

# Securing Your CMS for Mobility

Vince Salvino

[salvino@coderedcorp.com](mailto:salvino@coderedcorp.com)

@vincosalvino

Information Security Summit 2016

**CODERED**

Slides Available Online

[www.coderedcorp.com/resources](http://www.coderedcorp.com/resources)

# About This Talk

You have a beautiful new website. Users love it. You're proud of it. The company is well represented and looks good.

Now let's make sure that website is as trustworthy as it looks...

# About This Talk

You have a beautiful new website. Users love it. You're proud of it. The company is well represented and looks good.

Now let's make sure that website is as trustworthy as it looks...

1. Why is it important to secure a CMS?
2. Common features of a CMS
3. How these common features translate into security concerns
4. Examples of these features and security concerns in WordPress
5. Key takeaways

# Why Secure a CMS?

1. Why secure my CMS? **Everything on my website is public content anyhow.**
2. Why secure my CMS? **No one wants to hack me – I have no valuable data.**
3. Why secure my CMS? **I use the default settings so I should be covered, anything extra is just paranoia.**

# Why Secure a CMS?

To quote our presidential candidate...

1. Why secure my CMS? Everything on my website is public content anyhow.  
**WRONG!**
2. Why secure my CMS? No one wants to hack me – I have no valuable data.  
**WRONG!**
3. Why secure my CMS? I use the default settings so I should be covered, anything extra is just paranoia.  
**WRONG!**

# Myth 1: Everything is Public Content

Your website content may be public. But what about...

- **CMS User Accounts** – could someone obtain these emails and passwords to then use those to access a different, more important system?
- **Sign up for our newsletter** – could someone access this list of subscribers? Common uses are to email them masquerading as your company for nefarious purposes, or simply sell those emails to marketing lists.
- **Deface your website** – which could be used to damage reputation, or add code that harvests user info and/or links to external phishing sites.

# Myth 2: No One Wants to Hack Me

Aside from valuable data such as user accounts and subscribers, you may still be a target even without any data.

- **Entry point into the server** – an attacker could simply want to use your site as a way into the web server.
  - Are there other sites on the same server that might cause yours to be at risk as an entry point?
  - Does the web server have access to a more valuable system (i.e. database, API keys, VPN)
- **Used to attack a larger target** – could your server be compromised and used to participate in a DDoS attack? What if it is used to attack a Federal system?

