Hashing in Detail

◴ Created	@December 30, 2022 3:49 PM
☰ Tags	

Goal:

Explore and compare different hashing options to see how they would affect future attackers on the system.

Steps:

Since there are already cryptography libraries made for us to use, it is strongly recommended to use those instead of using our own solutions. Even the hashes that were made a few years ago are no longer usable for security. So we have to make sure we pick one that will provide the best security since all of them can be broken, but that doesn’t mean we should give attackers an inch.

Retrospective:

Argon2 proved to be the most usable one. Of course, it is still necessary for the user to use a password or even better a passphrase with high entropy to avoid their password appearing in a dictionary of common or solved passwords. It is also not enough to just pick a hash, it is important to consider other elements like if the user tries to log in to make sure that at least the server still runs the hash function and then checks the validity of the credentials so that the attacker cannot track response time. It is all about covering all the sources of info that an attacker can use, the only one that cannot be covered is time, as eventually, they will be cracked. It is an endless game of cat and mouse.