# HTTP & Browser Security

HTTP & Browser Security

# Security Headers Overview

## What This Covers

This page provides an overview of HTTP security headers and how they help protect your website.

Security headers are a set of instructions sent by your server to the browser to control how content is handled and secured.

---

## What Are Security Headers

Security headers are HTTP response headers that define how browsers should behave when interacting with your site.

They can:

- prevent certain types of attacks
- restrict how content is loaded
- control how your site is embedded or accessed

They are applied at the server level and affect all visitors.

---

## Why They Matter

Security headers help protect against common web-based attacks, including:

- cross-site scripting (XSS)
- clickjacking
- MIME-type sniffing
- data leakage through referrers

They add an additional layer of defense beyond your application code.

---

# How Steel Security Uses Security Headers

Steel Security provides guidance and controls for applying security headers safely.

Depending on your environment, this may involve:

- Apache `.htaccess` rules
- Nginx configuration guidance
- IIS web.config rules

Headers are applied at the server level to ensure consistent protection.

---

# Common Security Headers

Steel Security supports or references several important headers, including:

- Content Security Policy (CSP)
- X-Frame-Options
- X-Content-Type-Options
- Referrer-Policy

Each header serves a specific purpose and should be configured carefully.

---

# When to Apply Security Headers

Security headers are recommended for most production websites.

Apply them when:

- your site is publicly accessible
- you want to improve browser-level security
- you are following modern security best practices

---

# When to Be Cautious

Some headers, especially Content Security Policy (CSP), can affect how your site loads resources.

Be cautious when:

- your site loads external scripts or assets
- you use third-party integrations
- your configuration is complex

Always test after applying changes.

---

# What to Expect After Applying

After applying security headers:

- browsers will enforce stricter security rules
- some unsafe behaviors will be blocked
- your site may require adjustments if dependencies are restricted

Most basic headers will not impact functionality.

---

# How to Verify

To verify security headers:

1. Open your browser developer tools
2. Navigate to the Network tab
3. Inspect a page request
4. Review the response headers

You should see the applied security headers listed.

---

# How to Revert (Rollback)

To revert security headers:

1. Navigate to the hardening section in Steel Security
2. Disable the relevant control
3. Confirm the change
4. Re-check headers in your browser

# Common Issues

## Site Content Breaks

- often caused by overly strict policies (especially CSP)
- review which resources are being blocked
- adjust or revert the configuration

## Headers Not Appearing

- verify server supports header rules
- check for caching or CDN interference
- confirm configuration was applied correctly

## Conflicting Headers

- multiple configurations may overlap
- ensure only one source is managing headers
- review server and plugin interactions

# Related

- Content Security Policy (CSP)
- X-Frame-Options
- X-Content-Type-Options
- Referrer-Policy
- Safe Rollback Practices

# Content Security Policy (CSP)

## What This Does

Content Security Policy (CSP) defines which sources of content are allowed to load on your website.

It helps prevent unauthorized scripts, styles, and other resources from executing in the browser.

---

## Why It Matters

Modern websites load content from many sources, including:

- scripts
- stylesheets
- images
- fonts
- external services

Without restrictions, malicious content can be injected and executed.

Content Security Policy (CSP) helps protect against:

- cross-site scripting (XSS) attacks
- malicious script injection
- unauthorized third-party content

---

## When to Apply It

CSP is recommended for sites that want stronger browser-level protection.

Apply it when:

- you understand your site's resource loading behavior
- you are prepared to test and adjust policies
- you want to reduce reliance on browser trust

---

# When to Be Cautious

CSP can break site functionality if configured incorrectly.

Be cautious when:

- your site loads resources from multiple domains
- you use third-party scripts (analytics, ads, CDNs)
- your site relies on inline scripts or styles

Always test thoroughly after applying.

---

# How Steel Security Supports This

Steel Security does not currently provide full Content Security Policy (CSP) management.

CSP is a complex and highly environment-specific control that typically requires manual configuration.

Steel Security focuses on providing safe, broadly applicable protections first, while offering guidance for more advanced controls like CSP.

Support for CSP may be expanded in future versions.

---

# How to Apply This Manually

CSP is typically applied using HTTP response headers at the server level.

Depending on your environment, this may involve:

- Apache `.htaccess` configuration
- Nginx server configuration
- IIS web.config rules

Because CSP must be tailored to your specific site, it should be implemented carefully and tested thoroughly.

---

# What to Expect After Applying

After applying CSP:

- browsers will block unauthorized resources
- some scripts or assets may fail to load
- console warnings or errors may appear

This is expected if the policy is too restrictive or incomplete.

---

# How to Verify

To verify CSP:

1. Open your browser developer tools
2. Navigate to the Console or Network tab
3. Look for CSP-related messages

You may see:

- blocked resource warnings
- CSP violation messages

These help identify what needs adjustment.

---

# How to Revert (Rollback)

To revert CSP:

1. Remove or adjust the CSP header from your server configuration
2. Reload your site
3. Confirm that blocked resources are loading again

---

# Common Issues

## Site Functionality Breaks

This is the most common issue.

