

Queste de savoir

Présentation de HTTP Observatory

dimanche 14 juillet 2024

Table des matières

Introduction	1
1. Interface	1
1.1. Page d'accueil	1
1.2. Page de rapport	2
Conclusion	4

Introduction

Lancé en 2016, [HTTP Observatory](#) est un outil pour analyser la sécurité de sites internet qui dispose depuis peu d'une nouvelle version.

Sur leur site, Mozilla se targue d'avoir aidé à améliorer 6,9 millions de sites à travers 47 millions de scans effectués. Pour cela, l'outil effectue des tests automatisés sur la sécurité du site internet voulu, en tire un bilan et propose des solutions d'amélioration pour éviter de possibles vulnérabilités.

1. Interface

1.1. Page d'accueil

La page d'accueil explique ce qu'est l'outil et permet de lancer le scan pour un site voulu : <https://zestedesavoir.com/> par exemple.

HTTP Observatory

Launched in 2016, the HTTP Observatory enhances web security by analyzing compliance with best security practices. It has provided insights to over 6.9 million websites through 47 million scans. The [previous version of HTTP Observatory](#) is still available, however it is now deprecated and will soon be sunsetted.

Scan a website for free (e.g. mdn.dev)



FIGURE 1.1. – Page d'accueil et lancement du scan

Une fois le scan effectué, un rapport est généré.

1. Interface

1.2. Page de rapport

Le rapport généré contient une partie générale et une partie détaillée.

1.2.1. Rapport global

Le rapport global donne une indication sur les tests passés avec succès ainsi que le score global.