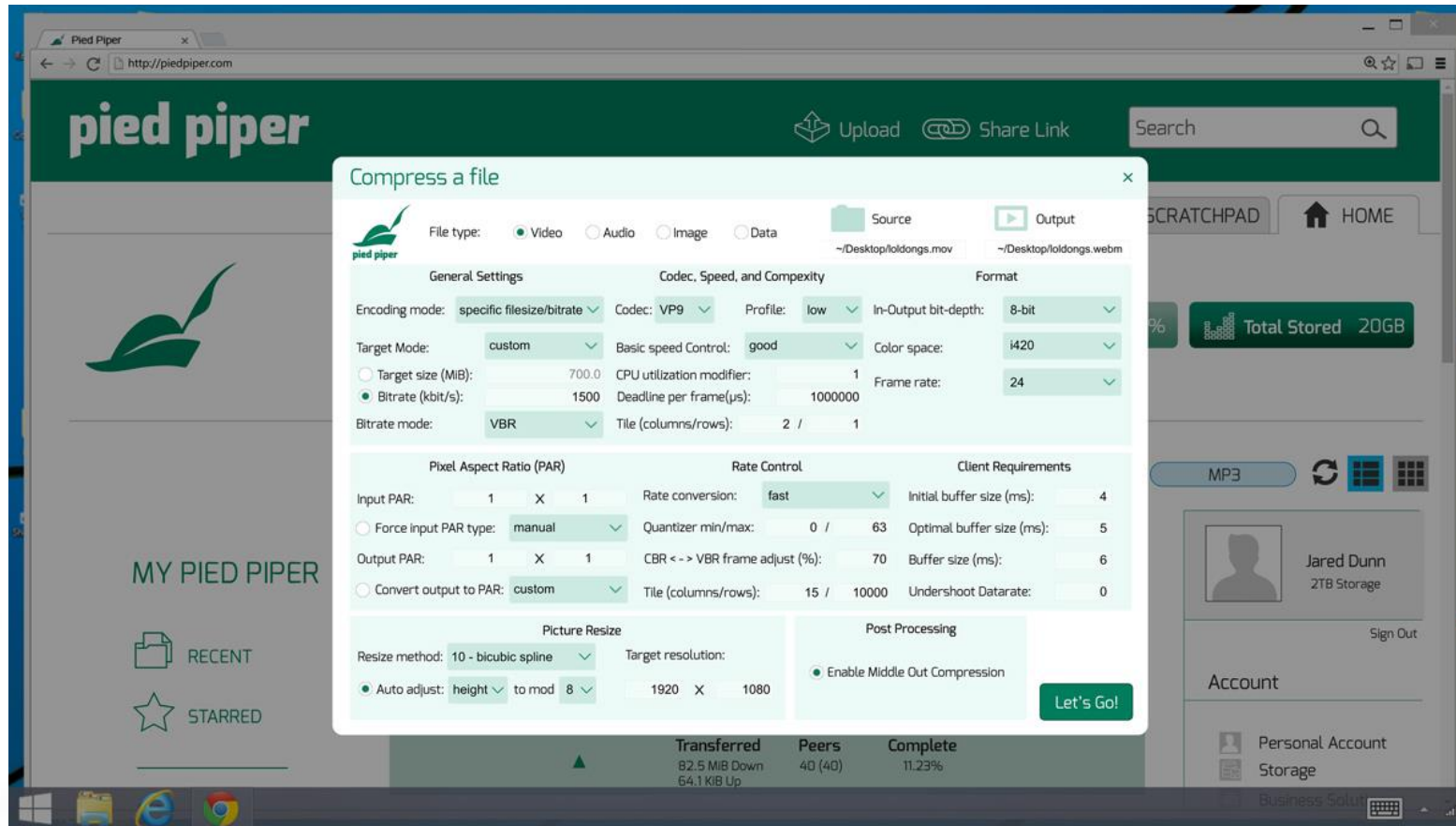


# Myth 3: Default Settings are Secure

Trusting the CMS to be secure out-of-box is a bad idea.

- **Unused features** – most CMSs have dozens of features that you may not be using.
- **3<sup>rd</sup> party features** – things such as plugins or themes can introduce vulnerabilities not normally present in the CMS.
- **External factors** – such as server configuration and SSL are also important. Even if you have SSL installed on the server, your CMS may not be configured to properly use it out-of-box.

# Features



# Common Features

## User Accounts

User accounts are used to manage the CMS.

Audit Trail

Forms

Plugins/Themes

Configurations

Mobile Access

# Common Features

## User Accounts

Audit Trail

Forms

Plugins/Themes

Configurations

Mobile Access

User accounts are used to manage the CMS.

## Security Concerns

- **Access Rights** – can the CMS provide granular access to content based on user's role? Freelancers, web devs, 3<sup>rd</sup> party marketing agency?
- **Password security** – how are passwords stored, and can password policies be enforced?
- **Identity Management** – can the CMS utilize OAuth to authenticate via centrally managed user accounts?

# Common Features

## User Accounts

Audit Trail

Forms

Plugins/Themes

Configurations

Mobile Access

Dashboard

Posts

Media

Pages

Comments

Projects

Contact

Appearance

Plugins 2

**Users**

All Users

Add New

Your Profile

Tools

Settings

Quick Redirects

Divi

Google Analytics

Collapse menu

### Add New User

Create a brand new user and add them to this site.

