X-Frame-Options

What This Does

This protection controls whether your site can be embedded inside an iframe on another website.

It helps prevent unauthorized framing of your content.

Why It Matters

Without restrictions, your site can be embedded within another page using an iframe.

This can be used for:

- clickjacking attacks
- tricking users into interacting with hidden elements
- overlaying malicious interfaces on top of your site

Restricting iframe usage helps protect users from these types of attacks.

When to Apply It

This protection is recommended for most websites.

Apply it when:

- your site should not be embedded on other domains
- you want to prevent clickjacking
- your site does not rely on being framed externally

When Not to Apply It

Do not apply strict restrictions if:

- your site must be embedded in another application
- you intentionally allow framing (e.g., widgets, integrations)

In these cases, more flexible policies may be required.

How Steel Security Applies This

Steel Security sets the `X-Frame-Options` HTTP header.

Common values include:

- `DENY` — prevents all framing
- `SAMEORIGIN` — allows framing only on the same domain

The appropriate value depends on your site's requirements.

What to Expect After Applying

After applying this protection:

- your site cannot be embedded in unauthorized iframes
- browsers will block framing attempts
- your site functionality will remain unchanged in most cases

---

How to Verify

To verify the protection:

1. Open your browser developer tools
2. Navigate to the Network tab
3. Inspect a page request
4. Look for the `X-Frame-Options` header

You should see the configured value (e.g., `DENY` or `SAMEORIGIN`).

How to Revert (Rollback)

To revert this protection:

1. Navigate to the hardening section in Steel Security
2. Disable or adjust the control
3. Confirm the change
4. Re-check the response headers

Common Issues

Site Cannot Be Embedded

This is expected if framing is restricted.

If embedding is required:

- adjust the policy
- use a more flexible approach if supported

Header Not Appearing

- verify server configuration supports headers
- check for CDN or caching layers
- ensure no conflicting rules exist

Conflicts with Other Policies

- Content Security Policy (CSP) may also control framing
- ensure policies are aligned

Related

- Security Headers Overview
- Content Security Policy (CSP)
- Safe Rollback Practices

Revision #1
Created 2026-04-04 18:49:18 UTC by Jason Wassing

Updated 2026-04-04 18:49:19 UTC by Jason Wassing