Live Empirical Study (2026-11-22) · 55 Newly Shipped Apps · 6,126 Read-Only Checks

State of AI & Vibe-Coded Web App Security (2026)

AI builders like Cursor, Lovable, Bolt, and v0 let solo founders ship production web apps in hours. We ran **VibeShield v7.0** (6-phase passive scanner, ~111 checks per app) across **55 freshly launched public GitHub web apps** to measure what actually ships unprotected on day one.

Scan Your Own App Free (6-Phase Deep Audit) →

Launch Special: Unlock Full Fixes $2 (was $9)

Open-Source Security Checklist (MIT)

74.5%
Missing 8–9 of 10 Security Headers (41/55)

20.0%
Ship Live Supabase Backends (11/55)

3.6%
Leaked Client Secret / API Key (2/55)

6,126
Total Passive Checks Executed (Avg Score 81/100)

Responsible Disclosure & Anonymization Policy: Every scan in this study was strictly passive and read-only (TLS handshake, public HTTP headers, client-delivered JS assets, and non-destructive metadata checks). To protect indie builders, **zero target domains with critical secret leaks or exposed files are named here, and zero raw key material is ever stored or published.**

Audit Your Own Production URL Free (Live VibeShield v7.0 Engine)

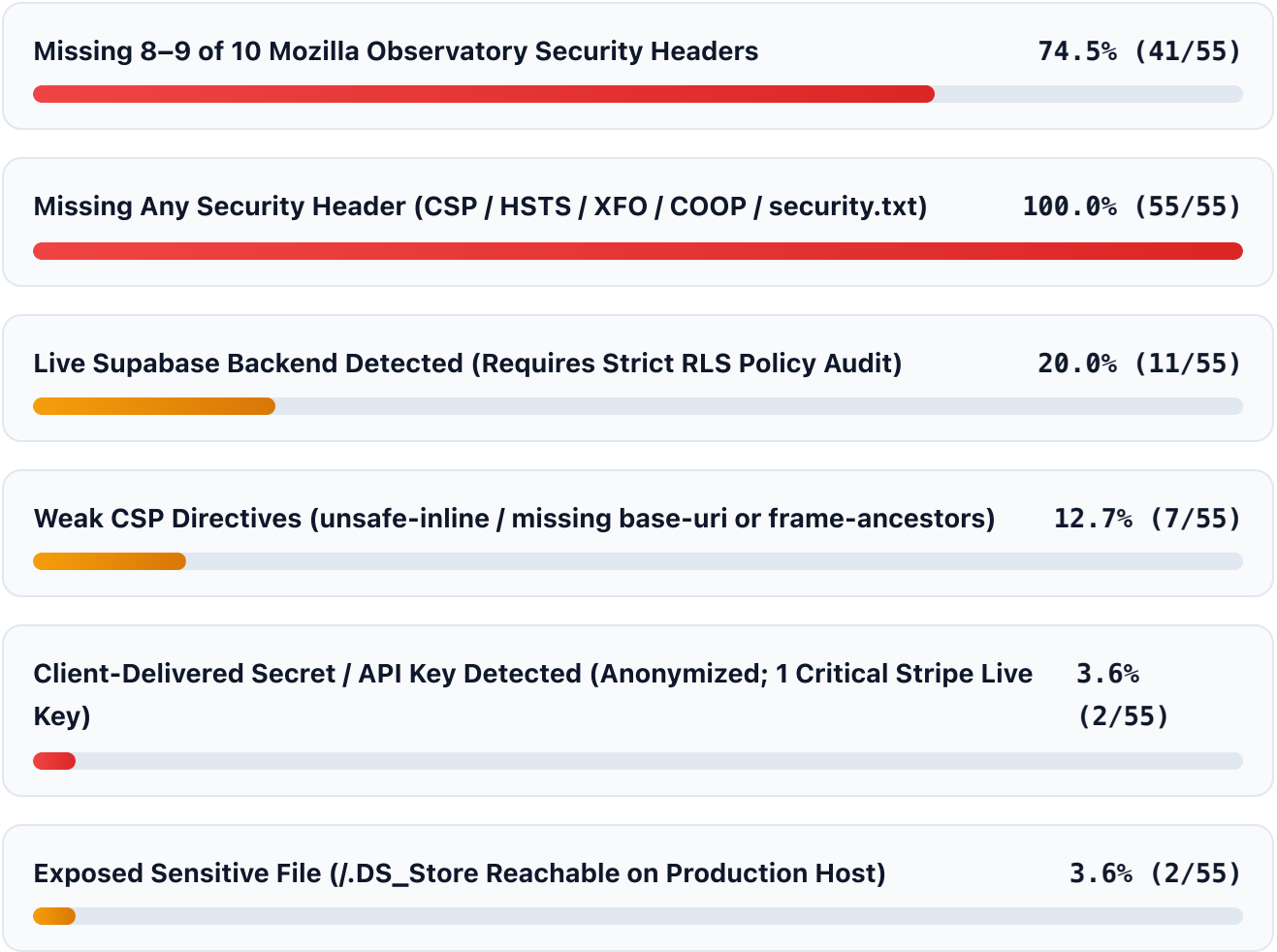
Paste your `.lovable.app`, `.vercel.app`, `.netlify.app`, or custom production domain to run all 6 passive phases (TLS, 24 JS bundles, 52 secret rules, Supabase/Firebase check, 28 probes, 10 Observatory headers):

https://your-app.vercel.app or yourdomain.com

Run 6-Phase Scan Free

Try benchmark demos: `supabase.com` `vercel.com` `linear.app`

1. Most Common Vulnerabilities Found Across 55 Newly Shipped Apps



2. Security Posture by Hosting Platform

HOSTING PLATFORM	APPS AUDITED	AVERAGE VIBESHIELD SCORE	APPS SCORING BELOW 70	PRIMARY GAP OBSERVED
Custom Domain	9	79 / 100	11%	Highest variance — includes exposed /.DS_Store, weak HSTS & client-side API key leaks
Vercel	41	82 / 100	0%	Default deployments ship without CSP, Permissions-Policy, COOP/CORP, or security.txt
GitHub Pages	4	78 / 100	0%	Cannot set custom HTTP security headers without a Cloudflare/edge proxy
Cloudflare Pages	1	98 / 100	0%	Strong edge defaults; verify CSP & backend RLS policies