Username *(required)*

Email *(required)*

First Name

Last Name

Website

Password

Send User Notification ☒ Send the new user an email about their account.

Role

- Subscriber
- Contributor
- Author
- Editor
- Administrator

WordPress does have basic user roles

WordPress lacks password policies out-of-box though.

WordPress also lacks OAuth support for user accounts out-of-box as well.

# Common Features

User Accounts

**Audit Trail**

Forms

Plugins/Themes

Configurations

Mobile Access

User and admin activity is logged.

# Common Features

User Accounts

Audit Trail

Forms

Plugins/Themes

Configurations

Mobile Access

User and admin activity is logged.

## Security Concerns

- **Is auditing possible** – can the CMS even provide an audit trail or logging? If not, how would you identify red flags or respond to a breach?
- **Logs expose sensitive data** – if auditing and logging is enabled, do logs scrub sensitive info such as emails, passwords, credit cards, etc.?
- **Integrity of audit trail** – how is the audit trail/logs managed? Can admins or users view and change them?



# Common Features

User Accounts

**Audit Trail**

Forms

Plugins/Themes

Configurations

Mobile Access

## Audit Trail

Audit Trail is a plugin to keep track of what is going on inside your blog by monitoring administration functions.

Download Version 1.2.4

[Description](#) [Installation](#) [Screenshots](#) [Other Notes](#) [Changelog](#) [Stats](#) [Support](#) [Reviews](#) [Developers](#)

Search: <input type="text"/> Results per page: 25 <input type="button" value="go"/>				
User	Action	Target	Date	IP
administrator	Save post	Small Yellow Inflatable Pigs	April 20, 2007 3:14 pm	127.0.0.1
administrator	Save post	Small Yellow Inflatable Pigs	April 20, 2007 3:14 pm	127.0.0.1

Requires: 3.5 or higher  
Compatible up to: 4.2.10  
Last Updated: 1 year ago  
Active Installs: 30,000+

Audit trail

Table	Action	Rows
<input type="checkbox"/> wp_commentmeta	<input type="checkbox"/> Browse <input type="checkbox"/> Structure <input type="checkbox"/> Search <input type="checkbox"/> Insert <input type="checkbox"/> Empty <input type="checkbox"/> Drop	
<input type="checkbox"/> wp_comments	<input type="checkbox"/> Browse <input type="checkbox"/> Structure <input type="checkbox"/> Search <input type="checkbox"/> Insert <input type="checkbox"/> Empty <input type="checkbox"/> Drop	
<input type="checkbox"/> wp_links	<input type="checkbox"/> Browse <input type="checkbox"/> Structure <input type="checkbox"/> Search <input type="checkbox"/> Insert <input type="checkbox"/> Empty <input type="checkbox"/> Drop	
<input type="checkbox"/> wp_options	<input type="checkbox"/> Browse <input type="checkbox"/> Structure <input type="checkbox"/> Search <input type="checkbox"/> Insert <input type="checkbox"/> Empty <input type="checkbox"/> Drop	
<input type="checkbox"/> wp_postmeta	<input type="checkbox"/> Browse <input type="checkbox"/> Structure <input type="checkbox"/> Search <input type="checkbox"/> Insert <input type="checkbox"/> Empty <input type="checkbox"/> Drop	
<input type="checkbox"/> wp_posts	<input type="checkbox"/> Browse <input type="checkbox"/> Structure <input type="checkbox"/> Search <input type="checkbox"/> Insert <input type="checkbox"/> Empty <input type="checkbox"/> Drop	
<input type="checkbox"/> wp_terms	<input type="checkbox"/> Browse <input type="checkbox"/> Structure <input type="checkbox"/> Search <input type="checkbox"/> Insert <input type="checkbox"/> Empty <input type="checkbox"/> Drop	

click SQL to let you run custom SQL commands on the database

WordPress lacks an audit trail other than basic page versioning.

