HTTP Observatory Report

Report Feedback

Scan summary: portfolio.mmi25a01.mmi-troyes.fr

A+

Score: 120 / 100
Scan Time: Just now
Tests Passed: 10 / 10

Scan results

Scoring

Test	Score	Reason	
Content Security Policy (CSP)	+5 ✓	Content Security Policy (CSP) implemented without **'unsafe-inline'** or **'unsafe-eval'**	Set **de**
Cookies	+5 ✓	All cookies use the **Secure** flag, session cookies use the **HttpOnly** flag, and cross-origin restrictions are in place via the **SameSite** flag.	None
Cross Origin Resource Sharing (CORS)	0 ✓	Content is not visible via cross-origin resource sharing (CORS) files or headers.	None
Redirection	0 ✓	Initial redirection is to HTTPS on same host, final destination is HTTPS	None
Referrer Policy	+5 ✓	**Referrer-Policy** header set to **no-referrer**, **same-origin**, **strict-origin** or **strict-origin-when-cross-origin**.	None
Strict Transport Security (HSTS)	0 ✓	**Strict-Transport-Security** header set to a minimum of six months (15768000).	Consi **prelo** settin submi
Subresource Integrity	-	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin.	Add S

Test	Score	Reason	
X-Content-Type-Options	0 ✓	**`X-Content-Type-Options`** header set to **`nosniff`**.	None
X-Frame-Options	+5 ✓	**`X-Frame-Options`** (XFO) header set to **`SAMEORIGIN`** or **`DENY`**.	None
Cross Origin Resource Policy	-	Cross Origin Resource Policy (CORP) is not implemented (defaults to **`cross-origin`**).	None

CSP analysis

✓ Content Security Policy (CSP) implemented without **`'unsafe-inline'`** or **`'unsafe-eval'`**

Test	Result	
Blocks execution of inline JavaScript by not allowing **`'unsafe-inline'`** inside **`script-src`**	✓	Blocking the ex strongest prote Moving JavaSc site more maint
Blocks execution of JavaScript's **`eval()`** function by not allowing **`'unsafe-eval'`** inside **`script-src`**	✓	Blocking the us prevent the exe
Blocks execution of plug-ins, using **`object-src`** restrictions	✓	Blocking the ex as inherited fro loading Flash o
Blocks inline styles by not allowing **`'unsafe-inline'`** inside **`style-src`**	✓	Blocking inline modifying the c styles to exter more maintaina
Blocks loading of active content over HTTP or FTP	✓	Loading JavaS to execute arbi policy and char
Blocks loading of passive content over HTTP or FTP	✓	This site's Cont passive conten protocols such load them over
Clickjacking protection, using **`frame-ancestors`**	✗	The use of CSP grained control
Deny by default, using **`default-src 'none'`**	✗	Denying by def your Content S resources you

Test	Result	
Restricts use of the **<base>** tag by using **base-uri 'none'**, **base-uri 'self'**, or specific origins.	✓	The **<base>** tag scripts from un
Restricts where **<form>** contents may be submitted by using **form-action 'none'**, **form-action 'self'**, or specific URIs	✓	Malicious Java sensitive form for data exfiltra
Uses CSP3's **'strict-dynamic'** directive to allow dynamic script loading (optional)	-	**'strict-dynam** load all your sit track **script-s**

Cookies

✓ All cookies use the **Secure** flag, session cookies use the **HttpOnly** flag, and cross-origin restrictions are in place via the **SameSite** flag.

Name	Expires	Path	Secure	Http
PHPSESSID	Session	/	✓	

Raw server headers

Header	V
Date	Thu, 25 Jun 2026 20:05:18 GMT
Vary	Accept-Encoding
Pragma	no-cache
Server	Apache/2.4.67 (Debian)
Expires	Thu, 19 Nov 1981 08:52:00 GMT
Connection	close
Set-Cookie	PHPSESSID=7nh8uajg3sa0rble3g2s4begnf;
Content-Type	text/html; charset=UTF-8
Cache-Control	no-store, no-cache, must-revalidate
Content-Length	5121
Referrer-Policy	strict-origin-when-cross-origin
X-Frame-Options	SAMEORIGIN
Permissions-Policy	camera=(), microphone=(), geolocation=()
X-Content-Type-Options	nosniff

Header	V
Content-Security-Policy	default-src 'self'; img-src 'self' data:; style-s action 'self'
Strict-Transport-Security	max-age=31536000; includeSubDomains

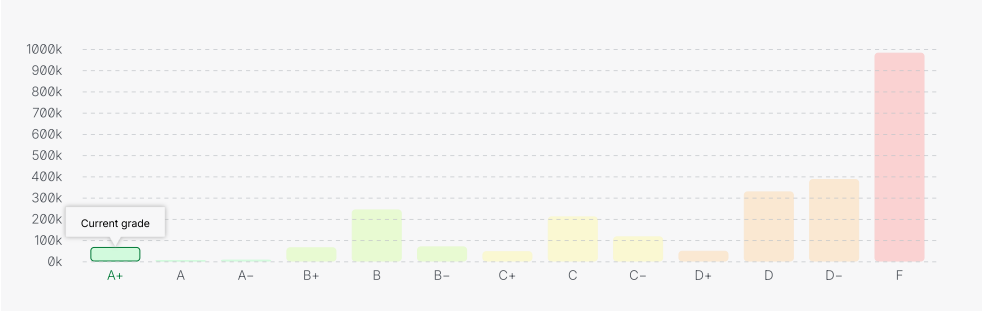
Scan history

Changes in score over time

Date	
25 juin 2026, 22:01:17	120
25 juin 2026, 21:49:27	105

Benchmark comparison

Performance trends from the past year



Refer to this graph to assess the website's current status. By following the recommendations provided and rescanning, you can expect an improvement in the website's grade.