1 free scanner · 5 steps

The SkillSpector Scanner.

NVIDIA checked over 42,000 real agent skills. 1 in 20 showed signs of being malicious. Here's their free scanner, and exactly how to point it at your own skills folder.

Fadè Adeniyi

THE PROBLEM

A skill isn't a harmless text file.

It runs with whatever access you've given it, which can include environment variables, API keys and local client folders. Dangerous instructions can hide in text you never see.

NVIDIA studied 42,447 real agent skills from major marketplaces. 26.1% had at least one security vulnerability. 5.2% showed patterns strongly suggestive of malicious intent.

WHO IT'S FOR

Anyone who's installed more than one Claude Code skill without checking what it does.

SCAN

Five steps.

1. **Get SkillSpector:** github.com/NVIDIA/SkillSpector. Free and open source.
2. **Clone and install:** git clone https://github.com/NVIDIA/SkillSpector.git && cd SkillSpector && pip install -e .
3. **Scan one skill:** skillspector scan ~/.claude/skills/some-skill. Or the whole folder: skillspector scan ~/.claude/skills/
4. **Read the risk score,** out of 100.
5. **Optionally wire it in as an MCP** so new skills are scanned before they run.

WHAT IT CHECKS

64 patterns across 16 categories, including credential exfiltration, hidden remote-script execution and cron jobs that outlive the terminal.

WHY TRUST IT

The source matters.

Real, published research	42,447 skills studied. NVIDIA's own findings.
NVIDIA uses it on itself	Nothing goes into their skills catalogue until it passes this scan.
Genuinely free	Open source, Apache 2.0, no cost to run on your own folder.

TRAP AND LIMITS

Clean on the page isn't clean.

The trap: malicious instructions hide in invisible text, comments or encoded scripts so a manual read won't catch them. A clean scan today also doesn't cover a later auto-update, so re-scan periodically.

What it won't do. A score isn't a guarantee. It only means nothing matched the known patterns.

> **DO IT TODAY**
>
> Scan your existing folder before installing anything new.

THE TAKEAWAY

Scan what you've already installed.

Today, not eventually.

One in twenty skills showed signs of malicious intent.

One in twenty skills people install is showing signs of malicious intent. You don't have to guess which ones.

github.com/NVIDIA/SkillSpector, Apache 2.0 licence. Published NVIDIA research: 42,447 skills, 26.1% vulnerable, 5.2% malicious.

Building something of your own? **The Audacity to Build** is my community for people building alongside me, with the systems I actually run. It is opening soon. Join the waitlist at fadeadeniyi.com/waitlist.

STAY IN THE ROOM

This is where the rest of it lives.

You have the guide. Here is the ongoing version.

THE BLUEPRINT · EVERY MONDAY

My weekly newsletter, and the best thing I make. One issue every Monday at noon, written to get you disgustingly good at AI. The tool I am actually using that week, the news that matters with the hype stripped out, and a hot take I would say to your face. Free, and you can leave whenever you like.
fadeadeniyi.com/newsletter

COME AND FIND ME

If this was useful, follow me. I share what I am actually building, the tools that survive my own testing, and the ones I quietly cancel. New plays every week.

INSTAGRAM
@thefadeadeniyi

TIKTOK
@thefadeadeniyi

LINKEDIN
Fadè Adeniyi

YOUTUBE
@fadeadeniyi

NEWSLETTER
fadeadeniyi.com/newsletter

XERUIT PROFILE
Find me on Xeruit

WEBSITE
fadeadeniyi.com

IN PARTNERSHIP WITH XERUIT

The other thing I build. Xeruit is the AI workforce intelligence and hiring platform I co-founded, with an AI recruiter that does the first pass so your team only meets people worth meeting. Hiring, or want to be found by someone who is? **xeruit.com**

Fadè Adeniyi

Fadè & The Machines