On peut voir que Zeste de Savoir a eu 75/100 soit B ! 🍊

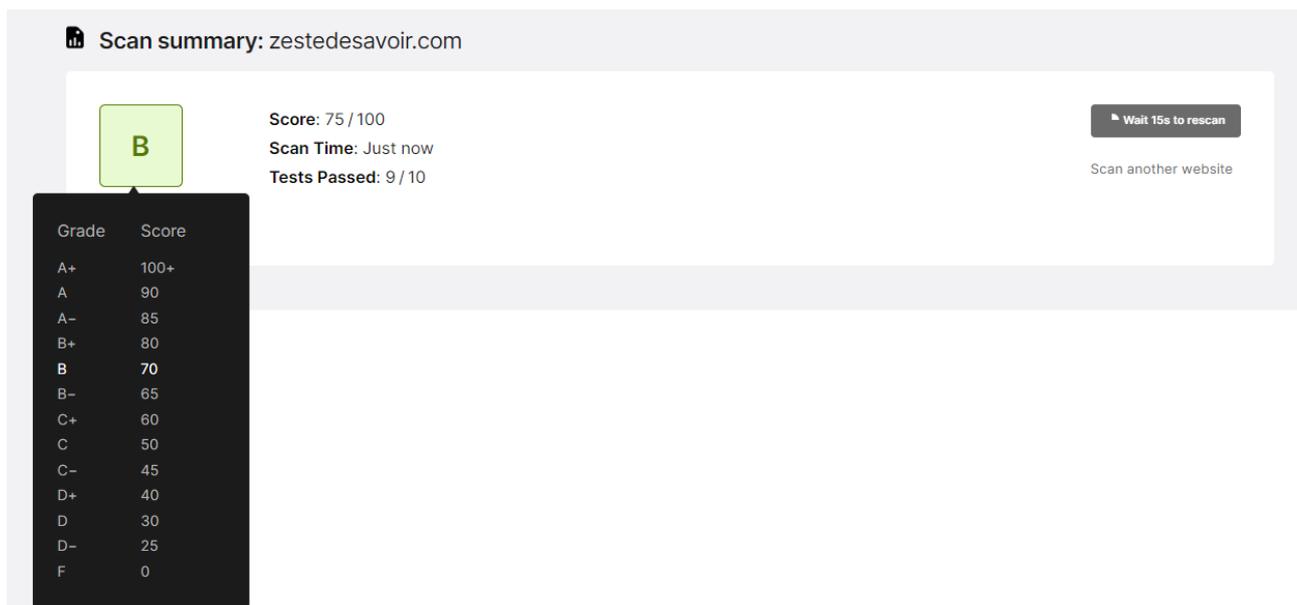


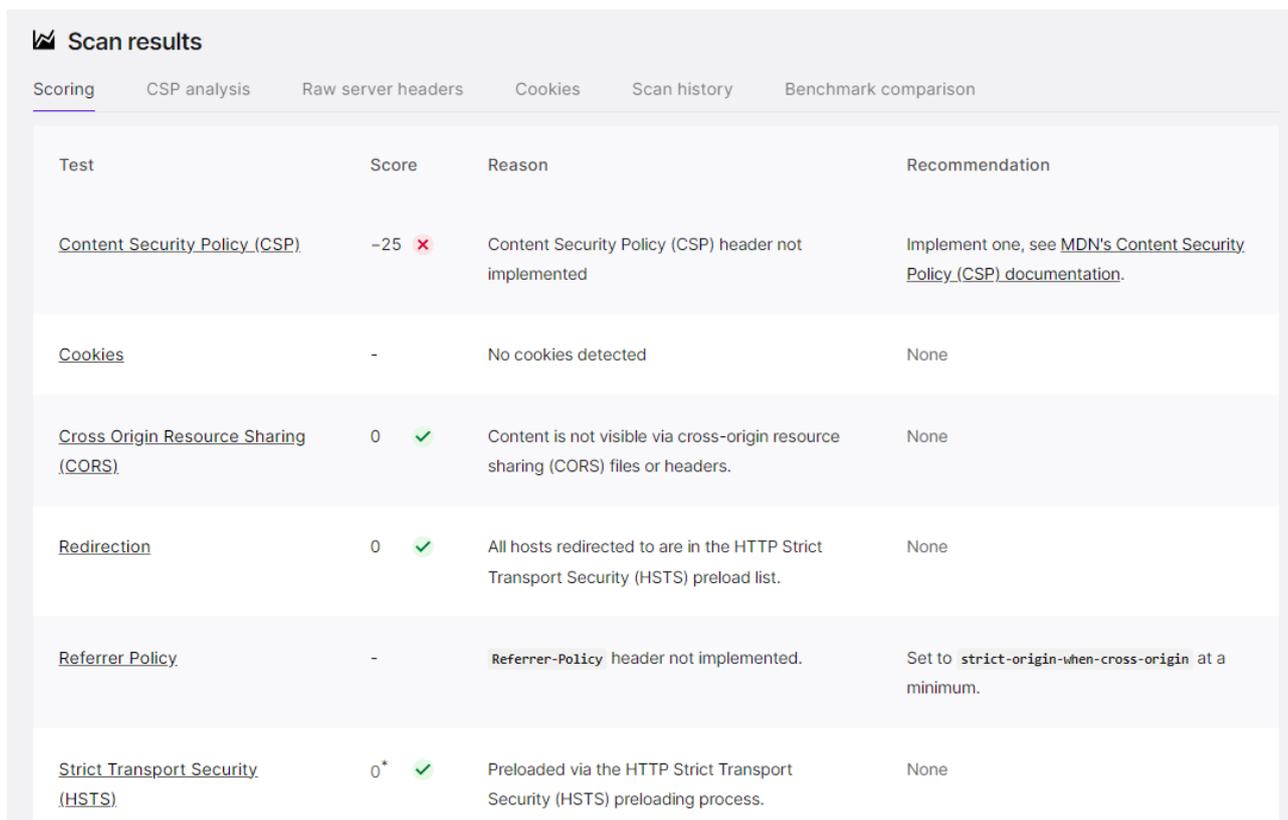
FIGURE 1.2. – Rapport global

1.2.2. Rapport détaillé

Le rapport détaillé contient une ligne de tableau par test effectué.

Pour chaque test, on a une indication sur le résultat du test, une explication sur ce résultat ainsi que des recommandations.

