GARLIC THREAT

STAY AHEAD OF THE THREAT.

what is Strike testing, actually

A Strike test is a 7-day, hands-on attack on one AI-built app, proven with working exploits. **Here is exactly what we test, and how.**

Strike, at a glance.

A 7-day, hands-on test of one app or one API, proven with working exploits.

THE NUMBERS

TESTING TIME

7

working days of testing

START TO FINISH

~6

weeks, start to closed report

SCOPE

25

endpoints max, one app or API

PRICE

$1,900

fixed, agreed before we start

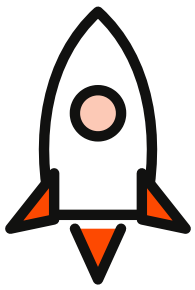
INCLUDED, EVERY TIME

- Audit-ready report
- Plain-English summary
- Attestation letter
- Walkthrough call
- 1 free retest

Who Strike is for.

A startup about to launch, raising money, or answering its first customer security questions.

BEST FOR



About to launch

Know what a stranger can reach.



Raising money

A report investors can trust.



First security questionnaire

Answer with proof, not promises.

HOW TO READ THIS DOCUMENT

Plain words first. If you are a developer, the technical term follows in brackets.

Can one user see another user’s data? IDOR

The free first step.

A passive check of what anyone on the internet can already see about your app. **No attack. No password. No card.**

BEFORE YOU PAY



Reads only what is already public.

1 We look | **2 We show proof** | **3 You decide**

If we find something worth fixing, you see the finding in full, with proof. Then you decide if you want a full test.

Four checks. *Every time.*

They catch the flaw behind the big AI-app breaches: access rules left open, so a stranger can read or change your data. Row Level Security / RLS

01

We try to read your data **without logging in**, using your app's own public key.

logged-out query

02

We walk through your protected pages **with no login**, to see what opens anyway.

logged-out route walk

03

We log in as one user and try to **open another user's data.**

two-account ownership swap / IDOR

04

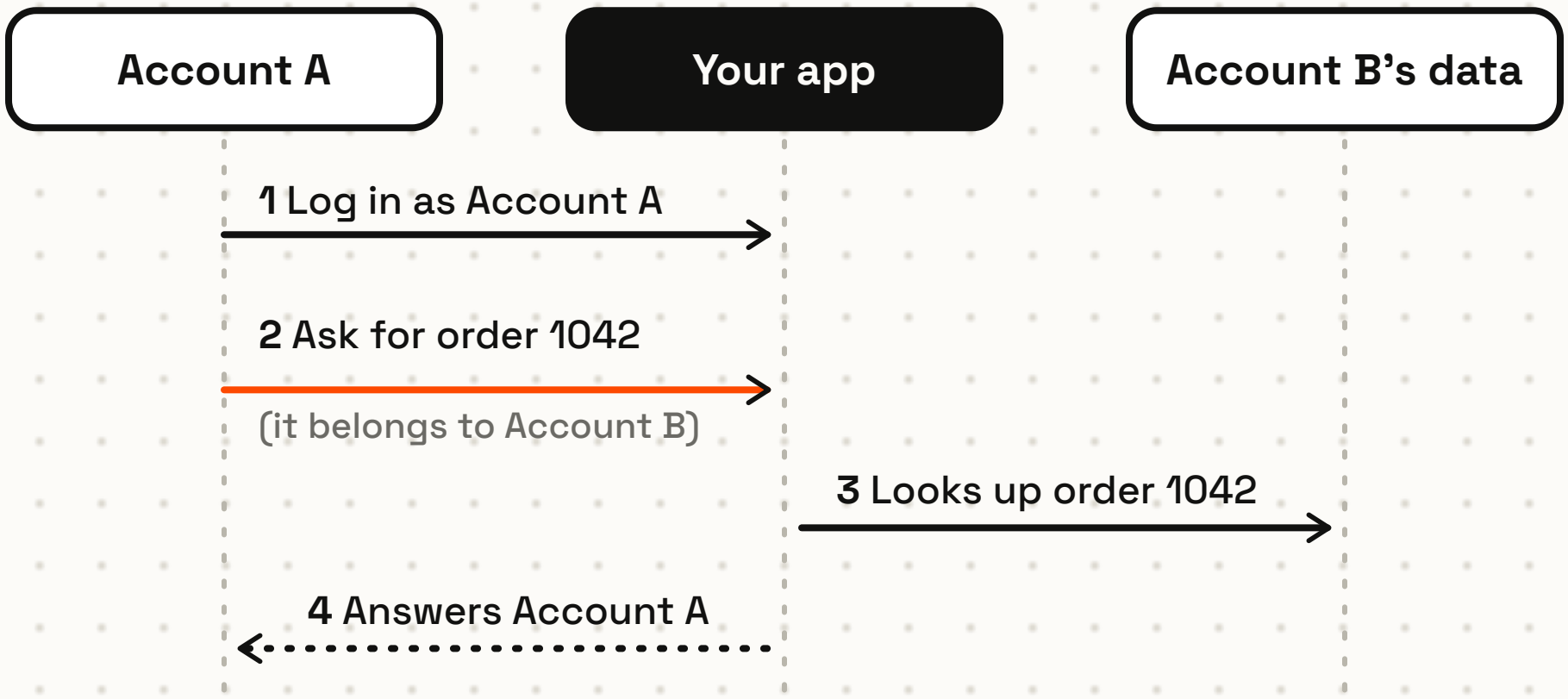
We search the code your app ships for **leaked keys and secrets.**

