

WordPress Meetup Activity

WordPress Security Essentials

60 minutes · Beginner · WordPress Playground

playground.wordpress.net

By the end of this activity, you will be able to:

1. Identify the security features WordPress provides out of the box
2. Perform a basic security audit using the WordPress dashboard
3. Configure two-factor authentication using the Two Factor plugin
4. Evaluate whether additional security plugins are needed for a given site
5. Build a monthly security routine you can repeat in under 15 minutes

What You Need

1. playground.wordpress.net — open this now and let it load (about 20-30 seconds)
2. A modern browser with the latest update installed (Chrome or Firefox recommended)
3. No WordPress account needed — Playground starts automatically
4. No prior security experience needed
5. Optional: an authenticator app on your phone (**Google Authenticator**, **Authy**, or **1Password**) for the 2FA demonstration

Activity Overview

Part 1 — Introduction and Discussion

10 min

Part 2 — What WordPress Provides Out of the Box

10 min

Part 3 — Hands-On Security Audit in Playground

25 min

Part 4 — Closing Common Security Gaps

10 min

Part 5 — Building a Security Routine

5 min

How WordPress Sites Get Hacked

Most Common Attack Vectors	Key Principles
Outdated plugins with known CVEs	Security is a spectrum, not a checkbox
Weak or reused passwords	The goal: not be the easiest target
Abandoned plugins left installed	WordPress core is actively maintained
Admin username: "admin"	The risk lives in plugins and themes
No HTTPS (credentials in plain text)	The fewer plugins, the better

What WordPress Provides Out of the Box

Feature	What It Does
Automatic background updates	Core minor releases, plugins, and themes can auto-update. Dashboard > Updates shows status.
Password strength indicator	Grades passwords in real time. WordPress will not save a password it considers too weak.
User role system	Five built-in roles: Administrator, Editor, Author, Contributor, Subscriber. Limit admin access.
Nonces and permission checks	Core uses one-time tokens to protect against cross-site request forgery. Good plugins follow this.
Regular security releases	The Security Team issues patches quickly. Release notes include CVE identifiers for everything patched.

What Is Not Included by Default

Gap	Notes
Two-factor authentication	We will add this in Part 3 using the Two Factor plugin.
Login attempt rate limiting	Some hosting environments add this at the server level. WordPress core does not.
File integrity monitoring	Detects unauthorized changes to core files. Only relevant if you suspect a compromise.
Web application firewall	Blocks malicious requests before they reach WordPress. Hosting-level is usually better.

Hands-On Security Audit in Playground

1. **Dashboard** — Look for any WordPress update notices or plugin update banners at the top.
2. **Dashboard > Updates** — Check the WordPress version, pending plugin updates, and theme updates.
3. **Plugins > Installed Plugins** — Review the list: Do you know what each one does? Any deactivated but not deleted?
4. **Users > All Users** — Look for accounts you don't recognize. Is Administrator access limited to those who need it?
5. **Users > Your Profile** — Click Generate Password. Watch the strength indicator grade complexity in real time. Close without saving.
6. **Settings > General** — Confirm Site Address starts with https. Verify Administration Email is actively monitored.

Install Two Factor and Enable 2FA

1. **Plugins > Add Plugin** — Search "Two Factor". Install the plugin by WordPress Contributors.
2. **Activate** — After activation, no redirect. Stay in the Plugins page.
3. **Users > Your Profile** — Scroll down to the Two-Factor Options section (below the password fields).
4. **Enable Email** — Toggle Email as the primary method. Click Update Profile to save.
5. **Confirm** — Scroll back up to verify Email shows as enabled. Note: Authenticator App is stronger for real sites.

Closing Common Security Gaps

1. **Outdated plugins and themes** — #1 attack vector. Automated scanners look for known CVEs. Update first, everything else second.
2. **The "admin" username** — Older sites may still use it. Fix: create a new Admin account, log in, delete the old "admin".
3. **No HTTPS** — Login credentials transmitted in plain text. Most hosts include free SSL. Check your address bar.
4. **No backups (or untested backups)** — Not a security tool, but the fastest recovery path. Know where they are and when they last ran.

Building a Security Routine

1. **Dashboard > Updates** — Apply all available WordPress, plugin, and theme updates.
2. **Users > All Users** — Remove any account(s) you do not recognize.
3. **Plugins > Installed Plugins** — Delete any plugin you are not actively using. Deactivated-but-installed plugins can still be exploited.
4. **Check your backups** — Log into your hosting control panel. Verify backups ran recently.

Note: Before installing any plugin: Last updated within 2 years? Over 1,000 active installs? Tested with your WordPress version? Does one thing rather than bundling features you do not need?

Debrief — 5 Minutes

- 1 You just ran the same audit a professional would run on your site. What surprised you most?
- 2 Looking at what you reviewed today, what is the first thing you will fix or check on your own site?
- 3 When will you do it? What would it take to set a monthly reminder?

Sources and Further Reading

Two-Factor Authentication for WordPress — Learn WordPress	https://learn.wordpress.org/lesson/two-factor-authentication/
WordPress Security Whitepaper	https://wordpress.org/about/security/
Hardening WordPress — WordPress Developer Resources	https://developer.wordpress.org/apis/security/
Two Factor plugin (free, by WordPress Contributors)	https://wordpress.org/plugins/two-factor/



Scan this QR code to provide feedback on this activity