1. Interface

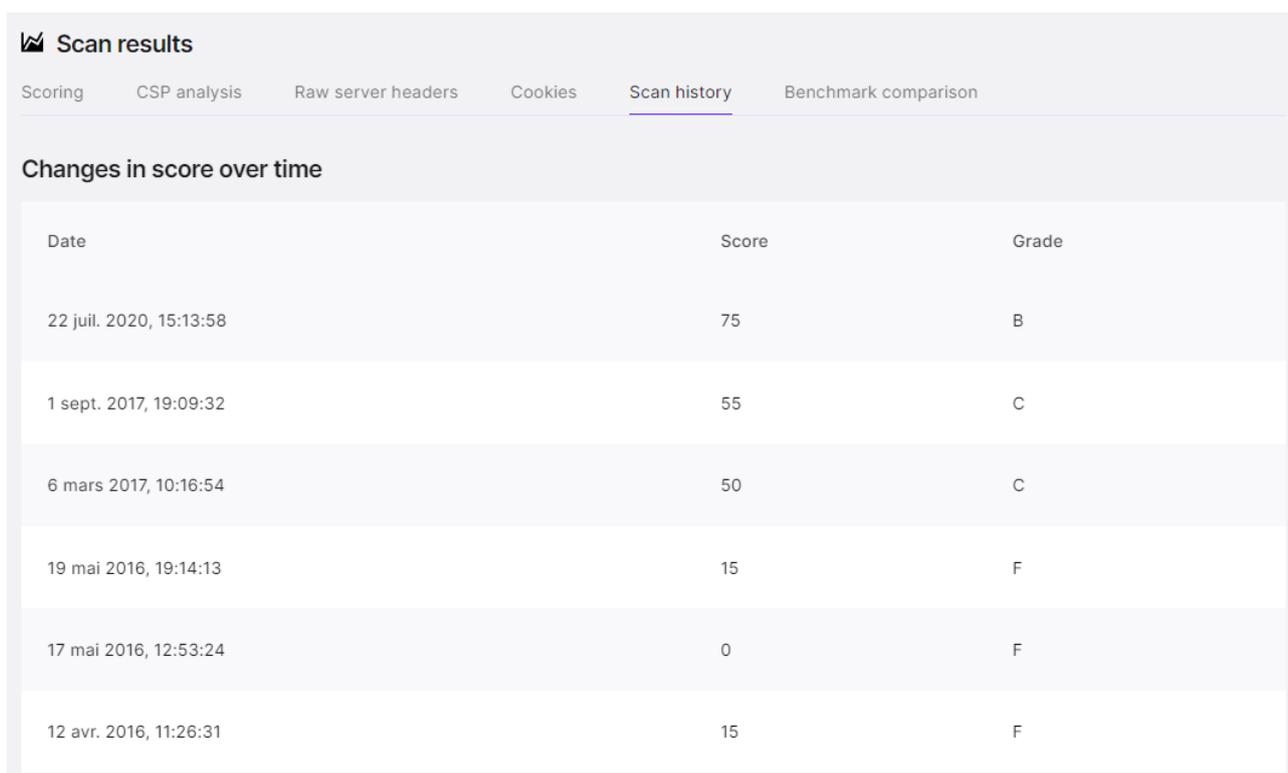


The screenshot shows the 'Scan results' page with a navigation bar containing 'Scoring', 'CSP analysis', 'Raw server headers', 'Cookies', 'Scan history', and 'Benchmark comparison'. The main content is a table with the following data:

Test	Score	Reason	Recommendation
Content Security Policy (CSP)	-25 ❌	Content Security Policy (CSP) header not implemented	Implement one, see MDN's Content Security Policy (CSP) documentation .
Cookies	-	No cookies detected	None
Cross Origin Resource Sharing (CORS)	0 ✅	Content is not visible via cross-origin resource sharing (CORS) files or headers.	None
Redirection	0 ✅	All hosts redirected to are in the HTTP Strict Transport Security (HSTS) preload list.	None
Referrer Policy	-	Referrer-Policy header not implemented.	Set to <code>strict-origin-when-cross-origin</code> at a minimum.
Strict Transport Security (HSTS)	0* ✅	Preloaded via the HTTP Strict Transport Security (HSTS) preloading process.	None

FIGURE 1.3. – Rapport détaillé

Il y a aussi différents onglets comme l'historique des notes, ce qui permet de voir l'amélioration, ou encore la comparaison, ce qui permet de voir que Zeste de Savoir est plutôt bon élève !



