security/vulnerabilities-disclosed/>

primary image

28

01Keep WordPress updated



- I alerted the Trade & Investment (UKTI) Government department in March they were using WP 3.4.2 for their blog:
 - released in 2012
 - 9 security updates had been issued



primary image

02 Keep plugins updated

29

- **WHY?** Can be a big hole for allowing attacks.
- **HOW?**

- ☐ If running multiple sites, use a service such as WP Remote (free) to check and install plugin updates in one dashboard.

– How often do you check & install plugin updates?

primary image

03 Only use trusted plugins

30

- **WHY?** Not all plugins can be trusted!
- **HOW?**

- ☐ Get the plugin from wordpress.org or a trusted source.
- ☐ How many downloads / reviews has it got?
- ☐ When was it last updated?

primary image

04 Only use trusted themes

31

- **WHY?** Themes can have poorly written code, or worse – purposely malicious code included.

- **HOW?**

- ☐ Get the theme from a trusted source.
- ☐ Examine the code yourself.

- ☐ Be aware of Base64 code:

TWfUIGlziGRpc3Rpbmd1aXNoZWQsIG5vdCBvbmx5IGJ5IGhpcyByZWZzb24sIGJ1dCBieSB0aGlzmd1aXNoZWQsIG5vdCft

primary image

05 Choose a secure password

32

- **WHY?** Brute force attacks mainly rely on using dictionary words.

- **HOW?**

- ☐ Use characters, numbers, capitals, etc.
- ☐ Use a unique password, don't use the same for every login on the internet!
- ☐ Change it regularly, at least every 3 months.
- ☐ Make sure other users also have strong passwords.
- ☐ This includes your FTP, cPanel & other passwords too!

primary image

06 No "admin" usernames 33

- **WHY?** Any element of predictability gives hackers an edge. Bots will try this first!
- **HOW?**
 - ☐ Setup a new admin account with a unique username.
 - ☐ Delete the existing admin account.

primary image

07 You need decent hosting 34

- **WHY?** Attacks can exploit vulnerabilities at a server-level. Don't let your hosting account be the weak link.
- **HOW?**
 - ☐ Choose a reputable host, perhaps those that specialise in WordPress.
 - ☐ Budget hosts may not always have their focus on security.

primary image

08 Keep regular backups! 35

- **WHY?** If the worst comes to the worst, have a clean backup you can restore to!
- **HOW?**
 - ☐ Download a copy to your computer.
 - ☐ Use an external service, e.g. myRepono.
 - ☐ Frequency to depend on how often your site is updated!



primary image



Want more powerful steps to secure your WordPress site...

primary image

09

Restrict login attempts

37

- WHY? Detect and block brute force attacks.
- HOW?
 - Install a plugin such as **iThemes Security**.




primary image

09

Restrict login attempts

38



Brute Force Protection ☒ Enable brute force protection.

Max Login Attempts Per Host Attempts
The number of login attempts a user has before their host or computer

Max Login Attempts Per User Attempts
The number of login attempts a user has before their username is locked. In addition, if they are using your login name you could be locked out your

Minutes to Remember Bad Login (check period) Minutes
The number of minutes in which bad logins should be remembered.

[Save All Changes](#)

- Setup differently depending on whether it's just you or members of the public logging-in!

primary image

09

Restrict login attempts

39

- BUT THERE ARE FLAWS IN THIS METHOD:
Botnet attacks can come from 1000s of IP addresses.

primary image

09

Restrict login attempts

40

- How about BruteProtect? It logs every failed attempt community-wide.



BruteProtect has guarded over 96,000 sites from more than 102 Million botnet attacks.

Are you protected? 

primary image

13

Two-Factor Authentication

45

• **WHY?** Provides another hurdle for unauthorised users trying to login.

• **HOW?**

☐

Google Authenticator

Username

Password

Google Authenticator code

☐ Remember Me

Log In

182100

899G86-UK

primary image

14

Monitor what's happening

46

• **WHY?** If you have a multi-author site, check what they're doing!

