

Vibecode 101 · ตอน 3/3

ฐานข้อมูล + ล็อกอิน

ให้แอปจำข้อมูลได้จริงด้วย Supabase แบบข้อมูลไม่หลุด
ชุดพร้อมต์ครบ 5 ชั้น + วิธีเทสว่าคนอื่นแอบอ่านไม่ได้



เตรียมของ

- ☐ แอปจากตอน 1 ที่ขึ้นเว็บแล้วจากตอน 2 (GitHub + Vercel) เปิดในแท็บ Code ของ Claude Desktop
- ☐ บัญชี Supabase (ฟรี) ที่ supabase.com — สมัครด้วยปุ่ม "Continue with GitHub"
- ☐ สมุดจด หรือตัวจัดการรหัสผ่าน ไว้เก็บรหัสฐานข้อมูล

3 คำที่ต้องรู้

1 ฐานข้อมูล (Database)

ที่เก็บข้อมูลกลางบนอินเทอร์เน็ต ตอนนี้แอปเก็บไว้ในเบราว์เซอร์ (localStorage) เปลี่ยนเครื่องหรือล้างเบราว์เซอร์ = หาย

2 RLS (Row Level Security)

กฎว่า "แต่ละแถวใครอ่าน/แก้ไขได้" เช่น รายจ่ายแถวนี้ อ่านได้เฉพาะเจ้าของ ถ้าไม่เปิด ใครมีคีย์ในหน้าเว็บก็อ่านได้ทั้งตาราง

พ.ค. 2025 มีแอปที่สร้างด้วย AI (Lovable) 170 แอปที่ข้อมูลผู้ใช้อ่านได้ด้วยคีย์สาธารณะ เพราะไม่ได้เปิด RLS (CVE-2025-48757)

3 คีย์ 2 แบบ

publishable

ขึ้นต้นด้วย `sb_publishable_`

ใส่ในแอปได้ ปลอดภัยเมื่อเปิด RLS ทุกตารางแล้ว

secret

ขึ้นต้นด้วย `sb_secret_`

ห้ามอยู่ในหน้าเว็บ ห้ามขึ้น GitHub คีย์นี้ข้ามสิทธิ์ RLS ได้

ทีละขั้น

1 สร้างโปรเจกต์ (ทำเองในเว็บ)

1. เข้า supabase.com ล็อกอินด้วย GitHub แล้วกด **New project**
2. ตั้งชื่อ เช่น `expense-app` กด Generate รหัสฐานข้อมูล แล้วจดเก็บไว้ เลือก Region ใกล้เคียง เช่น Singapore
3. กด **Create new project** รอสักครู่ แล้วไปที่ปุ่ม **Connect** (หรือ Project Settings → API Keys) ก๊อปปี้ Project URL กับ publishable key

2 ต่อแอป + ย้ายข้อมูล

พร้อมตัว 2

ต่อแอปนี้กับ Supabase
Project URL: (วางตรงนี้)
publishable key: (วางตรงนี้)

- สร้างตาราง expenses เก็บรายการเกี่ยวกับที่แอปใช้ตอนนี้ + คอลัมน์ user_id
- เปิด RLS ตั้งแต่ตอนสร้างตาราง
- ย้ายข้อมูลเดิมจาก localStorage ขึ้นไป
- ห้ามใช้ secret key ในโค้ดฝั่งหน้าเว็บ

อธิบายแผนก่อน แล้วค่อยลงมือ

3 หน้าล็อกอิน

พร้อมตัว 3

เพิ่มหน้าสมัคร / ล็อกอินด้วยอีเมล + รหัสผ่าน ด้วย Supabase Auth

- ยังไม่ล็อกอิน = เห็นแค่หน้าล็อกอิน
- รายจ่ายที่บันทึก ให้ผูก user_id ของคนที่ล็อกอิน
- มีปุ่มออกจากระบบ

แล้วลองสมัคร 2 บัญชีในปริวิว ให้ฉันดูว่าแต่ละบัญชีเห็นแค่ของตัวเอง

4 เปิด RLS + ทեսว่าแอบอ่านไม่ได้ (สำคัญที่สุด)

