**Task 3 - Analyze Website Security Headers Using Online Tools**

# Website Security Headers

## What are website security headers?

Website security headers are special instructions sent by a web server in the HTTP response to tell the browser how to handle certain security-related behaviours.

They don’t appear on the webpage itself — instead, they work in the background to protect users from attacks like XSS (Cross-Site Scripting), clickjacking, and data sniffing.Think of them like a set of safety rules a website gives to your browser before loading the page.

Common Security Headers and Their Purpose

| **Header Name** | **Purpose** |
| --- | --- |
| **Content-Security-Policy (CSP)** | Controls what resources (scripts, styles, images) the browser can load, preventing XSS attacks. |
| **Strict-Transport-Security (HSTS)** | Forces the browser to connect over HTTPS only, blocking HTTP. |
| **X-Content-Type-Options** | Stops browsers from guessing file types, reducing the risk of malicious file execution. |
| **X-Frame-Options** | Prevents the site from being loaded inside an iframe, protecting against clickjacking. |
| **Referrer-Policy** | Controls how much referrer information (URL) is sent when navigating to another page. |
| **Permissions-Policy** | Lets you control which browser features (camera, mic, location) are allowed for the site. |
| **Cross-Origin Resource Policy (CORP)** | Restricts how resources can be shared across domains. |

## How They Work

When you visit a website:

1. Your browser sends a **request** to the server.
2. The server responds with the website content **and** security headers.
3. The browser follows these header rules to enforce security.

## Analysing the website security headers using securityheaders.com and whynopadlock.com

**SecurityHeaders.com** is an online tool that checks a website’s HTTP security headers to see how well it is protected.

* Purpose: Identify missing or misconfigured security headers and give a security grade (A+ to F).
* What it tests: Important headers like Content-Security-Policy, HSTS, X-Frame-Options, X-Content-Type-Options, X-XSS-Protection, Referrer-Policy, Permissions-Policy.
* What it generates:
  + Security grade
  + Report of present/missing headers
  + Recommendations to improve security

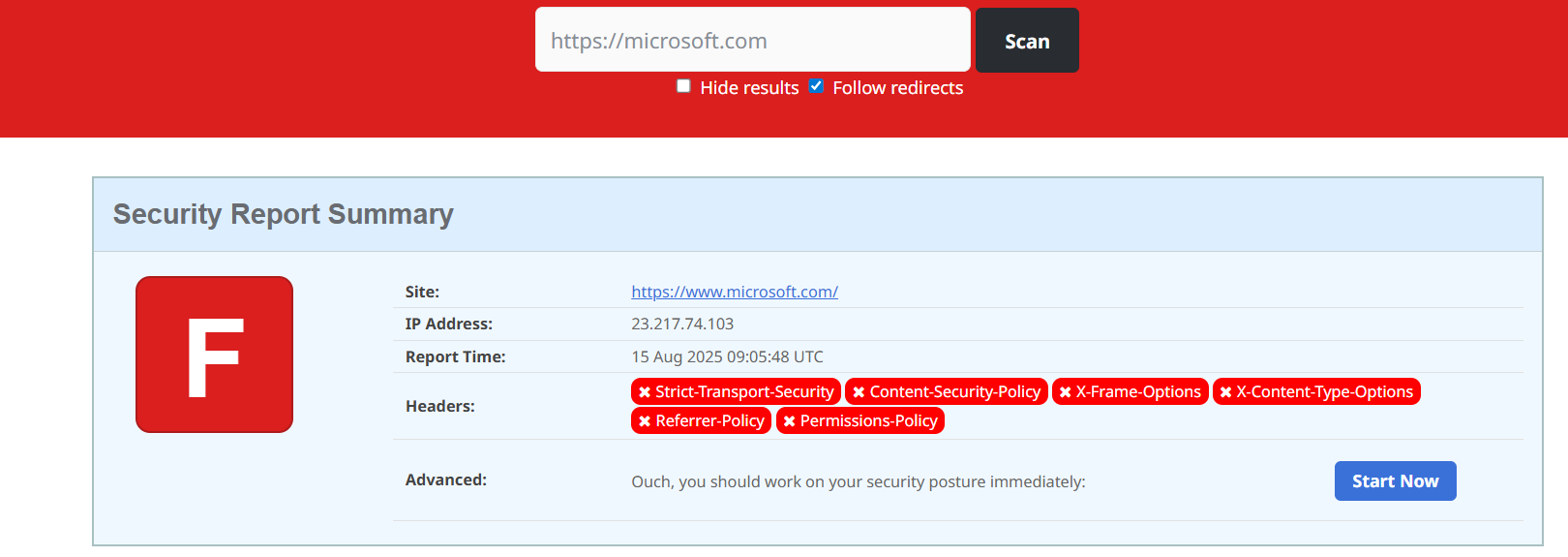
It helps quickly assess web security at the HTTP level, but does not scan for software vulnerabilities or malware.

