Intro to WordPress Security

By Adrian Mikeliunas, CISSP, CISA

https://learnwp.us/security/

Agenda

* WordPress Architecture
* Securing the server layer
* Securing the application layer
* Securing the user & admin

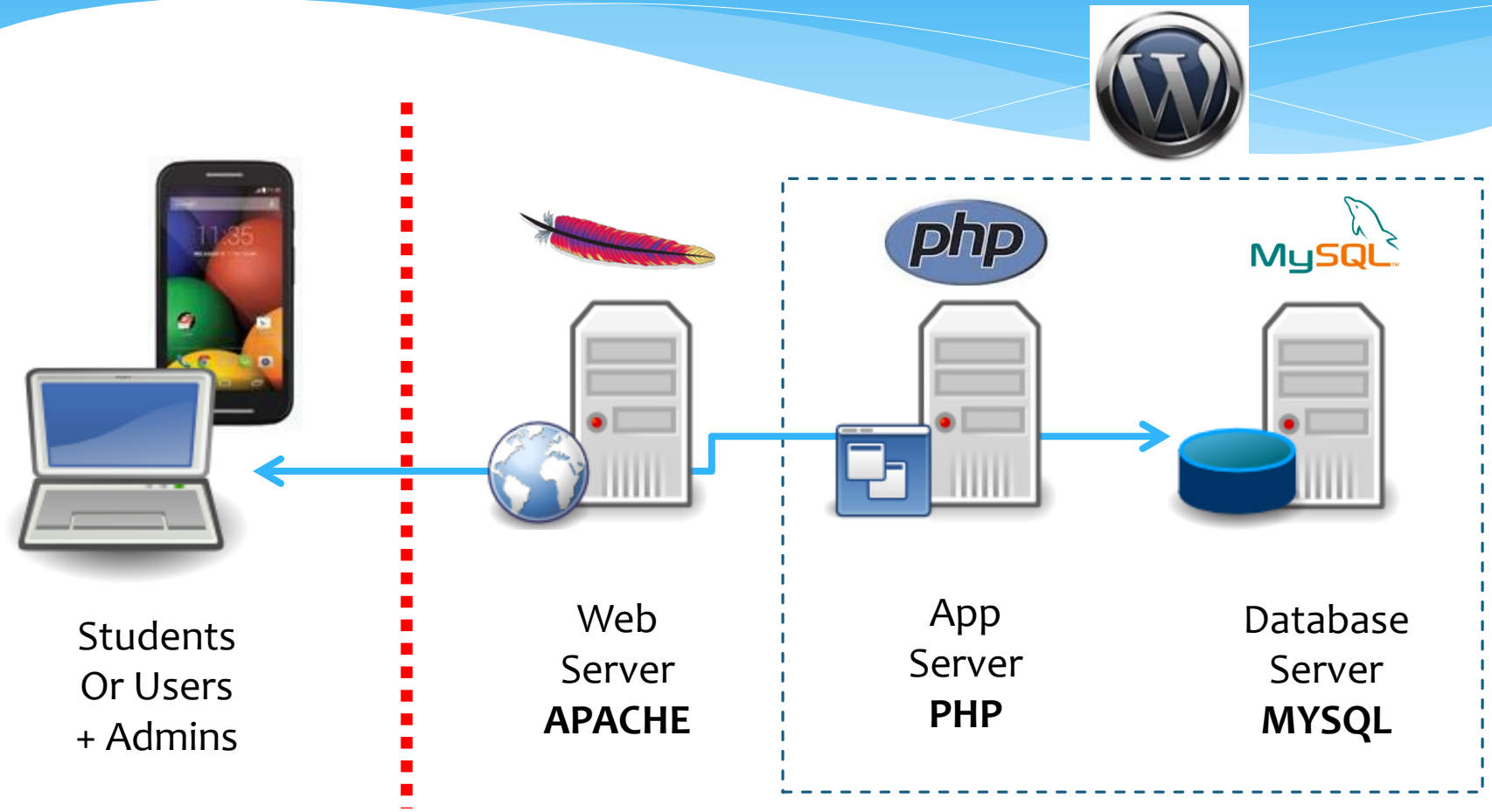
http://farm4.static.flickr.com/3036/2913018697_ccbb33e993_b.jpg

Speaker

* **Adrian Mikeliunas, FCPS Instructor**
* Certified Information System Security Professional (CISSP)
* Certified Information Systems Auditor (CISA)
* 30+ years of IT experience, 15 in Security
* 7+ years of WordPress experience