To resolve:

- identify blocked resources in the browser console
- update the policy to allow required sources
- apply changes incrementally

---

# Inline Scripts Are Blocked

CSP may block inline scripts by default.

Options include:

- allowing specific inline scripts (with caution)
- refactoring scripts to external files

---

# Third-Party Services Stop Working

Some services require specific domains to be allowed.

To resolve:

- identify required domains
- update the policy accordingly

---

# Too Many CSP Errors

This may indicate:

- an overly strict policy
- incomplete configuration

Start with a simpler policy and expand gradually.

---

# Best Practices

- start with a basic policy and refine it
- apply changes incrementally
- test thoroughly after each update
- monitor browser console for violations

---

# Tips

- CSP is powerful but requires careful tuning
- not all sites need a strict policy immediately
- prioritize stability over strictness

---

# What to Do Next

If you are considering CSP:

1. Review your site's external dependencies
2. Start with a simple policy
3. Test thoroughly
4. Refine over time

---

# Related

- Security Headers Overview
- X-Frame-Options
- X-Content-Type-Options
- Referrer-Policy
- Safe Rollback Practices

# 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

# X-Content-Type-Options

## What This Does

This protection prevents browsers from trying to guess (or “sniff”) the content type of a file.

It ensures files are interpreted only as the type declared by the server.

---

## Why It Matters

Some browsers attempt to determine a file’s type even if it is served incorrectly.

This behavior can lead to security issues such as:

- executing files as scripts when they should not be
- interpreting uploaded content in unintended ways
- increasing exposure to cross-site scripting (XSS) attacks

Disabling content type sniffing ensures files are handled safely.

---

## When to Apply It

This protection is recommended for all websites.

Apply it when:

- your site serves any type of content
- you want to enforce correct content handling
- you are following standard web security practices

---

## When Not to Apply It

In most cases, this protection should always be applied.

Only avoid applying if:

- your server is misconfigured and relies on browser sniffing (rare and discouraged)

---

# How Steel Security Applies This

Steel Security sets the `X-Content-Type-Options` HTTP header with the value:

- `nosniff`

This instructs browsers to strictly follow declared content types.

---

# What to Expect After Applying

After applying this protection:

- browsers will no longer attempt to guess file types
- improperly served files may fail to load
- your site becomes more resistant to content-based attacks

In most cases, there is no visible change.

---

# 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-Content-Type-Options` header

You should see:

- `nosniff`

---

# How to Revert (Rollback)

To revert this protection:

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

---

# Common Issues

## Files Fail to Load

This may occur if:

- files are served with incorrect MIME types
- server configuration is incomplete

To resolve:

- correct the server’s content-type configuration
- ensure files are served with proper headers

---

## No Visible Change

This is expected.

The protection works at the browser level and may not produce visible differences.

---

## Header Not Appearing

- verify server supports header rules
- check for CDN or caching layers
- confirm configuration was applied correctly

---

# Related

- Security Headers Overview

- X-Frame-Options
- Content Security Policy (CSP)
- Safe Rollback Practices

# Referrer-Policy

## What This Does

This protection controls how much referral information is shared when users navigate away from your site.

It determines what data is included in the `Referer` header sent to other websites.

---

## Why It Matters

When a user clicks a link, their browser may send the previous page's URL as a referrer.

This can expose:

- full URLs (including query parameters)
- internal paths
- sensitive information in links

Without a defined policy, more information may be shared than necessary.

---

## When to Apply It

This protection is recommended for most websites.

Apply it when:

- you want to limit information shared with external sites
- you are concerned about data leakage through URLs
- you want to follow modern privacy best practices

---

## When Not to Apply It

You may choose a less restrictive policy if:

- your site depends on referral data for analytics
- integrations require full referrer information
- marketing tools rely on detailed referral tracking

---

# How Steel Security Applies This

Steel Security sets the `Referrer-Policy` HTTP header.

Common values include:

- `no-referrer` — no referrer information is sent
- `same-origin` — referrer sent only within your site
- `strict-origin-when-cross-origin` — limited referrer for external requests (recommended default)

The selected policy balances privacy and functionality.

---

# What to Expect After Applying

After applying this protection:

- less referral data will be shared with external sites
- user privacy is improved
- some analytics or tracking tools may receive less information

In most cases, there is no visible impact on site functionality.

---

# 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 `Referrer-Policy` header

You should see the configured policy value.

---

# 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

## Analytics Data Is Reduced

This may occur if:

- a restrictive policy limits referrer information
- external tools rely on full URL data

To resolve:

- choose a less restrictive policy
- balance privacy with tracking needs

---

## No Visible Change

This is expected.

The protection affects how browsers send data, not how your site behaves visually.

---

## Header Not Appearing

- verify server supports header rules
- check for CDN or caching layers
- confirm configuration was applied correctly

---

# Related

- Security Headers Overview
- X-Frame-Options
- X-Content-Type-Options
- Content Security Policy (CSP)
- Safe Rollback Practices