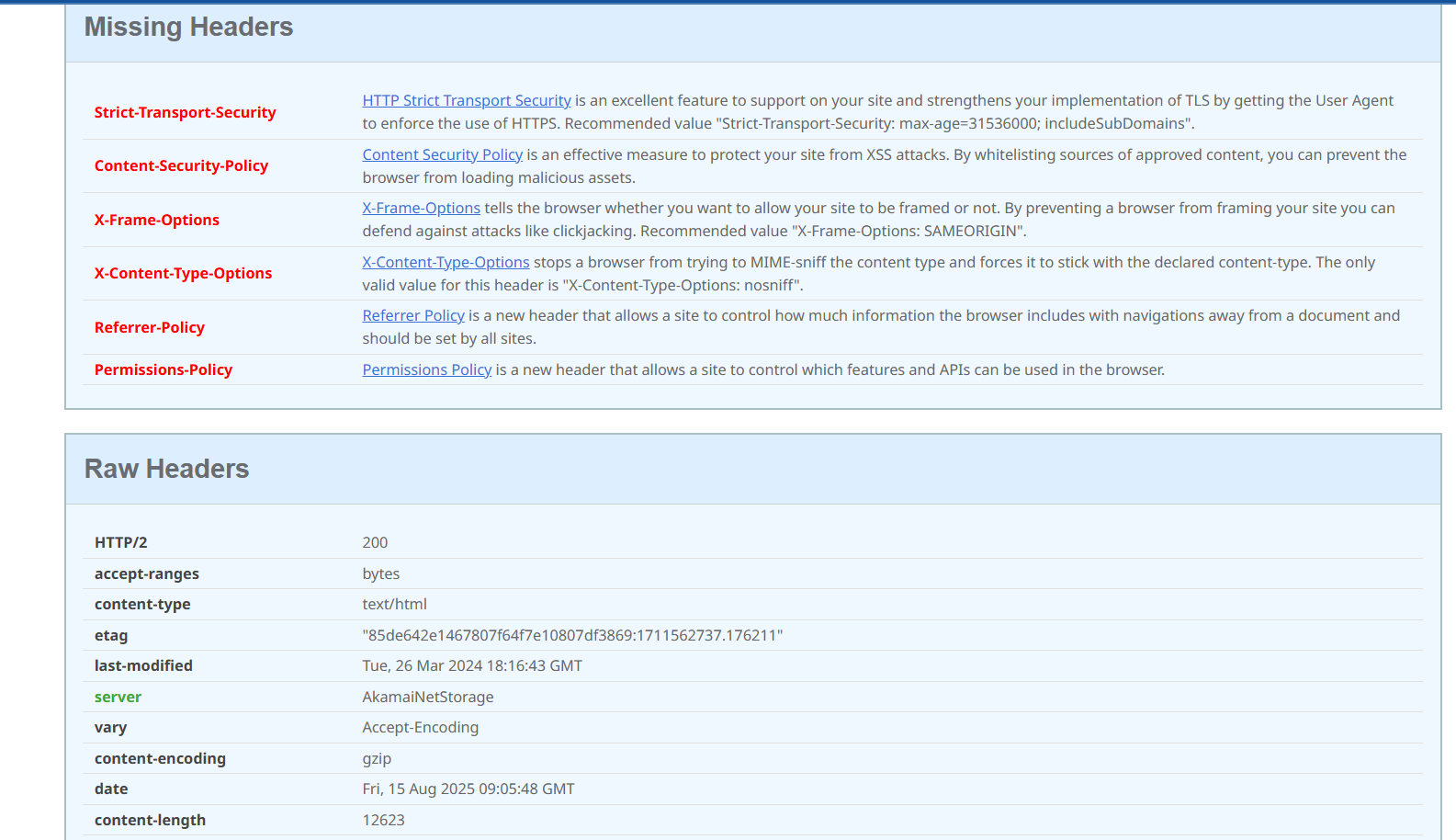
**Whynopadlock.com** is an online tool that checks a website’s HTTPS/SSL setup to see why it might not show the secure padlock in browsers.

