MINA SAAD · GUIDE

اعمل security audit لكودك بسطر واحد

الـ skill اللي Cloudflare بدأت بيها تدور على الثغرات في الكود بتاعها، مجانية.
تسطبها إزاي، تشغلها، تقرا التقرير، وليه تثق فيه.



رسم توضيحي. الثغرات للشرح بس.

مجانية ومفتوحة المصدر، MIT

أكتر من 70K نجمة على GitHub

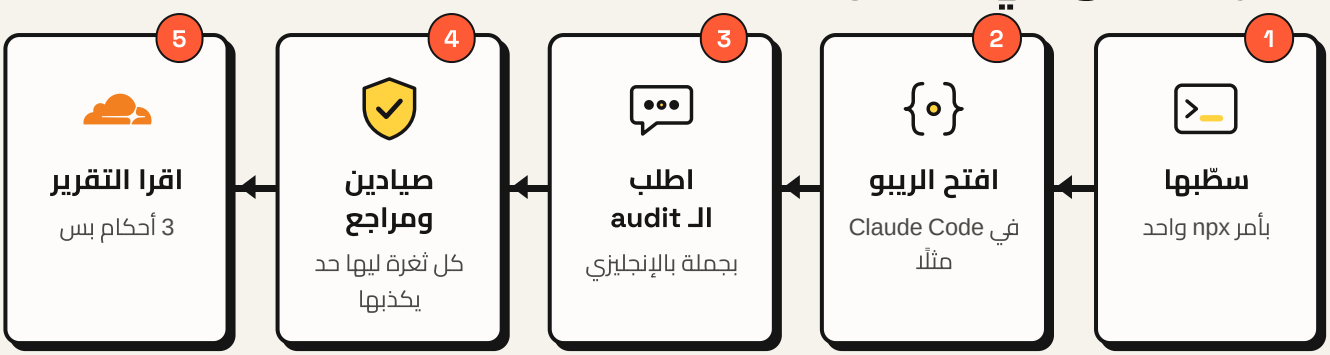
تسطبها بأمر واحد

IN/MINASAAD1 · MINA-SAAD.COM

FOLLOW LinkedIn Instagram TikTok GitHub

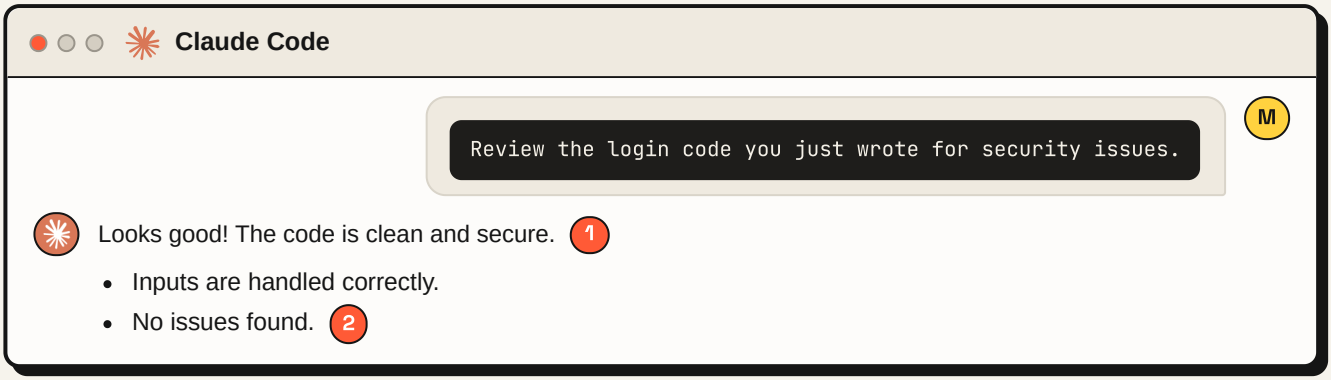
01

الطريقة كلها في 5 خطوات



02

ليه مينفعش الـ AI يراجع كوده بنفسه



1 رد مطمّن، بس من نفس الـ agent اللي كتب الكود. بيصحح ورقته بإيده.

2 محدش حاول يثبت العكس، ولا حد تاني بص على الكود.

مثال للتوضيح.

القاعدة جوه الـ skill: الـ agent اللي بيراجع الثغرة، عمره ما يكون هو اللي لقاها.

03

قبل ما تبدأ، محتاج 3 حاجات

coding agent

بيشغّل sub-agents بالتوازي، زي Claude Code مثلًا.

Node.js

للـ validators اللي بتراجع ملفات النتايج.

sandbox

عشان يشغّل كود الريبو. من غيره، الثغرة اللي محتاجة تشغيل بتفضل `needs_validation` ومبتتأكدش.

04

بيعمل إيه جوه: 6 مراحل

كل مرحلة بـ agents معزولين عن بعض، واللي بيلاقي مش هو اللي بيحكم.