The screenshot shows the 'Scan results' page with the 'Scan history' tab selected. The main content is a table titled 'Changes in score over time' with the following data:

Date	Score	Grade
22 juil. 2020, 15:13:58	75	B
1 sept. 2017, 19:09:32	55	C
6 mars 2017, 10:16:54	50	C
19 mai 2016, 19:14:13	15	F
17 mai 2016, 12:53:24	0	F
12 avr. 2016, 11:26:31	15	F

FIGURE 1.4. – Historique

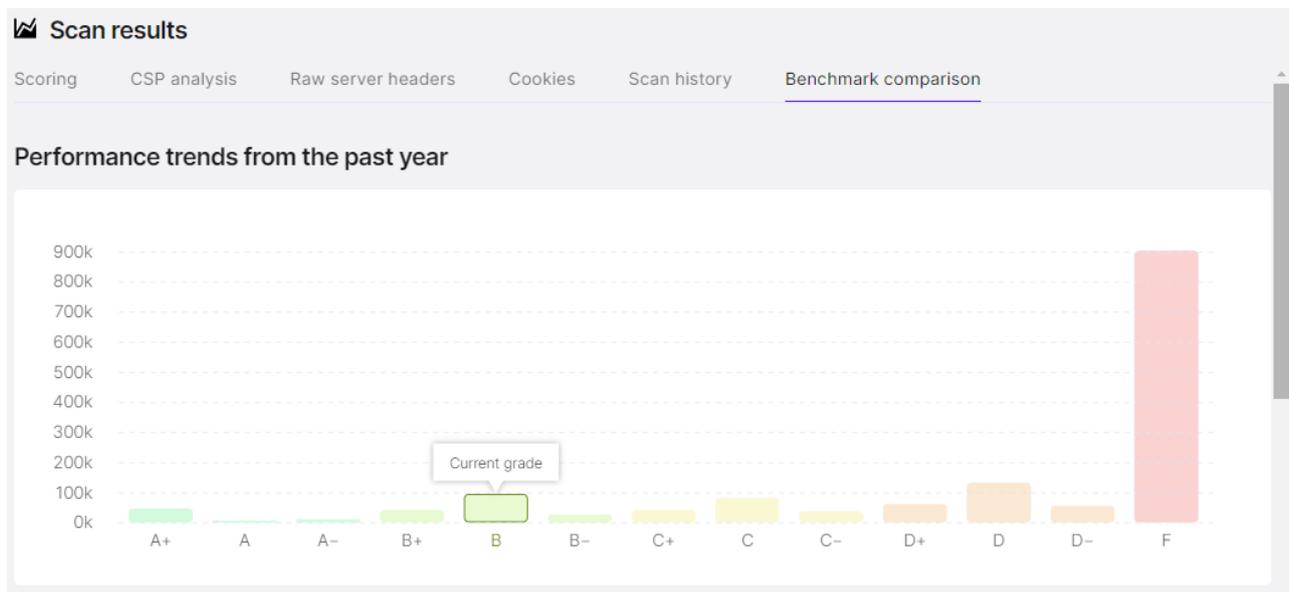


FIGURE 1.5. – Comparaison

Conclusion

Voilà, cette présentation concernant [HTTP Observatory](#) est terminée.



Comme mentionné dans la [foire aux questions](#), l'obtention de la note maximale n'est pas un gage de sécurité absolue, car il y a des choses que cet outil ne peut pas tester comme les [failles XSS](#).

L'icône provient d'[icon8](#).