RZOLUT

Data Salting

A concept that pertains to password hashing using salt, which a randomly generated, fixed-length value that is designed to be unique with each user password. Data Salting adds a layer of security to the hashing process, specifically against brute force attacks. Salt re-use can cause users with the same password to have the same hash, which is dangerous as cracking a single hash can result in other passwords being compromised too.

Benefits

- Combats the use of precomputed tables for cracking passwords by lengthening hashes
- Creates unique passwords even in the instance of two users choosing the same passwords, so that no one can discover this just by reading hashes
- Salts help us mitigate hash table attacks by forcing attackers to re-compute them using the salts for each user

Use Cases

- Spam Size of the salt should match the size of the hash function's output
- The salt should be unique for every user & password
- Use CSPRNG (Cryptographically Secure Pseudo-Random Number Generator) to produce a salt
- Add salt to the starting of the password
- Store salt & password separately
- Don't use usernames as hash values
- Don't use a systemwide salt

Trends

- Wattpad's breach had not affected its users as the company used salted & cryptographically hashed passwords to store data
- GoDaddy's approach to store passwords either in plaintext or reversible format allowed an attacker direct access to password credentials without the need to crack them & resulted in impacting 1.2 million customers
- Despite organizations' attempt to secure the passwords by hashing and salting them, they faced a total cost of $3,288.34 million from 2005 – 2017 due to data breaches