• **HOW?** Plainview Activity Monitor

Activity on all blogs

Blog Activity

Activity

Tools

Timezone	Blog	User	IP	Description
2014-05-07 12:53:12	Broadcast 1	admin	192.168.0.1	Post published: A brand new post about something
2014-05-07 12:53:04	Broadcast 5	admin	192.168.0.1	Post updated: Testing update to many blogs
2014-05-07 12:52:45	Broadcast 7	admin	192.168.0.1	Post updated: Testing update to many blogs
2014-05-07 12:52:42	Broadcast 6	admin	192.168.0.1	Post updated: Testing update to many blogs
2014-05-07 12:52:41	Broadcast 5	admin	192.168.0.1	Post updated: Testing update to many blogs
2014-05-07 12:52:41	Broadcast 4	admin	192.168.0.1	Post updated: Testing update to many blogs
2014-05-07 12:52:40	Broadcast 3	admin	192.168.0.1	Post updated: Testing update to many blogs
2014-05-07 12:52:39	Broadcast 2	admin	192.168.0.1	Post updated: Testing update to many blogs
2014-05-07 12:52:38	Broadcast 1	admin	192.168.0.1	Post updated: Testing update to many blogs

primary image

.htaccess file

primary image

15

Block access to system files

48


• **WHY?** You don't want prying eyes looking at these sensitive files!

• **HOW?**

☐ Add some rules to your .htaccess file.

primary image

12



wp-admin
wp-content
wp-includes
.htaccess

```
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
</IfModule>
# END WordPress
```

primary image

15 Block access to system files 50

# protect files	<files license.txt>
<files wp-config.php>	Order allow,deny
Order deny,allow	Deny from all
Deny from all	</files>
</files>	<files install.php>
<files readme.html>	Order allow,deny
Order allow,deny	Deny from all
Deny from all	</files>
</files>	<files error_log>
	Order allow,deny
	Deny from all
	</files>

primary image

15 Block access to system files 51

Recommended on the WordPress Codex:

```
# Block the include-only files.
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^wp-admin/includes/ - [F,L]
RewriteRule !^wp-includes/ - [S=3]
RewriteRule ^wp-includes/([^\.]*)\.php$ - [F,L]
RewriteRule ^wp-includes/js/tinymce/langs/.+\.php - [F,L]
RewriteRule ^wp-includes/theme-compat/ - [F,L]
</IfModule>
```

primary image

16 Build your own firewall 52

- **WHY?** Stop dodgy requests from even reaching your WordPress installation – block them at server level.
- **HOW?**
 - ❑ Again, add some rules to the .htaccess file.

primary image

17

Hide the .htaccess file itself!

57

• HOW?

STRONG HTACCESS PROTECTION

<Files ~ "^\.*\.[Hh][Tt][Aa]">

order allow,deny

deny from all

satisfy all

</Files>

primary image

18

Protect your WP-Admin area

58

• Problem with login limits plugins:

– Query database for every request

– Run a lot of server processes

– Fill up your MySQL database

primary image

18

Protect your WP-Admin area

59

➔

WP-Admin

MySQL Database

primary image

18

Protect your WP-Admin area

60

STEP 1: Use your hosting control panel to password protect the WP-Admin directory

MySQL Databases

Password Protection

Scheduled Tasks

Website Password Protection

Website Password Protection allows you to password protect a directory on y

the area

Add and Remove Password Protection

Enter the directory you would like to protect. If it does not exist we will create

username could be administrator and your password below.