* Adrian@Mikeliunas.com
* https://learnwp.us

WordPress Architecture



Defense in depth

* **Multiple layers** of security controls (defense) are placed throughout an information technology (IT) system.
  * Database --- inner layer
  * Application
  * Web server --- outermost layer
* The **Goal** is to provide **redundancy** in the event a security control fails or a vulnerability is exploited
* Also known as the "Castle Approach"

Securing the Database Server

* KEEP A FULL COPY (just in case) of:
  * Database with user list and content
  * Installed Themes and Plugins
  * Customizations and much more…

* Enable Secure Sockets Layer (SSL) and update server configuration
  https://wordpress.org/plugins/really-simple-ssl/

Backups

* How often should you back up?
* How many backups should I keep?
* Where should I keep the backups?

* Can backups be automated?
  * Online or Offline?
  * Check your Hosting provider

https://premium.wpmudev.org/blog/backup-plugins-compared/

https://wordpress.org/plugins/updraftplus
https://wordpress.org/plugins/backwpup
https://ithemes.com/purchase/backupbuddy $

VaultPress (if you use Jetpack)

With a PAID monthly subscription ($39/99/299 per year):

1. The VaultPress plugin will backup:
   * Your site's content
   * Themes & plugins in real time
2. Perform regular security scans for common threats and attacks

https://vaultpress.com/plans/
http://wordpress.org/plugins/vaultpress

Core Updates

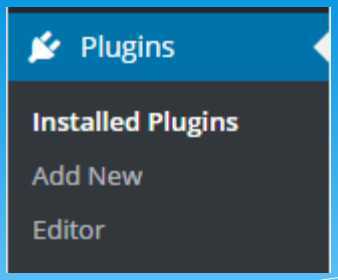
* Updating software is necessary to maintain or improve your security! Makes your website faster!
* Update your
  * WordPress site (core)
  * WordPress themes
  * WordPress plugins

* Which version? https://www.wappalyzer.com/

Automating Updates

* Easy Updates Manager
  * Better control of your updates!
    Avoids updating troublesome plugins or themes
  * https://wordpress.org/plugins/stops-core-theme-and-plugin-updates/
* Easy Theme and Plugin Upgrades
  * WordPress does not upgrade uploaded commercial themes or plugins by default
  * https://wordpress.org/plugins/easy-theme-and-plugin-upgrades/

