Storing Passwords

Computing

How passwords must be stored, and what each term in the recipe is for.

The current consensus, in the order the operations happen.

1. **Never store the password**
   Not encrypted, not encoded. Only a hash of it.

2. **Use a slow, purpose-built hash**
   Argon2id, scrypt or bcrypt. Never MD5, SHA-1 or plain SHA-256.

3. **Salt every password**
   A unique random value per user, so identical passwords hash differently.

4. **Tune the cost factor**
   Slow enough to hurt an attacker, fast enough for login — aim near 250 ms.

5. **Rehash on login when the cost changes**
   You have the plaintext at that moment and nowhere else.

WHY SLOW IS THE POINT

SHA-256: billions of guesses per second
bcrypt at cost 12: a few per second
The slowness is the entire defence

> **General-purpose hashes are designed to be fast. That is exactly the wrong property for a password.**