Working with Scan Findings

What This Covers

This guide explains how to work with scan findings within Steel Security.

It focuses on how to interpret, navigate, and act on findings efficiently as part of your workflow.

Where Findings Are Managed

Scan findings are managed on the **Scan** page.

To access them:

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

This is the primary location for reviewing and acting on detected issues.

Understanding the Findings List

The Scan page presents findings as a structured list.

Each entry represents a specific issue and includes:

- a description of the problem
- context explaining the risk
- recommended next steps

Findings are designed to be **actionable and easy to interpret**.

Working Through Findings Efficiently

A typical workflow:

1. Start with the highest-risk findings
2. Open each finding to review details
3. Determine whether action is required
4. Apply a fix or hardening control if appropriate
5. Re-scan to confirm resolution

Work through findings methodically rather than all at once.

Prioritization Strategy

When reviewing findings, prioritize:

High-Risk Issues

- exposed sensitive files
- publicly accessible data
- configuration leaks

These should be addressed first.

Moderate Issues

- debug settings
- unnecessary exposure
- non-critical misconfigurations

These should be reviewed and corrected where appropriate.

Informational Findings

- expected or intentional configurations

These may not require action but should still be understood.

Taking Action on Findings

Depending on the finding, actions may include:

- applying a hardening control
- removing or securing a file
- updating configuration settings
- making server-level changes

Always review the recommendation before taking action.

Using Hardening with Findings

Some findings can be resolved directly through Steel Security hardening features.

When available:

- review the hardening option
- confirm it is appropriate for your site
- apply the change
- re-scan to verify

Hardening provides a safe and structured way to address common issues.

Handling Intentional Findings

Not all findings indicate problems that need to be fixed.

You may choose to leave a finding unresolved if:

- it is required for your workflow
- the risk is understood and accepted
- the exposure is controlled

Be intentional with these decisions.

Re-Scanning After Changes

After addressing findings:

1. Reload the **Scan** page

2. A new scan will run automatically
3. Confirm that the issue no longer appears

This step is important to validate that changes were successful.

Avoiding Common Mistakes

- Do not apply fixes without understanding them
- Do not attempt to resolve everything at once
- Do not remove files without verifying their purpose

Work incrementally and verify each step.

When a Finding Persists

If a finding remains after applying a fix:

- confirm the change was applied correctly
- check for caching or server-level behavior
- verify the issue has been fully resolved

Some issues may require manual intervention beyond the plugin.

Tips

- Focus on high-impact issues first
- Work in small, controlled steps
- Re-scan frequently
- Use findings as an ongoing audit tool

What to Do Next

After working through your findings:

1. Apply additional hardening where appropriate
2. Monitor your Scan Risk Score

3. Continue periodic scans to maintain security

Related

- Reviewing Findings
- Applying Hardening Safely
- Scan Risk Score Explained
- Hardening Reference

Revision #1
Created 2026-04-04 18:51:53 UTC by Jason Wassing
Updated 2026-04-04 18:51:54 UTC by Jason Wassing