

SECURITY AUDIT YOUR APP

Cloudflare's open-source AI skill maps your app, sends agents to hunt for bugs, and double-checks every finding before it reports it.

The problem

Vibe-coded apps ship fast, and logins, databases and APIs often have holes nobody checked.

The skill

Maps the app, hunts for bugs, then a second agent tries to disprove each one.

Note: the repo name, stars and issue counts in the video come from the original creator's reel. Open the repo yourself, confirm it is Cloudflare's official one, and check its README before installing.

The 5 steps

- 1 Find the repo.** Search GitHub for Cloudflare's security audit skill and confirm the owner is Cloudflare.
- 2 Install it in Claude Code.** Give Claude the GitHub link and ask it to install the skill and read the README.

Install this skill: `[paste the GitHub link]`. Then tell me how to run an audit on this project.

- 3 It maps your app.** Pages, logins, database and API routes.
- 4 Agents hunt for bugs.** They check logins, database access, APIs and prompt injection if your app uses AI.
- 5 Every bug is double-checked.** A separate agent tries to disprove it. Only confirmed issues appear in the report, each with a fix.

Try these prompts

Run the audit: Run the security audit skill on this project and give me the verified report.

Focus: Check only my login, signup and password-reset flows for security problems.

Database: Look for tables or queries that any user could read or change without permission.

AI features: Test every place my app sends user text to an AI model for prompt injection.

Fix: Fix the verified issues one at a time, and show me the change before you apply it.

Safety: run audits only on your own code, review every fix before it ships, and never paste real passwords or API keys into a chat.

DM "hello" for this guide

Follow @oruim.tech for daily AI and tech videos.