Auditing plugins do exist though...

But can the audit tables be changed by your users? If so, integrity is questionable.



# Common Features

User Accounts

Audit Trail

**Forms**

Plugins/Themes

Configurations

Mobile Access

Forms exist on the website to submit user-entered data. This can include signups, search, contact, etc.

# Common Features

User Accounts

Audit Trail

**Forms**

Plugins/Themes

Configurations

Mobile Access

Forms exist on the website to submit user-entered data. This can include signups, search, contact, etc.

## Security Concerns

- **Injection attacks** – they aren't part of the OWASP Top 10 for nothing! Injection attacks are one of the most exploited vulnerabilities on the web. Does your CMS guard against them? Does the CMS provide a framework for implementing forms?
- **Sensitive data** – if you collect sensitive data such as credit card info, SSN, or file uploads – is that data stored and transferred in a secure manner? Does the CMS provide a way of handling and classifying this type of data?

# Common Features

User Accounts

Audit Trail

Forms

Plugins/Themes

Configurations

Mobile Access

## Protect Queries Against SQL Injection Attacks

For a more complete overview of SQL escaping in WordPress, see [database Data Validation](#). It is a **must-read** for code contributors and plugin authors.

All data in SQL queries must be SQL-escaped before the SQL query is executed to prevent against SQL injection attacks. The `prepare` method performs this functionality for WordPress, which supports both a `sprintf()`-like and `vsprintf()`-like syntax.

**Please note:** As of 3.5, `wpdb::prepare()` enforces a **minimum of 2 arguments**. [\[more info\]](#)

```
<?php $sql = $wpdb->prepare( 'query' , value_parameter[, value_parameter ... ] ); ?>
```

Forms that result in database queries should follow best practices in WordPress Codex.

ID	Added	Title
8623	2016-09-21	N-Media Website Contact Form with File Upload - Arbitrary File Upload
8565	2016-07-25	Contact Form to Email <= 1.1.47 - Authenticated Reflected Cross-Site Scr...
8452	2016-04-15	Easy Contact Form Builder <= 1.0 - Unauthenticated Reflected Cross-Site ...
8307	2015-11-24	Contact Form Maker <= 1.7.30 - Authenticated Blind SQL Injection
8303	2015-11-24	Contact Form Manager <= 1.4.1 - Authenticated Reflected Cross-Site Scrip...
8262	2015-11-22	Contact Form Builder <= 1.0.24 - Authenticated Blind SQL Injection
8235	2015-11-13	Contact Form Integrated With Google Maps 1.0-2.4 - Stored Cross-Site Scr...
8234	2015-11-13	Easy Contact Form Solution 1.0-1.6 - Stored Cross-Site Scripting (XSS)
8223	2015-10-27	Fast Secure Contact Form <= 4.0.37 - Authenticated Cross-Site Scripting ...
8201	2015-10-01	Jetpack <= 3.7.0 - Stored Cross-Site Scripting (XSS)
8176	2015-09-08	Contact Form Generator <= 2.0.1 - Multiple Cross-Site Request Forgery (C...
8089	2015-07-11	CP Contact Form with Paypal <= 1.1.5 - Multiple Vulnerabilities
8024	2015-06-03	N-Media Website Contact Form with File Upload <= 1.5 - Local File Inclusion
7992	2015-05-15	Encrypted Contact Form <= 1.0.4 - CSRF & XSS

WPScan database has dozens of known vulnerabilities for contact from plugins.

# Common Features

User Accounts

Audit Trail

Forms

**Plugins/Themes**

Configurations

Mobile Access

3<sup>rd</sup> party plugins, addons, and themes are great for quickly and cheaply adding awesome functionality.

# Common Features

User Accounts

Audit Trail

Forms

**Plugins/Themes**

Configurations

Mobile Access

3<sup>rd</sup> party plugins, addons, and themes are great for quickly and cheaply adding awesome functionality.

