

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](#)

Revision #1

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

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