Engineer

Посилила захист застосунку CSP на основі nonce

Посилила захист застосунку за допомогою CSP на основі nonce, HSTS, cookie SameSite, ролей бази даних за принципом найменших привілеїв та серверних повторних перевірок прав доступу.

2025

захист, що встоює навіть у ворожому браузері

Ситуація. Платформа зберігає професійні та організаційні дані — такі, з якими люди чекають належного поводження, тож однієї лінії оборони від початку не могло вистачити. Робоче припущення мусить бути таким: клієнт ворожий — усе, що забезпечує браузер, може вимкнути той, у чиїх руках цей браузер, — а безпека однаково має встояти.

Завдання. Платформу потрібно було захистити на кожному рівні — фронтенд, API, база даних, — так, щоб безпеку забезпечував сервер незалежно від того, що саме дозволяв інтерфейс.

Дія. На фронтенді проміжний шар proxy в Next.js — proxy.ts — встановлює Content-Security-Policy з nonce для кожного запиту та strict-dynamic, а також HSTS і SameSite cookies, тож браузер жорстко обмежено в тому, що він виконає й надішле. На рівні API працюють обмеження частоти запитів, CORS, ліміти на розмір запиту, валідація вхідних даних ще до того, як щось потрапить у базу даних, і журналювання подій, важливих для безпеки. У базі даних API входить під роллю з мінімальними привілеями, яка може лише виконувати (EXECUTE) функції застосунку, самі функції працюють як SECURITY DEFINER, а все параметризовано. А права доступу — тариф, роль, організацію, прив’язку до судна — сервер повторно перевіряє під час кожного запиту, а обмеження на фронтенді вважаються суто питанням UX. Ці обмеження визначають, що видно; сервер визначає, що дозволено робити.

Результат. Безпека не залежить від того, чи поводиться UI як слід. Захист побудовано шарами, щоб не покладатися на один засіб контролю. Серверну авторизацію спроєктовано незалежною від клієнтських перевірок, тож рішення про доступ ухвалює не інтерфейс.

Застосуйте цей досвід у своєму проєкті

Використайте «Посилила захист застосунку CSP на основі nonce» як відправну точку для схожого завдання у вашій організації. Послуги, що стоять за цією роботою, доступні й для вашого проєкту. Та частина, якої користувач не бачить: де зберігаються дані, які діють правила і як інші системи можуть із нею взаємодіяти.

Переглянути наші послуги Зв'язатися з нами →

Дізнайтеся, що привело до результату

Прочитайте про ситуацію, рішення та результат цього прикладу. Ми можемо обговорити, що відповідає вашим умовам, а що потребує іншого підходу. Посилила захист застосунку CSP на основі nonce — захист, що встоює навіть у ворожому браузері

Переглянути наші послуги Зв'язатися з нами →

Ваш застосунок справді захищений?

Обговоріть свій проєкт з інженером, відповідальним за виконання. Обсяг, основу розрахунку вартості та передачу результатів узгоджуємо письмово до початку робіт.

Роль у цій роботі: Інженер з безпеки. Тут задіяні Архітектура платформи, Backend-розробка, Frontend-розробка, API та інтеграції, Бази даних та Безпека. І, до речі, ми добре вмієм Backend- та API-розробка та Безпека та керування доступом.

Зв'язатися з нами Ознайомтеся з нашими послугами

Одна частина **довшого переліку** — і він увесь на цьому сайті.

Кожен запис написано однаково: ситуація, завдання, що ми зробили і що змінилося.

Переглянути весь перелік

Визначте потрібне покращення

Опишіть робочий процес, наявні інтерфейси та користувачів, яким потрібна зміна. Ми можемо визначити перевірюваний результат і спосіб передачі, який дасть вашій команді змогу підтримувати його.

Дивитися, скільки це коштує Зв'язатися з нами →

Ваш застосунок справді захищений?

Запитайте про рішення в роботі «Посилила захист застосунку CSP на основі nonce». Ви говоритимете з людьми, які можуть пояснити роботу й оцінити ваш проєкт.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

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

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/portfolio/hardened-the-application-with-nonce-based-csp/