Headers & Browser Security

Headers & Browser Security

Missing Security Headers

What This Means

This finding indicates that one or more recommended security headers are missing from your site's responses.

Security headers help enforce browser-level protections.

Why It Matters

Security headers instruct browsers on how to handle your site's content.

Without them, your site may be more vulnerable to:

- clickjacking attacks
- cross-site scripting (XSS)
- content type confusion
- unintended data exposure

Adding these headers strengthens client-side security.

How Steel Security Detects This

Steel Security checks your site's HTTP responses for the presence of key security headers.

If expected headers are missing, the site is flagged.

Commonly Missing Headers

Examples of important headers include:

- `X-Frame-Options`
- `X-Content-Type-Options`

- `Referrer-Policy`
- Content Security Policy (CSP)

Not all headers are required in every case, but missing core headers increases risk.

How to Fix It

To resolve this issue:

- apply recommended security headers
- use Steel Security hardening controls for header configuration
- implement server-level headers where necessary

What to Expect After Fixing

After applying headers:

- browsers will enforce additional protections
- certain attack vectors will be reduced
- site functionality should remain unchanged in most cases

How to Verify

To verify the fix:

1. open your browser developer tools
2. inspect a page request in the Network tab
3. review response headers

Confirm that expected security headers are present.

Common Causes

- default server configurations without security headers
- missing or incomplete hardening
- lack of browser-level protections

Best Practices

- apply a baseline set of security headers
- review header configuration regularly
- test after applying changes
- expand protections gradually where appropriate

Related

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

Weak Header Configuration

What This Means

This finding indicates that one or more security headers are present but not configured optimally.

While protections exist, they may be weaker than recommended.

Why It Matters

Security headers are only effective when properly configured.

Weak configurations may:

- provide limited protection
- allow unintended behavior
- fail to fully mitigate common attack vectors

In some cases, a misconfigured header may offer little to no benefit.

How Steel Security Detects This

Steel Security evaluates the values of detected security headers.

If a header is present but does not meet recommended standards, it is flagged.

Examples of Weak Configuration

Examples may include:

- `X-Frame-Options` set too permissively
- missing or overly broad `Referrer-Policy`
- incomplete or overly permissive CSP rules

The exact issue depends on how the header is configured.

How to Fix It

To resolve this issue:

- review the current header configuration
- adjust values to follow recommended best practices
- apply Steel Security hardening controls where available
- refine server-level configuration if needed

What to Expect After Fixing

After improving configuration:

- browser protections will be more effective
- risk from client-side attacks will be reduced
- site functionality should remain stable if properly tested

How to Verify

To verify the fix:

1. inspect response headers using browser developer tools
2. confirm that header values match recommended configurations
3. test site functionality after changes

Common Causes

- default or incomplete header configurations
- overly permissive settings for compatibility
- manual configuration without full validation

Best Practices

- use recommended baseline configurations
- avoid overly permissive settings
- test changes incrementally
- balance security with functionality

Related

- Missing Security Headers
- Security Headers Overview
- X-Frame-Options
- Referrer-Policy
- Content Security Policy (CSP)