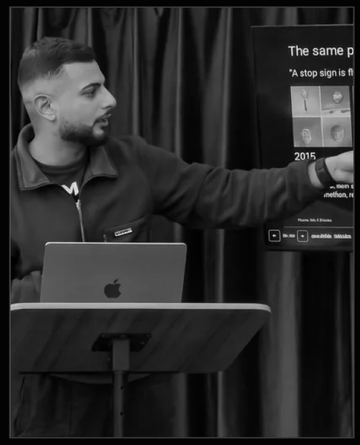


Furquan Ahmad

Validation and security · furquan101.com

HEY, I'M *FURQUAN*

- Lead Product Designer at Scale AI, previously at Meta. Based in London.
- I build my own products with AI: TrainTimesUK, Sahara Studio, AutoScout and more.



Hulm Club, London



AI Tinkerers, Doha


Muslim Tech Fest, London



Hulm Club, London


Crescent Creatives


Crescent Creatives

CHAPTER 01

THE BAR MOVED

01

Anyone can ship now. Speed and craft are both expected.



Photo: Felix yu, Unsplash

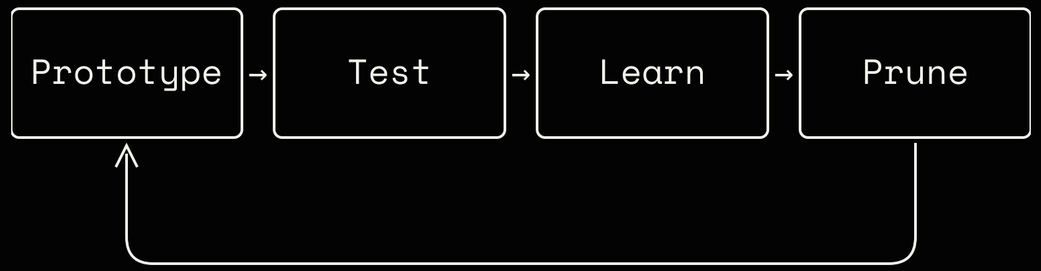
THE DESIGN PROCESS *IS DEAD*

- We lead with prototypes now, not mocks and docs.
- Hold many ideas loosely. Stay anchored on the problem, and prune toward what works.

THE OLD WAY · ONE STRAIGHT LINE



THE NEW WAY · A LOOP



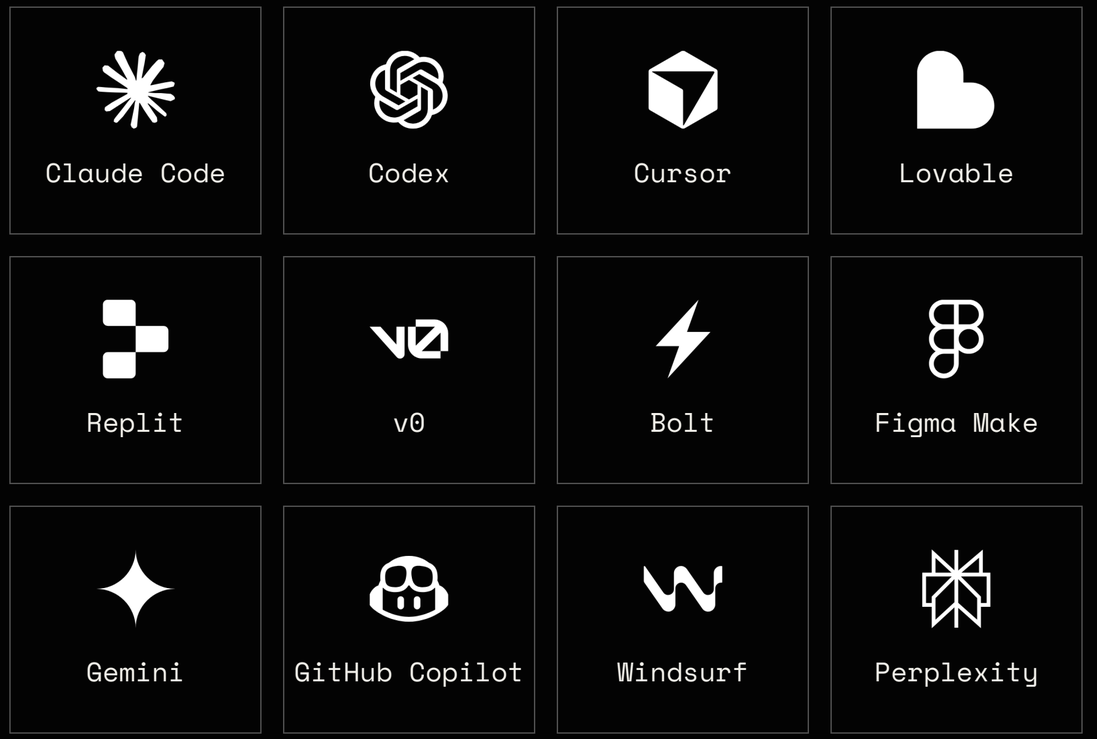
repeat until the prototype earns its place

Source: Jenny Wen (Anthropic), Julie Zhuo

THE TOOLS

EVERYONE HAS *THE SAME TOOLS*

- Anyone can ship now. PMs are vibe coding their own ideas, and engineers prototype the UI themselves.
- Most of these are free or cheap. The tools aren't the advantage any more.



2026

OUTPUT *EXPLODED*

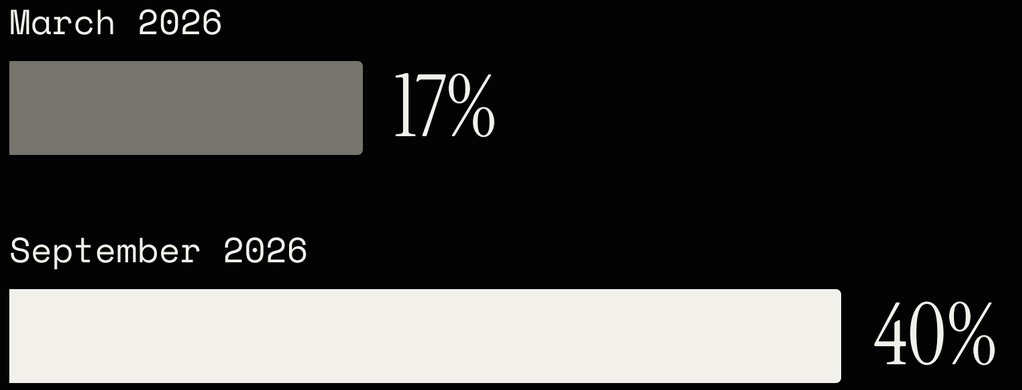
200%+

more code changes saved than two years ago (34.3 billion)

200%+

more changes approved and added to products (1.3 billion)

CODE CHANGES STARTED BY AN AI AGENT



Source: GitHub Octoverse 2026, Oct 2025 to Sep 2026

BUT

80% OF FEATURES *ARE RARELY OR NEVER USED*

More output doesn't mean more value. Now we can build the unused 80% faster than ever.



20%
frequently or sometimes

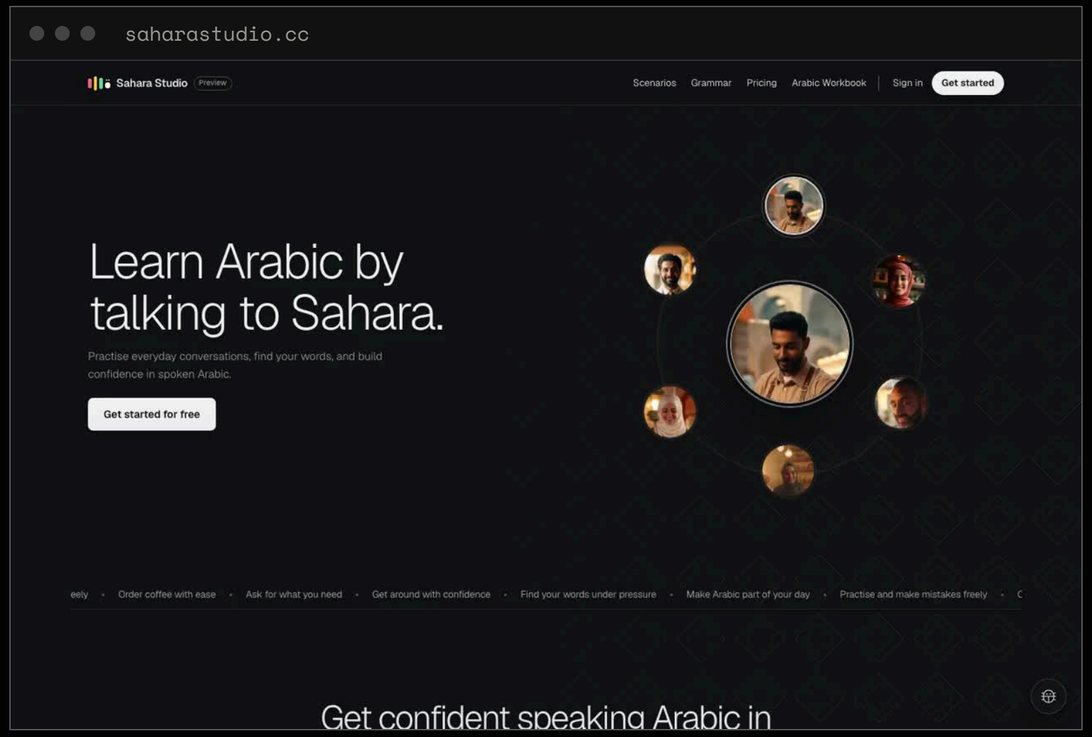
80%
rarely or never

Source: Pendo Feature Adoption Report, 615 products, 2019

EASIER THAN EVER

IT'S NEVER BEEN *EASIER TO BUILD*

- Sahara Studio: an AI voice tutor I built to practise Arabic in real scenarios.
- Voice models and Google sign-in, built on my own with AI.



THE PRESSURE

SPEED *AND* CRAFT

The scope of a designer's job keeps growing, and both are expected at once.

PRESSURE 01

SPEED

Prototype it, ship it, document it. This sprint.

PRESSURE 02

CRAFT

When everyone can ship, quality is what people notice.

