Scan

Scan

- Scan Risk Score Explained
- Working with Scan Findings

Scan Risk Score Explained

What This Covers

This guide explains how the Scan Risk Score is calculated and how to interpret it.

The Scan Risk Score provides a quick summary of your site's overall risk level based on detected findings.

What the Scan Risk Score Represents

The Scan Risk Score is an aggregated measure of risk based on the findings from your most recent scan.

It reflects:

- the presence of security issues
- the severity of those issues
- the potential exposure of sensitive data

The score is intended to give you a **high-level view**, not a complete assessment.

How to Interpret the Score

In general:

- A **higher score** indicates greater risk
- A **lower score** indicates fewer or less severe issues

However, the score should always be interpreted alongside the actual findings.

What Influences the Score

The Scan Risk Score is affected by:

- severity of findings
- number of findings
- type of exposure (e.g. public access vs internal configuration)

High-impact issues contribute more heavily than minor or informational findings.

Why the Score Is Not Everything

The Scan Risk Score is a guide, not a guarantee.

For example:

- A single high-risk issue may be more important than multiple minor ones
- Some findings may be intentional based on your setup
- Not all risks are equal in real-world impact

Always review individual findings before taking action.

How to Use the Score Effectively

Use the Scan Risk Score to:

- quickly assess overall risk
- track improvements over time
- identify when attention is needed

Do not use it as the sole basis for decisions.

Improving Your Score

To improve your Scan Risk Score:

1. Address high-risk findings first
2. Apply relevant hardening controls
3. Remove unnecessary or exposed files
4. Re-run the scan to confirm improvements

Changes to your configuration will be reflected in the score after the next scan.

When the Score Does Not Change

If your score remains the same after making changes:

- confirm the issue was fully resolved
- return to the Scan page to trigger a new scan
- review whether the finding still applies

Common Questions

Is a low score “secure”?

A lower score indicates fewer detected risks, but no system is completely risk-free.

Use the score as a guideline, not a guarantee.

Why is my score high?

Common reasons include:

- exposed backup or database files
- debug settings enabled
- publicly accessible sensitive information

These should be reviewed and addressed where appropriate.

Can I ignore the score?

You should not ignore the score entirely, but you should prioritize **understanding findings** over chasing a number.

Tips

- Focus on high-impact issues first

- Use the score to track progress, not define success
- Re-scan regularly after making changes

What to Do Next

After reviewing your Scan Risk Score:

1. Open the Scan page
2. Review individual findings
3. Apply hardening where appropriate

Related

- Reviewing Findings
- Applying Hardening Safely
- Understanding the Dashboard

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