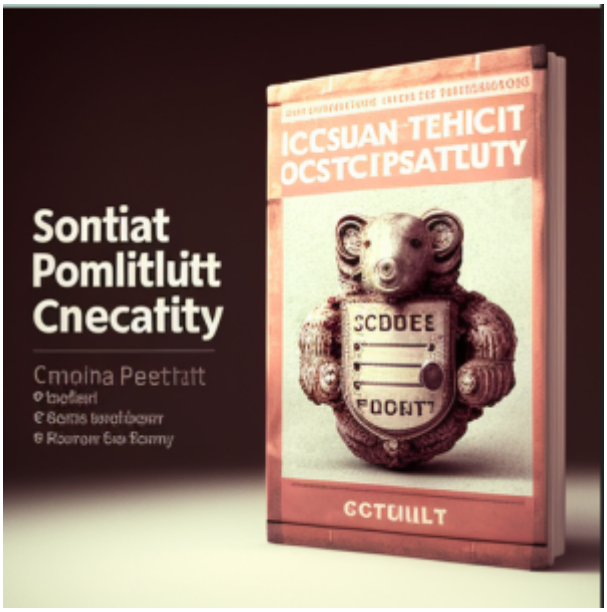
En-têtes HTTP : CSP ou comment sécuriser le contenu d'un site web

programmation



Les CSP (Content Security Policy) sont des en-têtes HTTP qui permettent de définir les règles de sécurité pour le contenu d'un site Web. Elles sont utilisées pour aider à protéger le site et ses utilisateurs contre diverses attaques de sécurité, telles que l'injection de code malveillant ou la fuite de données sensibles.

Pour activer CSP, vous devez configurer vos serveurs web afin d'ajouter un en-tête (header) aux réponses. Dans une configuration Apache, en fichier .htaccess ou dans une balise “Location”, par exemple :

```
Header always set Content-Security-Policy "default-src 'self'; scriptimg-src 'self' https://*; child-src 'none';"
```

Une autre possibilité consiste à utiliser l'élément HTML <meta> pour configurer la règle.

```
<meta http-equiv="Content-Security-Policy" content="default-src 'self'; img-src https://*; child-src 'none';">
```

Il existe de nombreuses directives que vous pouvez utiliser pour définir des règles de sécurité précises afin de :

- Empêcher les écoutes du trafic
- Réduire des attaques cross site scripting (XSS)

Voici comment utiliser les CSP dans un site Web.

Définissez les règles de sécurité que vous souhaitez appliquer à votre site. Par exemple, vous pouvez spécifier quelles sources de contenu (scripts, images, etc.) sont autorisées à être chargées sur votre site. Voir la page du W3C desdirectives pour contrôler les ressources que l'agent utilisateur est

autorisé à charger pour une page donnée.

Ajoutez l'en-tête HTTP `Content-Security-Policy` à votre site. Vous pouvez le faire soit en modifiant le fichier `.htaccess` de votre serveur, soit en ajoutant l'en-tête directement dans le code HTML de votre site.

```
Content-Security-Policy: règle
```

Définissez la valeur de l'en-tête Content-Security-Policy en spécifiant les règles de sécurité que vous avez définies. Par exemple :

```
Content-Security-Policy: default-src 'self'; script-src 'self'
https://example.com; img-src 'self' https://example.com;
```

Cet exemple autorise le chargement de contenu uniquement à partir de la même origine que le site ('self') pour le contenu par défaut (`default-src`) et les scripts (`script-src`), tandis que les images (`img-src`) peuvent être chargées à partir de l'origine du site ou de l'URL `https://example.com`.

Versions, crédits et ressources

- W3C : Content Security Policy Level 3
- Mozilla : Content Security Policy

— *Cédric ABONNEL dit Cédrix - Publié le Mercredi 11 Janvier 2023 à 07h41*

Crédit image : *Midjourney*