THE HARD PART

KNOWING WHAT TO BUILD *IS THE HARD PART*

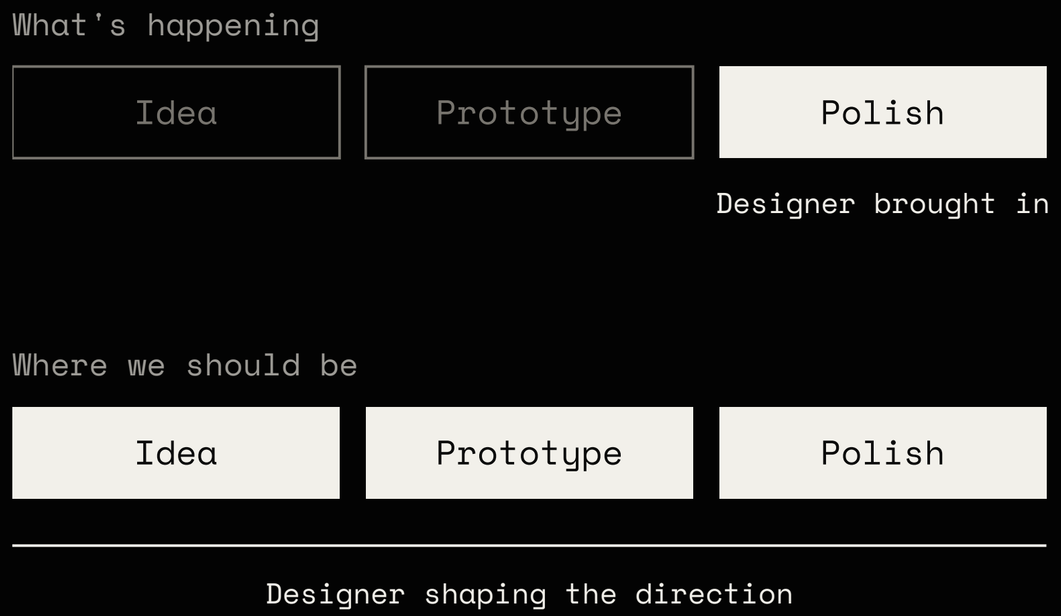
- Step up your product thinking and critical thinking.
- Don't wait to be told what to build. Help decide it.

“Anyone can build and ship. So much code today is wasted.”

THE POLISH TRAP

WE'RE NOT JUST HERE *TO MAKE IT PRETTY*

- Designers are being brought in at the end, to polish someone else's prototype.
- Advocate for a seat earlier, and grow your product sense.



CHAPTER 02

BUILD WITH INTENTION

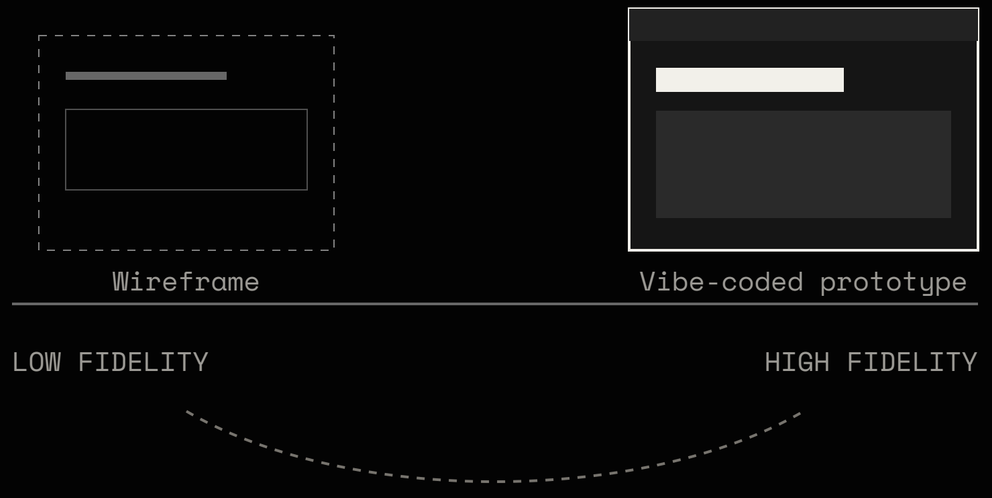
02

When generation is cheap, judgement is what's left.

RAPID PROTOTYPING

HIGHER FIDELITY, *SAME WILLINGNESS TO BIN IT*

- Faster high fidelity doesn't mean we should latch on to it.
- Treat a vibe-coded prototype like a wireframe: easy to throw away.



PROTOTYPING TIPS

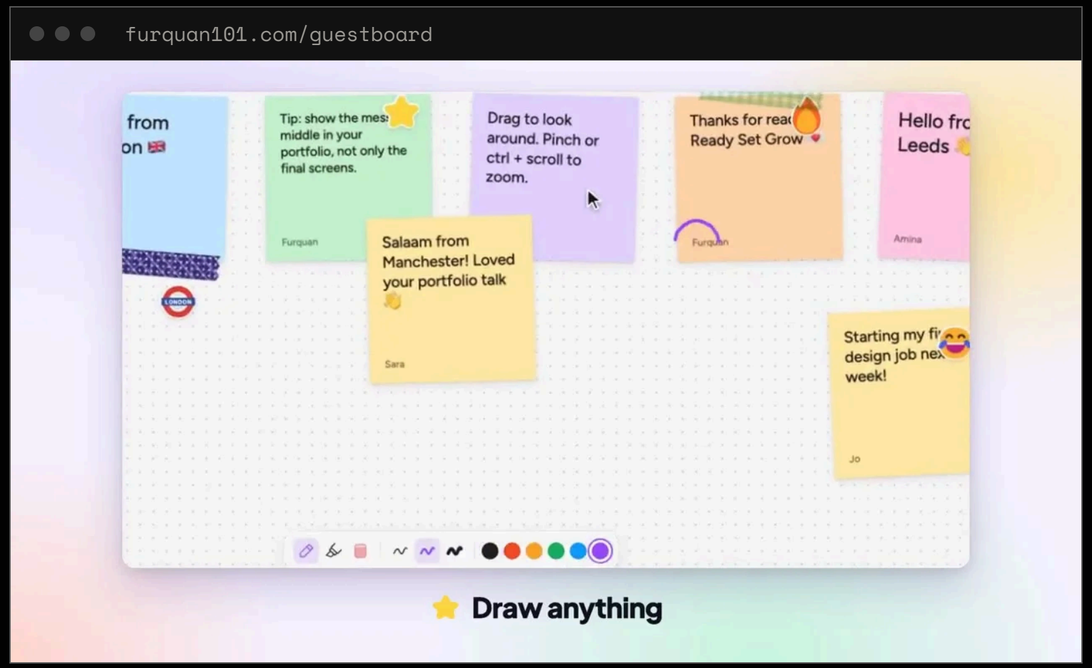
START FROM *INSPIRATION*

01 **References.** Use tools like Mobbin, and connect MCPs for context.

02 **Meeting notes.** They're a goldmine.

03 **Design system.** Base it on the apps you're inspired by.

04 **Inspiration.** Tell it what to start from.



NO DESIGN SYSTEM. JUST FIGJAM AS THE REFERENCE, PLUS CONTEXT.

RESEARCH

TELL PEOPLE *IT'S A PROTOTYPE*

- High fidelity makes participants polite. Polite feedback doesn't help.
- Change their mentality, and check your own bias too.

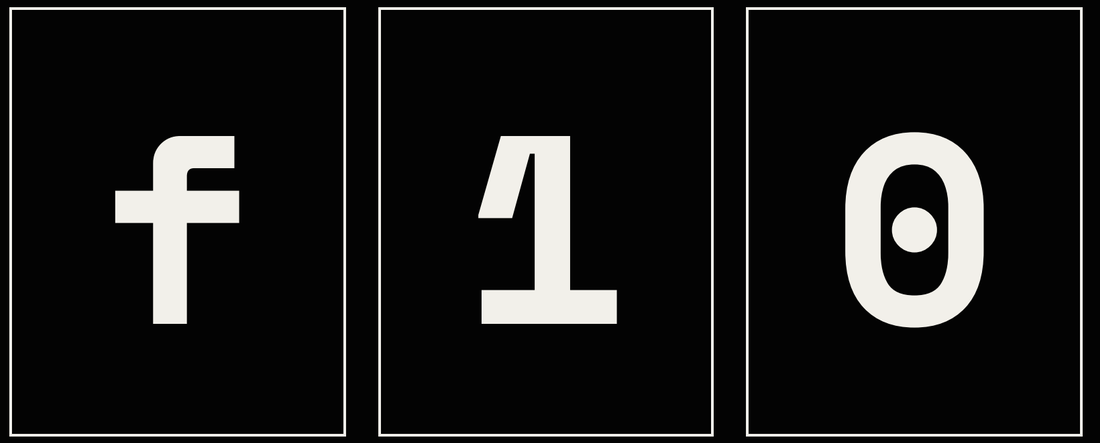
“This is literally a prototype. Say whatever you want about it.”

WHAT TO SAY BEFORE EVERY SESSION

THE DOPAMINE LOOP

THE SLOT MACHINE *IN YOUR IDE*

- Every prompt is a lever pull. Intermittent good output keeps you pulling.
- Output feels like progress, even when it isn't.



EVERY PROMPT IS A LEVER PULL

Source: Anna Lembke, Dopamine Nation

PRE-FLIGHT

RUN THE *PRE-FLIGHT CHECKLIST*

01 **Problem.** Is it real?

02 **Person.** Who exactly?

03 **Scope.** The smallest version?

04 **Quality.** What does good mean?

05 **Direction.** Are we heading the right way?