secret search

Check 03, shown.

We log in as one user and try to open another user's data. Here is how one test plays out.

OWNERSHIP SWAP IDOR



PASSES

403 — not your order

The app checks who is asking.

FINDING

200 — B's order returned

We capture it as proof.

Illustrative example. A result only becomes a finding when we can reproduce it with a working exploit.

Nine things we test.

One app or one API, up to 25 endpoints. Each area is a question an attacker would ask.

01
Can someone log in as someone else?
authentication

02
Can one user see another user's data?
IDOR

03
Can someone reach admin pages without being an admin?
access control

04
Can someone break in through a form, a link, or a file upload?
injection, XSS

05
Can someone trick the server into talking to private systems?
SSRF

06
Are passwords, password reset, and logins handled safely?
session handling

07
Are secret keys or passwords visible in the app's code?
exposed secrets

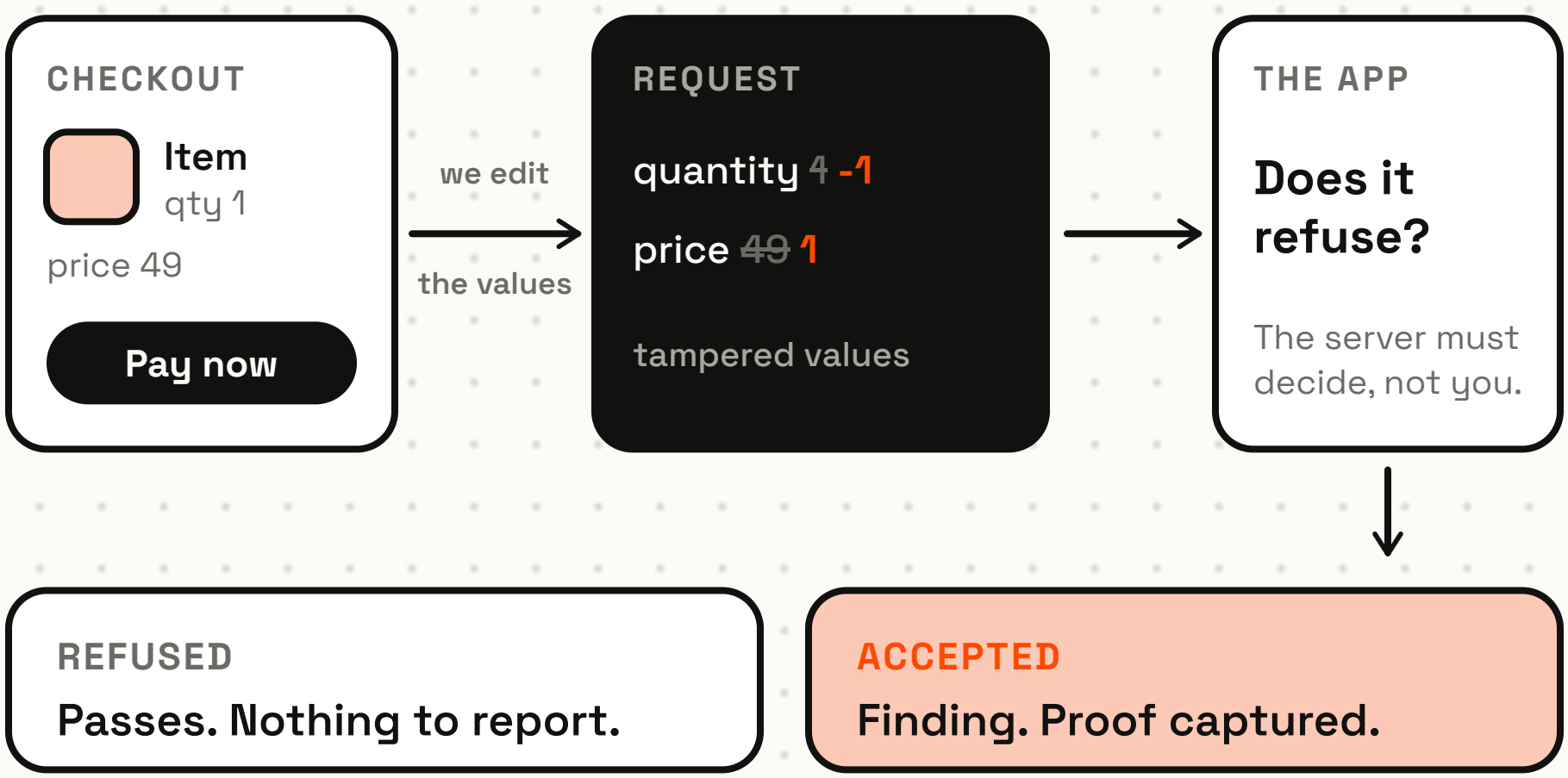
08
Is the connection safe, and are the safety settings on?
TLS, security headers

