

Backup Files Exposed

What This Means

This finding indicates that backup files are publicly accessible on your site.

These files may contain full or partial copies of your website or database.

Why It Matters

Backup files often include:

- complete site data
- database exports
- configuration information
- user data

If exposed, attackers may:

- download your entire site
 - extract sensitive information
 - identify vulnerabilities
 - gain access to your database structure
-

How Steel Security Detects This

Steel Security scans for common backup file patterns and locations.

This may include files with extensions such as:

- `.zip`
- `.tar`
- `.gz`
- `.sql`
- `.bak`

If these files are accessible via a browser, they are flagged.

How to Fix It

To resolve this issue:

- remove unnecessary backup files from public directories
- move backups to secure, non-public locations
- restrict access using server-level rules

You may also use Steel Security hardening controls related to file protection.

What to Expect After Fixing

After applying protections:

- backup files will no longer be accessible via browser
 - sensitive data will not be exposed publicly
 - your site structure will remain secure
-

How to Verify

To verify the fix:

1. attempt to access the backup file via its URL
 2. confirm that access is denied or the file no longer exists
-

Common Causes

- backups stored in the web root or uploads directory
 - automated backup plugins saving files in public locations
 - leftover files from manual backups
-

Best Practices

- store backups outside the public web directory
 - use secure storage locations (offsite or restricted access)
 - regularly clean up old backups
 - restrict access to any backup-related directories
-

Related

- [Protect Backup Files](#)
 - [Protect Configuration Files](#)
 - [Limit Exposure of System Info](#)
-

Revision #1

Created 2026-04-04 18:46:57 UTC by Jason Wassing

Updated 2026-04-04 18:46:57 UTC by Jason Wassing