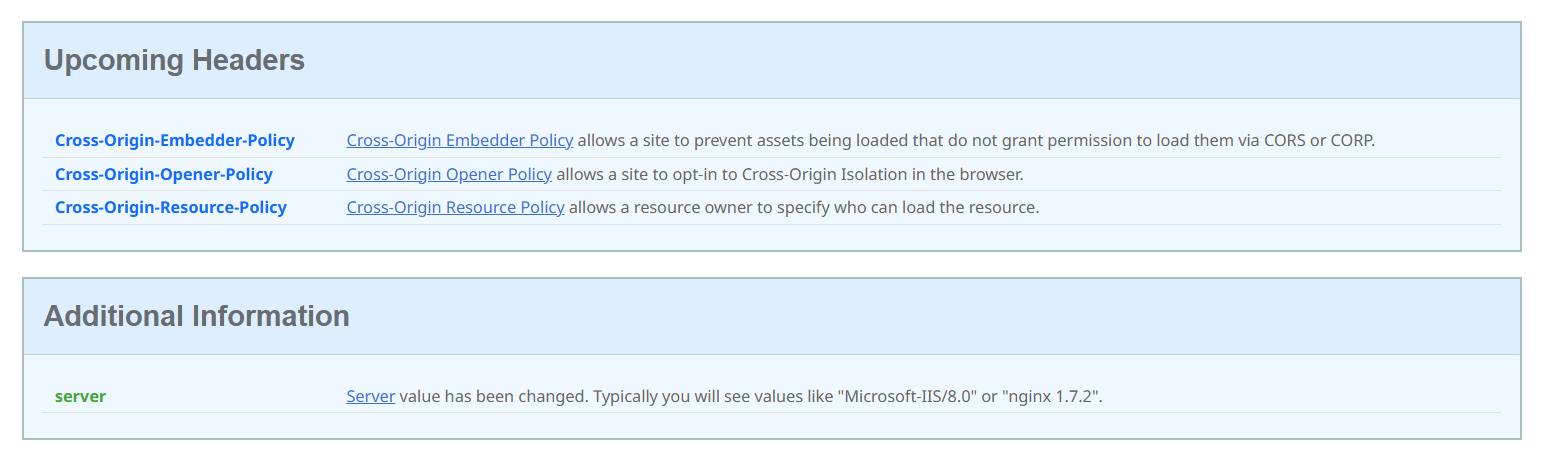
* Purpose: Identify SSL/TLS issues and mixed content problems.
* What it checks: SSL certificate validity, mixed HTTP content, HTTPS redirects, and weak protocols.
* Output: A report showing insecure elements and recommendations to fix HTTPS issues.

It helps ensure a website is fully secure and trusted by browsers.

