

Limit Exposure of System Info

What This Does

This protection reduces the amount of system and environment information exposed by your website.

It limits visibility into how your site is configured and how it operates.

Why It Matters

Websites often expose system information unintentionally, including:

- server details
- software versions
- file paths
- error messages
- configuration hints

This information can help attackers:

- identify vulnerabilities
- tailor attacks to your environment
- gain insight into your system structure

Reducing this exposure makes your site harder to profile and target.

When to Apply It

This protection is recommended for all production websites.

Apply it when:

- your site is publicly accessible
- you want to reduce information disclosure
- you are following security best practices

When to Be Cautious

Be cautious when:

- actively debugging issues
- working in a development environment
- relying on visible system output for troubleshooting

In these cases, temporary visibility may be useful.

How Steel Security Applies This

Steel Security limits system information exposure through a combination of protections, which may include:

- suppressing error output
- reducing server or application details in responses
- limiting visible system metadata

The exact implementation depends on your environment and configuration.

What to Expect After Applying

After applying this protection:

- less system information will be visible publicly
- error messages will be less detailed or hidden
- your site will reveal less about its internal structure

Functionality should remain unchanged.

How to Verify

To verify the protection:

1. Trigger or observe areas where system information may appear

2. Confirm that sensitive details are not exposed

Check for:

- error messages
 - page source output
 - response headers
-

How to Revert (Rollback)

To revert this protection:

1. Navigate to the hardening section in Steel Security
 2. Disable or adjust the control
 3. Confirm the change
 4. Re-test visibility of system information
-

Common Issues

Debug Information Is No Longer Visible

This is expected.

System output is being suppressed for security.

If needed:

- temporarily revert the change
 - use logs or development tools instead
-

No Visible Change

This may occur if:

- your environment was already configured securely
 - system information was not being exposed
-

Incomplete Protection

Some system information may still be exposed depending on:

- server configuration
- plugins or themes
- hosting environment

Additional hardening may be required.

Best Practices

- avoid exposing system details in production
 - use logs instead of visible errors
 - apply protections consistently across environments
 - combine with other hardening controls
-

Related

- [Disable Debug Mode](#)
 - [Hide Version Information](#)
 - [Security Headers Overview](#)
 - [Safe Rollback Practices](#)
-

Revision #1

Created 2026-04-04 18:49:19 UTC by Jason Wassing

Updated 2026-04-04 18:49:20 UTC by Jason Wassing