Directory name:

Username:

Password:

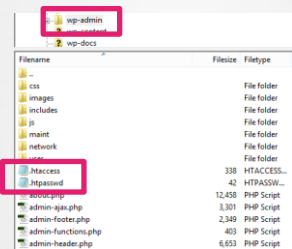
primary image

18

Protect your WP-Admin area

61

End up with this:



primary image

18

Protect your WP-Admin area

62

- STEP 2: New htaccess file in the WP-Admin folder:

AuthType basic
AuthUserFile "/home/example.co.uk/wp-admin/.htpasswd"
AuthGroupFile /dev/null
AuthName "ENTER YOUR LOGIN DETAILS"
Require valid-user

<Files admin-ajax.php>
Order allow,deny
Allow from all
Satisfy any
</Files>

ErrorDocument 401 /401error.html

primary image

18

Protect your WP-Admin area

63

- STEP 3: Add this to your root htaccess:

<Files wp-login.php>
AuthType Basic
AuthUserFile "/home/example.co.uk/wp-admin/.htpasswd"
AuthGroupFile /dev/null
AuthName "ENTER YOUR LOGIN DETAILS"
Require valid-user
</Files>

ErrorDocument 401 /401error.html

primary image

18

Protect your WP-Admin area

64

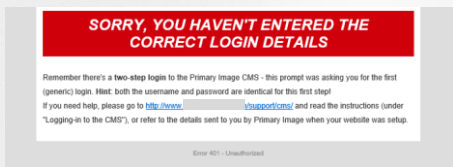
Presented to the user:



primary image

18 Protect your WP-Admin area 65

Create a custom 401 error page:



primary image

18 Protect your WP-Admin area 66

- **Benefits:**
 - Blocks bad bots at server-level
 - Less server resources needed than firing up WordPress
 - Works ok with public logins if using a front-end login form (e.g. 'Theme My Login' plugin with the front-end widget)

primary image

19 Block PHP in Uploads folder 67

- **WHY?** Uploads folder can be used by other users.
- **HOW?**
 - ❑ Create a .htaccess file in the WP-Content/Uploads folder, with the following:


```
<Files *.php>
Deny from All
</Files>
```

primary image

20 Tighten PHP configuration 68

- **WHY?** Helps block PHP code injection vulnerabilities caused by bad input filtering.
- **HOW?**
 - ❑ Add a php.ini file in your root directory and paste in some code...

primary image

20 Tighten PHP configuration

; Disable allow_url_fopen in php.ini for security reasons

allow_url_fopen = Off

; Disable allow_url_include in php.ini for security reasons

allow_url_include = Off

```
; Disable display_errors in php.ini for security reasons
```

```
display_errors = Off
```

```
log_errors = On
```

primary image

21 Create your own encryption keys

- **WHY?** Makes an attackers job harder.

[illegible]

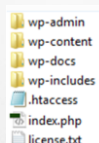
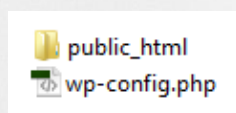
- HOW?

- ❑ Open up **wp-config.php**, scroll down to “Authentication Unique Keys and Salts”.
- ❑ Generate your own keys at:
<https://api.wordpress.org/secret-key/1.1/salt/>

primary image

22 Move WP-Config location

- **WHY?** Take `wp-config.php` out of a publicly accessible location.
- **HOW?** Move it one level up, outside of your `public_html` folder:



primary image

23 Folder permissions

- **WHY?** Can be a security hole if permissions are not strong enough.

- HOW?

- ❑ Use your FTP software's CHMOD feature.

Permissions
flcdmpe (0755)
flcdmpe (0755)
flcdmpe (0755)
flcdmpe (0755)
adfrw (0644)
adfrw (0644)
adfrw (0644)

primary image

23

Folder permissions

73

- ❖ All folders should have a CHMOD of 755.
- ❖ All "wp-" PHP files = 644.
- ❖ wp-config.php = 640.
- ❖ htaccess files = 644.
- ❖ robot.txt = 755.
- ❖ sitemap.xml = 666.

primary image

Don't forget the basics:

- Keep WordPress and your plugins updated.
- Have a secure password.
- Get decent quality hosting.

primary image



primary image

www.primaryimage.com
Twitter: @primaryimage
Also find us on Facebook,
Google+ & LinkedIn




primary image