Engineer Logiciels

Application durcie avec une CSP à nonces

Durci l'application avec une CSP fondée sur des nonces, HSTS, des cookies SameSite, des rôles de base de données au moindre privilège et une nouvelle vérification des droits côté serveur.

2025

des défenses qui tiennent face à un navigateur hostile

Situation. La plateforme conserve des données professionnelles et organisationnelles que les personnes s'attendent à voir traitées correctement. Une seule ligne de défense ne pouvait donc pas suffire. L'hypothèse de travail doit être celle d'un client hostile : toute restriction du navigateur peut être désactivée par la personne qui le contrôle, et la sécurité doit tenir malgré cela.

Tâche. Il fallait durcir chaque couche — frontend, API et base de données — pour que le serveur impose la sécurité indépendamment de ce que l'interface pouvait autoriser.

Action. Sur le frontend, le middleware proxy de Next.js, proxy.ts, définit une Content-Security-Policy avec un nonce par requête et strict-dynamic, ainsi que HSTS et des cookies SameSite, pour limiter ce que le navigateur exécute et envoie. L'API applique une limitation de débit, CORS, des limites de taille, la validation des entrées avant tout accès à la base et la journalisation des événements de sécurité. Dans la base, l'API utilise un rôle au moindre privilège disposant uniquement du droit EXECUTE sur les fonctions applicatives ; celles-ci s'exécutent en SECURITY DEFINER et tout est paramétré. Les droits — niveau d'offre, rôle, organisation et périmètre du navire — sont revérifiés côté serveur à chaque requête. Les barrières du frontend servent uniquement l'expérience utilisateur : elles décident de ce qui est affiché, tandis que le serveur décide des actions autorisées.

Résultat. La sécurité ne dépend pas du bon comportement de l'interface. Les protections sont organisées en couches pour éviter de dépendre d'un seul contrôle. L'autorisation côté serveur est conçue pour fonctionner

indépendamment des vérifications côté client ; l'interface ne fait donc pas autorité pour les décisions d'accès.

Mettez cette expérience au service de votre projet

Prenez « Application durcie avec une CSP à nonces » comme point de départ pour un défi similaire dans votre organisation. Les prestations mobilisées pour cette réalisation sont disponibles pour votre projet. La partie invisible pour les utilisateurs : où résident les données, quelles règles s'appliquent et comment les autres systèmes peuvent y accéder.

Découvrir nos prestations Contactez-nous →

Examinez ce qui a conduit au résultat

Découvrez la situation, les décisions et le résultat de cet exemple. Nous pouvons discuter des éléments transposables à vos contraintes et de ceux qui nécessitent une autre démarche. Application durcie avec une CSP à nonces — des défenses qui tiennent face à un navigateur hostile

Découvrir nos prestations Contactez-nous →

Votre application est-elle réellement sécurisée ?

Discutez de votre projet avec l'ingénieure responsable de sa réalisation. Nous convenons par écrit du périmètre, de la base tarifaire et de la transmission avant le début des travaux.

Rôle exercé dans ce contexte : Ingénieure sécurité. Cette réalisation fait appel à Architecture de plateformes, Ingénierie backend, Ingénierie frontend, API et intégration, Bases de données et Sécurité. Et puisque vous êtes ici, nous sommes aussi plutôt doués en Développement backend et API et Sécurité et gestion des accès.

Contactez-nous Découvrir nos prestations

Un élément **d'un parcours plus long** — entièrement présenté sur ce site.

Chaque entrée suit la même structure : la situation, la tâche, ce que nous avons fait et ce qui a changé.

Voir l'ensemble du parcours

Définissez l'amélioration nécessaire

Présentez le processus de travail, les interfaces existantes et les utilisateurs qui ont besoin du changement. Nous pouvons définir une livraison testable et une transmission permettant à votre équipe d'assurer la maintenance des éléments livrés.

Consulter les tarifs Contactez-nous →

Votre application est-elle réellement sécurisée ?

Interrogez-nous sur les décisions qui sous-tendent « Application durcie avec une CSP à nonces ». Vous parlerez aux personnes capables d'expliquer le travail et d'évaluer votre propre projet.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://software.engineer.company/fr/portfolio/hardened-the-application-with-nonce-based-csp/