WordPress Configuration Hardening

WordPress Configuration Hardening

- Disable Debug Mode
- Disable File Editing in Admin
- Restrict XML-RPC

Disable Debug Mode

What This Does

This protection ensures that WordPress debug mode is disabled in production environments.

It prevents error messages and diagnostic information from being displayed publicly.

Why It Matters

When debug mode is enabled, WordPress may display:

- PHP errors and warnings
- file paths and system structure
- plugin and theme information
- database query details

This information can expose sensitive details about your site and make it easier for attackers to identify vulnerabilities.

When to Apply It

This protection is recommended for all production websites.

Apply it when:

- your site is publicly accessible
- development is complete
- you want to prevent information leakage

When Not to Apply It

You may choose not to apply this protection if:

- you are actively developing or debugging your site
- you require visible error output for troubleshooting

In these cases, debug mode should only be enabled temporarily and never on a live site.

How Steel Security Applies This

Steel Security ensures debug settings are configured securely.

This typically involves:

- disabling `WP_DEBUG`
- preventing error display in the browser
- ensuring errors are not publicly exposed

Changes are applied directly to your WordPress configuration.

What to Expect After Applying

After applying this protection:

- errors will no longer be displayed publicly
- your site will appear cleaner and more stable to users
- sensitive debugging information will be hidden

This does not prevent errors from occurring — it only prevents exposure.

How to Verify

To verify the protection:

1. Trigger or observe an error on your site (if applicable)
2. Confirm that error details are not displayed publicly

You should not see:

- PHP warnings
- file paths
- stack traces

How to Revert (Rollback)

To revert this protection:

1. Navigate to the hardening section in Steel Security
2. Disable the control
3. Confirm the change
4. Verify that debug output is restored (if needed)

Only enable debug mode temporarily and with caution.

Common Issues

Errors Are No Longer Visible

This is expected.

Debug output is being hidden for security.

If needed:

- enable logging instead of display
- review server logs for diagnostics

Changes Do Not Take Effect

- confirm configuration was updated correctly
- check for conflicting settings in `wp-config.php`
- ensure hosting environment is not overriding values

Related

- Uploads PHP Execution Protection
- Disable Directory Listing
- Safe Rollback Practices

Disable File Editing in Admin

What This Does

This protection disables the built-in WordPress file editor within the admin dashboard.

It prevents users from editing theme and plugin files directly through the WordPress interface.

Why It Matters

By default, WordPress allows administrators to edit PHP files directly from the dashboard.

If an attacker gains admin access, they can:

- inject malicious code
- modify plugin or theme files
- create persistent backdoors

Disabling file editing removes an easy path for exploitation.

When to Apply It

This protection is recommended for most WordPress sites.

Apply it when:

- your site is in production
- you manage code through FTP, SSH, or version control
- you want to reduce risk from compromised admin accounts

When Not to Apply It

You may choose not to apply this protection if:

- you rely on the built-in editor for quick changes
- you do not have alternative access (FTP/SSH)
- your workflow depends on in-dashboard editing

If used, the editor should still be limited to trusted users only.

How Steel Security Applies This

Steel Security disables file editing by updating WordPress configuration.

This typically involves setting:

- `DISALLOW_FILE_EDIT` to true

This removes access to the theme and plugin editors in the admin interface.

What to Expect After Applying

After applying this protection:

- the Theme Editor and Plugin Editor will no longer be accessible
- users will not be able to edit files from the dashboard
- existing functionality of your site will remain unchanged

How to Verify

To verify the protection:

1. Log in to your WordPress admin
2. Navigate to Appearance → Theme File Editor
3. Navigate to Plugins → Plugin File Editor

These options should no longer be available.

How to Revert (Rollback)

To revert this protection:

1. Navigate to the hardening section in Steel Security
2. Disable the control
3. Confirm the change
4. Refresh the admin interface

The file editors will become available again.

Common Issues

Editor Is Missing

This is expected.

The file editing feature has been disabled for security.

Unable to Make Quick Changes

If you relied on the editor:

- use FTP or SSH instead
- revert the setting if necessary
- consider updating your workflow

Setting Does Not Take Effect

- check for conflicting definitions in `wp-config.php`
- ensure the configuration is not overridden by hosting

Related

- Disable Debug Mode
- Safe Rollback Practices

Restrict XML-RPC

What This Does

This protection restricts or disables access to the WordPress XML-RPC interface.

It reduces exposure to certain types of automated attacks that target this endpoint.

Why It Matters

XML-RPC is a remote access feature that allows external systems to interact with your WordPress site.

While useful in some cases, it is commonly targeted for:

- brute force login attacks
- pingback and amplification attacks
- automated abuse of authentication endpoints

If not needed, leaving XML-RPC enabled increases your attack surface.

When to Apply It

This protection is recommended for most WordPress sites.

Apply it when:

- you do not use XML-RPC functionality
- your site does not rely on remote publishing tools
- you want to reduce exposure to automated attacks

When Not to Apply It

Do not apply this protection if your site depends on XML-RPC.

This may include:

- certain mobile apps
- remote publishing tools
- integrations that rely on XML-RPC

If unsure, apply cautiously and test functionality.

How Steel Security Applies This

Steel Security restricts access to the XML-RPC endpoint (`xmlrpc.php`).

Depending on your environment, this may include:

- blocking access at the server level
- limiting allowed request types
- restricting access to specific conditions

This prevents unauthorized or unnecessary use of the interface.

What to Expect After Applying

After applying this protection:

- XML-RPC requests will be blocked or restricted
- automated attacks targeting the endpoint will be reduced
- your site functionality will remain unchanged if XML-RPC is not in use

---

How to Verify

To verify the protection:

1. Attempt to access `/xmlrpc.php` in your browser
2. Confirm that access is denied or restricted

Expected results include:

- a 403 Forbidden response
- a blocked or limited response

How to Revert (Rollback)

To revert this protection:

1. Navigate to the hardening section in Steel Security
2. Disable the control
3. Confirm the change
4. Re-test any integrations that rely on XML-RPC

Common Issues

Remote Publishing Stops Working

This indicates XML-RPC was in use.

If needed:

- revert the change
- confirm which tool requires XML-RPC
- consider alternative APIs (e.g., REST API)

Endpoint Still Accessible

- verify server rules are applied correctly
- check for caching or proxy interference
- confirm no conflicting configuration exists

Unexpected Behavior

- test all integrations after applying
- revert if functionality is impacted
- apply more targeted restrictions if needed

Related

- Disable File Editing in Admin
- Protect Configuration Files
- Safe Rollback Practices