Overview

Overview

Understanding Scan Findings

What Scan Findings Are

Scan findings are the results generated when Steel Security analyzes your WordPress site.

Each finding highlights a potential risk, exposure, or configuration issue that may affect your site's security.

Why Findings Matter

Findings help you understand where your site may be vulnerable.

They are designed to:

- identify potential security risks
- highlight areas of unnecessary exposure
- guide you toward practical improvements

Not all findings indicate an immediate threat, but each represents an opportunity to strengthen your site.

How Findings Are Organized

Steel Security groups findings into logical categories to make them easier to understand and act on.

These categories may include:

- file exposure
- execution risks
- system and information exposure
- endpoint and access risks
- security headers

Grouping findings helps you focus on specific areas of your site.

Understanding Severity

Each finding is assigned a severity level to help prioritize action.

Severity reflects the potential impact and likelihood of exploitation.

Typical severity levels include:

- **High** — significant risk, should be addressed promptly
- **Medium** — moderate risk, should be reviewed and resolved
- **Low** — lower risk, but still worth addressing

Severity helps guide your response, but should not be the only factor in decision-making.

How to Approach Findings

When reviewing findings:

1. start with higher severity items
2. review the context of each finding
3. determine whether the issue applies to your site
4. apply fixes where appropriate
5. test your site after making changes

Avoid applying changes blindly — understanding the impact is important.

Not All Findings Require Action

Some findings may:

- reflect intentional configuration choices
- be acceptable based on your use case
- require a balanced decision between security and functionality

Steel Security provides guidance, but final decisions depend on your environment.

How Findings Connect to Hardening

Each finding typically corresponds to a hardening control.

For example:

- exposed files → file protection controls
- execution risks → execution restrictions
- missing headers → security header controls

This relationship helps you move from detection to resolution.

What to Do Next

After reviewing your findings:

- prioritize based on severity and relevance
- apply appropriate hardening controls
- verify changes after implementation
- continue monitoring over time

Key Principle

Findings are not just warnings.

They are actionable insights that help you improve your site's security posture over time.

Related

- Reviewing Findings
- Hardening Reference
- [Defense in Depth with Steel Security](https://docs.steelsecurity.com/books/hardening-reference/page/defense-in-depth-with-Steel Security)

How Findings Are Categorized

Why Findings Are Categorized

Steel Security groups findings into categories to make them easier to understand and act on.

Each category represents a different type of security concern.

This structure helps you quickly identify where issues exist within your site.

Main Categories

Findings are organized into the following core categories:

File Exposure

Issues related to files that should not be publicly accessible.

Examples include:

- configuration files
- backup files
- directory listings

Execution Risks

Issues that allow code to run in unintended ways.

Examples include:

- PHP execution in upload directories
- direct access to internal scripts

System & Information Exposure

Issues where your site reveals internal details.

Examples include:

- debug mode enabled
- version information exposed
- system metadata leakage

Endpoint & Access Risks

Issues related to exposed entry points or access controls.

Examples include:

- XML-RPC enabled
- unrestricted access to sensitive endpoints

Security Headers

Issues related to missing or weak browser-level protections.

Examples include:

- missing security headers
- incomplete header configuration

How to Use Categories

Categories help you:

- focus on specific types of risk
- address related issues together
- understand how findings connect to hardening controls

You may choose to resolve findings category by category, or prioritize based on severity.

How Categories Connect to Hardening

Each category aligns with a set of hardening controls.

For example:

- file exposure findings → file protection controls
- execution risks → execution controls
- headers → security header configuration

This alignment makes it easier to move from detection to resolution.

What to Do Next

- review findings within each category
- prioritize based on severity and relevance
- apply corresponding hardening controls

Related

- Understanding Scan Findings
- Severity Levels Explained
- Hardening Reference

Severity Levels Explained

What Severity Means

Severity indicates how important a finding is based on its potential impact and likelihood of exploitation.

It helps you prioritize which issues to address first.

Severity Levels

Steel Security assigns each finding a severity level:

High

High severity findings represent significant security risks.

These issues:

- may expose sensitive data
- may allow unauthorized access or execution
- are more likely to be targeted or exploited

Recommended Action:
Address these findings as soon as possible.

Medium

Medium severity findings represent moderate risks.

These issues:

- may increase your site's attack surface
- may contribute to larger vulnerabilities
- are important but not immediately critical

Recommended Action:
Review and resolve these findings in a timely manner.

Low

Low severity findings represent lower-risk issues.

These issues:

- may involve minor exposure or best-practice gaps
- are less likely to be exploited directly
- still contribute to overall security posture

Recommended Action:
Address these as part of routine maintenance.

How Severity Is Determined

Severity is based on a combination of factors, including:

- potential impact if exploited
- likelihood of exploitation
- level of exposure
- common attack patterns

Severity provides guidance, but does not replace judgment.

Severity Is Not Everything

While severity is important, it should not be the only factor in decision-making.

Consider:

- your specific environment
- whether the behavior is intentional
- how the finding relates to other risks

Some lower severity findings may still be important in your context.

How to Prioritize Findings

A practical approach:

1. address high severity findings first
2. review medium severity findings next
3. resolve low severity findings over time

Also consider grouping related findings for more efficient fixes.

Avoid Overreaction

Not every finding requires immediate action.

Steel Security is designed to surface risks, not create urgency where it is not needed.

Take a measured and informed approach.

Key Principle

Severity helps guide your decisions, but effective security comes from applying multiple protections over time.

Related

- Understanding Scan Findings
- How Findings Are Categorized
- Reviewing Findings