09
Does the API give away more data than the screen shows?
excessive data exposure

One flow, *checked lightly.*

One important money or business flow, for example changing a price or a quantity at checkout.

BUSINESS LOGIC LIGHT TOUCH

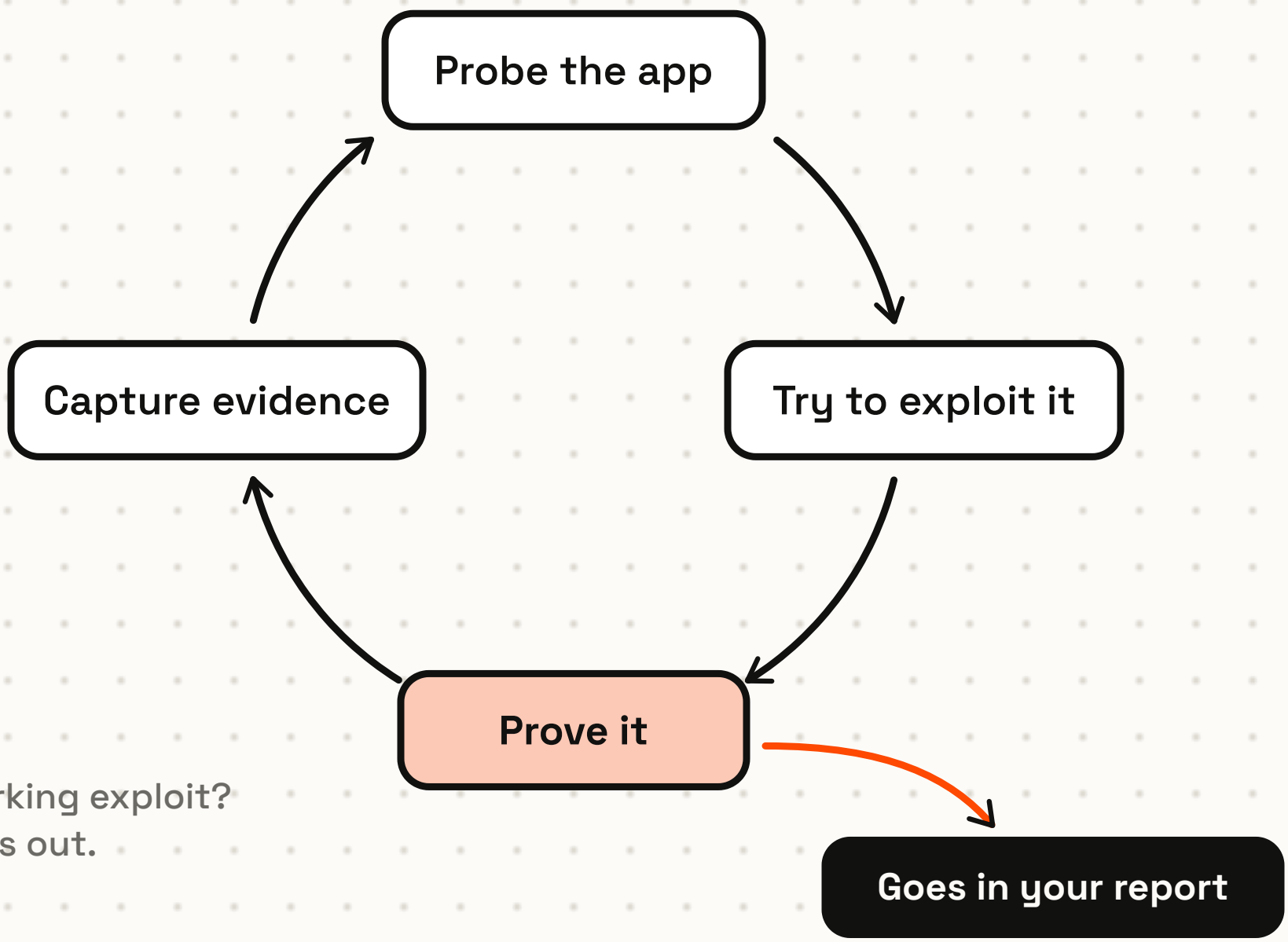


Illustrative values. Deeper testing of coupons, credits and refunds across every workflow sits in Breach.

No proof, *no report.*

We attack your app the way a real attacker would, with your written permission, and prove every finding with a working exploit.

THE METHOD



No working exploit?
It stays out.

Guided by OWASP, NIST and PTES. Every finding gets proof, a fix and a priority.

About 6 weeks, start to *closed.*

Three steps. You hear about critical problems as soon as we prove them, not at the end.

THE TIMELINE

1 **We test** · 7 working days

Critical problems reach you the moment we prove them.

2 **Report + letter** · within 2 working days

3 **You fix · we recheck once**

30 days from the report · retest free



Anatomy of a *finding.*

Every finding carries proof, a fix and a priority. Plain English first, technical terms in brackets.

EXAMPLE FINDING · NOT CLIENT DATA

FIX NOW

Any logged-in user can read other customers' invoices IDOR

PROOF

```
> GET /api/invoices/20417 as Account A
200 OK
{ "customer": "[redacted]", "total": "[redacted]" }
```

THE FIX

Check on the server that the invoice belongs to the person asking, on every request.

THREE PRIORITIES

FIX NOW · FIX THIS WEEK · FIX SOON

What you walk away with.

Five things, included in the fixed price.

INCLUDED

1 **A report you can show an auditor**
Every finding with proof, a fix and a priority.

2 **A plain-English summary**
Written for readers who are not technical.

3 **An attestation letter**
Arrives with your clean final report.

4 **A walkthrough call**
We talk you through the findings and the fixes.

5 **One free retest**
We check your fixes once, within 30 days of the report.

What we need.

FROM YOU



The web address of your app



Two test logins: one normal user, one admin