## Security Concerns

- **Is the plugin trusted** – does the CMS have a way of verifying plugins? Or are they all at your own risk? Do you know what the plugin is doing?
- **What plugins are in use** – does your existing site have plugins installed that are not needed? Does the developer plan to use plugins for key features? Does the plugin have dependencies?
- **Plugin updates** – do you monitor security releases and receive notifications when vulnerabilities are discovered by the plugin publisher?

# Common Features

User Accounts

Audit Trail

Forms

Plugins/Themes

Configurations

Mobile Access



This plugin hasn't been updated in over 2 years. It may no longer be maintained or supported and may contain compatibility issues when used with more recent versions of WordPress.

Hundreds of plugins exist that are no longer maintained. Yet many still have millions of installs. An absolute security nightmare.

## Limit Login Attempts

Limit rate of login attempts, including by way of cookies, for each IP. Fully customizable.

Download Version 1.7.1

♥ Favorite

[Description](#) [Installation](#) [FAQ](#) [Screenshots](#) [Changelog](#) [Stats](#) [Support](#) [Reviews](#) [Developers](#)

Limit the number of login attempts possible both through normal login as well as using auth cookies.

Requires: 2.8 or higher

Compatible up to: 3.3.2

Last Updated: 4 years ago

Active Installs: 1+ million

By default WordPress allows unlimited login attempts either through the login page or the wp-admin directory. This plugin will limit the number of login attempts for both.

## WPScan Vulnerability Database

Cataloging 5246 WordPress Core, Plugin and Theme vulnerabilities

Free Email Alerts

Submit a Vulnerability

Try our API

WPScan is a prime tool for identifying theme and plugin vulnerabilities. Thousands are known.



# CODERED

BUILDING BRILLIANT TECHNOLOGY

2016

# Common Features

User Accounts

Audit Trail

Forms

Plugins/Themes

**Configurations**

Mobile Access

Every CMS has its own default configuration. These settings usually make everything work smoothly on a fresh installation.



# Common Features

User Accounts

Audit Trail

Forms

Plugins/Themes

**Configurations**

Mobile Access

Every CMS has its own default configuration. These settings usually make everything work smoothly on a fresh installation.

## Security Concerns

- **Lowest common denominator** – most default settings are designed to work with the simplest possible use-case. The simplest use-case usually omits security in favor of convenience and ease of setup.
- **Prime examples is SSL support** – most CMSs may not work well with SSL unless the server is set up correctly and the CMS is set to account for using HTTPS in its URLs.

