Server & Environment

Server & Environment

- Server Rules Not Working
- Nginx Configuration Issues

Server Rules Not Working

What This Means

This issue occurs when server-level protections applied by Steel Security do not take effect.

You may enable a hardening control, but the expected behavior does not occur.

Common Symptoms

- restricted files or endpoints remain accessible
- directory listing is still enabled
- PHP execution is not blocked
- changes appear to have no effect

Why This Happens

Server-level rules depend on your hosting environment and configuration.

This issue may occur if:

- your server does not support the required rule type
- configuration overrides are disabled
- rules are not being read or applied
- another configuration is overriding the rules

How to Fix It

Try the following steps:

---

1. Confirm Your Server Type

- identify whether you are using Apache, Nginx, or IIS
- ensure the control you applied is supported in your environment

---

2. Check Apache Configuration (.htaccess)

If using Apache:

- ensure `.htaccess` overrides are enabled (`AllowOverride`)
- confirm the file exists and is readable
- verify no conflicting rules are present

---

3. Check Nginx Configuration

If using Nginx:

- note that `.htaccess` is not supported
- apply rules manually in your Nginx configuration
- reload or restart the server after changes

---

4. Check IIS Configuration (web.config)

If using IIS:

- confirm the `web.config` file is present
- ensure rules are applied correctly
- check for higher-level overrides

---

5. Review Hosting Restrictions

- some hosting providers restrict server-level configuration
- verify whether your hosting plan allows these changes
- consult your hosting provider if needed

What to Expect After Fixing

After resolving the issue:

- server rules should take effect immediately
- restricted behavior should function as expected
- hardening controls will apply correctly

How to Verify

- test access to restricted files or endpoints
- confirm expected responses (e.g., 403 Forbidden)
- re-check behavior after applying fixes

When to Seek Help

If the issue persists:

- note your server type and hosting environment
- document the specific control applied
- include any relevant error messages
- contact support with details

Key Principle

Server-level protections depend on your environment.

Understanding your server configuration is essential for effective hardening.

Related

- Apache (.htaccess) Hardening
- Nginx Hardening
- IIS (web.config) Hardening

Nginx Configuration Issues

What This Means

This issue occurs when expected protections are not applied on a server running Nginx.

Unlike Apache, Nginx does not support dynamic configuration through `.htaccess`.

Common Symptoms

- hardening controls appear enabled but have no effect
- restricted files or endpoints remain accessible
- security headers do not appear
- no visible change after applying protections

Why This Happens

Nginx uses centralized configuration files instead of per-directory rules.

This means:

- Steel Security cannot modify server behavior automatically
- changes must be applied manually in the server configuration
- rules will not take effect without proper configuration updates

---

How to Fix It

Try the following steps:

---

1. Confirm You Are Using Nginx

- check your hosting environment

- review server response headers
- consult your hosting provider if unsure

---

2. Apply Rules Manually

- locate your Nginx configuration files
- apply the required rules based on Steel Security recommendations
- ensure the configuration reflects the desired protections

---

3. Reload or Restart Nginx

- reload the configuration after making changes
- ensure updates are applied to the running server

---

4. Verify Configuration Scope

- confirm changes are applied to the correct server block
- ensure no other configuration overrides your rules

---

5. Check Hosting Limitations

- some hosting providers restrict access to Nginx configuration
- use available control panel tools if provided
- contact your hosting provider if necessary

What to Expect After Fixing

After resolving the issue:

- server-level protections should take effect
- restricted behavior should function as expected
- hardening controls will align with your configuration

How to Verify

- test access to restricted files or endpoints
- confirm expected responses (e.g., 403 Forbidden)
- inspect headers in browser developer tools

When to Seek Help

If the issue persists:

- document your server environment
- note which controls are not applying
- include configuration details if possible
- contact support or your hosting provider

Key Principle

Nginx requires manual configuration for server-level protections.

Steel Security provides guidance, but implementation depends on your environment.

Related

- Nginx Hardening
- Server Rules Not Working
- Changes Not Applying