Reviewing Findings

What This Covers

This guide explains how to review and interpret the findings from a Steel Security scan.

Understanding your findings is the key step before applying any hardening changes.

Where to View Findings

Findings are available on the **Scan** page.

To access them:

1. Navigate to **Steel Security → Scan**
2. A scan will run automatically
3. Review the list of findings once the scan completes

Each finding represents a potential security risk or configuration issue.

What a Finding Represents

A finding indicates something on your site that may:

- expose sensitive information
- weaken security
- reflect an unsafe or outdated configuration
- indicate leftover or unnecessary files

Not all findings require immediate action, but all should be understood.

Information Provided for Each Finding

Each finding includes:

- **What was detected**
- **Why it matters**
- **Recommended next steps**

This context is designed to help you make informed decisions, not just react to alerts.

How to Prioritize Findings

Start by focusing on:

High-Risk Findings

These typically include:

- exposed backup or database files
- configuration leaks
- publicly accessible sensitive data

These should be addressed as soon as possible.

Configuration Issues

Examples include:

- debug mode enabled
- unnecessary exposure of system information

These may not be immediately critical but should be corrected.

Informational Findings

Some findings may be:

- informational
- intentional based on your setup

Review these carefully before taking action.

When to Take Action

You should consider taking action when:

- the finding exposes sensitive data
- the risk is publicly accessible
- the issue is not required for your workflow

If a finding is intentional, you may choose to leave it as-is.

Applying Fixes

Some findings can be addressed using Steel Security hardening features.

Others may require:

- manual file removal
- configuration updates
- hosting-level changes

Always review the recommendation before applying changes.

Safe Approach to Fixing Issues

Follow this workflow:

1. Review the finding and understand the risk
2. Confirm whether the issue is intentional
3. Apply the recommended fix or hardening
4. Re-run the scan to verify resolution

Avoid applying multiple changes at once without verification.

What Not to Do

- Do not blindly apply all fixes

- Do not remove files without understanding their purpose
- Do not assume all findings are critical

Steel Security is designed to inform, not automate decisions.

Common Questions

Why am I seeing findings on a new site?

Many WordPress installations include:

- default files
- leftover artifacts
- development configurations

These are common and should be reviewed and cleaned up.

Can I ignore a finding?

Yes, if:

- the behavior is intentional
- the risk is understood and accepted

However, you should document or remember why it was ignored.

Why does a finding still appear after fixing it?

- Ensure the change was applied correctly
- Return to the **Scan** page to trigger a new scan
- Confirm the issue is fully resolved

Tips

- Focus on quality, not quantity of fixes
- Address high-risk issues first
- Make changes incrementally

- Re-scan after each set of changes

What to Do Next

After reviewing your findings:

1. Identify the most important issues
2. Begin applying hardening controls
3. Re-scan to confirm improvements

Related

- Running Your First Scan
- Understanding the Dashboard
- Applying Hardening Safely
- Hardening Reference

Revision #1
Created 2026-04-04 18:48:26 UTC by Jason Wassing
Updated 2026-04-04 18:48:26 UTC by Jason Wassing