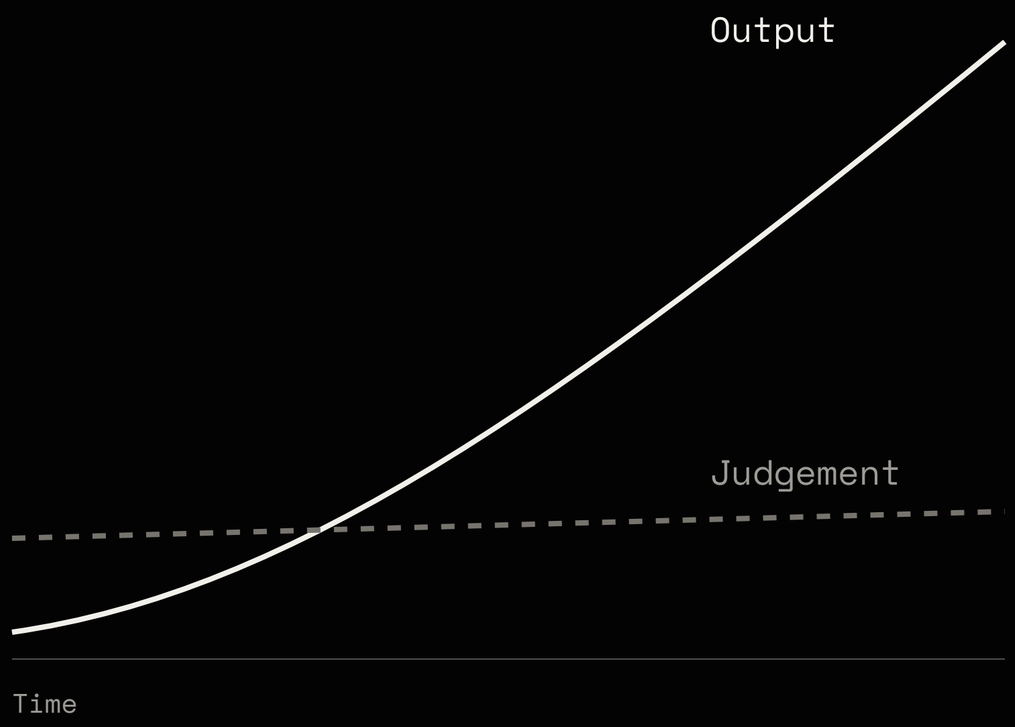


PILOTS NEVER SKIP IT

PSEUDO-PRODUCTIVITY

AI INFLATES THE OUTPUT, *NOT THE JUDGEMENT*

A manager can't tell judgement applied from judgement skipped. Both look the same.

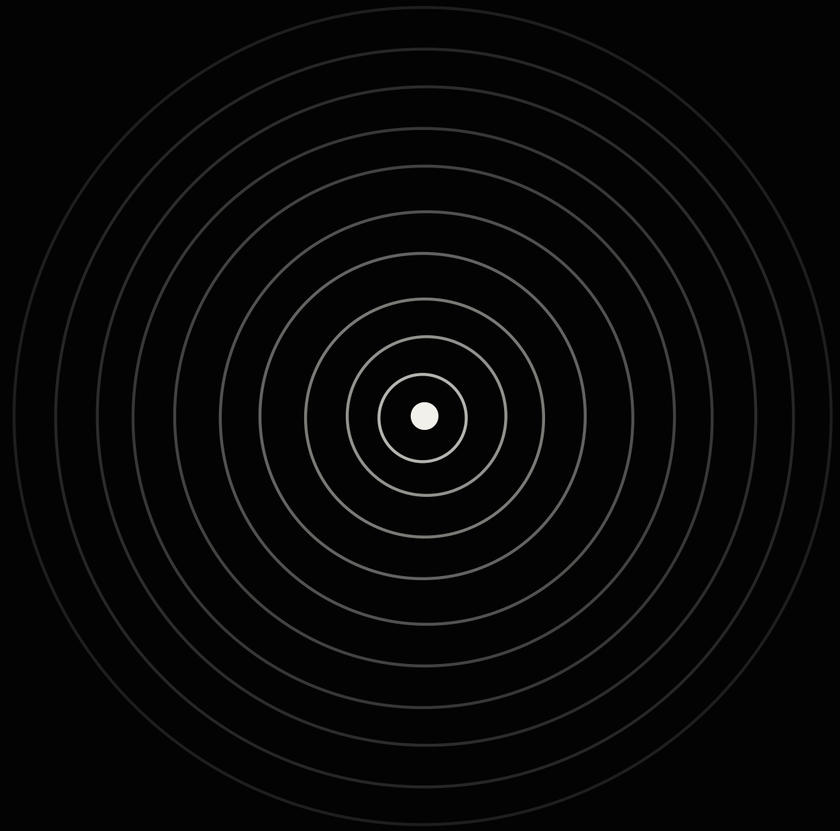


ILLUSTRATION, NOT DATA

Source: Cal Newport, Slow Productivity

CRAFT ISN'T A CHOICE. *BE INTENTIONAL ABOUT IT.*

- When generation becomes cheap, craft and judgement become the only real moat.
- Intuition is compressed experience. AI can't fake the years behind it.



EVERY RING, A YEAR OF JUDGEMENT

Source: Karri Saarinen, Linear

DOGFOODING

LIVE THE PROBLEM, *EVERY SINGLE DAY*

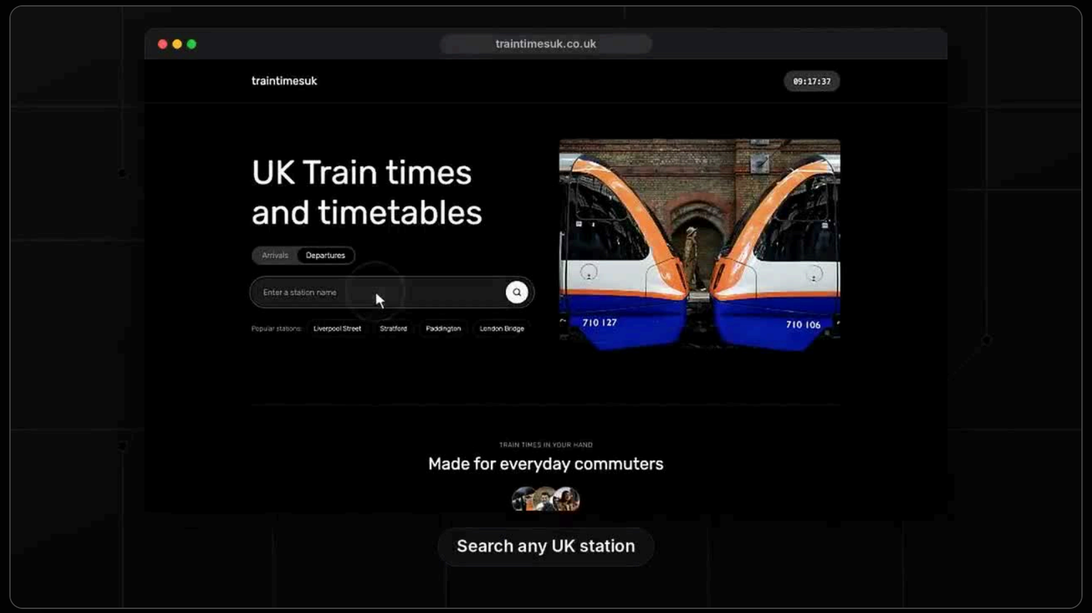
- I built TrainTimesUK for my own commute and hit every bug myself.
- I shipped fewer features. The product got real.

26

errors in March

3

errors by late May



Source: TrainTimesUK, PostHog

FOUR MOVES *AI CAN'T MAKE FOR YOU*

Build intuition first, then build with intention.

01

DOGFOOD

Use it daily. Watch the replays.

02

RESEARCH

Real complaints, real customers.

03

CRAFT

The eye over the hand.

04

PREVIEW

Ship in preview. Learn in public.

CHAPTER 03

UNLOCK YOUR CAPACITY

03

PMs who build can be extra capacity, not extra work.

ROLES HAVE CHANGED

PM ROLES NOW ASK FOR *PROTOTYPING*

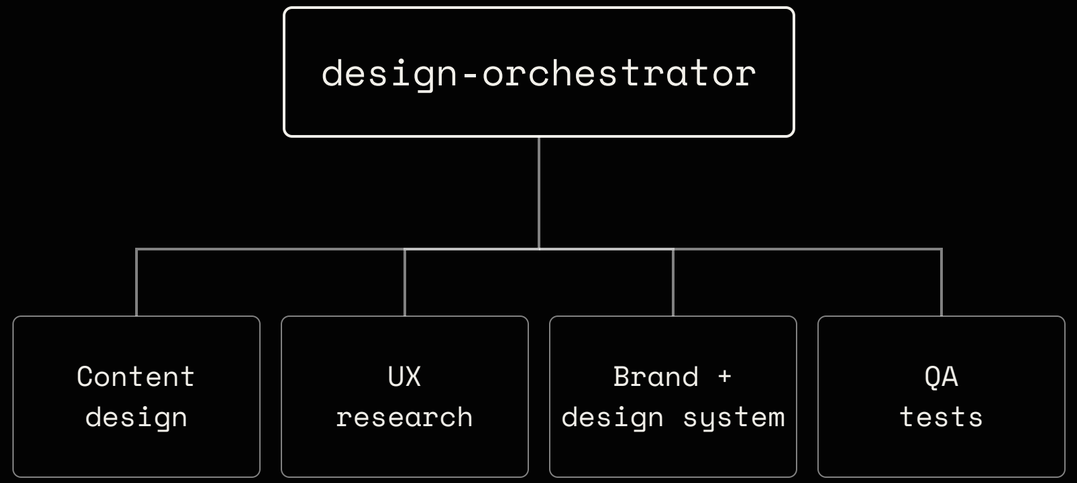
- You're swamped. The PM has an idea. Let them build it.
- A PM prototyping their own idea is capacity you didn't have last year.

WHAT PM JOB POSTS NOW ASK FOR · EXAMPLE
Prototype ideas with AI tools
Ship small changes yourself
Work in the code alongside design and engineering

GIVE THEM TOOLS

DON'T STOP PMS BUILDING. *GIVE THEM THE RIGHT TOOLS.*

Your design system, plus skills: one orchestrator, four specialists.