01

الخريطة: الكود بياخد input منين، وفين الحدود اللي محدش يعديها

02

الصيد: صيادين معزولين، كل واحد في جزء، ونقاد يدوروا على اللي متغطاش

03

المراجعة: كل ثغرة محتملة لـ agent جديد، شغلته يثبت إنها غلط

04

الحكم: كل نتيجة بتاخد حكم من 3، في ملف بيتراجع أوتوماتيك

05

مراجعة تانية: agents جديدة تراجع كل ادعاء على الكود نفسه

06

التقرير: بيطلع من النتايج اللي اتراجعت بس

05

سطّبها بأمر واحد

Terminal ~/shop-api

```
$ npx skills add https://github.com/cloudflare/security-audit-skill \
    --skill security-audit  (1)
? Install to which agents: Claude Code  (2)
✓ security-audit installed
$ npx skills add https://github.com/cloudflare/security-audit-skill \
    --skill security-audit --global  (3)
```

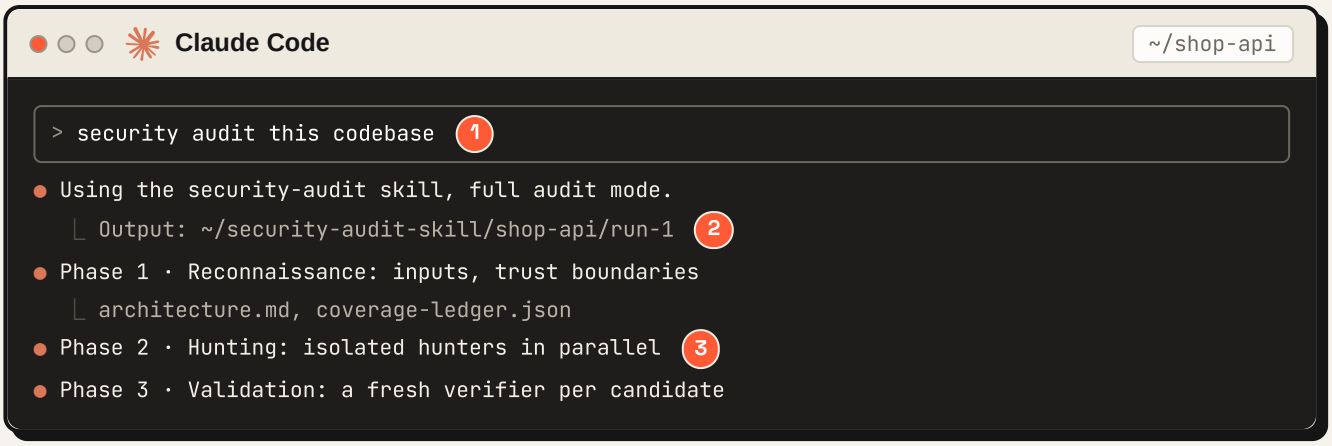
1. الأمر زي ما هو في الـ README بتاع Cloudflare، وبيختار الـ skill دي بالاسم من الريبو.
2. لو سألك تسطبها لأنهي agent، اختار اللي بتشتغل عليه.
3. النسخة دي بتسطبها لكل المشاريع على جهازك، مش للمشروع ده بس.

شاشة للتوضيح، الشكل الفعلي ممكن يختلف.

06

اطلب الـ audit بجملة واحدة

افتح الـ agent جوه الريبو، واكتب جملة من اللي تحت.



1. طلب audit مباشر بيشغّل الست مراحل ويطلع تقارير. سؤال أمان عادي بياخد نصيحة بس.
2. لو محددتش فولدر، النتايج بتتحفظ هنا، برا الريبو بتاعك.
3. كل صياد شغال لوحده في حتة، وفي نفس الوقت.

شاشة للتوضيح، الشكل الفعلي ممكن يختلف.

```
security audit this codebase
find security vulnerabilities in ./src
do a security review, output to ~/audits/my-project
```

07

متعملش كده، واعمل كده

✕ متعملش كده

- تسيبه يشغّل كود الريبو على جهازك وهو مفتوح على النت
- تخلي النتايج جوه الريبو وتعملها commit بالغلط
- تعتبر اللي لسه needs_validation ثغرة مؤكدة

✓ اعمل كده

- شغّله في sandbox: من غير network، وبيكتب في فولدر واحد بس
- سيب النتايج في الفولدر الافتراضي، برا الريبو
- صلّح الـ confirmed الأول، وبعدين اتحقق من الباقي بنفسك

08

اقرا النتيجة: 3 أحكام بس

كل ثغرة محتملة بتطلع بحكم واحد، ومعاه السبب.

