Protecting Passwords

Justin Boyer
PRINCIPAL CONSULTANT

@justinboyer4 justinboyerwriter.com

Why Passwords Need To Be Protected

Too Easy

People choose poor passwords that are easily guessed

Duplication

People tend to use the same passwords on multiple sites

Data Breaches

Passwords are stolen by attackers

What Does a Hash Algorithm Do?

P@$$w0rd1

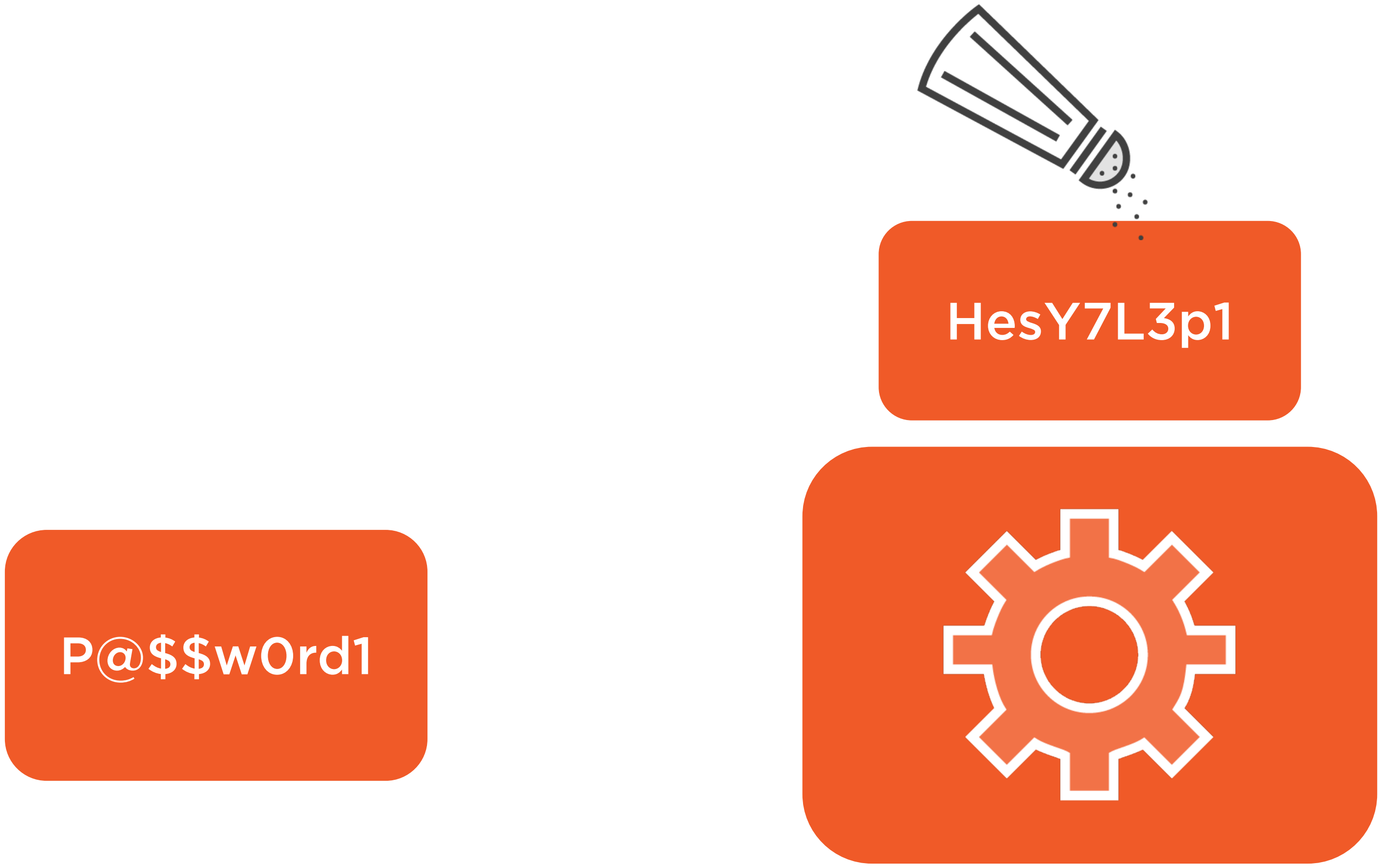
10,555 x 250 = 2,638,750

2,638,750 = ??? x ???

Good Hash Algorithms

- Argon2
- PBKDF2
- scrypt
- bcrypt

Salting the Hash



HesY7L3p1

P@$$w0rd1

Summary

Passwords are everywhere

If your application requires passwords, you need to protect them

Hashing algorithms can be used to protect passwords from prying eyes

Not all hashing algorithms are the same

Stick to the tried and true algorithms

- Argon2
- PBKDF2
- scrypt
- bcrypt