[**https://microsoft.com**](https://microsoft.com) **using securityheaders.com**

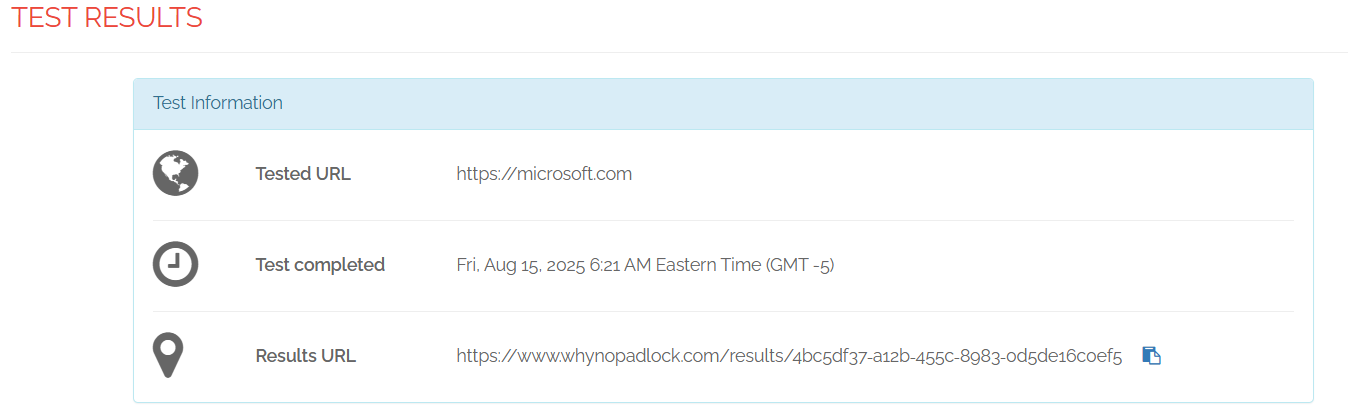


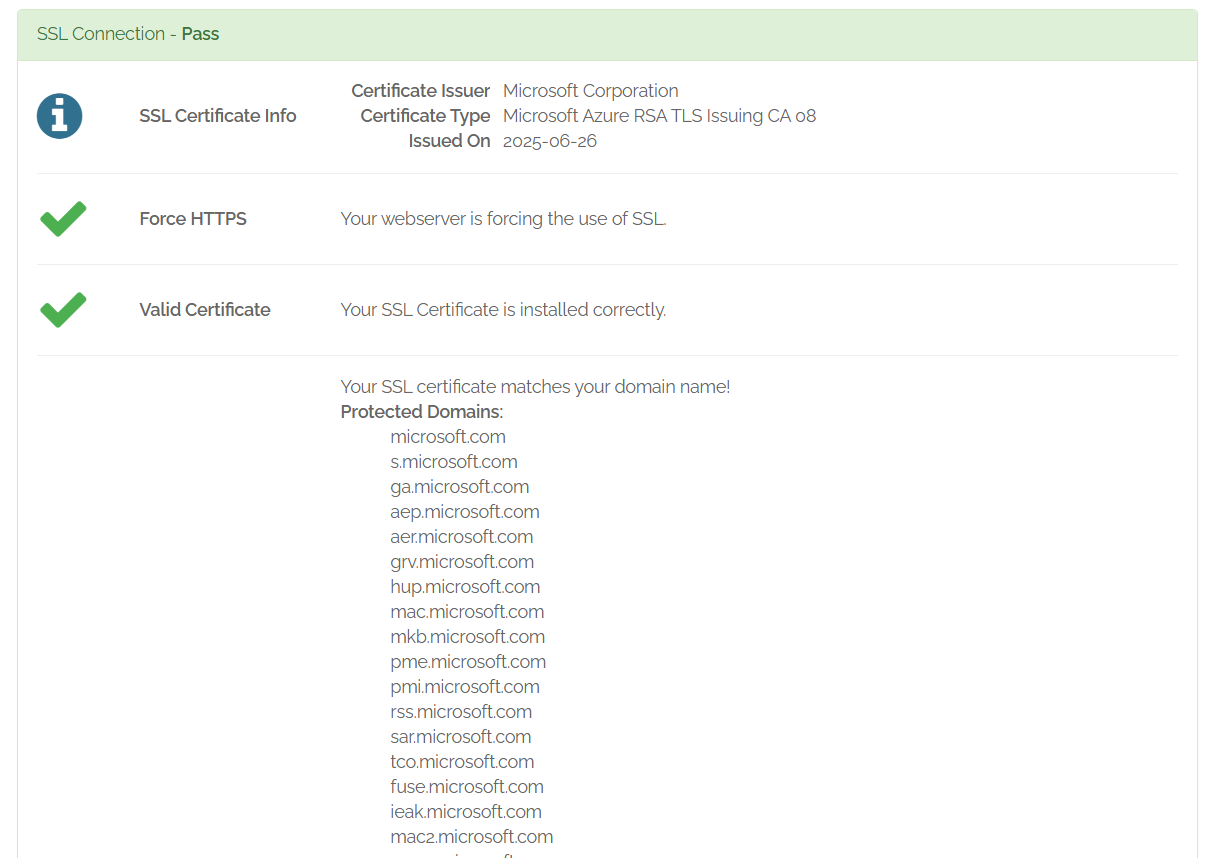


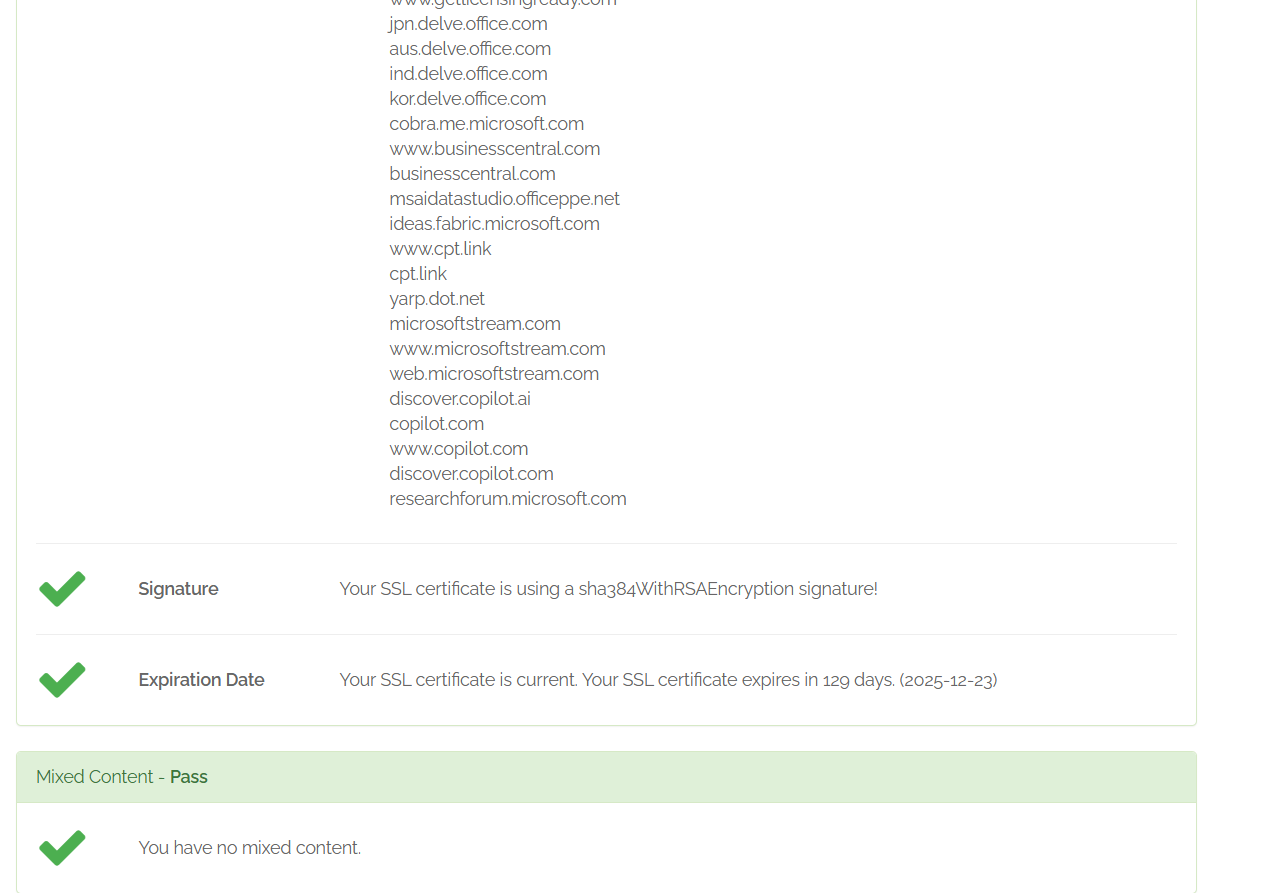


* **Grade**: Likely low because several important HTTP security headers are missing.
* **Missing Headers**:
  + **X-Frame-Options** → Helps prevent clickjacking attacks.
  + **Content-Security-Policy (CSP)** → Controls what resources can load, prevents XSS.
  + **Strict-Transport-Security (HSTS)** → Forces HTTPS, prevents downgrade attacks.
  + **X-XSS-Protection** → Mitigates some cross-site scripting attacks.
* **Observation**: The site does not fully implement all recommended headers, so while it may be secure in other ways, browser-level protections are not maximized.