# Common Features

User Accounts

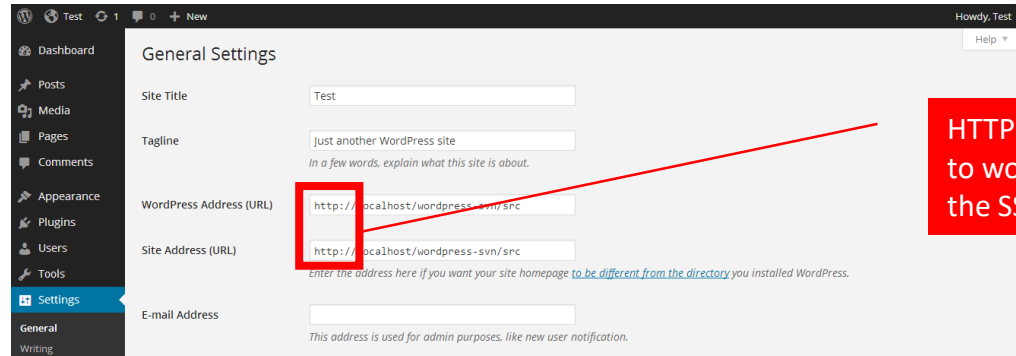
Audit Trail

Forms

Plugins/Themes

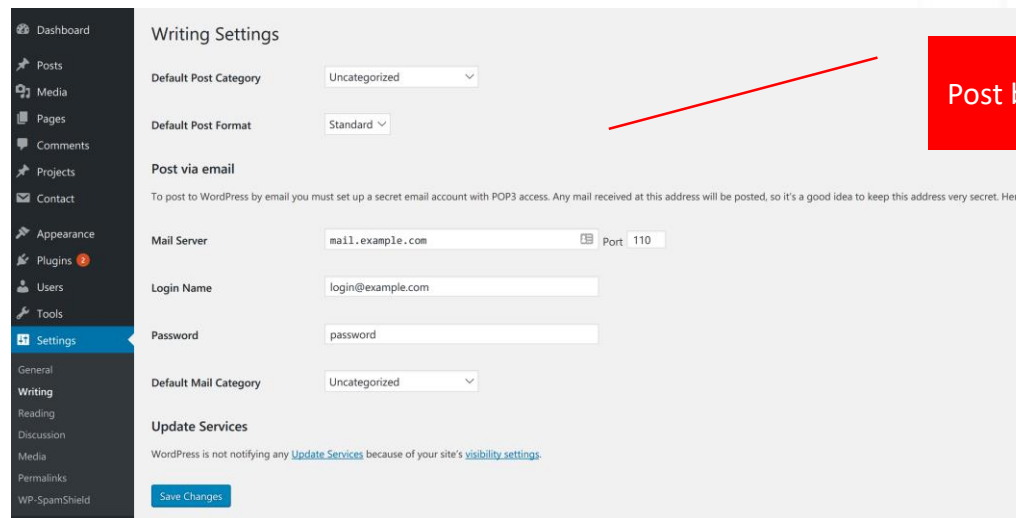
**Configurations**

Mobile Access



A screenshot of the WordPress 'General Settings' page. The left sidebar shows the 'Settings' menu item highlighted. The main content area includes fields for 'Site Title' (Test), 'Tagline' (just another WordPress site), 'WordPress Address (URL)' (http://localhost/wordpress-svn/src), 'Site Address (URL)' (http://localhost/wordpress-svn/src), and 'E-mail Address'. A red box highlights the URL fields, and a red arrow points from a text box on the right to this box.

HTTPS settings, must be changed for links to work properly, in addition to installing the SSL cert on the server.



A screenshot of the WordPress 'Writing Settings' page. The left sidebar shows the 'Settings' menu item highlighted. The main content area includes fields for 'Default Post Category' (Uncategorized), 'Default Post Format' (Standard), 'Post via email' (with a note about setting up a secret email account), 'Mail Server' (mail.example.com), 'Login Name' (login@example.com), 'Password' (password), and 'Default Mail Category' (Uncategorized). A red arrow points from a text box on the right to the 'Post via email' section.

Post by email settings

# Common Features

User Accounts

Audit Trail

Forms

Plugins/Themes

Configurations

**Mobile Access**

There's an app for that.

# Common Features

User Accounts

Audit Trail

Forms

Plugins/Themes

Configurations

**Mobile Access**

There's an app for that.

## Security Concerns

- **Remote access may be ON by default** – if your CMS has a mobile app, be sure that remote access is only turned on if you plan to use that app. Also, is the remote access feature plagued by vulnerabilities? If so, turn it off and use the mobile browser in favor of the app.
- **What mobile device is accessing your CMS** – having that mobile app is great, but if the device using the app does not conform to policy, you are creating a huge loophole. This is a BYOD problem in general.

