[redacted]

YOUR OTP ENDPOINT HAS NO WORKING RATE LIMIT.

Your only login mechanism can be spammed, drained, and mapped. This is the plain-language summary. The full technical reproduction ships as a separate companion report.

TARGET	ENDPOINT	SEVERITY	FIX TIME
[redacted]	[redacted]	Critical	[redacted]

WHAT WENT WRONG

One request, unlimited SMS.

To log in, a user asks [redacted] to text them a one-time code. The endpoint that sends that text does not properly limit how often it runs. So anyone can trigger those SMS messages over and over, for any number, with almost nothing stopping them.

STEP 1	STEP 2	STEP 3
Enter a phone number	**App sends an OTP by SMS**	**Repeat endlessly. Nothing blocks it.**

What that lets an attacker do

Drain your SMS budget

Every code costs you money. A flood during an event can burn the whole month's quota in minutes.

Lock users out

Once the budget is gone, paying customers can't get their code and can't log in. Support gets flooded.

Harvest phone numbers

The same flaw lets someone map which phone numbers have accounts, ready for spam or phishing.

THE BIGGER SIGNAL

This one bug is fixable in a day. What concerns us more is **why it exists.** The endpoint is missing several standard industry and security practices at once: correct error codes, retry headers, layered rate limits, and shared state across servers. When that many basics are absent in one place, it usually means the gap is not a single oversight. It points to a wider need for an **architectural and security audit** of the app, not just a patch here.

Why you're hearing this from us

This report is AI-native: we reproduced the bug with an AI-driven audit pipeline. But **a human found it first.** Someone who uses [redacted] likes it, and chose to tell you rather than exploit it. That is responsible disclosure. We are here to protect what you built, before anyone with worse intent gets there.

WHAT HAPPENS NEXT

LET'S FIX IT TOGETHER

We found it because we care about your app.

Your users trust you with their phone numbers. We found a way to break that trust before anyone else did. If you want a partner to stand behind the safety and reliability of what you build or invest in, so the people using it stay protected, that is exactly the work we do.

hello@gattyworks.com

Tell us when your team can start, who should be in the room, and whether you'd like us to build the fix or review the wider architecture.

How GattyWorks works

A senior-led studio whose flagship is software auditing: engineers, designers, and AI agents auditing what vendors built, for the people who paid for it. **We reply to any brief within 24 hours.**

Quick Fix

We patch the OTP rate limiting, harden the endpoint, and verify it holds under load.

UNDER 24 HOURS

Complete Fix

The patch plus monitoring, alerting, and a full re-test pass so it stays fixed.

UNDER 48 HOURS

Architecture Audit

End-to-end review of auth, API surface, and data flow. Where the real answer lives.

UNDER 1 WEEK

COMPANION REPORT Full technical detail, plus a ready-to-paste prompt your engineer can hand to an AI coding assistant to apply the whole fix in one pass, ships alongside this as [redacted] **Technical Appendix**.