[**https://microsoft.com**](https://microsoft.com) **using whynopadlock.com**



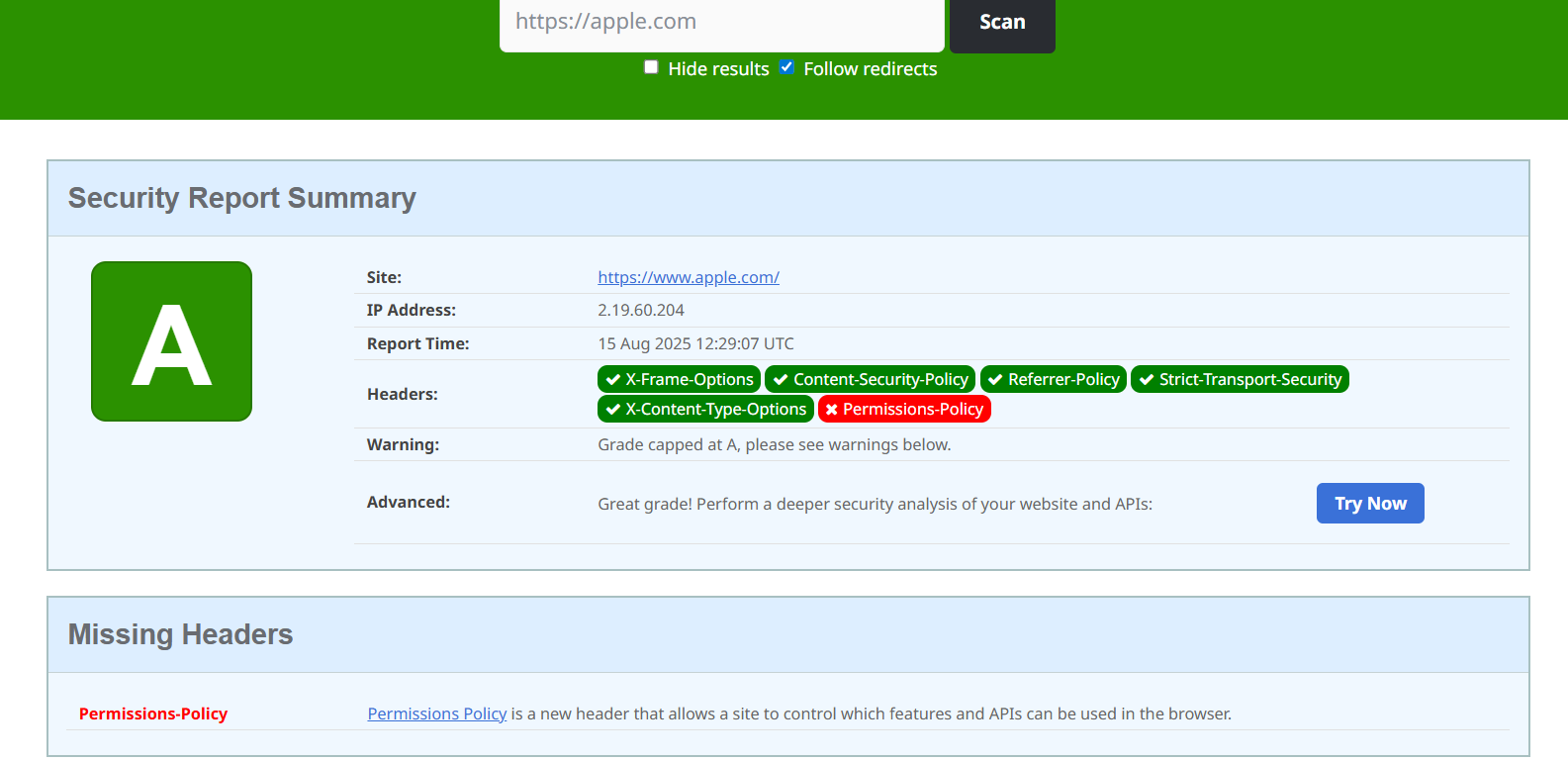


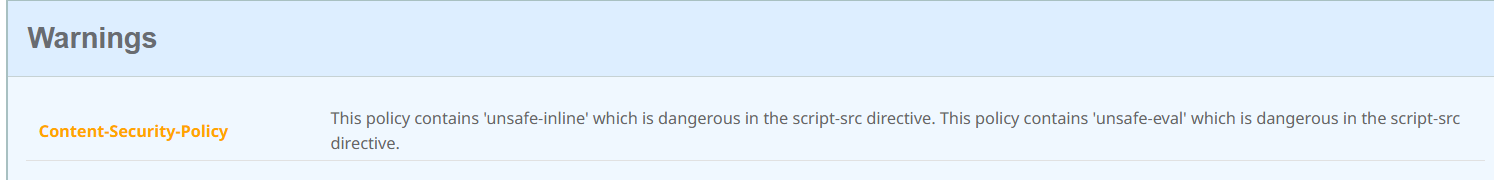


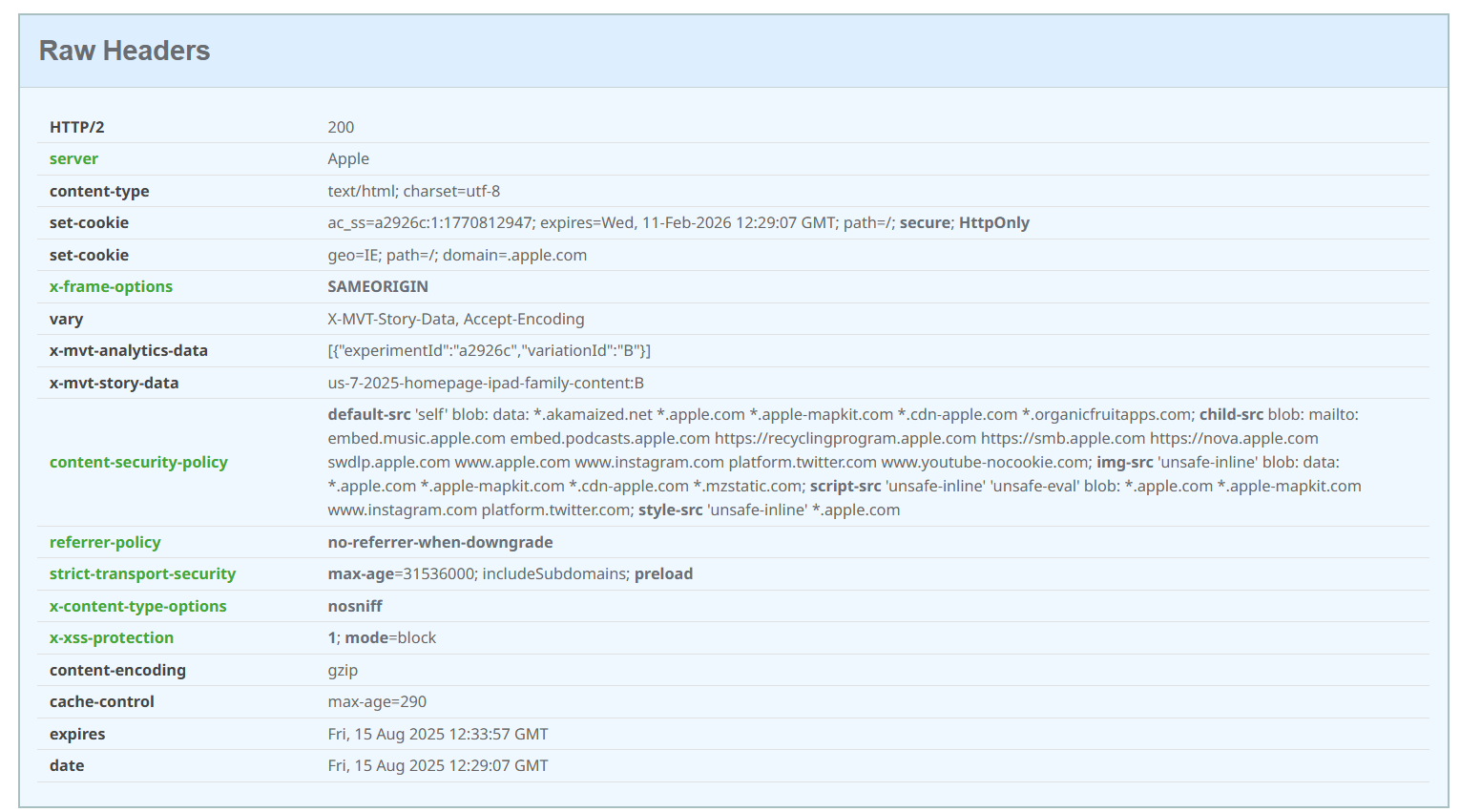
* No insecure (HTTP) content was detected — HTTPS is enforced.
* SSL certificate appears valid and up-to-date.

