OTP REUSE BUG IN E-COMMERCE LOGIN SYSTEM

**HOW I FOUND IT :**

I was checking the OTP login feature on an e-commerce site. I entered my phone number, clicked “Get OTP,” and received a code — 2620 — via SMS.

I didn’t use it right away. I thought, What happens if I ask for another OTP? Will I get a fresh code?

So, about two minutes later, I clicked “Resend OTP.” The SMS came in… and to my surprise, it was 2620 again — the exact same code as before.

**WHY THIS IS A PROBLEM :**

The whole point of an OTP (One-Time Password) is that it should be used only once. Every time you request one, it should be unique and valid for a single login.

**IF THE SYSTEM REUSES THE SAME OTP:**

Anyone who saw your old code can log in again.

If someone intercepted that OTP earlier, they could still use it — this is called a replay attack.

It basically breaks the main security promise of OTP authentication.

**WHAT MIGHT BE HAPPENING :**

It seems like the server isn’t generating a new OTP if the old one hasn’t expired yet. Instead, it might be storing it temporarily and sending the same code again. The front end clears the OTP field on the screen for the user, but in reality, the backend just keeps reusing the old code.

**PROOF I COLLECTED :**

I have two SMS messages sent at different times:

First request: 14:23:21 → OTP: 2620

Second request: 14:25:02 → OTP: 2620 (same as before)

That’s less than two minutes apart, but both were identical.

**WHY IT’S DANGEROUS :**

If someone has your old OTP, they can log in without needing a new one. This makes the system vulnerable to account takeovers and other attacks.

**HOW I WOULD FIX IT :**

Always generate a fresh OTP for every request.

Invalidate the previous OTP immediately when a new one is created.

Never allow OTP reuse within the same session.