AuthN vs AuthZ

Computing

Two words one letter apart that solve completely different problems.

AuthN — who are you

- Passwords, passkeys, biometrics
- Multi-factor: something you know, have, are
- Produces a session or a token
- HTTP 401 when it fails
- Happens once, at the start

AuthZ — what may you do

- Roles, permissions, policies
- Checked on every single request
- Ownership checks: is this row yours?
- HTTP 403 when it fails
- Happens continuously

THE DIFFERENCE THAT MATTERS

Broken authorisation is the more common breach: a valid user reaching another user's data by changing an id in the URL.

> **Authorise on the server against the session's identity. A client that sends its own user id is not a security control.**