harbourline.example

HTTP Security Headers | 13 October 2026, 06:40 UTC

C

Overall grading 60/100

4 of 6 core security headers are set; X-Content-Type-Options and Referrer-Policy are missing.

Grade driven by: Missing core headers: X-Content-Type-Options, Referrer-Policy

3
LOW

About this check

What we checked

We requested one page over HTTPS and read the security instructions the server sent back with it. These headers tell a browser what it may and may not do with your site — whether to allow it inside a frame, where scripts may be loaded from, whether to guess at file types.

Why it matters

Without them a browser falls back to permissive defaults. That is what makes clickjacking possible (your page loaded invisibly inside somebody else's), and it removes the last line of defence against a script injected into your page. It also shows when a server volunteers its exact software version, which tells an attacker which known flaws to try first.

How to read the grade

The grade is driven by how many of the six core protection headers are present and correct. The additional headers and the information-disclosure checks are reported but do not by themselves move the letter.

Findings (3)

#	Finding	Risk
1	Missing Security Header — Missing security header: X-Content-Type-Options	LOW
2	Missing Security Header — Missing security header: Referrer-Policy	LOW
3	Software Version Disclosure — Server discloses software: Server	LOW

LOW

1. Missing Security Header — Missing security header: X-Content-Type-Options

CWE-693

Without this header some browsers guess ("sniff") a response's type and may run a file as script that was never meant to be.

Inferred - read from published records or response headers, not tested directly.

For technical readers

A response header the browser would have used to constrain the page is absent, so a defence that costs nothing to deploy is not in place. These headers rarely stop an attack on their own; what they do is limit what an injection or a framing attack ACHIEVES, which is why they matter most on the day something else goes wrong. The repair is to set them at the edge, so every response carries them rather than each route remembering.

What to do

Add X-Content-Type-Options: nosniff.

LOW

2. Missing Security Header — Missing security header: Referrer-Policy

CWE-693

Without a Referrer-Policy the full URL of your pages (which can carry tokens or private paths) is sent to every third-party site your pages link to or load from.

Inferred - read from published records or response headers, not tested directly.

For technical readers

A response header the browser would have used to constrain the page is absent, so a defence that costs nothing to deploy is not in place. These headers rarely stop an attack on their own; what they do is limit what an injection or a framing attack ACHIEVES, which is why they matter most on the day something else goes wrong. The repair is to set them at the edge, so every response carries them rather than each route remembering.

What to do

Add Referrer-Policy: strict-origin-when-cross-origin (or stricter).

LOW

3. Software Version Disclosure — Server discloses software: Server

CWE-200

The Server header is advertising the exact software and version you run, which helps an attacker match it to known exploits.

Inferred - read from published records or response headers, not tested directly.

For technical readers

The response names the product and its version, which is not an exposure in itself but removes the reconnaissance step: an attacker matches the version against published advisories rather than probing to find out. The repair is to suppress the version in responses — and to read the finding as a prompt to check whether the named version is current, which is usually the more important question.

What to do

Remove the version (or the whole Server header) at your web server or reverse proxy.

Security headers

4 of 6 core security headers are in place and strong enough. Every assessed response header, in order.

OK **Strict-Transport-Security**

Set.

`max-age=31536000`

OK **Content-Security-Policy**

Set.

`default-src 'self'; script-src 'self' 'unsafe-inline'; frame-ancestors 'self'`

OK **X-Frame-Options**

Set.

`SAMEORIGIN`

ACTION **X-Content-Type-Options**

Missing.

ACTION **Referrer-Policy**

Missing.

OK **Permissions-Policy**

Set.

`camera=(), microphone=(), geolocation=()`

OK **X-XSS-Protection**

Not set (or disabled), which is correct — it is deprecated.

ACTION **Server**

Reveals software/version — consider hiding it.

`nginx/1.24.0`

Report generated 17 October 2026, 19:36 UTC. Scan reference ca9dc971-de56-4f3d-82e5-6347eb33b684.