Security

- Developing a Security Mindset
- Guiding principles

Congratulations, your code works! But is it safe?

The WordPress development team takes security seriously. With so much of the web relying on the integrity of the platform, security is critical. While the core developers have a dedicated team focused on securing the core platform, as a theme or plugin developer you are quite aware that there is potentially much that is outside the core which can be vulnerable. Because WordPress provides so much power and flexibility, plugins and themes are key points of weakness.

When writing code that will run across hundreds if not thousands of websites, you should be extra cautious of how you handle data coming into WordPress and how it's then presented to the end user. This commonly comes up when building a settings page for your theme, creating and manipulating shortcodes, or saving and rendering extra data associated with a post.

Developing a Security Mindset

When developing, it is important to consider security as you add functionality. Use the following principles as you progress through your development efforts:

- **Don't trust any data.** Don't trust user input, third-party APIs, or data in your database without verification. Protection of your WordPress themes begins with ensuring the data entering and leaving your theme is as intended. Always make sure to *validate* and *sanitize* user input before using it, and to *escape* on output.
- **Rely on the WordPress API.** Many core WordPress functions provide the build in the functionality of validating and sanitizing data. Rely on the WordPress provided functions when possible.
- **Keep your code up to date.** As technology evolves, so does the potential for new security holes in your plugin or theme. Stay vigilant by maintaining your code and updating as required.

Guiding principles

1. Never trust user input.
2. Escape as late as possible.
3. Escape everything from untrusted sources (e.g., databases and users), third-parties (e.g., Twitter), etc.
4. Never assume anything.
5. Sanitization is okay, but validation/rejection is better.

□□□ #2
□ □□□ □□□ 2026-10-31 18:07:25 UTC
□ □□□ □□□ 2026-10-31 18:07:27 UTC