Security Basics

Things to know.

WordCamp Baltimore 2017
@theandystratton
http://sizeable.is

Who am I?

WordPress Developer

WordCamp Speaker

Founder of Sizeable Interactive

Founder of WP Maintainer

Working with WordPress for nearly 12 years.

Building websites for over 20 years.

Why worry about security?

Attacks are automated

Protecting your assets

Protecting your search rankings

When it becomes a problem,
it's a BIG problem

How are attacks happening?

Brute Force

Exploits in insecure/out of date software

Exploits in server software
or insecure hosting

The best offense
is a good defense.

So, how do we protect ourselves?

UPDATE YOUR SOFTWARE

UPDATE YOUR SOFTWARE

WordPress Core

Plugins and Themes

Server/Hosting Software
(Cpanel/WHM, Apache, Linux Kernel)

UPDATE TOOLS

Infinite WP

Manage WP

May be others…

UPDATE SERVICES

Maintainn

WP Site Care

WP Maintainer

SECURE PASSWORDS

SECURE PASSWORDS

Combo of words, numbers, upper/lower case, special chars

Never use your username or something easily guessed, like dictionary words

More than 8 characters, 20+ is great!

SECURE PASSWORD TOOLS

1Password

LastPass

DashLane

SECURE HOSTING

SECURE PASSWORDS

Poor hosting can be a major issue

Investing in quality hosting is huge, not just for security, but performance/maintenance, too

Why buy a nice house
and put it in a bad neighborhood?

SOME RECOMMENDED HOSTS

BlueHost

Dreamhost

Liquid Web

SiteGround

WP Engine

MINIMAL PRIVILEGE

MINIMAL PRIVILEGE

Why allow access if it's not required?

If someone doesn't need access,
they should NOT have it.

Many sites don't need certain features
enabled to function

xmlrpc.php

xmlrpc.php

Used for remote procedure calls by applications/third-parties.

Can be used for brute force attacks to validate user credentials.

Not really necessary for most sites (check with site owner)

```
# .htaccess
<Files "xmlrpc.php">
Deny from all
</Files>
```

Don’t allow PHP execution from the uploads folder.

```
# .htaccess in /wp-content/uploads/
<Files “*.php">
Deny from all
</Files>
```

Don’t allow users to edit themes and plugins.

```php
<?php
// wp-config.php

define( ‘DISALLOW_FILE_EDIT', true );
```

Use a plugin to stop user enumeration attacks.

yoursite.com?author=1

…redirects to…

yoursite.com/authors/**mysecretusername**

…we now have your username…
50% progress to being inside.

Whitelist the WordPress login script.

```
<Files "wp-login.php">
Deny from all
Allow from 127.0.0.1
Allow from 127.0.0.2
Allow from 127.0.0.3
</Files>
```

OBFUSCATION

It means

HIDE STUFF.

OBFUSCATION

Number of plugins that will obfuscate the WP login, or at least protect it

iThemes Security

WordFence

Login Security Solution

THIRD PARTY TOOLS

THIRD-PARTY TOOLS

Proxy Services like
Sucuri CloudProxy, CloudFlare, and Incapsula

Monitoring / clean up services
like Sucuri Security

Riddle:

What don’t you worry about until you really need them?

BACKUPS

BACK

YOUR


SH*T


UP!

BACK YOUR SH*T UP.

Preferably off-site (S3 is a great place)

Use a plugin or server-side script for backups.

CPanel can backup your whole account in intervals to S3 now

Plugins like VaultPress, BackupBuddy, BackWPUp, UpdraftPlus, etc.

AHHH I'VE BEEN HACKED.

IF YOU GET HACKED

Restore to your latest backup, conveniently located off-site!

Try to find the source of the infection and kill it

Change all user passwords after clean up & prune the user accounts

Lock the site down with the previous info!

A clean up service like Sucuri is awesome

Q&A?

Thank You.