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

Revision #1
Created 2026-04-04 18:49:19 UTC by Jason Wassing
Updated 2026-04-04 18:49:19 UTC by Jason Wassing