พร้อมต์ 4

ตรวจทุกตารางใน Supabase ว่าเปิด RLS แล้ว

ตั้ง policy ให้แต่ละแถว อ่าน / เพิ่ม / แก้ / ลบ ได้เฉพาะเจ้าของ (user_id = ผู้ที่ล็อกอิน)
จากนั้นเทสให้ดู 3 แบบ:

- 1) ไม่ล็อกอิน ใช้แค่ publishable key ลองอ่านตาราง → ต้องได้ 0 แถว
 - 2) ล็อกอินบัญชี A ลองอ่านข้อมูลของบัญชี B → ต้องได้ 0 แถว
 - 3) บัญชี A ลองแก้ / ลบ แถวของบัญชี B → ต้องไม่สำเร็จ
- สรุปผลเป็นตาราง ผ่าน / ไม่ผ่าน

- ☐ ทุกตารางขึ้นว่า RLS enabled (ดูใน Table Editor หรือ Advisors → Security)
- ☐ ไม่มี policy แบบ "ทุกคนอ่านได้" (using (true)) บนข้อมูลส่วนตัว
- ☐ เทสทั้ง 3 แบบด้านบน ผ่านหมด

5 เช็กคีย์ แล้วขึ้นเว็บ

พร้อมต์ 5

เช็กทั้งโปรเจกต์ว่าไม่มี secret key หรือรหัสฐานข้อมูลอยู่ในโค้ด

และไม่มีในประวัติ commit ถ้าโปรเจกต์ใช้ .env ให้ออกว่าต้องตั้งค่าตัวไหน

ใน Vercel (Settings → Environment Variables) แล้วค่อย commit + push

ถ้าเคยเผลอ commit secret key ไปแล้ว ให้สร้างคีย์ใหม่ใน Supabase แล้วลบคีย์เก่าทิ้ง ลบไฟล์อย่างเดียวไม่พอ

แพ็คเกจฟรีของ Supabase

- ใช้งานได้พร้อมกัน 2 โปรเจกต์ · ฐานข้อมูล 500 MB ต่อโปรเจกต์ · ผู้ใช้ล็อกอิน 50,000 คน/เดือน
- ไม่มีใครใช้ 1 สัปดาห์ = โปรเจกต์ถูกพัก เข้า dashboard กดเปิดกลับได้
- ระบบส่งอีเมลที่ติดตาม ส่งได้แค่อีเมลของทีมในโปรเจกต์ และราว 2 ฉบับ/ชั่วโมง ถ้าจะให้เพื่อนสมัครด้วยการยืนยันอีเมล ต้องต่อบริการส่งอีเมลเอง (Custom SMTP) หรือแอปส่วนตัวเล็กๆ ปิด Confirm email ได้ที่ Authentication → Sign In / Providers → Email

ติดตามไหน ทำแบบนี้

อาการ	ลองทำ
ข้อมูลไม่ขึ้นเลยหลังเปิด RLS	ปกติ ถ้ายังไม่มี policy จะอ่านไม่ได้เลย บอก Claude: "เปิด RLS แล้วข้อมูลหาย ช่วยเพิ่ม policy ให้เจ้าของอ่านได้"
สมัครแล้วไม่ได้อีเมลยืนยัน	ดูข้อ 3 ของแพ็คเกจฟรีด้านบน
บนเว็บจริงต่อฐานข้อมูลไม่ได้	เช็คว่าตั้ง Environment Variables ใน Vercel แล้ว และ deploy ใหม่หลังตั้งค่า
Error อื่นๆ	ก๊อปปี้ข้อความ error ทั้งหมดไปให้ Claude แล้วบอก "อธิบายก่อนว่าเพราะอะไร แล้วค่อยแก้"

ที่มาของข้อมูลในคลิป

- 170 แอป / 303 endpoint ไม่ได้เปิด RLS: CVE-2025-48757 (Matt Palmer, พ.ค. 2025)
- แพ็คเกจฟรี: supabase.com/pricing · RLS และคีย์: supabase.com/docs/guides/database/postgres/row-level-security · อีเมล: supabase.com/docs/guides/auth/auth-smtp (ต.ค. 2026)
- หน้าจอในคลิปเป็นภาพวาดประกอบ ปุ่มและเมนูจริงอาจต่างเล็กน้อย

ครบซีรีส์ Vibecode 101 แล้ว · เอกสารนี้แจกฟรี แชร์ต่อได้ · ข้อมูล ณ ต.ค. 2026