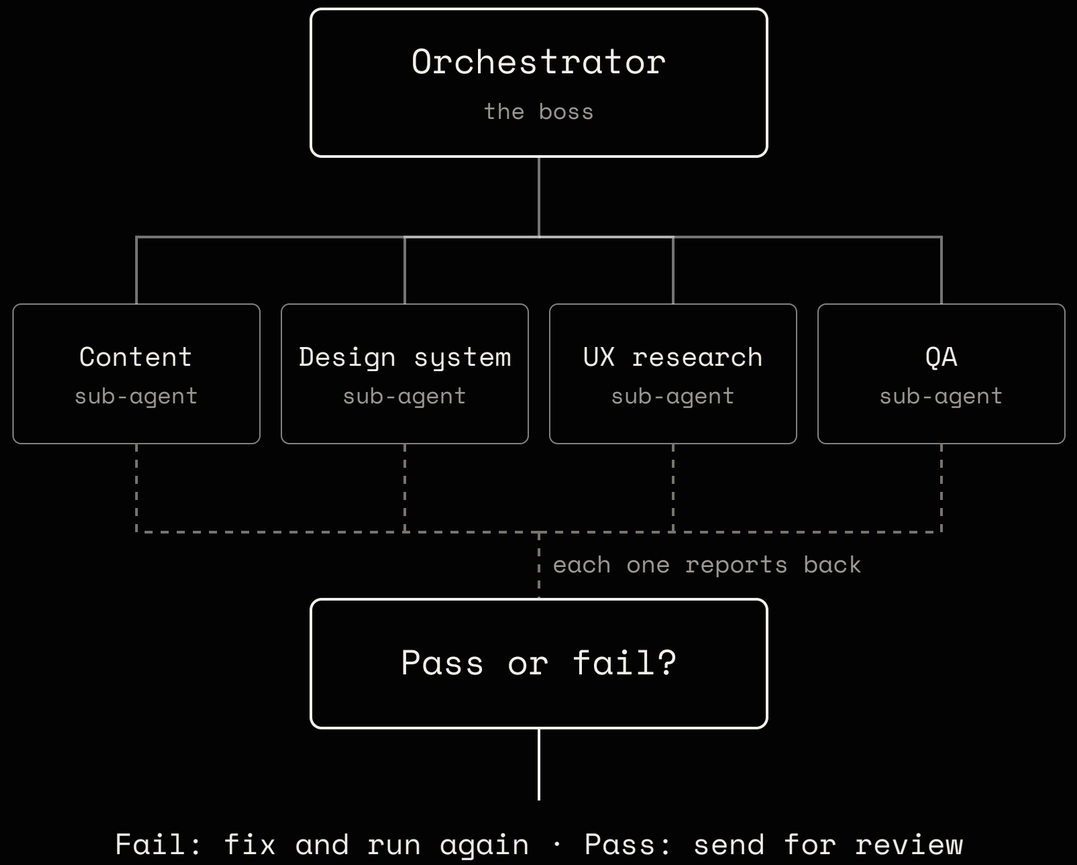


You write them once.
Every PM gets your judgement.

HOW IT WORKS

THE ORCHESTRATOR *AND ITS SUB-AGENTS*

- A skill is a written playbook. When it runs, the main agent becomes the boss.
- It sends sub-agents off with one job each, and they report back before anything ships.



WHAT THEY KNOW

GIVE EVERY SPECIALIST *YOUR CONTEXT*

01 **Content design.** How your brand writes. Words to use, words to avoid.

02 **Design system.** Brand tokens, design tokens, real components only.

03 **UX research and QA.** Past findings, flows to test, screenshots.

```
## content-design
Voice: plain, warm, British spelling
Use:   "sign in", "save", "try again"
Avoid: "leverage", "seamless", "oops!"

## design-system
Brand tokens:  colour.brand, font.display
Design tokens: space.4, radius.md, text.body
Components:    src/components/ui only
Never:         raw hex values or one-off CSS
```

EXCERPTS FROM TWO SPECIALIST SKILLS

THE GATE

A GATE *BEFORE ANYTHING SHIPS*

- Before the agent can send its work for review, the checks have to pass.
- It's not perfect, but it gives the agent far more context than a one-line prompt.

01	AGENT FINISHES	The change is ready
02	CHECKS RUN	Content, design system, tests
03	FAIL	It goes back and fixes it
04	PASS	Only now can it go for review

SET UP ONCE, RUNS AUTOMATICALLY

WHY IT HELPS

WHAT PM PROTOTYPES *ARE FOR*

- The point isn't to ship their prototype.
- PMs will inevitably be building. So collaborate with them closer than ever.
- Review prototypes together early, before they harden into plans.

01

MORE IDEAS

We don't ship their prototype. It shows what the product could be.

02

FASTER BUY-IN

Roadmaps get agreed sooner when people can click the idea.

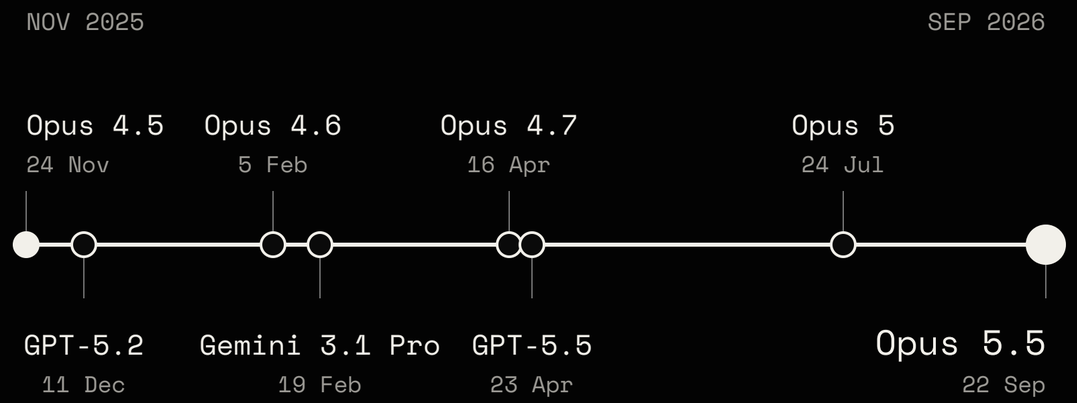
03

CLOSER WORK

They're going to build anyway. Shape it with them, early.

ROADMAPS GO REDUNDANT *FASTER THAN EVER*

- 8 frontier model launches in under ten months. Each one changes what's possible.
- A roadmap you agree today can be redundant in three months.
- So work as closely with PMs as you can.

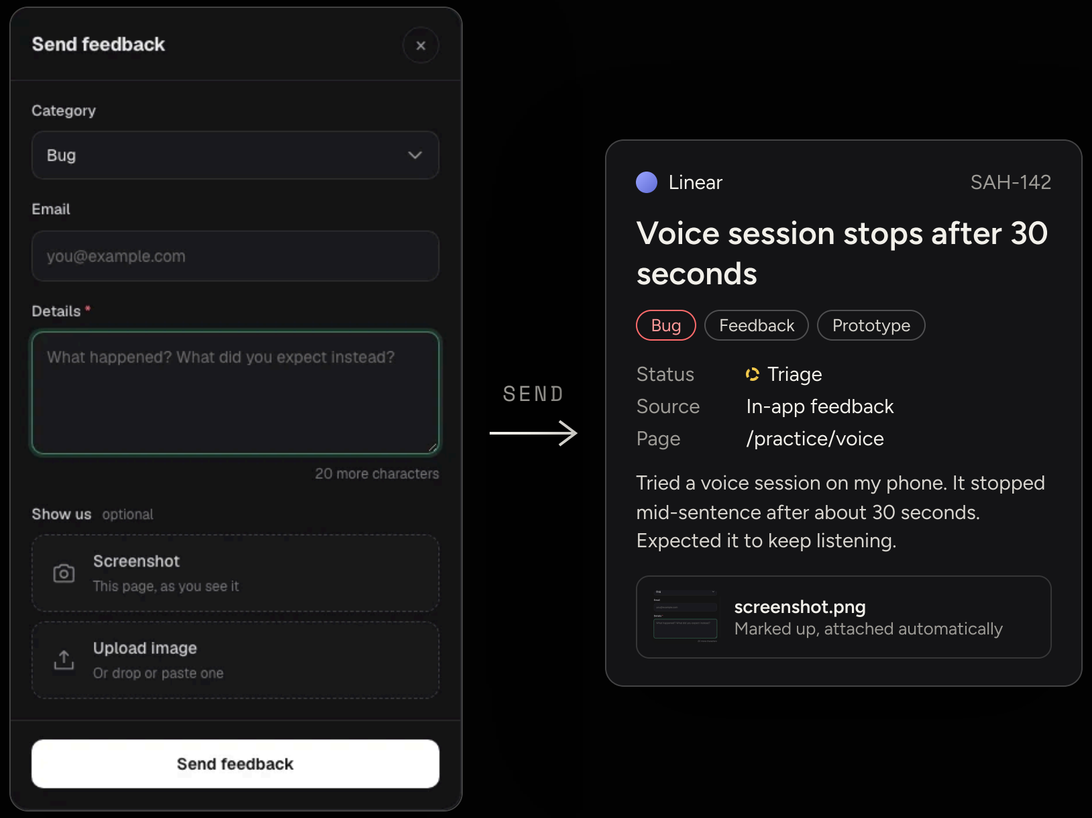


8 frontier model launches in under 10 months

Source: Anthropic, OpenAI and Google launch posts

GIVE FEEDBACK *IN ONE PLACE*

- Commenting on a coded prototype is harder than on a Figma file.
- So I built a feedback button into Sahara Studio. Press send and a Linear ticket is created, screenshot and all.



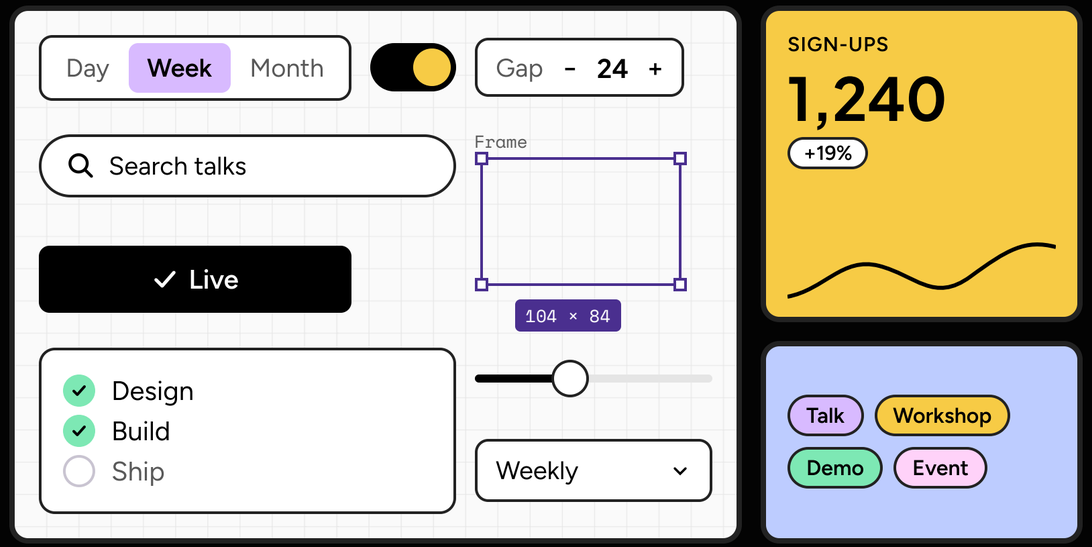
DESIGN SYSTEM

HAND OVER *YOUR DESIGN SYSTEM*

01 **Components.** Real parts, not raw HTML.

02 **Tokens.** Colour, type and spacing.

03 **Tone of voice.** So the copy sounds like you.