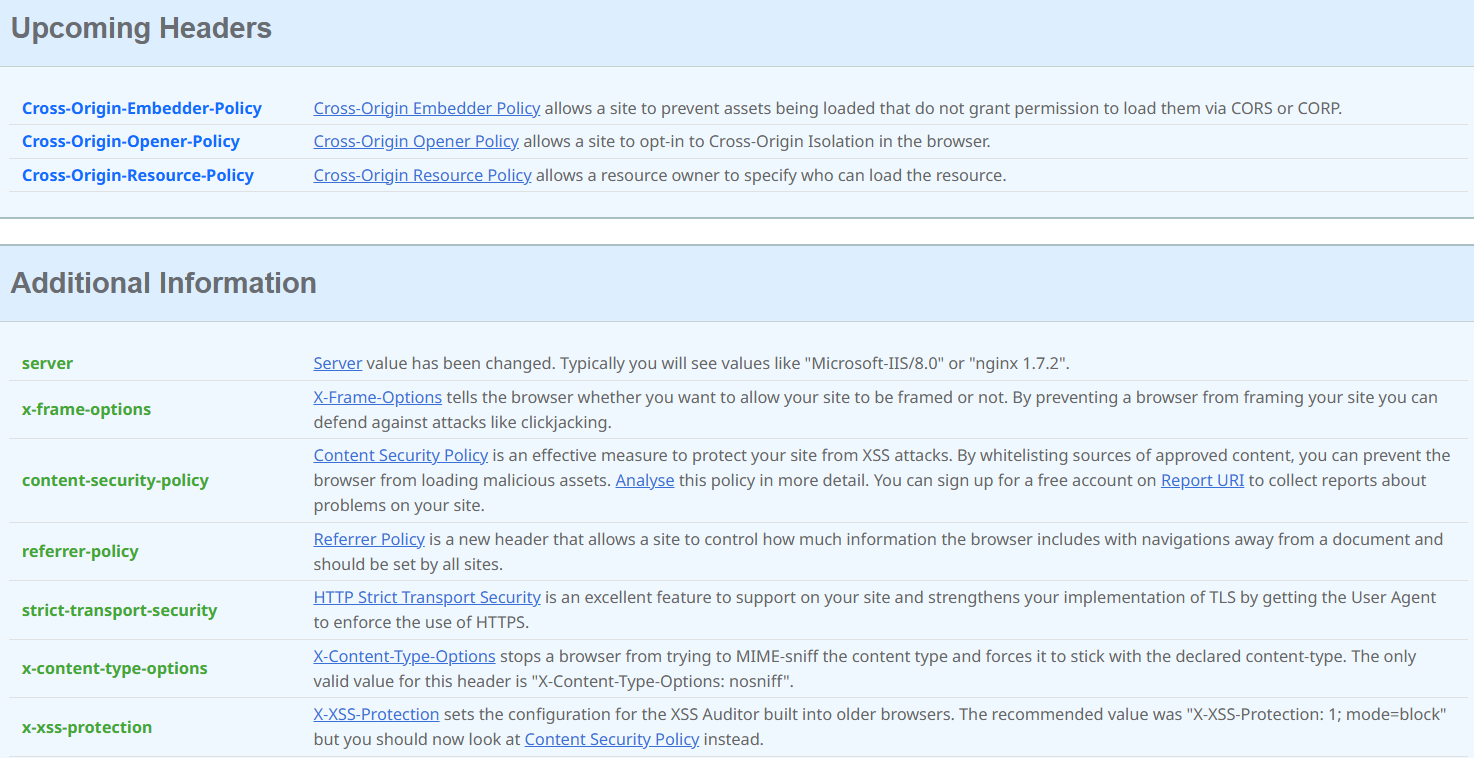
**Observation**: Encryption is fine, but site security headers could be improved.

