Engineer Software

Aplicación reforzada con CSP basada en nonces

Reforcé la aplicación con CSP basada en nonces, HSTS, cookies SameSite, roles de base de datos de mínimo privilegio y nuevas comprobaciones de derechos de acceso en el servidor.

2025

defensas que se mantienen ante un navegador hostil

Situación. La plataforma almacena datos profesionales y de organizaciones, de los que las personas esperan un tratamiento adecuado, por lo que una sola línea de defensa nunca iba a bastar. El supuesto de trabajo debe ser que el cliente es hostil — que quien controla el navegador puede desactivar cualquier cosa que este imponga — y la seguridad debe resistir de todos modos.

Tarea. Había que reforzar la plataforma en cada capa — frontend, API y base de datos — para que el servidor impusiera la seguridad con independencia de lo que permitiera la interfaz.

Acción. En el frontend, el middleware proxy de Next.js — proxy.ts — establece una Content-Security-Policy con un nonce por solicitud y strict-dynamic, además de HSTS y cookies SameSite, restringiendo lo que el navegador puede ejecutar y enviar. En la API hay limitación de frecuencia, CORS, límites de tamaño de solicitud, validación de entradas antes de que nada llegue a la base de datos y registro de los eventos relevantes para la seguridad. En la base de datos, la API inicia sesión con un rol de privilegios mínimos que solo puede ejecutar EXECUTE sobre las funciones de la aplicación, las funciones se ejecutan con SECURITY DEFINER y todo está parametrizado. Y los derechos de acceso — nivel, rol, organización y alcance por barco — se vuelven a comprobar en el servidor en cada solicitud, tratando las restricciones del frontend únicamente como UX. Esas restricciones deciden lo que se ve; el servidor decide lo que se puede hacer.

Resultado. La seguridad no depende de que la interfaz se comporte correctamente. Las protecciones se disponen en capas para evitar depender de un único control. La autorización del servidor está diseñada para funcionar con independencia de las comprobaciones del cliente, de modo que la interfaz no es la autoridad que decide el acceso.

Aplique esta experiencia a su proyecto

Utilice «Aplicación reforzada con CSP basada en nonces» como punto de partida para un reto similar en su organización. Los servicios que respaldan este trabajo están disponibles para su proyecto. La parte que el usuario no ve: dónde se guardan los datos, qué reglas se aplican y cómo pueden comunicarse otros sistemas con ella.

Explore nuestros servicios Póngase en contacto →

Mire más allá del resultado

Lea la situación, las decisiones y el resultado de este ejemplo. Podemos hablar de qué partes se adaptan a sus restricciones y cuáles necesitan otro enfoque. Aplicación reforzada con CSP basada en nonces — defensas que se mantienen ante un navegador hostil

Explore nuestros servicios Póngase en contacto →

¿Es realmente segura su aplicación?

Converse sobre su proyecto con la ingeniera responsable de la entrega. Acordamos por escrito el alcance, la base del precio y el traspaso antes de empezar a trabajar.

Contexto de la función: Ingeniera de seguridad. Se apoya en Arquitectura de plataformas, Ingeniería de backend, Ingeniería de frontend, API e integración, Bases de datos y Seguridad. Y ya que está aquí, también se nos da bien Desarrollo de backend y API y Seguridad y gestión de accesos.

Póngase en contacto Explore nuestros servicios

Una parte de **una trayectoria más amplia** — y toda ella está en este sitio.

Cada entrada sigue la misma estructura: la situación, la tarea, lo que hicimos y lo que cambió.

Vea la trayectoria completa

Defina la mejora que necesita

Describa el flujo de trabajo, las interfaces existentes y los usuarios que necesitan el cambio. Podemos definir una entrega comprobable y un traspaso que permita a su equipo mantener lo entregado.

Vea cuánto cuesta Póngase en contacto →

¿Es realmente segura su aplicación?

Pregunte por las decisiones detrás de «Aplicación reforzada con CSP basada en nonces». Hablará con las personas que pueden explicar el trabajo y valorar su propio proyecto.

Explore nuestros servicios

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

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

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

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://software.engineer.company/es/portfolio/hardened-the-application-with-nonce-based-csp/