# Common Features

User Accounts

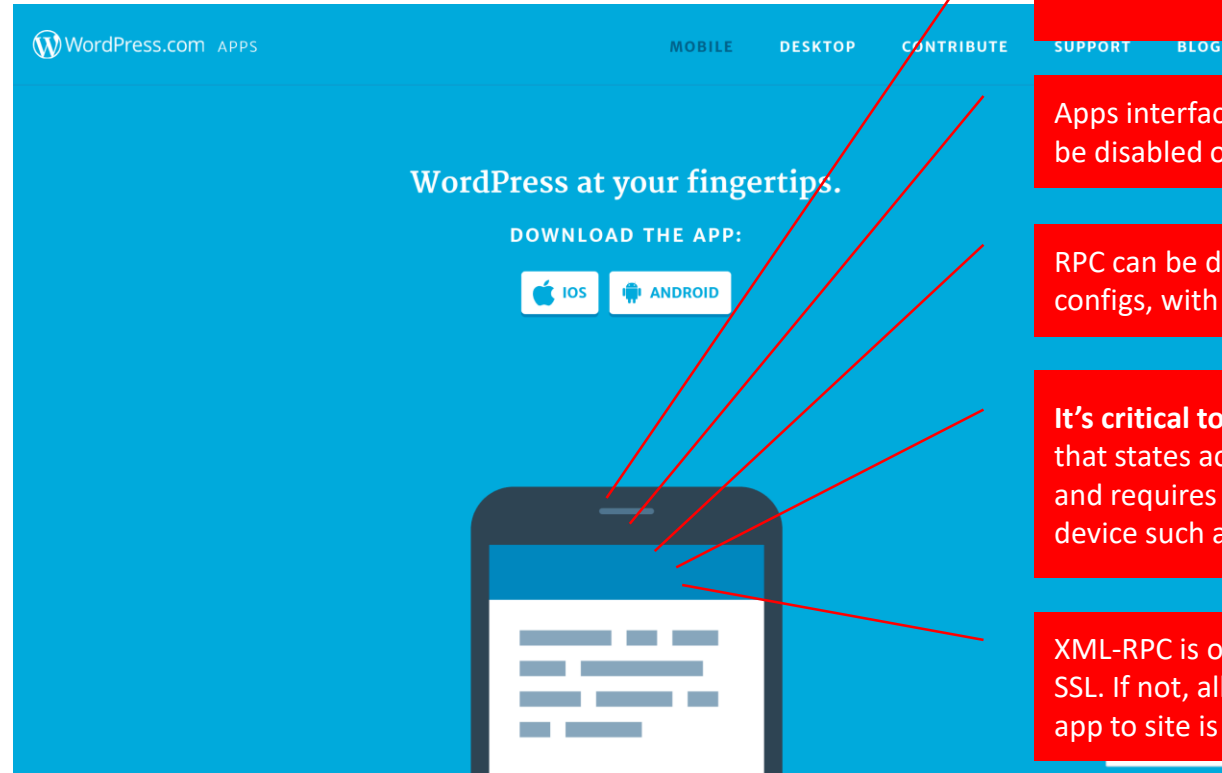
Audit Trail

Forms

Plugins/Themes

Configurations

**Mobile Access**



WordPress does have mobile apps.

Apps interface via XML-RPC – which can't be disabled out of the box.

RPC can be disabled via plugins or server configs, with some feature-loss.

**It's critical to have a written security policy** that states acceptable use of mobile app, and requires basic configurations on mobile device such as a lockscreen password.

XML-RPC is only secure if your site is using SSL. If not, all communication from mobile app to site is done in cleartext.

# Recap: For Your Next CMS Project

Next time you are planning a website or CMS project, be sure to consider:

- **User accounts** – policies are enforced via the CMS or manual process.
- **Audit trail** – an audit trail is present. Even if that means web server logs.
- **Forms** – are scrubbed for injection attacks and a form framework is present.
- **Plugins** – are reviewed for integrity and updated frequently.
- **Default configuration** – is double-checked before going live with the site.
- **Mobile access** – is controlled and planned out before allowing remote access.

# Thank You!

[salvino@coderedcorp.com](mailto:salvino@coderedcorp.com)

Twitter: @vincosalvino