**https://apple.com using securityheaders.com**

****

****

****

****

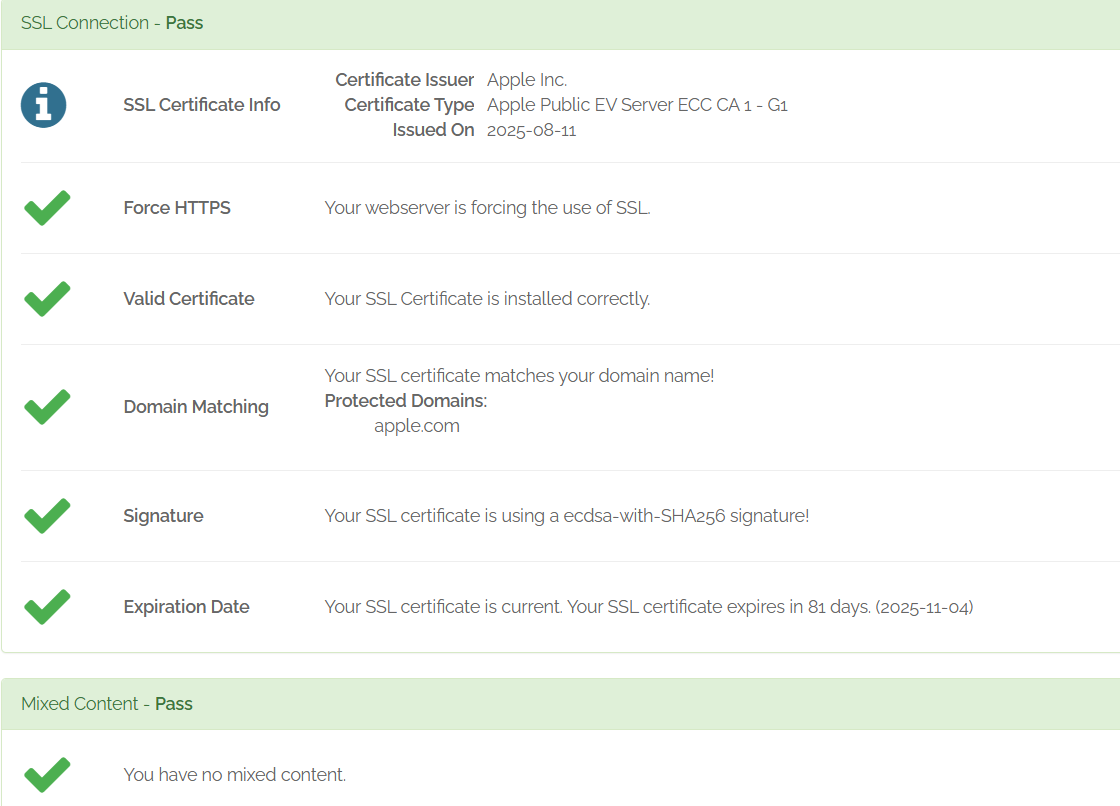
**Grade**:likely low/average due to missing security headers.

**Missing Headers**:

* X-Frame-Options
* Content-Security-Policy (CSP)
* Strict-Transport-Security (HSTS)
* X-XSS-Protection

**Observation**: Similar to Microsoft, encryption is fine, but lack of certain headers means some attacks could be easier.

**https://apple.com using whynopadlock.com**



* No mixed content issues detected.
* SSL certificate valid.

**Observation**: HTTPS is configured correctly, but same improvement points apply to missing headers.

## Overall Observation Summary:

Both Microsoft.com and Apple.com have good HTTPS/TLS configurations with no mixed content issues, meaning data in transit is secure. However, both are missing several important HTTP security headers (like CSP, HSTS, and X-Frame-Options), which could help prevent attacks such as clickjacking, XSS, and protocol downgrade. Strengthening these headers would enhance overall security by adding an extra protective layer on top of their existing encryption measures.