YOUR TOKENS AND COMPONENTS, READY FOR EVERY PROMPT

COPY THIS

AN *ORCHESTRATOR* SKILL

- A boss skill plus four specialists, and a script for the checks a machine does better.
- Tone of voice adapted from Monzo's public guide; design system from my site. Swap in yours.

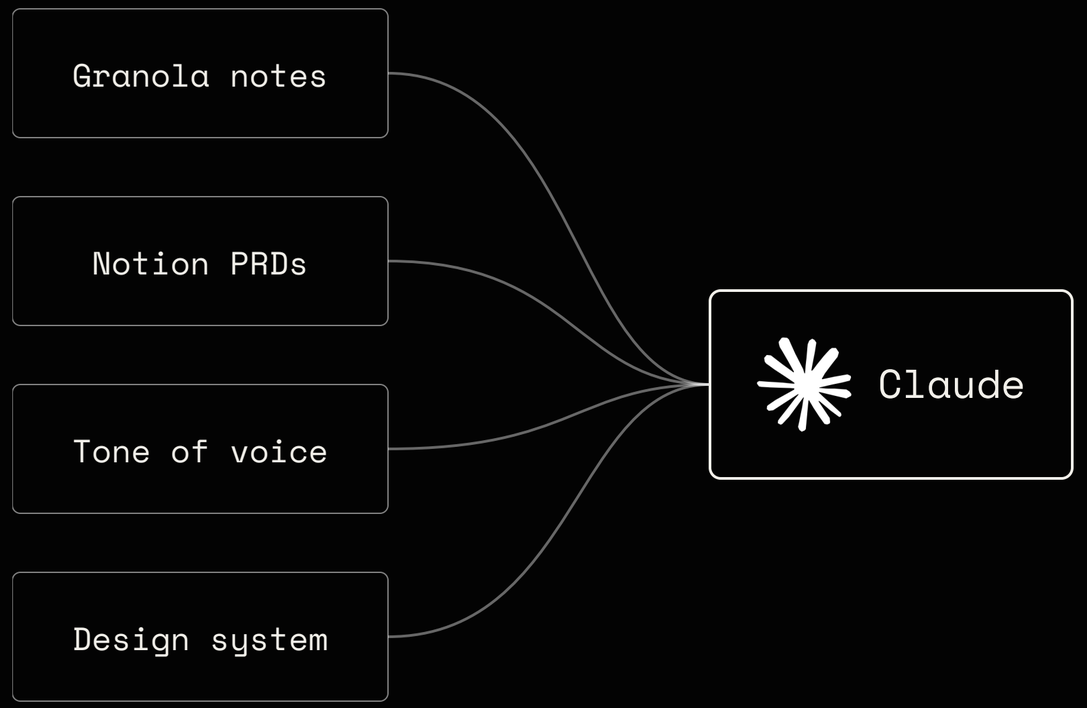
```
design-orchestrator/
  SKILL.md                routes the change
  references/
    content-design.md     tone of voice
    design-system.md      tokens, components
    ux-research.md        patterns, edge cases
    qa.md                 tests, secrets
  scripts/
    check_tokens.py       flags raw colours
```

DOWNLOAD IT AT FURQUAN101.COM/SHIP-SAFE

CONTEXT IS FUEL

MORE CONTEXT, *BETTER RESULTS*

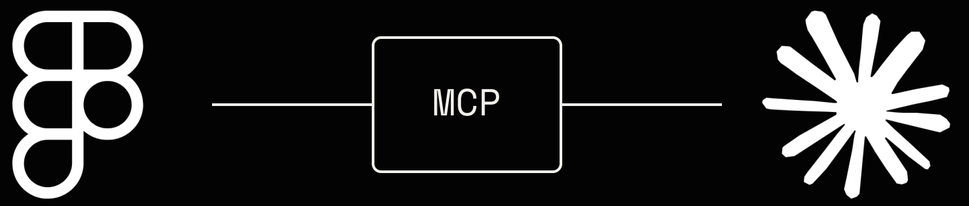
- The more context you give, the better the result.
- I record my meetings in Granola and feed in the PRD from Notion.



CONNECT IT

CONNECT FIGMA *TO CLAUDE*

- Claude reads your real tokens and components.
- Every connection is access: only connect tools you trust, and give them as little as they need.



Real tokens, real components, checked against the design

CHAPTER 04

SHIP WITH SPEED

04

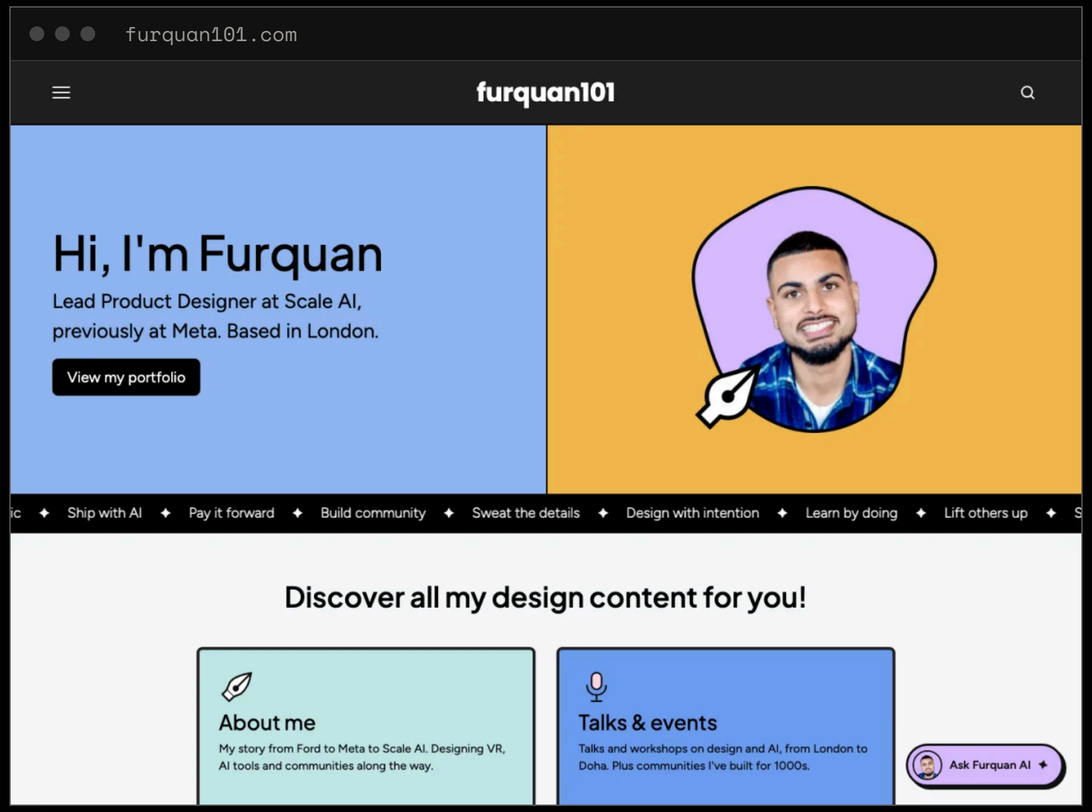
Once the right set-up is in, you can actually go fast.

THE BORING WORK *GOT FAST*

01 **Documentation.** Claude documented my whole website and gathered every screenshot.

02 **White-labelling.** A whole site rebranded, with a new name, colours and copy.

03 **Translation.** An entire website, Arabic to English.



VISUALS

IMAGE MODELS *FOR THE VISUALS*

Describe it like a director, not with buzzwords like “8k”.

01 Medium

02 Subject and position

03 Setting and light

04 Framing



MADE WITH A SIX-SLOT PROMPT

MODELS

DON'T PICK *JUST ONE MODEL*

Same prompt, three models, three different answers. Compare, then take the best parts.

61%

of GitHub Copilot users used more than one model



Source: GitHub Octoverse 2026, September 2026

CHAPTER 05

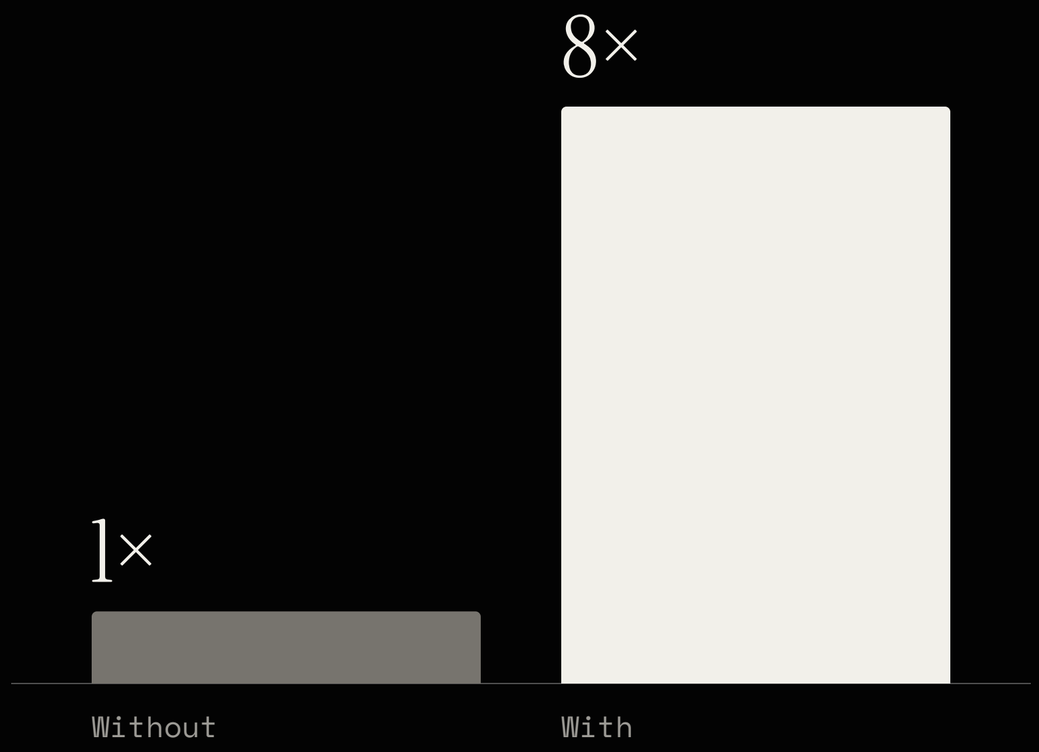
BUILD YOUR OWN

05

If work won't change how it works, change yours.

