SeeCure Misr

Introduction To Password Policies & Weak Hashing

CYBERUS Stud

TABLE OF CONTENTS

01

Introduction To Password Policies

Intro To The Password Policies

What are the guidelines?

- Password Length.
- Complexity Requirements.
- Avoid Common Passwords.
- Password Expiration.
- Password History.

CYBERUS Stud

TABLE OF CONTENTS

02

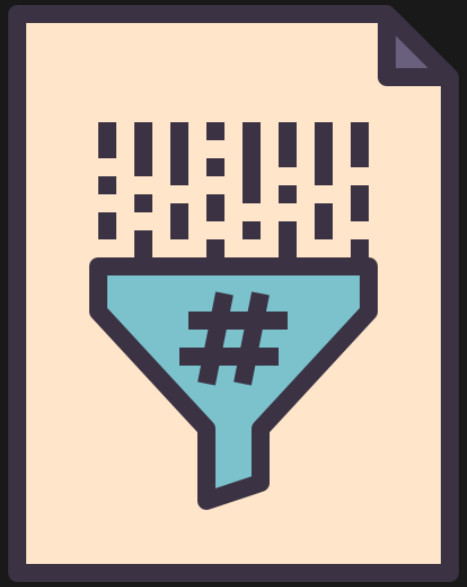
Bypassing Password Policies

CYBERUS Stud

TABLE OF CONTENTS

03

Intro To Hashing



What is Hashing?

- Hashing is a process of transforming data (such as password, message, or file) into a fixed-length sequence of characters, typically a string of numbers and letters.
- The output of a hash function, known as a hash value or hash code, is unique to the input data, meaning even a small change in the input will produce a significantly different hash value.

Hashing Purposes

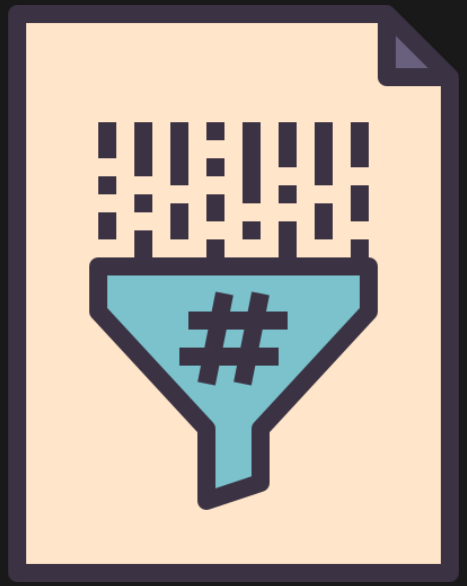
- Hashing serves several purposes, including data integrity verification, password storage, and data indexing.

CYBERUS Stud

TABLE OF CONTENTS

04

Weak Hashing Salt Technique



What is weak hashing?

- Weak hashing refers to the use of hashing algorithms that are considered to be insecure or vulnerable to cryptographic attacks. These algorithms have known weaknesses that make them unsuitable for certain security-sensitive applications.

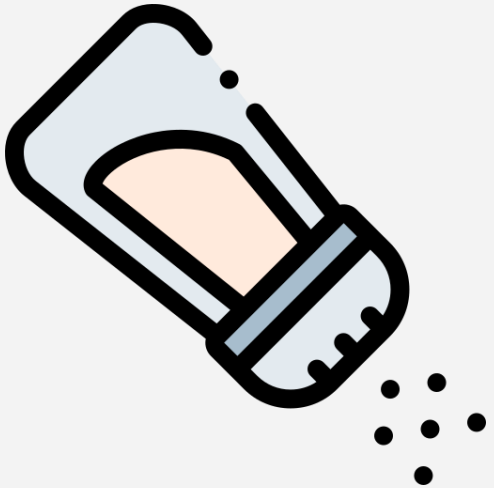
Examples of weak hashes

- MD5. (Message Digest Algorithm 5).
- SHA-256. (Secure Hash Algorithm 256-bit)
- SHA-1. (Secure Hash Algorithm 1).

What is salt technique?

- Salting is a technique used in hashing to enhance the security of stored passwords. It involves adding a random value called a salt to the password before hashing it.

- Bcrypt is a strong hash that use the salt technique.



RESOURCES

https://en.wikipedia.org/wiki/Bcrypt

https://en.wikipedia.org/wiki/Password_policy

https://emeritus.org/blog/cybersecurity-what-is-hashing-in-cybersecurity/

CYBERUS Stud

Thank You

Presented by Abdelrahman Salah