Plugins



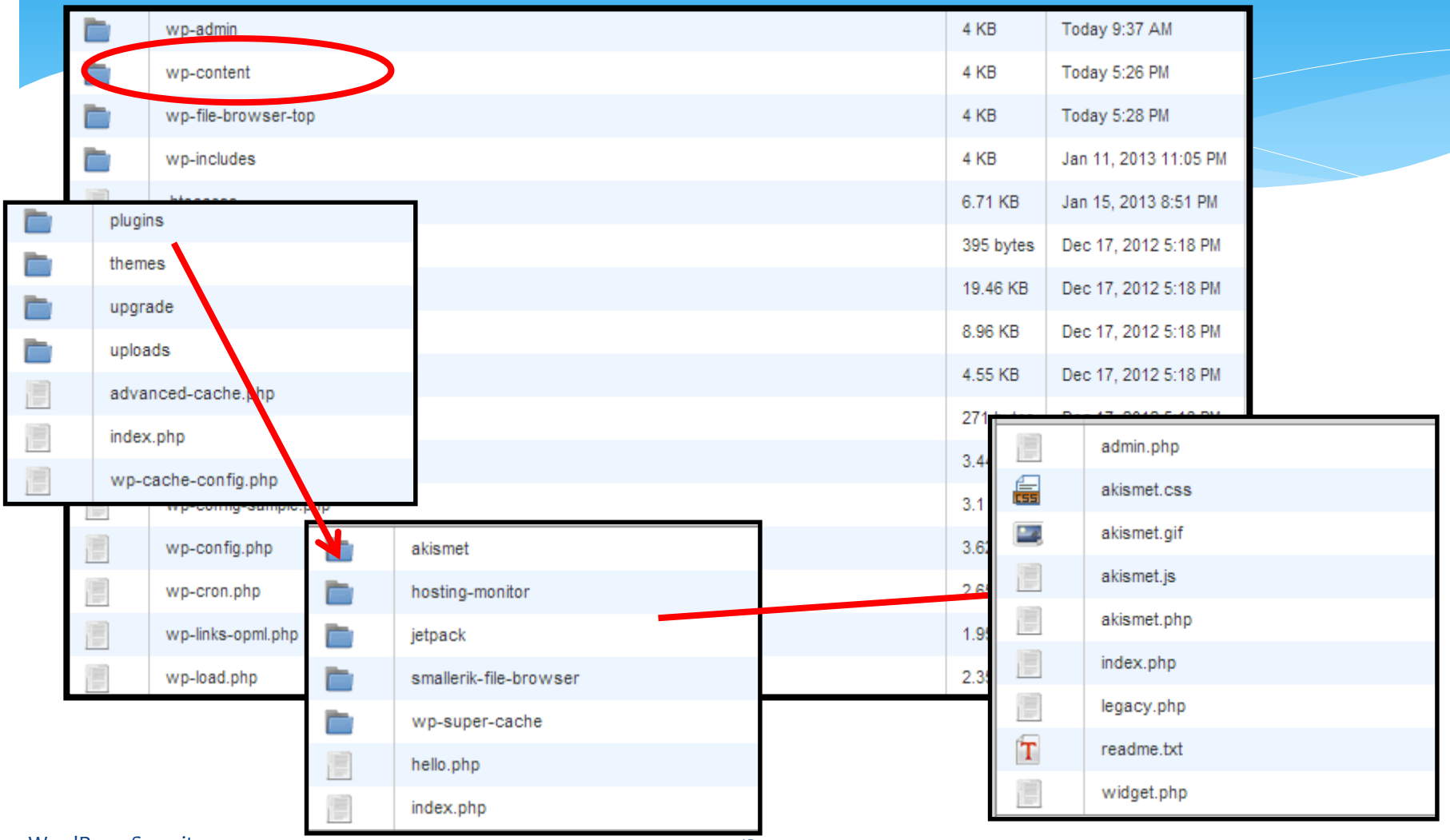
* Plugins can **extend** WordPress to do almost **anything** you can imagine!
  * Active plugins run in your server as ADMINISTRATOR
  * Plugins from the WordPress community are located at https://wordpress.org/plugins/
  * Unfortunately NOT all plugins are safe, secure or supported
    * WordPress got the memo and started to clean up the directory!
    * https://wordpress.org/plugins/tags/deprecated/
  * Newer versions of WP have many media enhancements (YouTube, images, …) so you may NOT need extra plugins

Plugin Selection Criteria

My 3 factors **criteria** for selecting a good plugin
[or widget or theme]

* Check **Rating**, at least 4 out of 5 stars,
  and from more than 1000 installs!
* At least **version** 1.01!
  [many plugins are still version 0.x or BETA]
* **Date:** preferably less than 1 year old
  [older plugins may NOT be compatible with your site]

WordPress Plugins Folder



Protect Content

* Apache web server has an **.htaccess** file to restrict content among other functions
  * Can be used to block bad people or hide content!
    * Like Lesson material, backups, etc.
* Protect uploads is a easy plugin to protect **content**
  * https://wordpress.org/plugins/protect-uploads/

Accounts & Passwords

* Don't use the "Admin" username to administer your site
  * Use a new, separate account…
* Don't share admin accounts. Create as few as necessary!
* Don't use the default login URL!
  [It's UGLY! Hackers know it!]
  * Brand login form with your school logo!
    * https://wordpress.org/plugins/theme-my-login/
  * Login plugins and two factor authentication
    https://wordpress.org/plugins/search/login+two+factor/

Other Accounts

* Hosting Account [or Operating System if self managed]
* Server login (via SSH or third party plugins)
* FTP or SFTP account and password
* Database account and password
* Email account and password

Multifunctional Security

* Firewall
* Detect and Block malicious activity!
* Two-Factor Authentication
* Malware Scan Scheduling
* Password Security / Expiration

Security Plugins

* Install a security plugin… from free to paid
  * WordFence https://wordpress.org/plugins/wordfence
  * iThemes https://wordpress.org/plugins/better-wp-security/
  * https://wordpress.org/plugins/bulletproof-security/

* Other security options:
  * Hosting provider (extra $)
  * Content Delivery Network (CDN)

WordPress Security Tips

* OWASP WordPress Security Implementation Guideline
  * https://www.owasp.org/index.php/OWASP_Wordpress_Security_Implementation_Guideline
* The Ultimate Guide to WordPress Security
  * https://premium.wpmudev.org/blog/ultimate-guide-wordpress-security/
  * https://premium.wpmudev.org/blog/a-complete-guide-to-wordpress-password-security/
* WordPress Setup Checklist – 72 steps
  * http://www.wpmentor.net 14 steps in security

Questions?

???

?