

Forum:[Hack Forums](#)

Thread: [11% of vibe coded apps are leaking Supabase keys](#)

Hackers - January 17, 2026, 8:42 pm

Quote: We scanned 20,000 indie apps; 1 in 9 leaked their database keys. Here is what that means for builders and users.

Something remarkable happened in 2024-2025: building a full-stack app became easy. Tools like Supabase, combined with AI coding assistants and no-code builders, let solo founders ship production apps in days, not months.

But speed comes at a cost. As we started using SupaExplorer to audit projects, we noticed a pattern: many apps were misconfiguring their Supabase setup. The anon key in client-side code is fine; it's designed to be public. But we found apps exposing the service_role key (which bypasses RLS), or using the anon key with tables that had no RLS policies at all.

We decided to quantify the problem. Over the past month, we collected launch URLs from five major indie product directories and systematically scanned each one.

The stats are abysmal:

20,052 URLs Scanned

2,217 Domains Exposed

11.04% Exposure Rate

2,325 Critical Exposures

Source: <https://supaexplorer.com/cybersecurity-insight-report-january-2026>

I found the article over here:

<https://bbl.wtf/>

I made the software that powers bbl on Lovable and gave to a friend to manage.

I wrote about lovable here, I am worried about it as it is easy to mess up security & they also use Supabase:

<https://hackforums.net/showthread.php?pid=62903609>

Here are some other things I built with it:

<https://hackforums.net/showthread.php?tid=6314202>

<https://hackforums.net/showthread.php?tid=6314197>

<https://hackforums.net/showthread.php?tid=6310065>

This guide is interesting too for lovable:

<https://hackforums.net/showthread.php?tid=6309175>

This is a good article too if you are wanting to export the frontend or hookup a custom backend / do both:

<https://hackernoon.com/openapi-or-bust-how-i-made-lovable-play-nice-with-a-real-backend>

LiNixx - January 18, 2026, 8:10 am

Yeah this is a legit problem.

The anon key is supposed to be public, but the service_role key is not, that one skips all RLS. If that leaks, someone can hit your Supabase REST endpoint and dump or edit the whole DB with a single request. A lot of no-code/AI-generated apps don't set up RLS correctly, so it's even easier to mess up.

If someone is using Lovable or anything similar, you really need to check what it generates, because it'll happily produce something that works on the surface but is basically wide open underneath.

Hackers - March 16, 2026, 8:11 pm

There should be more awareness about this issue, it's still a major problem