

Check if an AI skill is safe before you install it

SkillSpector is a free security scanner from NVIDIA for Claude Code, Codex and MCP skills. From nothing installed to your first scan, in about ten minutes.

WHAT IT IS

A scanner that reads a skill and tells you if it is safe to install

A "skill" is a folder of instructions, and often a few scripts, that you drop into an AI assistant like Claude Code to teach it a new job. Once installed it runs with your permissions, on your machine, and nobody checks it first. SkillSpector reads those files before you install them and gives you a score out of 100 with a plain verdict: safe, caution, or do not install. It never runs the skill.

WHAT IT DOES

Reads the files a skill ships and flags the parts that should worry you

- Scans a folder on your machine, a single SKILL.md file, a GitHub link, or a zip
- Checks 68 known-bad patterns across 17 categories: hidden instructions, API-key harvesting, data sent to outside servers, commands that download and run code, and more
- Looks up every dependency the skill declares against the live OSV.dev vulnerability database
- Gives a 0–100 risk score with the file and line number for each finding
- Prints to your screen, or writes a JSON, Markdown or SARIF report

WHAT IT REPLACES

Reading a stranger's code line by line — or installing on trust

The research behind the tool scanned 42,447 skills from the major marketplaces: 26.1% contained at least one vulnerability and 5.2% showed likely malicious intent. Skills that ship executable scripts were 2.12x more likely to be vulnerable. The alternative to a scan is reading every file yourself, which almost nobody does. SkillSpector is Apache 2.0, free, and runs on your own machine.

BEFORE YOU START

A computer, an internet connection, and the Terminal app

You do not need Python, a developer account, or anything paid. Everything below is typed into Terminal, which is already on your Mac.

- **To open Terminal:** press **⌘ + Space**, type *Terminal*, press Enter. A plain black-and-white window opens with a blinking cursor. This is normal — it is just a place to paste text commands.

On Windows, press the Start button, type *PowerShell*, press Enter, and use the Windows commands noted below.

- **To check if you can skip Step 1:** paste `uv --version` and press Enter. If it prints a version number you already have `uv` — skip to Step 2. If it says "command not found", do Step 1.

STEP 1

Install uv

`uv` is a free, widely used tool from Astral that installs command-line programs and the Python they need in one line, so you never have to set Python up yourself.

1 Paste this into Terminal and press Enter

```
curl -LsSf https://astral.sh/uv/install.sh | sh
```

Windows PowerShell instead: `powershell -ExecutionPolicy Bypass -c "irm https://astral.sh/uv/install.ps1 | iex"`

2 Close Terminal and open it again

Until you do, your computer still does not know the word "`uv`". This trips up almost everyone. If you already use Homebrew, **`brew install uv`** does the same job.

STEP 2

Install SkillSpector

1 Paste this in and press Enter

```
uv tool install git+https://github.com/NVIDIA/skillspector.git
```

The first run takes a few minutes and prints a long wall of text while it downloads Python and the dependencies. That is the install working, not an error.

2 Check it worked

```
skillspector scan --help
```

A short list of options means you are done. Later on, **uv tool update skillspector** gets you the newest version.

STEP 3

Scan a skill

Point it at wherever the skill lives. You do not have to download anything first — a GitHub link is enough.

1 Scan a skill from GitHub

```
skillspector scan https://github.com/someone/their-skill --no-llm
```

Replace the link with the skill you are about to install.

2 Or scan a folder already on your machine

```
skillspector scan ./my-skill/ --no-llm
```

Rather than typing the folder path, type **skillspector scan** then a space, then drag the folder from Finder into the Terminal window — it fills the path in for you. Add **--no-llm** at the end.

3 Read the report that prints out

You get a score, a verdict, a list of the files it looked at, and one entry per issue with the file and line number. That's it.

STEP 4

Read the verdict

The score is the only number that matters. Everything below 21 is fine; above 50, walk away.

SCORE	SEVERITY	WHAT TO DO
0-20	Low	Safe — install it
21-50	Medium	Caution — read the listed findings before deciding
51-80	High	Do not install
81-100	Critical	Do not install

A medium score is common and often harmless — unpinned dependency versions alone will get you there. Read what the findings actually say before writing a skill off.

OPTIONAL

Let Claude Code run the scan for you

If you use Claude Code, you can hand it the scanner and ask it to check a skill before installing, instead of running the command yourself.

1 Reinstall with the add-on it needs

```
uv tool install --force 'skillspector[mcp] @ git+https://github.com/NVIDIA/skillspector.git'
```

2 Register it with Claude Code

```
claude mcp add skillspector -- skillspector mcp
```

Then just ask Claude to scan a skill link before you install it.

GOOD TO KNOW

Keep --no-llm on unless you know why you dropped it. Without it, SkillSpector sends the skill's file contents to an AI provider you have to configure with your own paid API key. With it, the scan is free and stays on your machine — only the dependency names go out, to the public OSV.dev database. The trade-off is precision: the AI pass explains findings in plain language and filters out false alarms.

It is a check, not a shield. SkillSpector never runs the skill, and it does not sandbox anything you install anyway. It reads text, so it can miss instructions hidden in images and is weaker on non-English content. Treat a clean score as one good signal, not a guarantee.