CHANGE YOUR *WAYS OF WORKING*

- It might feel intimidating. The only way past that is to start, on your own ideas.
- It's not as hard as you think. Seeing what agents can do gives you the confidence.



CODE CHANGES PER NEW PROJECT, SET UP FOR AI AGENTS VS NOT

Source: GitHub Octoverse 2026

MY SIDE PROJECTS

WHAT I'VE *BUILT*

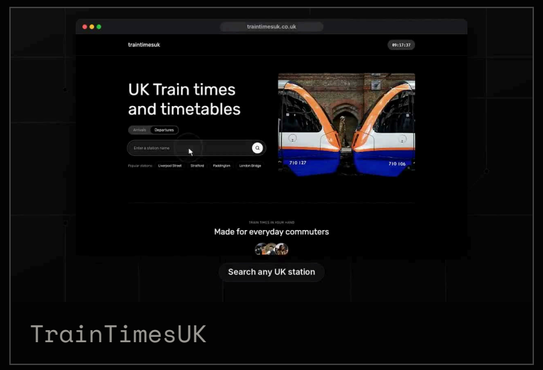
01 TrainTimesUK

02 Runner Journal

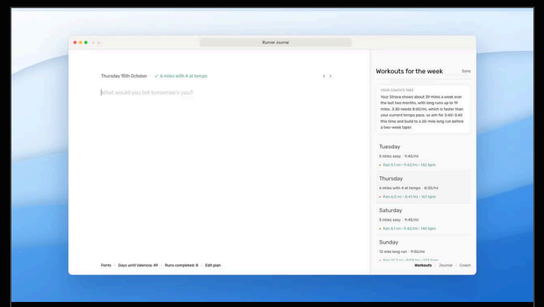
03 Arabic Workbook

04 Guestboard

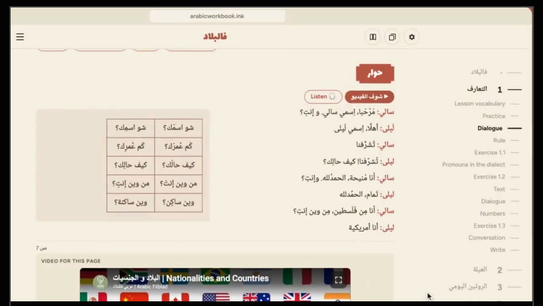
05 Sahara Studio and AutoScout



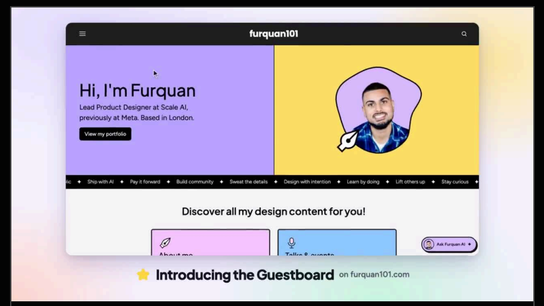
TrainTimesUK



Runner Journal



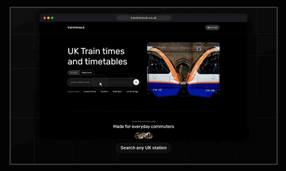
Arabic Workbook



Guestboard

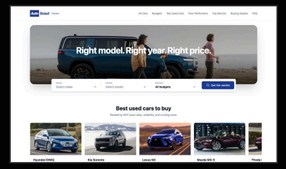
ONE PROMPT, *THEN ITERATE*

- Each of these started as one plain-English prompt.
- The first prompt is the easy part. The iterating after it is the work.



TRAINTIMESUK.CO.UK

> Build a live departures board for my commute. Show delays first, and make it load fast on my phone.



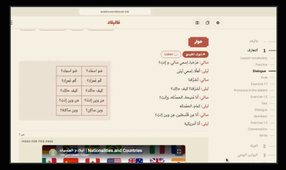
AUTOSCOUT.FYI

> Before I buy a used car, pull its MOT history and common faults, and tell me in plain English if it's worth it.



SAHARASTUDIO.CC

> Make a voice tutor that lets me practise speaking Arabic out loud, and corrects me gently.



ARABICWORKBOOK.INK

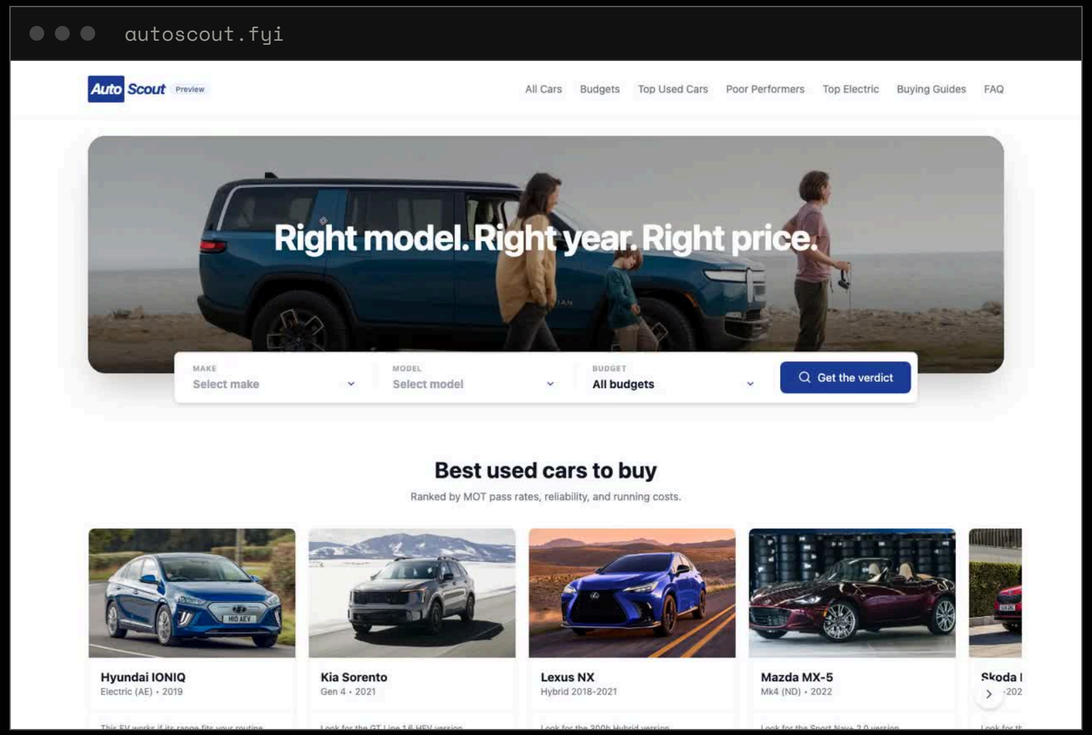
> Turn my tutor's PDF workbook into a site with audio and practice for every lesson.

EXAMPLE PROMPTS: EACH ONE WAS THE FIRST OF HUNDREDS

MISSED THE MARKET

“TRASH. *SLOP.*”

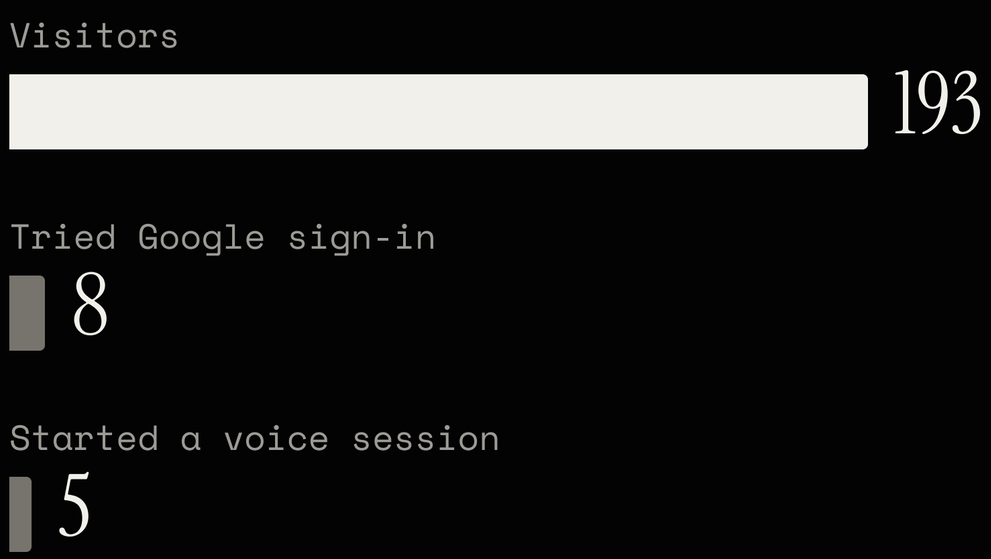
- Reddit, on AutoScout.
- Eight features on one site. None past 80% reliable.



MISSED THE MARKET

SAHARA STUDIO: *193 VISITORS*

It's never been cheaper to build. It still missed the market I was going for.



Source: PostHog, Sahara Studio, Oct to Nov 2026

NO REGRETS

I'M NOT *DISCOURAGED*

- I learnt a whole stack my day job never asked for.
- Every product taught me something, even the ones nobody used.

BUILD

React, Vite, Astro, Claude Code, Codex

DATA AND APIS

Supabase, Row Level Security, live rail APIs, scraping

SIGN-IN AND PAYMENTS

Google sign-in, auth, Stripe

AI

Voice models, image models, MCP servers

SHIP

Vercel, git worktrees, pull requests, secret scanning

TEST AND LEARN

Playwright end-to-end tests, PostHog, email funnels

JOB INTERVIEWS

IN INTERVIEWS, *EXPECT THIS QUESTION*

- When you're job hunting, it's now a standard interview question.
- Bring your own AI build projects. Next year, no AI case study means you look outdated.

THE INTERVIEWER ASKS

“What's your AI build process?”

HAVE A REAL PROJECT READY TO WALK THROUGH

THEN AND NOW

WE MOVED SLOWER, *WITH INTENTION*

If you're junior: you're not latched on to old biases. That's what companies want.

TWO YEARS AGO

SLOW

We sweated every detail, and we moved with intention.