3. Why AI Code Generators Miss These 4 Controls by Default

1. Zero HTTP Security Headers on Default Deployments

Vercel, Netlify, and Lovable provide automatic HTTPS, which lulls builders into thinking transport and browser security are finished. In our sample, **74.5% of apps** shipped without `Content-Security-Policy`, `X-Frame-Options`, `Permissions-Policy`, or `Cross-Origin-Opener-Policy`, leaving apps exposed to XSS script injection and clickjacking.

2. Client-Side Secret Leaks in Bundled JS

When AI assistants wire Stripe, OpenAI, or Gemini SDKs quickly, they occasionally import server secrets into client components or `NEXT_PUBLIC_` / `VITE_` variables. Even a **3.6% live key leak rate** (including a live Stripe secret key in our 55-app batch) translates to catastrophic billing or data exposure.

3. Unprotected Supabase Tables (Missing RLS)

20.0% of freshly launched apps shipped with Supabase. Creating a table in the SQL editor or via an AI migration prompt without `ENABLE ROW LEVEL SECURITY` and explicit `auth.uid()` policies allows anyone holding the public anon key to query or mutate rows via PostgREST.

4. Forgotten Static Files & Source Maps

Pushing local build directories without strict ignore rules leaves `/.DS_Store`, `.env` backups, or full production `.js.map` source maps reachable on public hosts — handing attackers your entire folder layout and unminified business logic.

4. Copy-Paste 60-Second Hardening Snippets (Free MIT)

A. Baseline Security Headers for `vercel.json` (Fixes 7 of 10 Observatory Checks Immediately)

```
{
  "headers": [
    {
      "source": "/(.*)",
      "headers": [
        { "key": "Strict-Transport-Security", "value": "max-age=63072000; includeSubD
        { "key": "X-Content-Type-Options", "value": "nosniff" },
        { "key": "X-Frame-Options", "value": "DENY" },
        { "key": "Referrer-Policy", "value": "strict-origin-when-cross-origin" },
        { "key": "Permissions-Policy", "value": "camera=(), microphone=(), geolocatio
        { "key": "Cross-Origin-Opener-Policy", "value": "same-origin" },
        { "key": "Content-Security-Policy", "value": "default-src 'self'; base-uri 's
      ]
    }
  ]
}
```

B. Mandatory Supabase Row Level Security Baseline SQL

```
ALTER TABLE public.profiles ENABLE ROW LEVEL SECURITY;

CREATE POLICY "Users read own profile only"
  ON public.profiles FOR SELECT
  USING (auth.uid() = id);

CREATE POLICY "Users update own profile only"
  ON public.profiles FOR UPDATE
  USING (auth.uid() = id)
  WITH CHECK (auth.uid() = id);
```

Launch Special: Fix Every Finding in 5 Minutes — $2 Once (was ~~$9~~)

Run a free 116-check scan on **VibeShield v7.0**, then unlock exact JS chunk locations, line-level evidence, and tailored 5-platform fix scripts (Cursor/Lovable, Next.js/Vercel, Cloudflare, Nginx, Supabase SQL) for **$2 once (78% off Launch Special, was ~~$9~~)** — zero monthly subscription, 14-day refund guarantee.

Run Free 6-Phase Scan →

Unlock VibeShield — $2 (was $9)

Complete 3-App Suite — $5 (was $29)

Stack-Specific Hardening Guides & Live Scanners

Lovable + Supabase

Lovable App Security Checklist

Live scanner + RLS SQL lockdown for .lovable.app and custom domains.

Open Lovable guide →

Cursor + Next.js

Cursor & Next.js Hardening Guide

Drop-in next.config.mjs headers(), .cursor/rules & source-map lockdown.

Open Cursor guide →

Bolt.new + Netlify

PostgreSQL RLS

Bolt.new & Netlify Security Audit

Fix VITE_ secret leaks & deploy public/_headers cleanly.

Open Bolt guide →

Supabase RLS Audit & SQL Guide

Two-query audit catching every public table missing Row Level Security.

Open Supabase guide →

Complete Your Pre-Launch Checklist (Zero-Install Free Web Tools)

100% Free Domain + USPTO

Moving Off `.vercel.app` or `.lovable.app`?

Check 78+ domain extensions via direct IANA RDAP, live USPTO Class 009/042 trademarks, and aftermarket availability on **BrandShield v6.2**.

Check Your Launch Domain →

Email Deliverability ($2 Launch Special)

Signup Emails Landing in Spam?

Verify SPF <=10 lookup limits, 24 DKIM selectors, DMARC policy, and 5 DNSBL blacklists in 2 seconds on **InboxShield v7.0**.

Audit Email DNS Free →

AI Search GEO ($2 Launch Special)

Invisible to ChatGPT & Perplexity?

Check 10 global & China AI crawlers, score Schema.org Entity Graph depth, and generate `/llms.txt` on **CiteReady v6.0**.

Check AI Visibility Free →

228 SaaS Benchmarks 4 Honest Comparisons Support 14-Day Refund agentarenastudio@proton.me

@agentarenastudi