Version Information Exposed

What This Means

This finding indicates that your site is exposing version information for WordPress or related components.

This information may be visible in page source, headers, or other outputs.

Why It Matters

Version information can help attackers identify:

- known vulnerabilities
- outdated software
- specific attack methods

Even if your site is up to date, exposing version details makes it easier to target.

How Steel Security Detects This

Steel Security checks for common locations where version information may be exposed.

This may include:

- meta tags in page output
- response headers
- publicly visible scripts or assets

If version details are detectable, the site is flagged.

How to Fix It

To resolve this issue:

- remove or hide version information from public output
- limit exposure in headers and metadata
- apply Steel Security hardening controls related to version hiding

---

What to Expect After Fixing

After applying protections:

- version information will no longer be easily visible
- your site will be harder to fingerprint
- there should be no impact on functionality

How to Verify

To verify the fix:

1. view the page source of your site
2. inspect response headers
3. check for visible version strings

Confirm that version details are no longer exposed.

Common Causes

- default WordPress behavior exposing version meta tags
- plugins or themes revealing version information
- server headers including version details

Best Practices

- avoid exposing version information publicly
- keep WordPress and plugins updated
- combine with other information exposure controls
- review headers and output regularly

Related

- Hide Version Information
- Limit Exposure of System Info
- Disable Debug Mode

Revision #1
Created 2026-04-04 18:46:58 UTC by Jason Wassing
Updated 2026-04-04 18:46:58 UTC by Jason Wassing