Engineer

Anwendung mit Nonce-basierter CSP gehärtet

Die Anwendung mit Nonce-basierter CSP, HSTS, SameSite-Cookies, Datenbankrollen mit minimalen Berechtigungen und erneuten serverseitigen Zugangsprüfungen gehärtet.

2025

Schutz, der auch einem feindlichen Browser standhält

Situation. Die Plattform verwaltet berufliche und organisationsbezogene Daten, deren sorgfältige Behandlung Menschen erwarten. Eine einzige Schutzlinie reichte deshalb nie aus. Die Arbeitsannahme muss ein feindlicher Client sein: Alles, was der Browser erzwingt, kann dessen Nutzer ausschalten. Die Sicherheit muss trotzdem bestehen.

Aufgabe. Frontend, API und Datenbank sollten gehärtet werden. Der Server musste Sicherheit unabhängig davon erzwingen, was die Oberfläche erlaubte.

Massnahmen. Im Frontend setzt die Next.js-Proxy-Middleware proxy.ts eine Content-Security-Policy mit anfragespezifischer Nonce und strict-dynamic sowie HSTS und SameSite-Cookies. Das begrenzt, was der Browser ausführt und sendet. Die API hat Ratenbegrenzung, CORS, Größenlimits für Anfragen, Eingabevalidierung vor jedem Datenbankkontakt und Protokollierung sicherheitsrelevanter Ereignisse. In der Datenbank verwendet die API eine minimal berechtigte Rolle mit ausschließlich EXECUTE auf Anwendungsfunktionen. Diese laufen als SECURITY DEFINER; alle Abfragen sind parametrisiert. Zugangsrechte nach Tarif, Rolle, Organisation und Schiff werden bei jeder Anfrage serverseitig erneut geprüft. Frontendschranken dienen allein der Nutzerführung: Sie bestimmen die Anzeige, der Server die erlaubten Handlungen.

Ergebnis. Sicherheit hängt nicht vom korrekten Verhalten der Oberfläche ab. Die Schutzmaßnahmen sind mehrschichtig angelegt, um nicht von einer einzigen Kontrolle abzuhängen. Die serverseitige Autorisierung ist so konzipiert, dass sie unabhängig von clientseitigen Prüfungen arbeitet. Die Oberfläche ist damit nicht die maßgebliche Instanz für Zugriffsentscheidungen.

Diese Erfahrung für Ihr Projekt nutzen

Nutzen Sie „Anwendung mit Nonce-basierter CSP gehärtet“ als Ausgangspunkt für eine ähnliche Herausforderung in Ihrer Organisation. Die Leistungen hinter dieser Arbeit stehen auch für Ihr Projekt zur Verfügung. Der Teil, den Nutzer nie sehen: wo die Daten liegen, welche Regeln gelten und wie andere Systeme darauf zugreifen dürfen.

Unsere Leistungen entdecken Kontakt aufnehmen →

Hinter das Ergebnis schauen

Lesen Sie die Situation, die Entscheidungen und das Ergebnis dieses Beispiels. Wir können besprechen, welche Teile sich auf Ihre Rahmenbedingungen übertragen lassen und welche einen anderen Ansatz erfordern. Anwendung mit Nonce-basierter CSP gehärtet — Schutz, der auch einem feindlichen Browser standhält

Unsere Leistungen entdecken Kontakt aufnehmen →

Ist Ihre Anwendung tatsächlich sicher?

Besprechen Sie Ihr Projekt mit der Ingenieurin, die für die Umsetzung verantwortlich ist. Wir vereinbaren Umfang, Preisgrundlage und Übergabe schriftlich, bevor die Arbeit beginnt.

Rollenkontext: Sicherheitsingenieurin. Die Arbeit baut auf Plattformarchitektur, Backend-Entwicklung, Frontend-Entwicklung, APIs und Integration, Datenbanken und Sicherheit. Und wenn Sie schon hier sind: Wir sind auch ziemlich gut in Backend- und API-Entwicklung und Sicherheits- und Zugriffsverwaltung.

Kontakt aufnehmen Unsere Leistungen entdecken

Ein Teil einer **längeren Arbeitsbilanz** — vollständig auf dieser Website zu finden.

Jeder Eintrag folgt demselben Aufbau: die Situation, die Aufgabe, unser Vorgehen und die Veränderungen.

Alle Arbeiten ansehen

Die benötigte Verbesserung definieren

Beschreiben Sie den Arbeitsablauf, die vorhandenen Schnittstellen und die Nutzer, die die Veränderung benötigen. Wir können eine prüfbare Lieferung definieren und die Übergabe so gestalten, dass Ihr Team die gelieferten Bestandteile warten kann.

Preise ansehen Kontakt aufnehmen →

Ist Ihre Anwendung tatsächlich sicher?

Fragen Sie nach den Entscheidungen hinter „Anwendung mit Nonce-basierter CSP gehärtet“. Sie sprechen mit den Menschen, die die Arbeit erklären und Ihr eigenes Projekt einschätzen können.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

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

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://engineer.company/de/portfolio/hardened-the-application-with-nonce-based-csp/