

How Quarantine Works

What This Covers

This guide explains how the Steel Security quarantine system works and how it helps safely isolate potentially risky files.

Quarantine provides a controlled way to remove files from active use without permanently deleting them.

What Quarantine Does

Quarantine moves a file out of its original location into a secure, non-public storage area.

This means:

- the file is no longer accessible via the web
- it cannot be executed or loaded by WordPress
- it is preserved for review or restoration

This allows you to safely handle suspicious or unnecessary files.

When Quarantine Is Used

Quarantine is typically used when:

- a scan identifies a potentially sensitive or risky file
- you want to remove a file without deleting it permanently
- you are unsure whether a file is safe to remove

It provides a safe alternative to immediate deletion.

How the Process Works

When a file is quarantined:

1. The file is moved from its original location
2. It is stored in a protected directory within your site
3. Access to the file is restricted
4. A record is kept to allow restoration

The original file path is preserved for reference.

What Happens After Quarantine

After a file is quarantined:

- it will no longer appear in scans as an exposed file
- any functionality depending on that file may change
- the file remains available for restoration

You should verify your site after quarantining any file.

Safety Considerations

Quarantine is designed to be safe, but you should still:

- understand what the file does before quarantining
- avoid quarantining core or required files
- test your site after making changes

When in doubt, proceed cautiously.

Where Quarantined Files Are Stored

Quarantined files are stored in a protected location within your WordPress environment.

This location:

- is not publicly accessible
- prevents direct execution of files
- is managed by Steel Security

This ensures quarantined files cannot pose a risk while stored.

Quarantine vs Deletion

Quarantine is not the same as deletion.

Quarantine	Deletion
Reversible	Permanent
Safe for testing	No recovery
Preserves file	Removes file entirely

Quarantine is recommended when you are unsure about a file.

Limitations

- Quarantine does not analyze file contents for malware
- Some files may be required for site functionality
- Manual review may still be necessary

Steel Security focuses on safe handling, not automatic classification.

Common Questions

Will quarantining a file break my site?

It can, if the file is required.

Always test your site after quarantining any file.

Can I view quarantined files?

Yes, files remain stored and can be restored if needed.

Are quarantined files secure?

Yes.

They are stored in a protected location and are not accessible via the web.

Tips

- Use quarantine when you are unsure about a file
 - Avoid deleting files immediately
 - Always test after quarantining
 - Review findings before taking action
-

What to Do Next

After quarantining a file:

1. Test your site functionality
 2. Confirm no issues are introduced
 3. Decide whether to keep the file quarantined or restore it
-

Related

- [Restoring Quarantined Files](#)
 - [Working with Scan Findings](#)
 - [Safe Rollback Practices](#)
-

Revision #1

Created 2026-04-04 18:51:53 UTC by Jason Wassing

Updated 2026-04-04 18:51:54 UTC by Jason Wassing