REPORT.md `run-1`

CANDIDATES
5

CONFIRMED
2 (1)

NEEDS VALIDATION
1 (2)

REJECTED
2 (3)

Finding	Where	Verdict	Severity
SQL injection	POST /login	confirmed	High
IDOR	GET /orders/:id	confirmed	Medium
Stored XSS	/search	needs_validation	-
Auth bypass	/admin	rejected	-
Open redirect	/logout	rejected	-

Also in this folder: FINDINGS-DETAIL.md, NEEDS-VALIDATION.md, findings.json

1. confirmed: ليها تتبع كامل في الكود، ونتيجة اتشافت فعلًا. دي تصلحها الأول.
2. needs_validation: فاضل فيها معلومة واحدة محددة، وملهاش severity لسه. راجعها بنفسك.
3. rejected: اللي راجعها أثبت إنها مش ثغرة، فمتضيعش وقتك عليها.

مثال للتوضيح، بيانات وهمية.

الـ severity عندهم احتمال الهجوم في حجم الضرر، مش مجرد مخالفة لـ checklist معينة.

09

شغّلها أكتر من مرة

الـ runs بتكمّل على بعض، مش بتبدأ من الصفر.

~½

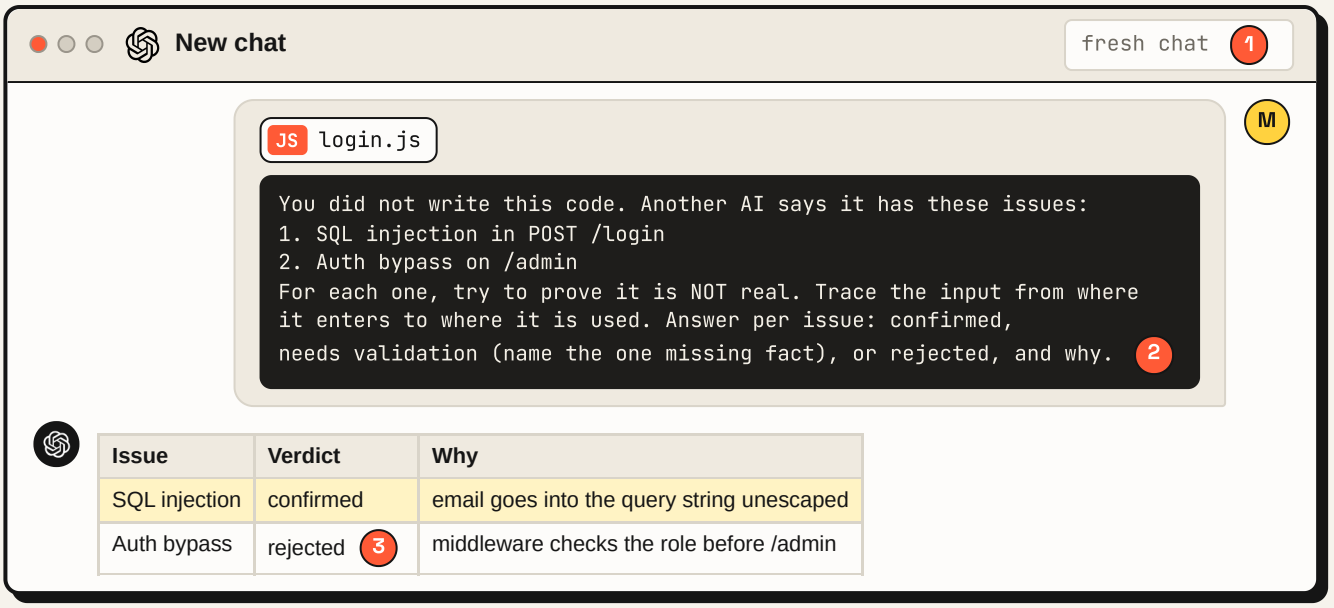
اللي لقاه run واحد، من كل اللي لقوه الـ runs كلها مع بعض، في تجارب Cloudflare

run-2

بيقرا الخريطة والنتايج اللي قبله، يدور في اللي متغطاش، ويراجع الكود اللي اتغير

لو في طبقة حماية بتمنع الهجوم، غياب طبقة تانية مش ثغرة. الـ skill بتكتبها ملاحظة تحسين.

مش بتستخدم coding agent؟ طبّق القاعدة بإيدك



1 شات جديد، مش اللي كتب الكود أو لقى الثغرات.

2 اطلب منه يكذّب كل ثغرة، مش يأكدها.

3 اللي اتنفى يطلع من القايمة، وتركز في الباقي.

ده مش الـ skill، بس نفس فكرتها بإيدك. مثال للتوضيح، بيانات وهمية.

عايز أكتر من كده؟

كل أسبوع بشرح أداة أو فكرة في الـ AI والـ automation بالعربي.

TikTok
@minasaadwahba

Instagram
@minasaad.ai

LinkedIn
in/minasaad1

X
@MinaSaad__

GitHub
MinaSaad1

Website
mina-saad.com

المصادر

1. security-audit-skill README (2026-11-11) https://github.com/cloudflare/security-audit-skill
2. Cloudflare Blog (2026-06-18) https://blog.cloudflare.com/build-your-own-vulnerability-harness
3. skills CLI README https://github.com/vercel-labs/skills