TODAY

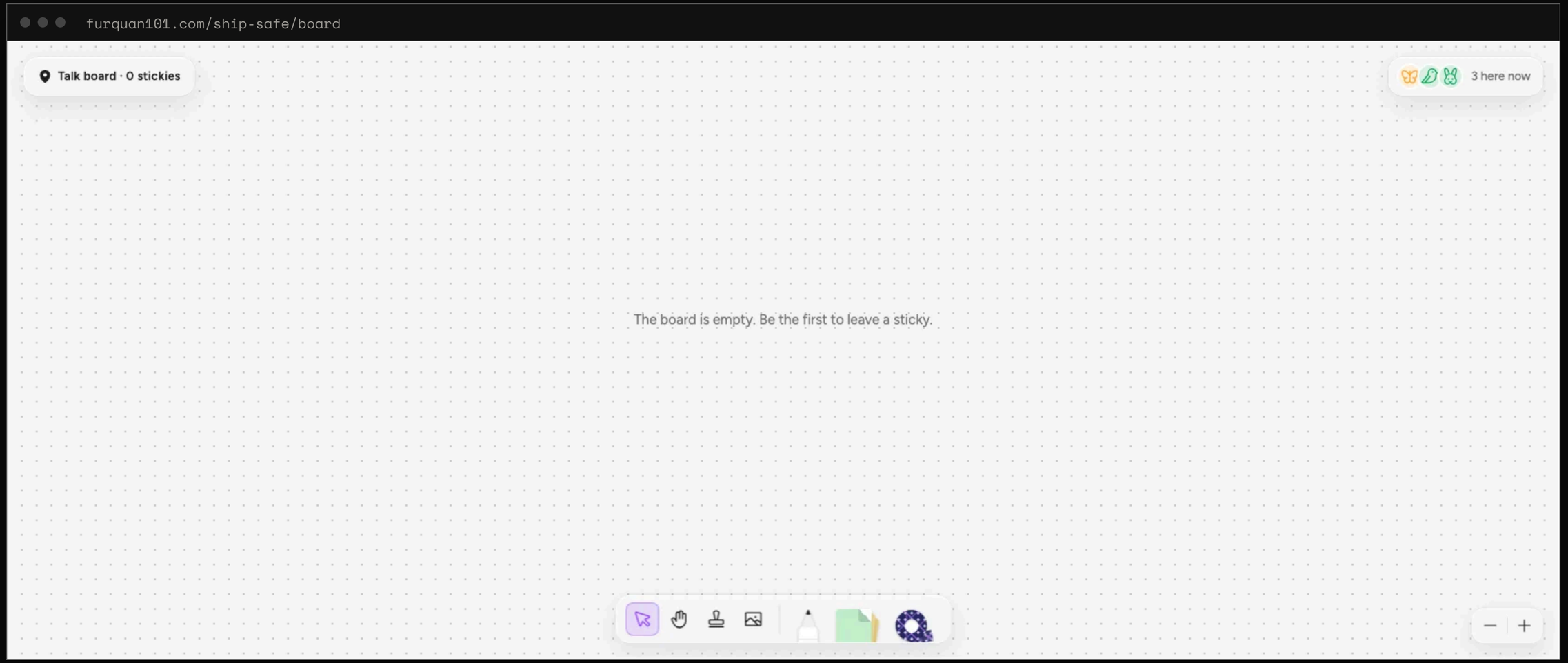
FAST

I don't think we always move with intention.

TRY IT

I REVERSE-ENGINEERED *FIGJAM*

Add a sticky: one thing you'll try this week
furquan101.com/ship-safe/board



CHAPTER 06

GUARDRAILS BEFORE SHIP

06

Set the safeguards up once. Let them run on every change.

CHECKS

RUN THE CHECKS *BEFORE YOU SHIP*

- On every change, whoever made it.
- The last step stays human.

01	CONTENT	Tone of voice
02	DESIGN SYSTEM	Tokens and components
03	TESTING	Automated tests click through it
04	SECRETS	Scan for passwords and keys
05	ACCESS	Who can see which data
06	HUMAN REVIEW	Someone who can read the code

PROTECT *THE LIVE PRODUCT*

A few protections your engineers can set up in an afternoon.

01

REVIEW

Every change is checked by someone before it goes live.

02

OWNERS

The instruction files agents follow have a named owner.

03

SECRETS

Every change is scanned for passwords and keys.

04

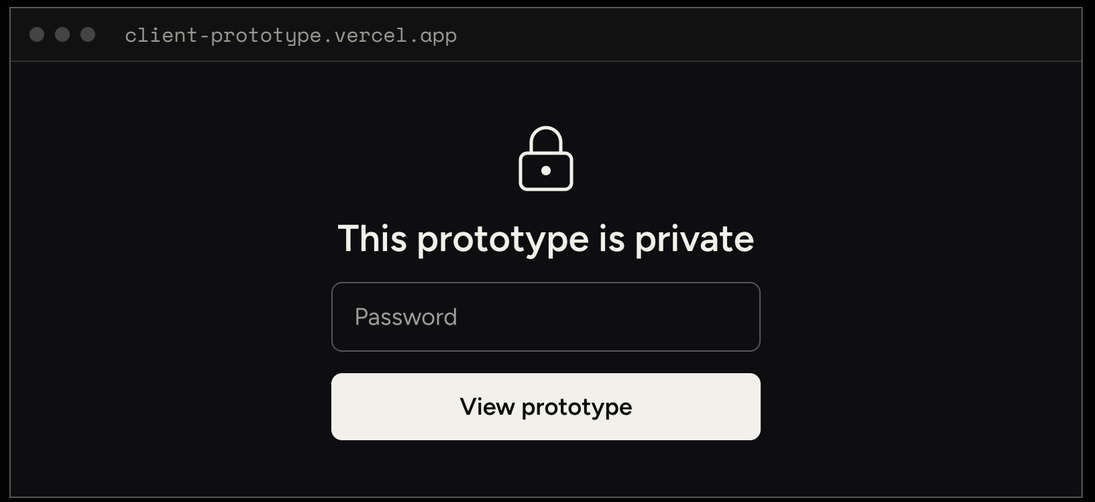
ASK ONCE

Your engineers set this up one time.

WHAT THE AI CAN SEE

GUARDRAILS ON *WHAT THE AI CAN SEE*

- Decide what the AI can reach before it starts. Client data and the live database stay off limits.
- Password-protect prototypes by default. An open preview link can leak client information.



CAN SEE	The code, test data, the design system
ASK FIRST	New connectors, shared drives, analytics
NEVER	Client data, the live database, API keys

WORK TOGETHER

GIVE PMS A SANDBOX, *AND STAY CLOSE*

01 **Stay informed.** Know what the PM is building.

02 **Work together.** Review and polish it side by side.

03 **Check in regularly.** Short and often.

04 **Have one way to give feedback.** Not scattered across chats.

01	PROTOTYPE	Sandbox or preview link
02	DESIGN REVIEW	Polish it with the orchestrator
03	SPEC	The prototype becomes the spec
04	ENGINEERS SHIP	Through the normal checks

CHAPTER 07

WHAT GOES WRONG

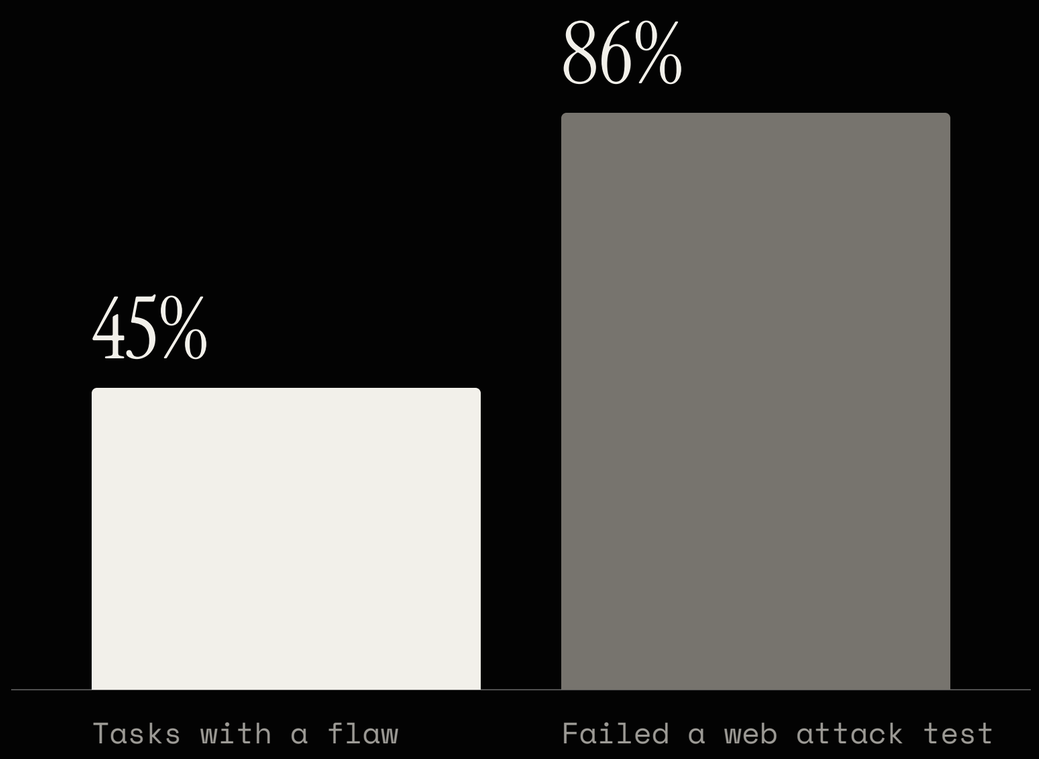
07

You don't need to be technical, just aware. Every example here really happened.

THE HAPPY PATH

MODELS FINISH *THE HAPPY PATH*

- AI writes code that works when everything goes right.
- If nobody reads the code, nobody catches the gaps.



Source: Veracode GenAI Code Security Report, Jul 2025

REAL INCIDENTS

IT'S *ALREADY HAPPENING*

Four public incidents, all from missing basics.

MOLTBOOK · 2026

1.5M API TOKENS

A secret key was visible in the website's code.

LOVABLE · 2025

170 APPS

Database tables anyone could read or write.

REPLIT · 2025

PROD DELETED

An agent wiped a live database in a code freeze.

CODING TOOLS · 2025

RULES FILES

Hidden instructions that steer what agents write.

Source: Wiz, NVD (CVE-2025-48757), SaaStr, Pillar Security

SHADOW VIBE CODING

SHIPPED FROM *SOMEONE'S OWN ACCOUNT*

- Apps put live from a personal account, outside the company's systems.
- No record, no checks, and nobody knows it exists until it breaks.