One person we can ask questions

Our rules, every test.

- **Written permission and an agreed scope** come before any testing starts. We test nothing outside it.
- We never **delete data, crash your site,** email your staff, or test systems you do not own.
- Production gets **safe, gentle checks.** A staging copy is better when you have one.
- Proof stays **private** and is shared only with you. We publish nothing without written permission.
- **Critical problems** are told to you as soon as we prove them.
- You can **stop the testing** at any time by telling your contact.

What Strike *leaves out.*

NOT IN STRIKE

- ✕ More than one app, or more than 25 endpoints
- ✕ Deep business-logic testing across every workflow
- ✕ Cloud settings checks

NEED MORE? STEP UP TO

Breach 3 weeks of testing

Your full app and full API, every role, money flows tested deep, login with Google, file uploads and your cloud settings.

Unsure? Start with Strike. Go to Breach within 60 days and your Strike fee counts toward it.

Internal networks, emails to your staff and systems owned by other companies sit in Custom.

Price and how you pay.

STRIKE · FIXED PRICE

$1,900

Agreed before we start.

INCLUDED

7 working days of testing, the audit-ready report, plain-English summary, attestation letter, walkthrough call and one free retest.

TWO PAYMENTS

50%
When you sign the scope

→

50%
When the watermarked draft report arrives

→

Final payment
clears, then the clean report and the letter are yours

You read the draft first, then pay the balance.

Our promise, in *one line.*

THE GUARANTEE

If your auditor, insurer or enterprise customer rejects this report as a valid penetration test, **we refund you in full.**

Send us the written rejection within 30 days of the report. We do not promise a clean result, and we do not promise to find problems. We promise a real test and a report that stands up.

START FREE

Try the free passive check. No card needed.

BOOK A FREE SCOPING CALL

www.garlicthreat.tech

GARLIC THREAT

STAY AHEAD OF THE THREAT.