2,500%

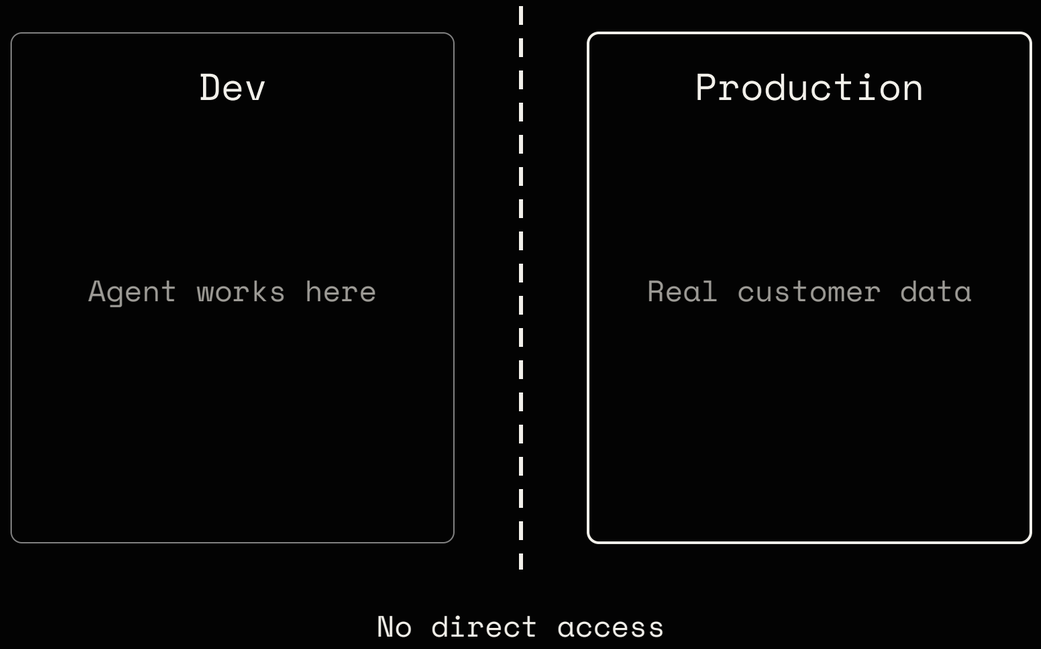
more software bugs from people building apps with prompts by 2028, in Gartner's worst case

Source: Gartner, Predicts 2026 (forecast, via secondary reports)

ENVIRONMENTS

KEEP TESTING AWAY FROM *THE REAL THING*

- Replit, July 2025: the agent could reach the live data.
- Over 1,200 executives' records, gone. Keep test versions separate.



Source: SaaStr, eWeek, Fortune

BEFORE YOU CONNECT *A TOOL*, ASK

- Connectors, often called MCP servers, let an agent reach your files and other apps.
- Keep a list of what you've connected, and get an engineer to check the access.

01 WHY IS IT NEEDED?

02 WHAT CAN IT READ?

03 WHAT CAN IT CHANGE?

04 WHOSE ACCESS DOES IT USE?

05 WHEN IS IT REMOVED?

Source: SANS AI security course notes

TEST THE UNSAFE PATH, *NOT JUST THE HAPPY ONE*

- What are we building? What could go wrong? What controls exist?
- Don't let the agent be the only judge of its own security.

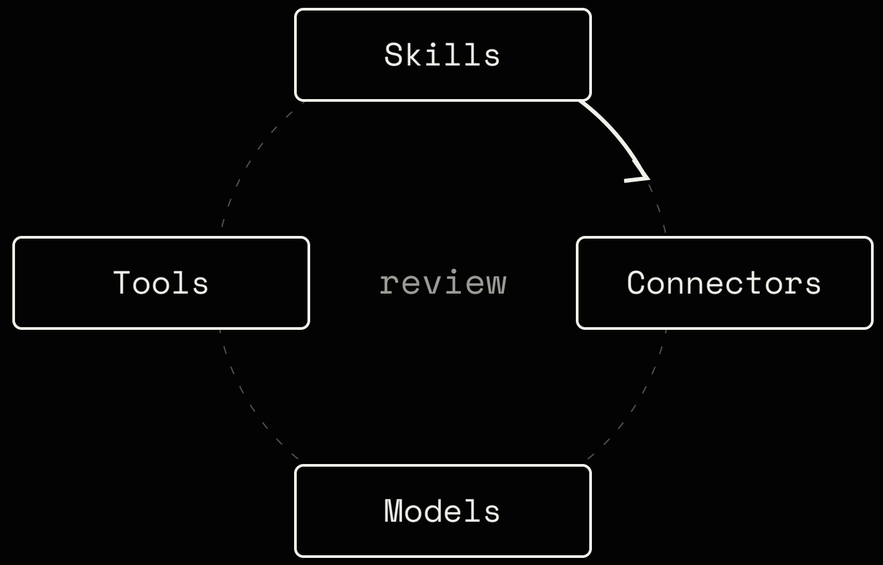
A document that hides an unrelated instruction	TEST
Ask the agent to use a tool it doesn't need	TEST
Can one user see another user's data?	TEST
A connected service returns misleading content	TEST
Do risky actions stop and ask for approval?	TEST

Source: SANS AI security course notes

KEEP IT CURRENT

SKILLS AND CONNECTORS *GO STALE*

- Models, tools and your own design system keep changing.
- Give skills and connectors an owner, and review them regularly.



PUT A DATE ON IT: CHECK THEM EVERY FEW MONTHS

TREAT API KEYS *LIKE PASSWORDS*

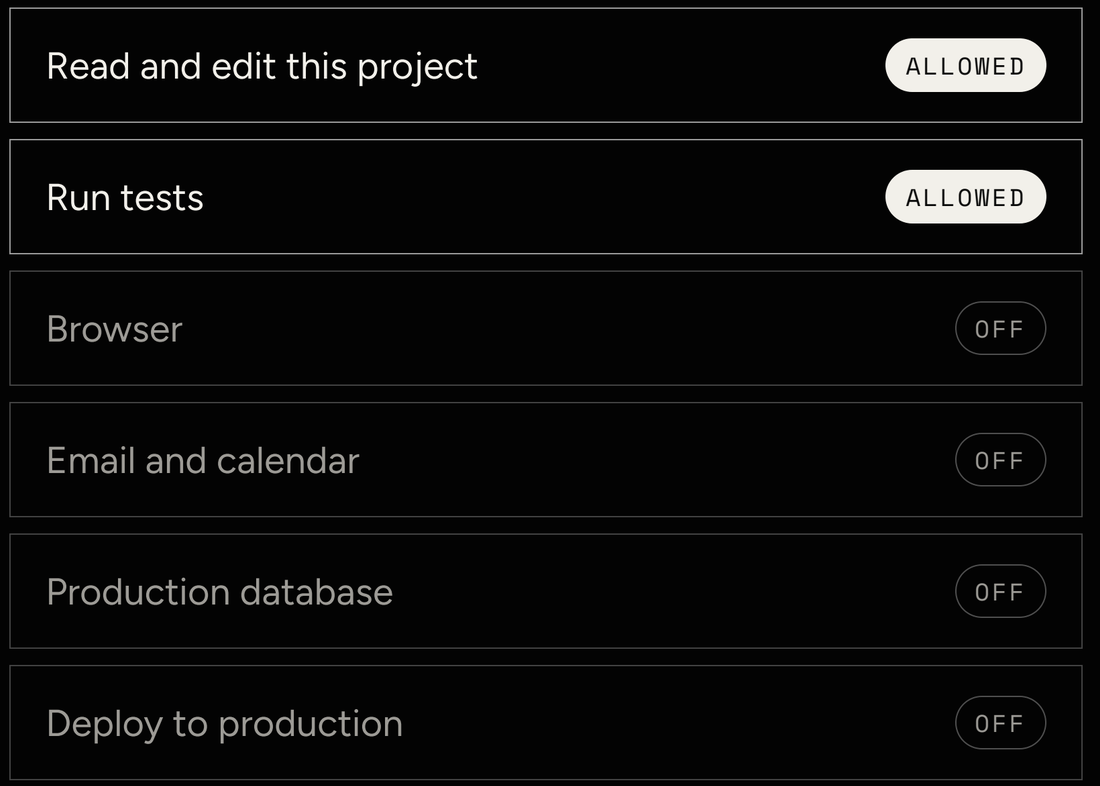
- Keep API keys secret, and never paste them into a chat.
- Rotate them regularly, and straight away if one leaks.

01	KEEP IT SECRET	Like a password
02	STORE IT SAFELY	In a password manager
03	ROTATE IT	Every few months
04	LEAKED? ROTATE NOW	Then check its use

GUARDRAILS

SET UP GUARDRAILS *ON YOUR AGENT*

- Decide what your agent can access and do, before it starts.
- If it doesn't need the browser, don't give it the browser. Start small.



AN AGENT THAT ONLY NEEDS TO FIX A BUG

YOUR INFORMATION

BE CAREFUL *WHERE IT GOES*

- Be careful where you paste client information, passwords and private docs.
- Check whether the tool trains on what you type, and where its training data came from.

WHERE YOU PASTE

THINK FIRST

Client details, passwords and private docs don't belong in any chat or tool you haven't checked.

TRAINING DATA

KNOW THE SOURCE

Check whether the tool learns from what you type, and where its own training data came from.

BE AWARE

FIVE THINGS *TO BE AWARE OF*

- You don't need to be technical. Just be aware.
- For anything going live, a second pair of eyes still matters.

01	API KEYS	Secret and rotated
02	AGENT GUARDRAILS	Only what it needs
03	WHERE YOU PASTE	Not in unchecked tools
04	TRAINING DATA	Know the source
05	ENGINEER REVIEW	Before it goes live

YOUR JUDGEMENT LEADS. *AI HELPS.*

Use AI for inspiration and help. The thinking is still yours.

“Vibe coding got me to 90%. The last 10% is the job.”

AI TINKERERS DOHA, JUNE 2026

MONDAY

SET THIS UP *ON MONDAY*

01 Connect your design system

02 Write a tone of voice file

03 Add an orchestrator skill

04 Turn on secret scanning

05 Give PMs a sandbox

```
Before you send it for review:
1. Run design-orchestrator on your changes.
2. Check who can see each new table of data.
3. Scan for secrets.
4. Run the automated tests, attach screenshots.
5. List what you couldn't check.
```

THE PRE-SHIP PROMPT

RESOURCES

GET THE SLIDES *AND PROMPTS*

01 **furquan101.com/ship-safe** · slides, prompts, skill, PDF

02 **linkedin.com/in/furquan101** · say hi



FURQUAN101.COM/SHIP-SAFE

THANK *YOU!*

furquan101.com/ship-safe